Säkrare verifiering av identitet

Volym 2

Betänkande av Utredningen om säkrare verifiering av identitet

Stockholm 2026

STATENS OFFENTLIGA UTREDNINGAR

SOU 2026:55

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Multiply Solutions
Tryck och remisshantering: Multiply Solutions, Stockholm 2026

ISBN 978-91-525-1597-6 (tryck)
ISBN 978-91-525-1598-3 (pdf)
ISSN 0375-250X

Innehåll

VOLYM 2

Del 3 – Ett system för biometrisk verifiering av identitet

Del 4 – Avslutande del

Bilaga

DEL 3

Ett system för biometrisk verifiering mot handlingar

23 En ny lag om biometrisk verifiering av identitet

23.1 Inledning

I kapitel 22 har vi bedömt att ett system för säkrare verifiering av identitet med grund i biometriska uppgifter bör bygga på en möjlighet för fler myndigheter att kontrollera sådana uppgifter mot handlingar av olika slag. Vi har i kapitel 19 och 20 beskrivit hur ett sådant system skulle kunna utformas, bland annat i fråga om vilka handlingar som bör kunna användas. I avsnitt 10.2.3 har vi även bedömt att utökade möjligheter för myndigheter att kräva personlig inställelse kan stärka kopplingen mellan etablerad identitet och verifiering av identiteten, och att detta kan vara en viktig komponent i att kunna genomföra verifiering med hjälp av biometriska uppgifter, mot handlingar. I detta kapitel lämnar vi förslag om hur ett sådant system avseende biometrisk verifiering mot handlingar som vi beskrivit i tidigare kapitel kan utformas lagtekniskt. Förslagen kommer av naturliga skäl att utgå från de bedömningar i sak av olika frågor som vi har gjort i tidigare kapitel, varför hänvisningar till dessa kommer att göras i stor utsträckning.

23.2 En särskild lag ska införas

Vi har i avsnitt 21.2 bedömt att en möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar behöver regleras i lag. Detta med hänsyn till dels de krav som följer av relevanta EU-förordningar som reglerar pass och identitetshandlingar, dels ett övergripande behov av tydlighet och förutsebarhet som följer av det intrång i den personliga integriteten som behandlingen av personuppgifter – i syn-

nerhet biometriska uppgifter – innebär. Vi ser inte skäl att göra en annan bedömning här.

Vi kan i detta sammanhang vidare notera att Grundlagsutredningen (2008) i sitt betänkande *En reformerad grundlag* anförde att starka skäl talar för att föreskrifter av central betydelse för medborgarna och samhällslivet i övrigt ska kunna meddelas endast av riksdagen, det vill säga genom lag.[1] Med hänsyn till den breda personkrets som vi anser ska kunna omfattas och att biometrisk verifiering ska kunna användas av ett stort antal myndigheter – i ärendeslag som innefattar exempelvis beviljande av socialförsäkringsförmåner – kan föreskrifter om detta anses vara av sådan central betydelse som avsågs i nämnda betänkande.

Mot denna bakgrund kan vi inte komma till någon annan slutsats än att en möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar bör regleras i lag. Med detta sagt kan ett system för att mer generellt ge myndigheter möjlighet att biometriskt verifiera identitet behöva innehålla viss flexibilitet och i vissa avseenden regleras på annat sätt än i lag. Vi återkommer i avsnitt 23.9 till möjligheterna för regeringen eller den eller de myndigheter som regeringen bestämmer att meddela tillämpningsföreskrifter.

23.2.1 En lag om biometrisk verifiering av identitet ska införas

Vårt förslag

En möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar ska regleras i en särskild lag. Lagen ska benämnas *lagen om biometrisk verifiering av identitet*.

Biometrisk verifiering av identitet mot handlingar är redan i dag möjlig för vissa myndigheter att genomföra i olika ärendeslag, vilket vi har redogjort för i avsnitt 7.4.2, exempelvis vid gränskontroller, inre utlänningskontroller, ansökan om pass och vissa situationer i folkbokföringsärenden. Stöd för detta finns i relevanta författningar som styr dessa ärendeslag och som tillämpas av Polismyndigheten, Migrationsverket och Skatteverket. Med utgångspunkt i vår bedömning att utökade möjligheter att använda biometriska uppgifter för att verifiera identitet mot handlingar bör omfatta en mycket bred krets av myn-

[1] SOU 2008:125, s. 554.

digheter – dels i varierande ärendeslag som dessa handlägger, dels i den faktiska verksamheten – står det som vi ser det klart att det inte är lämpligt att reglera detta genom att bestämmelser förs in i befintliga författningar. Det skulle kräva ändringar i och anpassningar av ett närmast oöverskådligt antal författningar. Om justeringar skulle behöva göras senare skulle detta kräva omfattande arbete. Den enskilde skulle även bli hänvisad till ett antal olika regelkomplex för att ta reda på vad som gäller i det enskilda fallet. För en och samma myndighet skulle det också kunna krävas reglering i flera olika författningar som styr olika ärendeslag; som exempel kan nämnas Skatteverkets folkbokförings- respektive beskattningsverksamhet. En reglering skulle därmed kunna behöva göras inte endast för olika myndigheter, utan även för olika särskilda ärendeslag, vilket ytterligare motverkar en tydlighet och minskar överskådligheten. Med hänsyn till att exempelvis utlänningslagen (2005:716) redan innehåller bestämmelser om biometrisk verifiering av identitet mot handlingar på utlänningsrättens område finns det också en risk för att ytterligare bestämmelser av likartat slag i samma författning, men med ett annat mer generellt tillämpningsområde, leder till en otydlighet för myndigheten i fråga.

Den behandling av personuppgifter som behöver utföras vid biometrisk verifiering av identitet mot handlingar behöver regleras, vilket vi återkommer till i kapitel 24. Det är som vi ser det inte lämpligt att införa sådana bestämmelser i befintliga författningar som reglerar biometrisk verifiering mot handlingar, eller i relevanta registerförfattningar. Detta talar som vi ser det också för att det är lämpligt att samla den reglering som behövs för att införa en mer generell möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar i en och samma lag. Vi har inte funnit någon omständighet som talar mot att en sådan möjlighet bör regleras i en särskild lag. I stället kan en tydlighet och förutsebarhet främjas genom en särskild lag. Vi föreslår därför att en ny lag ska införas, som reglerar möjligheten för myndigheter att biometriskt verifiera identitet mot handlingar och vad som då ska gälla i fråga om personuppgiftsbehandling.

Den nya lagens namn

Den nya lagen bör ha ett namn som avspeglar dess innehåll och tillämpningsområde. Det huvudsakliga syftet med lagen är att göra det möjligt för myndigheter att verifiera identitet genom att genomföra jämförelser av biometriska uppgifter mot olika handlingar och på så sätt koppla en individ till en påstådd identitet. Vi anser inte att det är nödvändigt att det av namnet framgår att lagen avser myndigheter, då vi föreslår dels att lagen ska innehålla en definition av vad vi avser med myndigheter, dels att det i relevanta bestämmelser i lagen uttryckligen anges att endast myndigheter omfattas (se avsnitt 23.5.6 och 23.6.3). Att ange att det är fråga om verifiering av identitet *mot handlingar* skulle visserligen kunna tydliggöra att lagen endast ska omfatta sådana kontroller. Dessa begränsningar ska dock – som vi återkommer till i avsnitt 23.6 – också tydligt anges i lagen. Ett mer koncist namn kan enligt vår bedömning vara att föredra.

Vi anser mot denna bakgrund att den nya lagen bör benämnas *lagen om biometrisk verifiering av identitet*. I detta betänkande använder vi för läsbarhetens skull, fortsättningsvis kortformen ”den nya lagen”, om inget annat särskilt anges.

23.2.2 Lagens syfte

Vårt förslag

Syftet med den nya lagen är att motverka identitetsmissbruk genom att ge myndigheter möjlighet att med hjälp av biometriska uppgifter som kan tas fram ur en handling kontrollera om en påstådd identitet är riktig och att skydda den som kontrolleras mot att hans eller hennes personliga integritet kränks vid en sådan kontroll.

Bestämmelser om syftet med en viss reglering saknar normalt egentligt materiellt innehåll och kan i stället ses som en slags deklaration av de bakomliggande och övergripande målen med regleringen. Ett uttryckligt fastslående av lagens syfte har som vi ser det emellertid inte enbart en symbolisk eller informativ betydelse. Att uttryckligen ange syftet med den nya lagen kan få relevans i rättstillämpningen genom att det ger viss vägledning för tolkningen av de materiella be-

stämmelserna i lagen.[2] Vi anser därför att det finns skäl att införa en bestämmelse som anger den nya lagens syfte.

En syftesbestämmelse bör av naturliga skäl vara övergripande. I kapitel 9 har vi redogjort för olika former av identitetsmissbruk som förekommer i Sverige. Vårt övergripande uppdrag syftar till att motverka detta missbruk, vilket därför bör lyftas fram i en syftesbestämmelse. Vi kan vidare konstatera att identitetsmissbruk riktar sig både mot samhället som sådant och mot enskilda personer. Myndigheter har ett stort behov av att kunna säkerställa att den person som man möter är den som han eller hon utger sig för att vara, framför allt för att kunna handlägga ett ärende på ett korrekt sätt och säkerställa att beslut avser rätt person. Som vi lyft fram i bland annat avsnitt 17.5.2 är målet att skydda enskilda mot att deras identitet utnyttjas i olika sammanhang också av stor betydelse från samhällssynpunkt. Vi bedömer att en bestämmelse som föreskriver att den nya lagens syfte är att motverka identitetsmissbruk – genom att ge myndigheter möjlighet att med hjälp av biometriska uppgifter som kan tas fram ur en handling kontrollera om en påstådd identitet är riktig fångar regleringens målsättning på ett sätt som passar för samtliga myndigheter som kan komma att tillämpa lagen, oavsett vilken slags verksamhet de bedriver. Att identitetsmissbruk motverkas innebär även att människor skyddas mot att deras identitet utnyttjas.

Biometrisk verifiering av identitet med stöd av den nya lagen innebär att personuppgifter – däribland känsliga sådana – behöver behandlas. Detta medför en viss risk för intrång i skyddet för den personliga integriteten. Den nya lagen ska, enligt våra förslag, innehålla bestämmelser som är utformade på ett sätt som syftar till att skydda enskilda personer mot att deras personliga integritet kränks vid myndigheternas behandling av personuppgifter i samband med att identiteten verifieras biometriskt med stöd av lagen. Även detta ska enligt vår mening tydliggöras i en syftesbestämmelse.

[2] Jfr *Myndighetsdatalag*, SOU 2015:39, s. 220.

23.3 Den nya lagen ska komplettera befintliga möjligheter till biometrisk verifiering av identitet mot handlingar

Vårt förslag

Om en annan lag eller förordning innehåller en bestämmelse som ger en myndighet uttrycklig rätt att kontrollera om en persons fingeravtryck eller ansiktsbild motsvarar dem som finns i en handling ska den bestämmelsen tillämpas.

Avsikten med den nya lagen är att införa en utökad, generell möjlighet för myndigheter att använda biometrisk verifiering av identitet mot handlingar. Det är som vi ser det dock av vikt att befintliga bestämmelser – i exempelvis 9 kap. utlänningslagen – som ger vissa myndigheter en uttrycklig rätt att i särskilda ärenden och situationer använda sådana kontroller, tillämpas i den ordning som är föreskriven i det aktuella ärendeslaget eller den aktuella situationen. Särskilda överväganden ligger normalt till grund för dessa bestämmelser och de kan innehålla särskilda begränsningar som snävar in tillämpningen, till exempel avseende mot vilka typer av handlingar som en biometrisk jämförelse får göras. Dessa begränsningar kan ha sin grund i EU-förordningar eller följa av internationella åtaganden.

En generell möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar på det sätt som vi föreslår ska ses som en utvidgning av och ett komplement till de möjligheter att genomföra sådana kontroller som kan följa i annan ordning och som normalt tar sikte på ett visst ärendeslag eller en viss konkret situation som en myndighet ansvarar för. Avsikten är att biometrisk verifiering av identitet mot handlingar enligt den nya lagen ska få tillämpas av en viss myndighet endast vid handläggning av ärenden eller i situationer när det saknas stöd för en sådan kontroll i ett myndighets- eller verksamhetsspecifikt regelverk; den nya lagen ska därmed komplettera sådana bestämmelser. Det bör förtydligas att den nya lagen avser att utöka de *enskilda ärenden och situationer* när biometrisk verifiering mot handlingar får användas, och inte att exempelvis utöka vilka typer av handlingar som får användas i de fall som redan är reglerade i annan ordning. Som exempel kan Migrationsverkets rätt att biometriskt verifiera identitet i samband med en gränskontroll eller en inre

utlänningskontroll med stöd av 9 kap. 8 b § utlänningslagen nämnas. I bestämmelsen anges att vissa uppräknade typer av handlingar får användas för den biometriska jämförelsen. Pass och identitetskort omfattas inte. Den nya lagen ska i detta fall inte kunna användas för att utöka vilka handlingar som kan användas i de situationer som regleras i 9 kap. 8 b § utlänningslagen. Inte heller ska den nya lagen kunna användas för att kringgå eventuella andra inskränkande rekvisit som kan följa av en annan bestämmelse om biometrisk verifiering av identitet mot handlingar. Det nyss anförda ska dock inte uppfattas som att en möjlighet som följer av annan författning att använda biometrisk verifiering mot handlingar i en viss angiven situation vid handläggningen i ett *ärendeslag* helt och hållet utesluter att den nya lagen får användas i någon annan del av handläggningen av ärendet, exempelvis i ett inledande skede, under förutsättning att detta inte kan anses särskilt reglerat i den aktuella författningen.

Förhållandet till bestämmelser i annan lag eller förordning som ger myndigheter en uttrycklig rätt att biometriskt verifiera identitet mot handlingar ska som vi ser det anges särskilt i den nya lagen. Bestämmelser som antas genom föreskrifter på myndighetsnivå eller som efter bemyndigande beslutas av en kommun ska däremot inte ha företräde framför bestämmelserna i den nya lagen. Med hänsyn till att det är fråga om åtgärder som normalt innebär ett intrång i den personliga integriteten kan det emellertid med fog antas att detta inte är aktuellt.

En bestämmelse i den nya lagen som reglerar förhållandet till befintliga möjligheter att biometriskt verifiera identitet mot handlingar bör enligt vår mening inte utformas med ett rekvisit som anger att endast om en bestämmelse i annan lag eller förordning *avviker* från den nya lagen ska den bestämmelsen tillämpas; det ska endast vara fråga om att konstatera att det finns en annan tillämplig bestämmelse som uttryckligen ger myndigheten rätt att – i en viss situation som är för handen – kontrollera om en persons fingeravtryck eller ansiktsbild motsvarar dem som finns i eller på en handling. Huruvida bestämmelsen i annan författning avviker – exempelvis genom att andra typer av handlingar får användas eller att det ställs högre krav för att alls få genomföra en kontroll – ska inte påverka. Mot denna bakgrund anser vi att det ska anges i den nya lagen att om en annan lag eller förordning innehåller en bestämmelse som ger en myndighet en uttrycklig rätt att kontrollera om en persons fingeravtryck eller ansikts-

bild motsvarar dem som finns i eller på en handling ska den bestämmelsen tillämpas. En sådan bestämmelse gör det tydligt att den nya lagen endast ska tillämpas som ett komplement till befintliga bestämmelser om biometrisk verifiering mot handlingar.

23.4 Undantag för brottsbekämpande verksamhet

Vårt förslag

Biometrisk verifiering av identitet mot handlingar med stöd av den nya lagen ska inte få genomföras i verksamhet som en sådan behörig myndighet som avses i brottsdatalagen (2018:1177) utför i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Vi har i avsnitt 21.4 bedömt att en generell möjlighet för myndigheter att i brottsbekämpande verksamhet biometriskt verifiera identitet mot handlingar bör utredas i annan ordning. I enlighet med det anser vi att den nya lagen, vid ett genomförande av våra förslag, inte ska få användas i myndigheters brottsbekämpande verksamhet. Vi anser att denna gränsdragning ska framgå uttryckligen av den nya lagen.

I reglering som avser behandling av personuppgifter – det vill säga en registerförfattning – görs en gränsdragning mot brottsbekämpande verksamhet ofta genom att det anges att författningen inte gäller vid behandling av personuppgifter som omfattas av tillämpningsområdet för brottsdatalagen; ett exempel är 4 c § utlänningsdatalagen (2016:27). Eftersom biometrisk verifiering enligt den nya lagen förutsätter att behandling av personuppgifter utförs, skulle en sådan gränsdragning kunna övervägas. Den nya lagen kommer emellertid inte att vara en renodlad registerförfattning, i likhet med exempelvis utlänningsdatalagen, utan den kommer i första hand att innehålla materiella bestämmelser om när myndigheter ska få använda biometriska underlag som finns i handlingar för att verifiera identitet, på liknande sätt som bland annat 9 kap. 8 b § utlänningslagen. Med hänsyn till detta anser vi att en gränsdragning som tar sikte på de materiella bestämmelserna i den nya lagen om när biometrisk verifiering alls ska få användas är att föredra. Som vi återkommer till i avsnitt 24.9 ska personuppgifter få be-

handlas endast för att en biometrisk verifiering av identitet med stöd av lagen ska kunna genomföras. En avgränsning som tar sikte på när sådana kontroller alls ska få användas kommer därmed indirekt att utgöra en avgränsning mot behandling av personuppgifter med stöd av brottsdatalagen, varför det inte behöver komma till uttryck i den nya lagen.

En gränsdragning skulle kunna göras indirekt, genom att den nya lagen innehåller bestämmelser om tillämpningsområde och ändamål som pekar ut endast en viss eller vissa verksamheter. Detta är emellertid inte en möjlig lösning, eftersom tanken är att den nya lagen ska kunna tillämpas av en mycket vid krets myndigheter i många olika ärendeslag, även sådana som kan tillkomma efter att den nya lagen har trätt i kraft. I stället anser vi att gränsdragningen ska göras direkt, genom att det i lagen anges att biometrisk verifiering av identitet mot handlingar med stöd av den nya lagen inte får genomföras i brottsbekämpande verksamhet.

Det saknas en generell legaldefinition av begreppet *brottsbekämpande verksamhet*, även om det förekommer i olika författningar. Exempelvis anges i 3 § förvaltningslagen (2017:900) att vissa bestämmelser i lagen inte ska tillämpas i brottsbekämpande verksamhet hos Kustbevakningen, Polismyndigheten, Skatteverket, Säkerhetspolisen, Tullverket eller en åklagarmyndighet. En indirekt avgränsning av vad som faller in under begreppet brottsbekämpande verksamhet kan utläsas av 1 kap. 2 § brottsdatalagen (2018:1177), som anger att lagen gäller vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att ”förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder”. Lagen gäller också vid behandling av personuppgifter som en behörig myndighet utför ”i syfte att upprätthålla allmän ordning och säkerhet”. En i allt väsentlig likartad avgränsning har gjorts i förarbetena till lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område och i betänkandet *En ny organisation av ekobrottsbekämpningen*.[3] I 3 § lagen (2025:170) om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna görs emellertid en något snävare avgränsning; i bestämmelsen anges att med brottsbekämpande verksamhet avses sådan verksamhet som en brottsbekämpande myndighet bedriver för att förebygga,

[3] *Integritet och effektivitet i polisens brottsbekämpande verksamhet*, prop. 2009/10:85, s. 74 och SOU 2025:81, s. 429.

förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott.[4] Vad som i praktiken avses med brottsbekämpande verksamhet för en viss myndighet kan tänkas skilja sig åt, beroende på myndighetens uppgifter.

Vi kan konstatera att det kan anses ingå i många olika myndigheters uppdrag att på olika sätt arbeta för att förebygga och motverka brottslighet av olika slag. Detta framgår exempelvis av 6 kap. 8 § socialtjänstlagen (2025:400) avseende socialnämnder och av 6 § förordningen (2017:154) med instruktion för Skatteverket. Kretsen av myndigheter som anses utgöra brottsbekämpande myndigheter är dock mer begränsad; som utgångspunkt är det sådana behöriga myndigheter som avses i 1 kap. 6 § brottsdatalagen, nämligen myndigheter som har till uppgift att utföra brottsbekämpande verksamhet, exempelvis på det sätt som framgår av lagen (1997:1024) om Skatteverkets brottsbekämpande verksamhet. Kretsen av brottsbekämpande myndigheter är som vi ser det snävare än vad som skulle kunna anses följa av en sådan mer allmän bestämmelse som exempelvis 6 kap. 8 § socialtjänstlagen, och utgörs av sådana behöriga myndigheter som avses i 1 kap. 6 § brottsdatalagen. I nuläget omfattar detta Polismyndigheten, Skatteverket, Migrationsverket, Tullverket, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Kustbevakningen, de allmänna domstolarna och Kriminalvården. Enligt förslag som lämnats i promemorian *En brottsbekämpande verksamhet hos Försäkringskassan* ska även denna myndighet omfattas.[5] Vi anser att ett undantag i den nya lagen i fråga om biometrisk verifiering i den brottsbekämpande verksamheten endast ska avse de myndigheter som utgör behöriga myndigheter enligt 1 kap. 6 § brottsdatalagen. I annat fall finns en risk för att undantaget blir alltför brett.

För att undantaget från möjligheten att verifiera identitet biometriskt med stöd av den nya lagen ska bli tillämpligt ska det dock inte krävas att brottsdatalagen är tillämplig; det ska räcka att myndigheten är behörig myndighet enligt denna lag och att det är fråga om brottsbekämpande verksamhet. Som exempel kan nämnas att Säkerhetspolisen är behörig myndighet enligt brottsdatalagen, men att lagen inte gäller vid myndighetens behandling av personuppgifter som rör nationell säkerhet (1 kap. 4 § brottsdatalagen); då blir i stället lagen

[4] *Ökat informationsflöde till brottsbekämpningen*, prop. 2024/25:65, s. 68 ff.
[5] Ds 2026:4, s. 228.

(2019:1182) om Säkerhetspolisens behandling av personuppgifter tillämplig.

Mot denna bakgrund anser vi att det i den nya lagen ska anges att biometrisk verifiering inte får genomföras med stöd av lagen i verksamhet som en sådan behörig myndighet som avses i brottsdatalagen utför i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Det bör understrykas att en myndighet är behörig myndighet bara när den utför sådana uppgifter. En myndighet kan alltså vara både behörig och icke behörig i lagens mening beroende på vilka uppgifter som utförs. Det bör enligt vår bedömning dock normalt inte medföra några svårigheter för en viss myndighet att avgöra om en åtgärd vidtas inom ramen för den brottsbekämpande verksamhet som man bedriver.

23.5 Definitioner av vissa begrepp

Som vi konstaterat i avsnitt 3.2 saknas såväl en legaldefinition av begreppet *identitet* som vägledande förarbetsuttalanden om hur begreppets närmare innebörd generellt sett ska tolkas. Vi har därför i nämnda avsnitt definierat detta begrepp inom ramen för detta betänkande. I avsnitt 21.3.1 har vi tagit ställning till vilka myndigheter vi anser bör omfattas av en möjlighet att biometriskt verifiera identitet mot handlingar. Med hänsyn till att vi föreslår att en ny lag ska införas kan det därför finnas anledning att överväga om nämnda – och vissa andra – begrepp uttryckligen bör definieras i lagen, i syfte att främja en tydlighet i tillämpningen.

23.5.1 Barn

Vår bedömning

Begreppet *barn* behöver inte definieras i den nya lagen.

Vad som aves med barn definieras särskilt i vissa författningar. Exempelvis anges i 2 kap. 1 § andra stycket lagen (2024:79) om placering av barn i skyddat boende att med barn avses varje människa under 18 år och enligt 1 kap. 2 § utlänningslagen avses med barn en person

som är under 18 år. I nämnda författningar aktualiseras vissa särskilda bestämmelser eller bedömningar när någon betraktas som barn vid tillämpningen. Som exempel kan nämnas att ett uppehållstillstånd på grund av anknytning, enligt 5 kap. 3 § 2 a utlänningslagen, kan beviljas ett utländskt barn som är ogift och har en förälder som är bosatt i eller har beviljats uppehållstillstånd för bosättning i Sverige. När det gäller nämnda lag om placering av barn i skyddat boende är lagens tillämpning helt knuten till att den som en insats enligt lagen beviljas för är ett barn. Det är då givetvis lämpligt att definiera vad som avses med barn, för att inte varje gång barn nämns i lagtexten behöva definiera vem som ska anses vara barn.

Vi har i avsnitt 20.4 bedömt att en utökad möjlighet att biometriskt verifiera identitet mot handlingar på det sätt vi föreslår inte bör gälla för barn under sex år. Det är ostridigt att den som är under sex år alltid är att betrakta som ett barn. I avsnitt 23.6.4 föreslår vi dessutom att det av den nya lagen ska framgå att myndigheter får biometriskt verifiera identitet mot handlingar för den som har fyllt sex år. Vi föreslår inte i övrigt några särskilda bestämmelser som endast tar sikte på barn eller innehåller rekvisit som är tillämpliga endast vad gäller barn. Med hänsyn till detta saknas anledning att särskilt definiera vad som avses med begreppet barn i den nya lagen.

23.5.2 Identitet

Vår bedömning

Det ska framgå av den nya lagen att med identitet avses i lagen uppgifter om namn, födelsetid och medborgarskap.

Med hänsyn till att den nya lagen ska reglera myndigheters möjlighet att biometriskt verifiera identitet mot handlingar och det saknas en övergripande legaldefinition av begreppet identitet, kan det tyckas naturligt att den nya lagen bör innehålla en definition av begreppet. Vi har i avsnitt 3.2 också, inom ramen för detta betänkande, avgränsat *identitet* till uppgifter om en individs namn, födelsetid och medborgarskap. Vi kan emellertid konstatera att det i andra författningar där begreppet förekommer, och också kan ha en central roll vid tillämpningen av en viss bestämmelse, inte finns någon definition. Som ex-

empel kan nämnas 9 kap. 8 § utlänningslagen och 22 § folkbokföringslagen (1991:481).[6] Detta talar som vi ser det mot ett behov av att i den nya lagen införa en legaldefinition. Som vi anfört i avsnitt 3.2 finns också delvis olika tolkningar av vad som omfattas; exempelvis ansågs i betänkandet *Ett säkert statligt ID-kort – med e-legitimation* begreppet identitet i huvudsak avse en persons namn och person- eller samordningsnummer, men även andra uppgifter om en person, såsom födelsetid, medborgarskap och bostadsadress ansågs kunna hänföras till identitetsbegreppet.[7] Även detta talar mot att i den nya lagen införa en särskild legaldefinition.

Vi anser emellertid att en definition av vad som avses med begreppet identitet i den nya lagen utgör ett viktigt led i att upprätthålla en tydlighet och förutsebarhet i tillämpningen. Detta är som vi ser det av särskild vikt med hänsyn till att den nya lagen ska få användas av en mycket bred krets av aktörer, och att upptagning av biometriska underlag utgör ett visst intrång i den personliga integriteten. Som vi återkommer till i avsnitt 23.6.3 ska den nya lagen endast få användas när det är nödvändigt att biometriskt verifiera någons identitet. Syftet är att kunna ta ställning till om en viss påstådd identitet är riktig. Om det överlåts till myndigheterna att tolka vad som ryms i begreppet identitet finns, som vi ser det, en risk för att tillämpningsområdet för den nya lagen utvidgas till andra situationer än avsett. Som vi noterat i avsnitt 11.4.2 förekommer exempelvis *könsidentitet* för att beteckna en persons självupplevda kön och i vissa EU-förordningar omfattar begreppet identitetsuppgifter också uppgifter om kön. Utan en definition i den nya lagen av vad som avses med identitet skulle det därmed kunna finnas en risk för att en myndighet – som i en viss situation anser att identitet kan jämställas med kön – i praktiken använder biometrisk verifiering med stöd av den nya lagen för att kontrollera en enskilds juridiska kön.

Någon nackdel med att inom ramen för den nya lagens tillämpning definiera begreppet identitet har vi svårt att se. Genom en uttrycklig definition är det också tydligt vad som menas med att biometrisk verifiering syftar till att fastställa om en påstådd identitet är riktig (jfr avsnitt 23.5.5). Det bör dock erinras om att det inte innebär att endast uppgifter om identitet – det vill säga namn, födelsetid och medborgarskap – får användas vid den jämförelse som görs vid verifiering

[6] Jfr *Stärkt kontroll och kvalitet i folkbokföringen*, prop. 2021/22:217, s. 35 f.
[7] SOU 2019:14, s. 90.

av identitet, utan även andra sidouppgifter kan användas, på det sätt som vi beskrivit i avsnitt 7.2.1.

Mot denna bakgrund anser vi att det ska framgå av den nya lagen att med begreppet identitet avses i lagen uppgifter om namn, födelsetid och medborgarskap.

23.5.3 Biometriska underlag

Vår bedömning

Begreppet *biometriska underlag* behöver inte definieras i den nya lagen.

Som vi konstaterat i avsnitt 4.3 används begreppet *biometriska underlag* sällan i författning. Biometriska underlag är olika former av fysiska karaktärsdrag hos en person. De kan bestå av ansiktsbilder och fingeravtryck, men även andra individuella kännetecken så som ögats utseende, röst, händers utseende och gångstil.

I det nyss nämnda avsnittet har vi begränsat våra överväganden i detta betänkande till fingeravtryck och ansiktsbilder, som är de biometriska underlag som för närvarande används i andra sammanhang för att verifiera identitet eller identifiera någon, exempelvis vid en gränskontroll eller ansökan om uppehållstillstånd. När det gäller biometrisk verifiering mot handlingar på det sätt som vi nu föreslår ska införas har vi i avsnitt 20.2 bedömt att såväl fingeravtryck som ansiktsbilder bör få användas för sådana kontroller. Med hänsyn till det integritetsintrång som upptagning och behandling av biometriska underlag medför, och med beaktande av den tekniska utvecklingen, anser vi att det bör tydliggöras i den nya lagen vilka biometriska underlag som får användas. En definition av begreppet skulle kunna uppnå detta. Det kan samtidigt konstateras att andra författningar som rör upptagning och behandling av biometriska underlag ofta inte innehåller någon definition av vilka typer av underlag som omfattas utan detta följer i stället direkt av relevanta bestämmelser. Till exempel anges i bestämmelsen i 9 kap. 8 a § utlänningslagen att en utlänning som ansöker om uppehållstillstånd är skyldig att låta relevanta myndigheter fotografera honom eller henne och ta hans eller hennes fingeravtryck. I 26 c § folkbokföringslagen finns en liknande precisering

av vilka biometriska underlag som får användas för en biometrisk verifiering av identitet vid personlig inställelse i ett folkbokföringsärende. I flera av de EU-förordningar som vi redogjort för i kapitel 7 definieras inte heller begreppet biometriska underlag utan det anges att fotografier och fingeravtryck får användas i olika sammanhang. Däremot definieras begreppet biometriska uppgifter, exempelvis i 3.13 i gränsförordningen[8]. Vi återkommer till detta i nästa avsnitt.

Som vi noterat ovan kan biometriska underlag omfatta även andra fysiska kännetecken än fingeravtryck och ansiktsbilder. Med hänsyn till detta och då en definition saknas i andra författningar anser vi att det inte är nödvändigt att definiera begreppet biometriska underlag i den nya lagen. I stället bör *fingeravtryck* och/eller *ansiktsbild* anges i de bestämmelser i den nya lagen då sådana underlag aktualiseras.

23.5.4 Biometriska uppgifter

Vårt förslag

Det ska framgå av den nya lagen att med *biometriska uppgifter* avses i lagen personuppgifter som genom en särskild teknisk behandling har tagits fram ur fingeravtryck eller ansiktsbild, i syfte att verifiera en persons identitet.

Vi har i avsnitt 4.4 kommit fram till att med biometriska uppgifter avses – i detta betänkande – personuppgifter som genom en särskild teknisk behandling har tagits fram ur biometriska underlag i syfte att identifiera en unik person eller verifiera en persons identitet. Begreppet biometriska uppgifter förekommer bland annat i dataskyddsförordningen[9] och i brottsdatalagen och definieras även i olika EU-förordningar, bland annat i artikel 3.13 i gränsförordningen och i artikel 3.18 i in- och utreseförordningen[10]. Vi kan notera att i passlagen (1978:302) och utlänningslagen används uttrycket *biometriska data*. Någon skillnad mot biometriska uppgifter är emellertid inte

[8] Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018.
[9] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.
[10] Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017.

avsedd.[11] Det uttryck som förefaller dominerande i nyare lagstiftningsarbete är biometriska uppgifter, exempelvis i regeringens proposition *Biometri i brottsbekämpningen* och i 12 § i förslaget till en ny pass- och identitetskortsdatalag.12 I de EU-förordningar som vi redogjort för i kapitel 7 används uteslutande begreppet biometriska uppgifter. Vi anser därför att detta begrepp är lämpligt att använda i den nya lagen.

Eftersom biometriska uppgifter tas fram ur biometriska underlag är de till sin natur inte begränsade till vissa fysiska kännetecken. I brottsdatalagen och dataskyddsförordningen är begreppet inte heller begränsat på så sätt att det är knutet till en viss typ av biometriska underlag. Vi kan emellertid konstatera att i bland annat gränsförordningen görs en uttrycklig avgränsning i definitionen av begreppet till att avse fotografier, ansiktsbilder och fingeravtrycksuppgifter; det är bara dessa typer av biometriska underlag som får användas vid tillämpning av förordningen. För att tydliggöra att det endast är biometriska uppgifter som kan tas fram ur fingeravtryck och en ansiktsbild som ska få användas vid biometrisk verifiering med stöd av den nya lagen anser vi att det är lämpligt att en motsvarande avgränsning görs vid definitionen av begreppet biometriska uppgifter. På detta sätt främjas ett stärkt skydd för den personliga integriteten, genom att det även genom definitionen av biometriska uppgifter framgår att endast vissa biometriska underlag ska få användas vid tillämpning av den nya lagen. En sådan tydlighet motiveras som vi ser det också av att en bred krets av myndigheter ska kunna använda den nya lagen.

Mot denna bakgrund anser vi att det ska definieras i den nya lagen att med *biometriska uppgifter* avses personuppgifter som genom en särskild teknisk behandling har tagits fram ur fingeravtryck eller ansiktsbild. Den tekniska behandlingen ska, som vi redogjort för i avsnitt 4.4, syfta till att antingen identifiera en unik person eller verifiera en persons identitet. Den nya lagen ska emellertid endast kunna användas i syfte att verifiera identiteten biometriskt. Vi anser därför att definitionen av begreppet biometriska uppgifter i den nya lagen ska återspegla detta; att i stället utgå från den definition av biometriska uppgifter som framgår av artikel 4.14 i dataskyddsförordningen – som anger att det är fråga om att identifiera en unik person – skulle

[11] *Passdatalag – en ny lag som kompletterar EU:s dataskyddsförordning*, Ds 2019:5, s. 143 och *Ökad säkerhet för vissa identitets- och uppehållshandlingar – anpassning av svensk rätt till en ny EU-förordning*, Ds 2020:22, s. 70.
[12] Prop. 2024/25:37 och promemorian *Ett statligt identitetskort,* Ju2026/01595, s. 14.

som vi ser det kunna ge intryck av att den nya lagen även omfattar identifiering.

23.5.5 Biometrisk verifiering av identitet

Vårt förslag

Det ska framgå av den nya lagen att med *biometrisk verifiering av identitet* avses i lagen en-till-en-jämförelse av en grupp av uppgifter, däribland biometriska uppgifter, med en annan för att fastställa om en påstådd identitet är riktig.

Vi har i avsnitt 7.2.1 redogjort för vad vi avser med begreppet *verifiering av identitet*, nämligen att en uppsättning uppgifter jämförs med en annan, för att fastställa om en påstådd identitet är riktig. I nämnda avsnitt har vi beskrivit att detta i praktiken görs i två steg, där jämförelser mellan olika typer av uppgifter görs i de olika stegen. Det bör tydliggöras att detta kan innefatta jämförelse av flera olika typer av uppgifter, inte bara uppgifter om identitet. För att det ska vara fråga om biometrisk verifiering av identitet måste, som vi ser det, emellertid ett av stegen utgöras av en jämförelse av biometriska uppgifter för att – på ett tillförlitligt sätt – koppla ihop uppgifter hänförliga till den påstådda identiteten med uppgifter om identitet och eventuella andra uppgifter som är lagrade i en sådan handling som vi i avsnitt 23.6.2 föreslår ska få användas. Den möjlighet för myndigheter att kräva att någon gör en sådan handling tillgänglig och låter myndigheten ta upp biometriska underlag, som vi föreslår ska införas i den nya lagen (se avsnitt 23.6.3 och 23.6.4), ska endast få användas i syfte att biometriskt verifiera identitet. Genom att lagen innehåller en särskild definition av detta begrepp främjas enligt vår mening en tydlighet och förutsebarhet, både för myndigheter som ska tillämpa den nya lagen och för enskilda vars identitet kan komma att verifieras med stöd av lagen.

Vi anser därför att det uttryckligen ska anges i den nya lagen vad som avses med *biometrisk verifiering av identitet*, nämligen en-till-en-jämförelse av en grupp av uppgifter, däribland biometriska uppgifter, med en annan för att fastställa om en påstådd identitet är riktig.

23.5.6 Myndighet

Vårt förslag

Det ska framgå av den nya lagen att med begreppet *myndighet* avses statliga och kommunala organ, med undantag för beslutande politiska församlingar.

Genom våra förslag om att myndigheter ska få verifiera identitet biometriskt (se avsnitt 23.6.3) utökas kretsen av offentliga aktörer som får en möjlighet att biometriskt verifiera identitet mot handlingar betydligt, jämfört med i dag. Med hänsyn inte minst till det integritetsintrång som sådana kontroller kan anses medföra (se avsnitt 21.7.3) anser vi att det är av vikt att det i den nya lagen tydliggörs vad som avses med myndigheter vid tillämpning av lagen. Som vi redogjort för i avsnitt 21.3.1 jämställs vissa organ med myndigheter i olika rättsliga sammanhang. Vi har emellertid i nyss nämnda avsnitt bedömt att kretsen av organ som bör få möjlighet att biometriskt verifiera identitet mot handlingar bör begränsas till myndigheter, genom att beslutande politiska organ (det vill säga riksdagen och beslutande kommunala församlingar), organ som anges i bilagan till offentlighets- och sekretesslagen (2009:400) samt bolag, föreningar och stiftelser där kommuner eller regioner utövar ett rättsligt bestämmande inflytande inte bör jämställas med myndigheter. Att nämnda organ jämställs med myndigheter i andra sammanhang motiveras – som vi redogjort för i avsitt 21.3.1 – framför allt av ett insynsintresse, vilket inte går att jämställa med ett behov av att kunna biometriskt verifiera identitet.

Sammantaget gäller att med begreppet myndighet avses – enligt regeringsformens terminologi – samtliga statliga och kommunala organ med undantag för beslutande politiska församlingar. Det betyder för staten bland annat att regeringen och Regeringskansliet är myndigheter. Även domstolarna är statliga myndigheter. Med kommunala organ avses regioner och kommuner. Inom regionerna och kommunerna finns det nämnder som är regionala respektive kom-

munala förvaltningsmyndigheter; dessa anser också utgöra kommunala organ.[13]

I syfte att främja en tydlig och förutsebar tillämpning av den nya lagen anser vi därför att det ska särskilt anges i lagen att med begreppet myndighet avses statliga och kommunala organ, med undantag för beslutande politiska församlingar. Det behöver enligt vår mening inte särskilt anges att de organ som i vissa sammanhang jämställs med myndigheter *inte* ska omfattas.

23.6 En generell möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar

Vi har i avsnitt 21.3 tagit ställning till vilka aktörer som bör ges en utökad möjlighet att använda biometrisk verifiering av identitet mot handlingar och i avsnitt 21.5 till i vilka situationer sådan verifiering ska få användas. De överväganden vi gjort i nämnda avsnitt ligger till grund för våra förslag nedan.

23.6.1 En möjlighet, inte en skyldighet

Vårt förslag

Bestämmelsen om biometrisk verifiering av identitet mot handlingar i den nya lagen ska ha en fakultativ utformning.

Våra överväganden i avsnitt 21.5 omfattar endast frågan om en *möjlighet* för myndigheter att biometriskt verifiera identitet mot handlingar bör införas. Om sådana kontroller används i stor utsträckning, exempelvis i samband med ansökan om olika socialförsäkringsförmåner, skulle det kunna få tydliga effekter på omfattningen av identitetsmissbruk som riktar sig mot det allmänna. Enskilda skulle även i större utsträckning kunna förlita sig på att deras identitet inte utnyttjas i sådana sammanhang. Med hänsyn till detta skulle det kunna övervägas om den nya lagen bör utformas så att myndigheter – generellt eller under vissa förutsättningar – ska vara skyldiga att använda

[13] Jfr *Nya regler om cybersäkerhet*, SOU 2024:18, s. 127 f. och *Styra och ställa – förslag till en effektivare statsförvaltning*, SOU 2008:118, s. 230.

biometrisk verifiering av identitet mot handlingar, i de situationer vi redogjort för i avsnitt 21.5.1 och 21.5.2. Vi anser dock att det inte är lämpligt att utforma den nya lagen på sådant sätt, av följande skäl.

Redan den omständigheten att den nya lagen ska kunna tillämpas av en bred krets av myndigheter, som bedriver vitt skilda verksamheter och därmed har olika behov av att biometriskt verifiera identitet, talar enligt vår mening starkt mot att biometrisk verifiering ska utgöra en skyldighet. Det är inte möjligt att utan en noggrann analys av samtliga myndigheter begränsa en skyldighet till exempelvis vissa ärendeslag. Skyldigheten skulle därför som utgångspunkt behöva göras generell. En skyldighet utan en möjlighet till undantag är som vi ser det dock uteslutet. En sådan ordning skulle leda till ett oproportionerligt integritetsintrång, om biometrisk verifiering av identitet skulle behöva användas även när det står helt klart att det inte är nödvändigt; ett exempel kan tänkas vara en ansökan om ekonomiskt bistånd som görs på plats av en person som biståndshandläggaren har personlig kännedom om från tidigare ärenden. En skyldighet att verifiera identitet biometriskt skulle också kunna medföra betydande merarbete och kostnader för myndigheter som handlägger ett mycket stort antal ärenden som normalt behöver handläggas snabbt, exempelvis om tillfällig föräldrapenning.

Med hänsyn till det nyss anförda står det klart att en skyldighet i den nya lagen skulle behöva kompletteras med någon form av undantagsmöjlighet. Ett undantag skulle till exempel kunna utformas så att det anges att biometrisk verifiering av identitet inte behöver användas om identiteten kan verifieras på annat sätt, eller om det finns särskilda skäl. Sådana undantagsmöjligheter skulle dock som vi ser det i praktiken kunna medföra en motsvarande tillämpning som en fakultativt utformad bestämmelse. Vi kan konstatera att en myndighets bedömning av om det i ett enskilt fall finns särskilda skäl som utgångspunkt inte skulle kunna bli föremål för prövning – till exempel i domstol – utan särskilt stöd för det i den nya lagen, vilket innebär att bedömningsutrymmet i princip skulle kunna anses lika stort som det som följer av en helt fakultativ bestämmelse. Respektive myndighet har som vi ser det bäst möjlighet att avgöra i vilka fall sådan biometrisk verifiering som den nya lagen syftar till att möjliggöra bör användas, däribland om det är nödvändigt med en sådan kontroll (se avsnitt 23.6.3). Även om en bestämmelse som innebär att myndigheter – som utgångspunkt – skulle vara skyldiga att använda biometrisk

verifiering av identitet kan anses sända en signal om vikten av säker verifiering av identitet i olika sammanhang, och därmed främja ett effektivt genomslag av den nya lagen, anser vi att en fakultativ utformning inte motarbetar en ändamålsenlig tillämpning. Även med en fakultativ utformning har regeringen en möjlighet att genom regleringsbrev, myndighetsinstruktioner och särskilda uppdrag styra tillämpningen på lämpligt sätt, om detta behövs för att främja den nya lagens genomslag.

Utifrån våra överväganden i avsnitt 21.5.1 och 21.5.2 ska – som vi återkommer till nedan – biometrisk verifiering mot handlingar enligt den nya lagen förutsätta att sådan verifiering är nödvändig. Detta innebär ett visst bedömningsutrymme för myndigheterna. Att biometrisk verifiering av identitet med stöd av den nya lagen endast ska få användas när det är nödvändigt ska däremot inte tolkas så att det måste motiveras utifrån omständigheterna i varje enskilt fall, eller att lagen inte kan tillämpas i bredare sammanhang, exempelvis genom att stickprovskontroller används. Biometrisk verifiering kan även i sådana fall anses nödvändig, om kontrollen exempelvis bygger på att myndigheten sett ett mönster av felaktigheter relaterade till identitet i ett visst eller vissa ärendeslag, eller om det är fråga om ärenden som har inletts på distans.

Vid en sammantagen bedömning av det ovan anförda anser vi att den nya lagen ska utformas så att den ger myndigheter en *möjlighet* att använda biometrisk verifiering mot handlingar. Det ska alltså inte vara en skyldighet att använda sådana kontroller. Självfallet hindrar inte detta att det för en myndighet kan finnas tvingande regler om verifiering i annan lagstiftning.

En fråga i detta sammanhang är om en skyldighet för myndigheter att biometriskt verifiera identitet kan uppkomma genom att enskilda kan begära att en myndighet alltid använder sådan verifiering för honom eller henne med stöd av den nya lagen, exempelvis i ett visst ärendeslag. En sådan möjlighet skulle som vi ser det kunna fylla ett viktigt ändamål, nämligen att den nya lagen ska kunna fungera som en skyddslagstiftning. En jämförelse kan göras med den möjlighet som enskilda har i dag att spärra obehörig adressändring, genom att meddela Skatteverket att flyttanmälan och anmälan av särskild postadress alltid ska göras via Skatteverkets e-tjänster, med användning av e-legitimation. Detta skydd skulle kunna förstärkas ytterligare genom att den enskilde kan ange att det också ska krävas biometrisk

verifiering av hans eller hennes identitet enligt den nya lagen i dessa situationer. På så sätt skulle användning av en e-legitimation som någon obehörig person har kommit över hindras. En sådan form av ”spärrtjänst” hade, som vi ser det, också kunnat vara av intresse i ärenden hos bland annat Bolagsverket, för att hindra att enskilda används som målvakter i bolag, utan deras vetskap. En möjlighet för den enskilde att på förhand begära att biometrisk verifiering enligt den nya lagen alltid ska användas i ett visst ärendeslag, som avser honom eller henne, skulle enligt vår mening alltså kunna utgöra ett effektivt skydd mot id-kapning. För att vara förenligt med våra förslag om när biometrisk verifiering ska få användas, förutsätter det emellertid att det nödvändighetskriterium som vi redogjort för i avsnitt 21.5.1 och återkommer till i avsnitt 23.6.5 är uppfyllt. En bedömning behöver då göras av myndigheten för det aktuella ärendeslaget som sådant; *Är det, som utgångspunkt, nödvändigt med en biometrisk verifiering i ärendeslaget?* För att en myndighet ska kunna erbjuda en spärrtjänst, som innebär att handläggningen av ärenden kräver biometrisk verifiering med stöd av den nya lagen, behöver myndigheten alltså i förväg bedöma att det är nödvändigt med sådan verifiering vid handläggningen av det aktuella ärendeslaget. För det fall en myndighet gör det praktiskt och tekniskt möjligt för enskilda att på förhand registrera en ”spärr” av det aktuella slaget hos myndigheten, exempelvis via Mina sidor eller liknande, i ett ärende som avser honom eller henne, skulle det kunna anses medföra att det i sådana fall de facto finns en större, däremot inte absolut, skyldighet för myndigheten att genomföra en sådan kontroll, så länge de förutsättningar som vi redogör för i avsnitt 23.6.3 är uppfyllda. Det bör understrykas att det inte skulle vara fråga om att den biometriska verifieringen, eller den behandling av personuppgifter som utförs med anledning av den, utförs med den enskildes samtycke i den mening som avses i artikel 6.1 a i dataskyddsförordningen, utan på de rättsliga grunder som vi redogjort för i avsnitt 21.7.

23.6.2 Typer av handlingar som ska få användas

Vårt förslag

Hemlandspass och identitetskort som har utfärdats av behörig myndighet och som har ett lagringsmedium där fingeravtryck eller ansiktsbild är sparade ska få användas för att biometriskt verifiera innehavarens identitet. Även uppehållstillståndskort som har utfärdats av svenska myndigheter ska få användas för sådan verifiering.

Som vi har redogjort för i avsnitt 19.3 anser vi att det endast är vissa typer av handlingar som bör kunna användas inom ramen för en mer generell möjlighet för myndigheter att biometriskt verifiera innehavarens identitet. I avsnitt 19.4 har vi begränsat dessa till i första hand hemlandspass och identitetskort som har utfärdats av behörig myndighet och som innehåller ett lagringsmedium med biometriska underlag. Vi har även bedömt att uppehållstillståndskort som utfärdats av svenska myndigheter bör kunna användas för att biometriskt verifiera innehavarens identitet.

Lagringsmediet i samtliga handlingar som vi i nämnda avsnitt har bedömt är lämpliga innehåller identitetsuppgifter, det vill säga namn, födelsetid och medborgarskap; det statliga identitetskortet *utan resefunktion* kommer däremot inte att innehålla en uppgift om medborgarskap (se avsnitt 27.2). Att lagringsmediet även innehåller uppgifter om identiteten har särskilt betydelse för att handlingen ska kunna användas för biometrisk verifiering på distans, exempelvis på det sätt vi beskriver i avsnitt 27.4. De uppgifter om identitet som kan hämtas ur (lagringsmediet på) handlingen utgör också det huvudsakliga jämförelseunderlaget, när myndigheten ska kontrollera om de stämmer med den påstådda identiteten. Som vi redogjort för i avsnitt 7.2.1 kan även andra alfanumeriska uppgifter som finns på handlingen användas vid jämförelsen, exempelvis en identitetsbeteckning eller en uppgift om innehavarens kön. För det fall handlingen kan kontrolleras på plats av myndigheten kan identitetsuppgifterna som ska användas för jämförelsen visserligen ”hämtas” genom att handläggaren läser de uppgifter som är synliga på handlingen. Tryckta uppgifter får emellertid anses vara betydligt lättare att manipulera än identitetsuppgifter som är lagrade digitalt i ett chip på handlingen. Det är alltså,

som vi ser det, av vikt att lagringsmediet i de handlingar som ska få användas för biometrisk verifiering av identitet med stöd av den nya lagen också innehåller identitetsuppgifter. Vi anser emellertid att det inte behöver framgå uttryckligen av den nya lagen, utan den centrala avgränsningen som bör komma till uttryck i lagen är, som vi ser det, att endast handlingar som har ett lagringsmedium med biometriska underlag ska få användas.

När det gäller uppehållstillståndskort är det i praktiken i dagsläget endast Migrationsverket som utfärdar dessa. I lagen bör det, enligt vår mening, dock anges att uppehållstillståndskort som utfärdats av svenska myndigheter får användas för biometrisk verifiering av identitet. Detta för att lagen inte ska behöva ändras om andra myndigheter än Migrationsverket får i uppdrag att utfärda uppehållstillståndskort. Det är som vi ser det inte nödvändigt att det anges uttryckligen i den nya lagen att endast uppehållstillståndskort som innehåller ett lagringsmedium ska få användas, då detta alltid är fallet för sådana handlingar som utfärdas av svenska myndigheter.

Vi anser att det är lämpligt att det anges i en särskild bestämmelse i den nya lagen vilka typer av handlingar som ska få användas för att biometriskt verifiera identitet, på liknande sätt som i 26 b § folkbokföringslagen. Som vi redogjort för i avsnitt 19.4 anser vi emellertid att en snävare utformning bör användas i den nya lagen för att främja en ändamålsenlig tydlighet och förutsebarhet, utifrån att lagen ska kunna användas av en mycket stor krets av myndigheter.

Mot denna bakgrund anser vi att det ska anges i den nya lagen att hemlandspass och identitetskort som har utfärdats av behörig myndighet och som har ett lagringsmedium där fingeravtryck eller ansiktsbild är sparade ska få användas för att biometriskt verifiera innehavarens identitet. Begreppet hemlandspass avser att utgöra en avgränsning mot främlingspass och resedokument, och ska vid tillämpning av lagen – i fråga om passhandlingar som utfärdas av svenska myndigheter – omfatta sådana pass som avses i 3 § passlagen, det vill säga vanligt pass och särskilt pass; i sistnämnda grupp ingår provisoriskt pass, extra pass, tjänstepass och diplomatpass. Även uppehållstillståndskort som utfärdats av svenska myndigheter ska få användas. Vi återkommer i avsnitt 23.9 till frågan om att genom förordning eller föreskrifter ytterligare begränsa vilka handlingar som får användas.

23.6.3 Grundläggande förutsättningar

Vårt förslag

Myndigheter ska få använda biometriska uppgifter för att verifiera identitet mot handlingar, om det är nödvändigt vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde, eller, i annat fall, när myndigheten, inom ramen för sin verksamhet, genomför identitetskontroller.

I avsnitt 21.5 har vi bedömt att en utökad möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar bör begränsas till när det är nödvändigt vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde eller, i annat fall, när myndigheten, inom ramen för sin verksamhet, genomför identitetskontroller. Det saknas anledning att här göra en annan bedömning. Några förtydligande kan dock göras i detta sammanhang.

Handläggningen av ett ärende

Vi har i avsnitt 21.5.1 bedömt att myndigheter bör få använda biometrisk verifiering av identitet mot handlingar vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde. Vad som kännetecknar ett sådant ärende framgår av våra överväganden i nämnda avsnitt. I det avsnittet har vi också påpekat att ett ärende kan omfattas av förvaltningslagens tillämpningsområde även i de fall det finns verksamhetsspecifika bestämmelser i annat regelverk som reglerar handläggningen av det aktuella ärendet, till exempel i skatteförfarandelagen (2011:1244). Det ankommer på den myndighet som vill tillämpa den nya lagen att ta ställning till om det är fråga om ett ärende som omfattas av förvaltningslagens tillämpningsområde. I de allra flesta fall kan det, som vi ser det, antas att denna avgränsning inte medför några svårigheter.

Möjligheten att använda biometrisk verifiering enligt den nya lagen i ärenden ska vidare vara knuten till handläggningen av ett ärende. Uttrycket *handläggning* är mycket brett och innefattar i princip alla åtgärder som en myndighet vidtar från det att ett ärende inleds till

dess att det avslutas.[14] Det kan röra sig om allt från att registrera en handling i ett ärende till att ringa ett telefonsamtal, upprätta en tjänsteanteckning, skicka ett brev eller upprätta ett beslutsförslag. Uttrycket täcker även det beslut varigenom ärendet avgörs.[15] Det är som vi ser det inte möjligt eller nödvändigt att i den nya lagen närmare ange vad som avses med handläggningen av ett ärende utan det ankommer på den myndighet som vill verifiera identitet biometriskt med stöd av lagen att ta ställning till detta och säkerställa att rekvisitet är uppfyllt.

Det kan i detta sammanhang framhållas att syftet med en bestämmelse som ger myndigheter rätt att biometriskt verifiera identitet vid handläggningen av ett ärende inte endast är att identiteten hos den som inlett ett ärende eller som är part ska kunna verifieras biometriskt med stöd den nya lagen, utan det kan även vara fråga om att verifiera identiteten för andra personer som förekommer i ett visst ärende. Det skulle till exempel kunna vara en anhörig till den som ärendet avser eller någon som tar kontakt med myndigheten i syfte att lämna information. Som vi återkommer till i avsnitt 23.8 anser vi däremot att ett föreläggande om att medverka till att en biometrisk verifiering faktiskt kan genomföras endast ska kunna riktas mot den som har inlett ett ärende. När det gäller rekvisitet att biometrisk verifiering av identitet ska vara nödvändig hänvisar vi till de överväganden vi gjort i avsnitt 21.5.1.

Sammantaget anser vi att myndigheter ska få verifiera identitet biometriskt mot handlingar om det är nödvändigt vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde.

Identitetskontroller i myndigheters faktiska verksamhet

I avsnitt 21.5.2 har vi bedömt att myndigheter bör få använda biometrisk verifiering av identitet mot handlingar om det är nödvändigt när myndigheten, inom ramen för sin verksamhet, genomför identitetskontroller. Det är alltså fråga om situationer som inte är knutna till handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde, utan som främst har koppling till den faktiska verksamhet som myndigheter bedriver. Det kan därför framför allt antas bli fråga om att genomföra biometriska kontroller i samband

[14] *En modern och rättssäker förvaltning – ny förvaltningslag,* prop. 2016/17:180, s. 286.
[15] Lundmark och Säfsten, *Förvaltningslagen*, 26 augusti 2024, JUNO version 1C, kommentaren till 1 §, under rubriken *Vad är handläggning?*

med att den person vars identitet kontrolleras är på plats hos myndigheten, exempelvis i samband med ett besök i vården eller vid genomförande av högskoleprovet. Det ankommer på myndigheten att säkerställa att en biometrisk verifiering med stöd av den nya lagen görs inom ramen för den verksamhet som myndigheten är ålagd att bedriva. Detta bör som vi ser det normalt inte medföra några svårigheter, utan framgår av bland annat av förordningar med myndighetsinstruktioner.

En biometrisk verifiering med stöd av den nya lagen – på det sätt vi redogjort för i avsnitt 21.5.2 – ska få användas endast i samband med att identitetskontroller genomförs i annat fall än vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde. Även i detta avseende ankommer det på respektive myndighet att se till att det finns stöd för att alls genomföra identitetskontroller. Genom att möjligheten till biometrisk verifiering knyts till att identitetskontroller genomförs av annan anledning tydliggörs – som vi lyft fram i avsnitt 21.5.2 – att syftet inte är att skapa en självständig möjlighet för myndigheter att kontrollera identitet, utan att det är fråga om en kompletterande åtgärd som kan användas när det vid en identitetskontroll anses nödvändigt att verifiera identiteten biometriskt. När det gäller rekvisitet att biometrisk verifiering ska vara nödvändig hänvisar vi till de överväganden vi gjort i avsnitt 21.5.2.

Det bör här lyftas fram att det inte ska krävas att en identitetskontroll faktiskt har genomförts i ett enskilt fall, och att denna inte bedömts tillräcklig, för att den nya lagen ska få tillämpas. Det ska alltså inte krävas att myndigheten först okulärt kontrollerar en fysisk identitetshandling. Under förutsättning att biometrisk verifiering av identitet bedöms vara nödvändig ska en bedömning kunna göras på förhand genom att myndigheten, i samband med identitetskontroller som man genomför i verksamheten, använder biometrisk verifiering med stöd av den nya lagen. För att tydliggöra detta anser vi att en bestämmelse som reglerar den nu aktuella möjligheten att biometriskt verifiera identitet bör utformas så att det anges att detta får användas när myndigheten, inom ramen för sin verksamhet, *genomför identitetskontroller*; att i stället ange att de får användas när myndigheten *genomför en identitetskontroll* riskerar som vi ser det att leda tanken till att en okulär kontroll också måste ha genomförts i det enskilda fallet, innan en biometrisk verifiering är möjlig.

Sammanfattningsvis anser vi att myndigheter ska få använda biometriska uppgifter för att verifiera identitet mot handlingar om det,

i annat fall än vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde, är nödvändigt när myndigheten, inom ramen för sin verksamhet, genomför identitetskontroller.

23.6.4 En skyldighet att lämna biometriska underlag för kontroll mot dem som är lagrade i en handling

Vårt förslag och vår bedömning

Den som har fyllt sex år och innehar en sådan handling som anges i avsnitt 23.6.2 ska på begäran av en myndighet göra handlingen tillgänglig och låta myndigheten ta fingeravtryck och ansiktsbild, för kontroll av att de motsvarar dem som finns i eller på handlingen.

Diplomatisk personal och personer som tillhör en främmande stats militära styrka eller ett Natohögkvarter och som vistas i Sverige bör inte undantas.

Vi har i avsnitt 21.4.1 bedömt att en möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar behöver regleras i lag. För att en sådan kontroll ska kunna genomföras förutsätts att myndigheten har stöd för att begära att den vars identitet ska kontrolleras gör en handling tillgänglig och att han eller hon lämnar fingeravtryck och ansiktsbild som kan jämföras med de som finns lagrade i handlingen. Fråga är hur en bestämmelse i den nya lagen som reglerar detta lämpligen bör utformas.

En jämförelse kan göras med några av de bestämmelser som i dag reglerar biometrisk verifiering av identitet mot handlingar, i folkbokföringslagen respektive utlänningslagen. I förstnämnda författning har en uppdelning gjorts mellan den enskildes skyldighet att vid personlig inställelse överlämna vissa uppräknade handlingar för kontroll (26 b §), respektive att låta Skatteverket ta hans eller hennes fingeravtryck och ansiktsbild i digitalt format, för att kontrollera att dessa motsvarar dem som finns i handlingen (26 c §). Detta är, som vi uppfattar det, naturligt med hänsyn till att bestämmelserna i folkbokföringslagen syftar till att mer generellt främja en stärkt identitetskontroll i samband med bland annat flyttning till Sverige; den biometriska verifieringen av identiteten är endast en sekundär del av kontrollen. I regeringens proposition *Utökade befogenheter för Skatteverket inom*

folkbokföringsverksamheten föreslås att 26 c § folkbokföringslagen ska justeras och att det i en ny 26 d § ska anges att Skatteverket ska få kontrollera att uppgifterna som har tagits enligt 26 c § motsvarar dem som finns *i eller på en handling* som har överlämnats enligt 26 b §. Detta med anledning av att lagförslagen syftar till att möjliggöra kontroll mot en synlig ansiktsbild på en handling.[16]

I exempelvis 9 kap. 8 b § utlänningslagen regleras å andra sidan i första hand den biometriska verifieringen av identitet mot handlingar. Någon uppdelning av de olika momenten på det sätt som följer av tidigare nämnda bestämmelser i folkbokföringslagen har därför inte gjorts utan i bestämmelsen anges att den som innehar vissa uppräknade handlingar är skyldig att låta tjänstemän hos angivna myndigheter fotografera honom eller henne och ta hans eller hennes fingeravtryck, för kontroll mot de biometriska underlag som finns sparade i handlingen.

Enligt vår mening ligger en reglering i den nya lagen närmast bestämmelsen i utlänningslagen. Detta med hänsyn till att tillgängliggörande av handlingen utgör ett integrerat led i den biometriska verifieringen, inte ett självständigt moment för att kontrollera identiteten. Syftet med den nya lagen är inte att ge myndigheter en generell möjlighet att – okulärt – kontrollera vissa typer av handlingar, som ett led i att den enskilde ska styrka sin identitet, utan den nya lagen ska möjliggöra en säkrare verifiering av identitet mot handlingar, *med hjälp av biometriska uppgifter*. Vi anser därför att en bestämmelse som reglerar detta i den nya lagen inte bör utformas på ett sätt som innebär att enskilda är skyldiga att göra handlingar tillgängliga för myndigheter av andra skäl än att möjliggöra en kontroll av de biometriska underlag som är lagrade i eller synliga på dem, och därmed en verifiering av innehavarens identitet. När det gäller användning av biometriska underlag i form av en synlig ansiktsbild på handlingen bör det – som vi redogjort för i avsnitt 20.2.4 – endast vara aktuellt i samband med personlig inställelse, med hänsyn till att det med nuvarande teknik inte går att på distans säkerställa att ansiktsbilden härrör från handlingen. En sådan begränsning är emellertid i första hand av teknisk natur. Vilken metod som är lämplig bör överlåtas till rättstillämparen. Vi anser därför att det inte bör regleras i den nya lagen att en synlig ansiktsbild *endast* ska få användas när den biometriska verifieringen görs på plats.

[16] Prop. 2025/26:261, s. 102 f.

En handling kan, som vi redogjort för i avsnitt 21.4.1, göras tillgänglig på olika sätt. Vid personlig inställelse är det mer naturligt att prata om att överlämna handlingen, medan det vid biometrisk verifiering av identitet på distans på det sätt vi beskriver i avsnitt 27.4 är fråga om att göra handlingen *tillgänglig*, så att den kan användas för den biometriska verifieringen. Att göra handlingen tillgänglig bör enligt vår mening omfatta även att den överlämnas vid personlig inställelse. Beroende på vilken teknisk lösning som är tillgänglig i det enskilda fallet kan en skyldighet för den enskilde att göra handlingen tillgänglig alltså i praktiken komma att indirekt innefatta en skyldighet att inställa sig personligen. Detta behöver som vi ser det däremot inte komma till uttryck särskilt i den nya lagen (jfr avsnitt 20.3). Biometrisk verifiering av identitet innefattar inte bara en jämförelse av biometriska uppgifter utan även av de alfanumeriska uppgifter om i första hand identitet som finns lagrade i eller på den handling som används för verifieringen. I skyldigheten att på begäran från myndigheten göra en handling tillgänglig ligger som vi ser det därför även att låta myndigheten ta del av sådana uppgifter, i syfte att kunna genomföra en biometrisk verifiering av identiteten.

Den enskilde behöver också åläggas en skyldighet att, på begäran av den myndighet som vill verifiera identitet, låta myndigheten ta fingeravtryck och ansiktsbild; för att en datorstödd jämförelse ska kunna göras behöver de vara i digitalt format. I den ovan nämnda propositionen bedömde regeringen dock att det i 26 c § folkbokföringslagen respektive 2 kap. 4 § lagen om samordningsnummer saknas skäl att föreskriva att ansiktsbild ska tas i digitalt format. Reglering bör enligt regeringen vara teknikneutral på så sätt att formen för upptagande av ansiktsbild inte behöver regleras särskilt.[17] Vi gör samma bedömning här.

Skyldigheten att låta myndigheten ta fingeravtryck och ansiktsbild ska framgå av en bestämmelse i den nya lagen. Med utgångspunkt i en sådan verifieringsprocess som vi beskriver i avsnitt 27.3 och 27.4 – där verifiering framför allt ska kunna göras på distans – skulle man kunna se det som att den enskilde lämnar biometriska underlag genom att han eller hon använder en särskild applikation på en mobiltelefon, snarare än att myndigheten tar upp dem. Det är dock inte fråga om att den enskilde ska lämna in uppgifter till myndigheten, utan det kommer fortfarande vara myndigheten som tar upp biometriska

[17] Prop. 2025/26:261, s. 49.

underlag – vid personlig inställelse eller på distans – för att verifieringen ska kunna genomföras. Det bör därför anges i bestämmelsen att den enskilde på begäran ska låta myndigheten ta biometriska underlag. Av bestämmelsen ska det vidare uttryckligen framgå att de typer av biometriska underlag som den enskilde ska vara skyldig att lämna är fingeravtryck och ansiktsbild.

Särskilt om åldersgräns

Den krets av personer vars identitet ska kunna verifieras biometriskt med stöd av den nya lagen begränsas till viss del genom att endast vissa typer av handlingar ska få användas, enligt vårt förslag i avsnitt 23.6.2. I avsnitt 20.4 har vi även bedömt att en möjlighet att biometriskt verifiera identitet mot handlingar inte bör gälla för barn under sex år. Detta med hänsyn bland annat till att det endast i undantagsfall kan antas finnas ett behov av att verifiera identitet för så små barn. Det saknas anledning att nu göra en annan bedömning.

Det skulle kunna övervägas att låta denna åldersgräns ingå som en del i en lämplighetsbedömning, inom ramen för myndigheternas bedömning av om de i ett visst fall vill utnyttja den nya lagens möjligheter till biometrisk verifiering av identitet mot handlingar. En sådan ordning skulle dock kunna leda till en godtycklig och mindre förutsebar tillämpning. Vi anser därför att det ska framgå uttryckligen av den nya lagen att endast den som har fyllt sex år är skyldig att på begäran göra en handling tillgänglig och lämna fingeravtryck och ansiktsbild. Hur en sådan begäran fullgörs i praktiken när den riktas mot ett barn anser vi inte bör regleras i den nya lagen utan detta får följa den ordning som normalt tillämpas i det ärendeslag eller den situation som har föranlett begäran. Upptagning av biometriska underlag ska dock alltid göras på ett barnvänligt och barnanpassat sätt, med beaktande av principen om barnets bästa.

Personer som kan vara förhindrade att lämna fingeravtryck

En fråga i detta sammanhang är om det bör införas ett uttryckligt undantag i den nya lagen från skyldigheten att på begäran lämna fingeravtryck i digitalt format för personer som av fysiska skäl är permanent förhindrade att lämna fingeravtryck. Ett sådant undan-

tag framgår av bland annat 9 kap. 8 d § utlänningslagen. Med hänsyn till att vi föreslår att biometrisk verifiering av identitet med stöd av den nya lagen inte ska vara en skyldighet utan att sådan verifiering ska vara fakultativ anser vi att det inte är nödvändigt att ett uttryckligt undantag av nämnda slag införs i lagen. Möjligheterna för den enskilde att lämna fingeravtryck får i stället beaktas inom ramen för myndighetens bedömningsutrymme i det enskilda fallet. Det kan i detta sammanhang även erinras om att fingeravtryck endast är ett av två biometriska underlag som ska kunna användas för att biometriskt verifiera identitet med stöd av den nya lagen. Vid verifiering på distans inom ramen för en sådan process som vi beskriver i avsnitt 27.4 är det inte heller möjligt att använda fingeravtryck. Det talar ytterligare mot ett behov av ett särskilt undantag i den nya lagen. En begäran om att den enskilde ska medverka till att biometriskt verifiera sin identitet kan också i ett visst fall utformas så att den endast omfattar en skyldighet att lämna ansiktsbild.

Särskilt om diplomatisk personal

Vi har i avsnitt 12.4.6 bedömt att det saknas behov av att diplomatisk personal och personer som tillhör en främmande stats militära styrka eller ett Natohögkvarter och som vistas i Sverige omfattas av ett identitetsindex. Detta med hänsyn bland annat till att de inte anses vara bosatta eller ha hemvist i Sverige, och med beaktande av deras särskilda ställning och därtill följande immunitet och privilegier. Frågan är om det av samma anledningar finns skäl för att undanta dem från en skyldighet att låta en myndighet verifiera deras identitet med stöd av den nya lagen.

Vi kan för det första konstatera att intrånget i den personliga integriteten skiljer sig betydligt från intrånget vid biometrisk verifiering mot ett identitetsindex, genom att tillämpningen av den nya lagen inte förutsätter att det finns några uppgifter lagrade om den enskilde, varken identitetsuppgifter eller biometriska uppgifter. Den särskilda ställning som diplomatisk personal åtnjuter i olika sammanhang utgör, med hänsyn till det betydligt mer begränsade intrånget i den personliga integriteten, enligt vår mening inte tillräckligt skäl för att undanta dem. Tvärtom kan det vara så att deras särskilda ställning gör dem mer utsatta för försök till kapning av deras identitet. Att i

olika sammanhang kunna biometriskt verifiera identitet, exempelvis vid tillträde till myndighetsbyggnader, kan därför vara en viktig komponent i att motverka detta. Till detta kommer att dessa personkategorier ofta tilldelas personnummer, trots att de inte ska folkbokföras, med hänsyn till att detta underlättar deras vardagliga liv i Sverige (se avsnitt 12.4.6). Även detta talar enligt vår mening för att det finns ett behov av att kunna biometriskt verifiera deras identitet med stöd av den nya lagen.

Vi anser mot denna bakgrund att diplomatisk personal och personer som tillhör en främmande stats militära styrka eller ett Natohögkvarter inte bör undantas från en skyldighet att göra en handling tillgänglig och låta en verifierande myndighet ta fingeravtryck och ansiktsbild, för kontroll av att de biometriska underlagen motsvarar dem som finns i eller på handlingen.

Särskilt om företrädare för juridiska personer

Av naturliga skäl är det endast fysiska personer som i praktiken kan fullgöra en begäran om att biometriskt verifiera identitet med stöd av den nya lagen. Som vi nämnt i avsnitt 9.2.2 kan identitetsmissbruk manifesteras genom att så kallade målvakter används för att bemanna bolagsstyrelser och som firmatecknare, och falska identiteter kan användas i syfte att dölja vem den verkliga företrädaren i ett bolag är. Det kan därför finnas behov för myndigheter – exempelvis Skatteverket och Bolagsverket – att säkerställa företrädarens identitet; vi kan notera att en möjlighet för Skatteverket att bland annat förelägga en bolagsföreträdare att inställa sig personligen därför har föreslagits.[18] Något som hindrar att en begäran med stöd av den nya lagen riktas även mot en företrädare för ett bolag som är en fysisk person anser vi saknas, och en möjlighet att vidta en sådan kompletterande utredningsåtgärd skulle enligt vår mening kunna vara värdefull för att motverka användning av så kallade målvakter i bolag av olika slag. Vi anser mot denna bakgrund att företrädare för juridiska personer inte bör undantas från den nya lagens tillämpning. Detta behöver emellertid inte särskilt komma till uttryck i lagen.

[18] *Åtgärder mot mervärdesskattebedrägerier*, SOU 2024:32, s. 274 f.

23.7 Konsekvenser av att verifieringen inte visat att den påstådda identiteten är riktig

Vår bedömning

Det bör inte i den nya lagen regleras vilka konsekvenser som kan följa av att en biometrisk verifiering enligt lagen inte visat att den påstådda identiteten är riktig.

Om den enskilde medverkar till en biometrisk verifiering av identiteten enligt den nya lagen på avsett sätt, kan kontrollen visa att de biometriska underlag som tagits upp eller de identitetsuppgifter som den enskilde har lämnat, och motsvarande uppgifter som finns lagrade i handlingen som använts för jämförelsen, inte stämmer överens. I sådant fall har det alltså inte kunnat visas genom verifieringen att den påstådda identiteten är riktig. Fråga är om det bör regleras i den nya lagen vilka eventuella konsekvenser detta ska kunna leda till.

Att den biometriska jämförelsen inte lyckas kan ha flera tänkbara anledningar. En möjlighet är att handlingen som den enskilde använder tillhör en annan person, som har samma identitetsuppgifter. Detta kan tänkas inträffa exempelvis vid kapning av någons identitet eller vid användning av så kallade look-a-like-handlingar. I sådana fall kan det framstå som naturligt att följden blir att en framställan avslås eller avvisas, med stöd av en uttrycklig bestämmelse i den nya lagen. En misslyckad verifiering – i den mening att kontrollen inte visat att den påstådda identiteten är riktig – skulle dock även kunna bero på att den datorstödda jämförelsen inte kunnat utföras på ett tillräckligt bra sätt, eller att det tröskelvärde som används för när en matchning ska anses föreligga inte har uppnåtts. Det kan bero på att handlingen är skadad eller att de biometriska underlagen inte har kunnat tas upp med tillräcklig kvalitet av någon anledning. I sådana fall behöver det inte vara fråga om ett försök till identitetsmissbruk. Det tekniska system som används kan då behöva notifiera användaren om att en ny ansiktsbild behöver tas upp, genom att en signal om detta skickas till en mobilapplikation som använts för upptagningen eller, om personen vars identitet ska verifieras är närvarande på plats hos en myndighet, genom att han eller hon uppmanas att göra ett nytt försök. Att den misslyckade biometriska jämförelsen i sådana situationer inte automatiskt bör leda till exempelvis att en ansökan avslås eller

avvisas framstår enligt vår mening som självklart, utan myndigheten kan i stället först behöva vidta ytterligare utredningsåtgärder av olika slag. Detta talar som vi ser det tydligt mot att i den nya lagen reglera hur den omständigheten att en verifiering enligt lagen inte visat att den påstådda identiteten är riktig generellt ska hanteras av myndigheterna.

Att verifieringen inte har kunnat visa att den påstådda identiteten är riktig kan även bero på att uppgifterna om den påstådda identiteten och de som finns lagrade i den handling som använts för jämförelsen, inte stämmer överens. I sådana fall kan det tyckas lättare att konstatera att någon form av identitetsmissbruk är för handen. Verifieringen visar alltså i dessa fall att den påstådda identiteten inte är riktig. Om kontrollen gjorts vid handläggningen av ett ärende enligt förvaltningslagen ligger det också nära till hands att anse att det finns en sådan brist att myndigheten inte kan pröva ärendet i sak; en myndighet behöver alltid kunna säkerställa att de åtgärder som vidtas i ett ärende avser rätt person. Vi kan här konstatera att förvaltningslagen innehåller bestämmelser om bland annat hur ärenden inleds. Av 19 § förvaltningslagen framgår att en framställan bland annat ska innehålla uppgifter om den enskildes identitet. Med uttrycket *den enskildes identitet* avses då framför allt uppgifter om namn, men bestämmelsen ger även utrymme för att lämna uppgift om identiteten genom att ange person- eller samordningsnummer. Uppgifterna får anses vara en förutsättning för att myndigheten i ett inledande skede ska kunna ta ställning till om den som gjort framställningen är saklegitimerad och därmed har rätt att inleda ärendet, det vill säga om denne kan anses vara berörd av en fråga på ett sådant sätt att myndigheten är skyldig att ta upp en framställning till saklig bedömning.[19] Enligt vår uppfattning kan en framställan som myndigheten kan konstatera har gjorts i någon annans identitet – exempelvis vid id-kapning – anses brista på så sätt att det helt saknas en viljeyttring, avseende vad myndigheten ska göra, från den person vars identitet har använts. En sådan brist skulle som vi ser det kunna medföra att framställan inte kan prövas i sak. Det skulle därför kunna övervägas att i den nya lagen ange att en misslyckad verifiering ska kunna medföra att framställan i det ärende i vilket den biometriska verifieringen genomfördes avvisas eller avslås.

[19] Prop. 2016/17:180, s. 305 och 132 f.

Som vi anfört ovan kan det emellertid finnas olika anledningar till att verifieringen har misslyckats. Om det exempelvis har sin grund i tekniska faktorer – som kan vara okända för den enskilde och myndigheten vid tidpunkten för kontrollen – behöver det inte vara fråga om något försök till identitetsmissbruk utan de identitetsuppgifter som den enskilde lämnat kan vara de riktiga. Ytterligare utredningsåtgärder kan i sådana fall behövas. Att – med stöd av en bestämmelse i den nya lagen – regelmässigt kunna avvisa en framställan endast med hänvisning till att den biometriska jämförelsen inte kunnat visa att den påstådda identiteten är riktig framstår enligt vår bedömning därför som mycket vanskligt. Att biometrisk verifiering med stöd av den nya lagen ska kunna användas av ett stort antal myndigheter, i många olika ärendeslag, talar i samma riktning. Det är inte osannolikt att det kan finnas faktorer som skulle göra att en generell möjlighet att avvisa eller avslå en framställan inte kan eller bör tillämpas i praktiken, exempelvis i ärendeslag där den enskilde har en långtgående rätt till en förmån; så kallat nödbistånd enligt socialtjänstlagen (2025:400) är ett exempel på detta. EU-gemensamma regelverk och principer skulle även kunna utgöra hinder i ett visst ärendeslag. I betänkandet *Åtgärder mot mervärdesskattebedrägerier* lämnades förslag om att utebliven medverkan till personlig inställelse ska kunna medföra att registrering till mervärdesskatt vägras eller att den registrerade avregistreras; regeringen valde att inte gå vidare med förslaget, eftersom det bedömdes kunna stå i strid med EU-rätten[20].

Det bör också beaktas att biometrisk verifiering av identitet enligt den nya lagen – vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde – ska kunna användas även avseende andra aktörer än den som har inlett ärendet. Detta talar enligt vår mening starkt mot att det skulle vara möjligt att på ett generellt sätt, i den nya lagen, reglera eventuella konsekvenser av att en verifiering enligt den nya lagen inte visat att den påstådda identiteten är riktig. Om den biometriska verifieringen görs när myndigheten i annat fall än vid handläggningen av ett ärende genomför identitetskontroller – det vill säga vanligen inom ramen för den faktiska verksamheten – framstår det än mindre som möjligt att på ett generellt sätt reglera eventuella konsekvenser av en misslyckad verifiering.

[20] Jfr SOU 2024:32, s. 172 och *Åtgärder mot mervärdesskattebedrägerier*, prop. 2025/26:128, s. 44 f.

I sådana fall är konsekvensen normalt sett helt verksamhets- och situationsberoende.

Vid en sammantagen bedömning anser vi att det varken är lämpligt eller möjligt att i den nya lagen införa en bestämmelse som anger att en misslyckad verifiering ska leda till en viss konsekvens, exempelvis att en framställan avvisas eller avslås. I stället får det ankomma på myndigheten att i det enskilda fallet ta ställning till lämplig konsekvens. Det bör understrykas att myndigheten givetvis – utifrån en bedömning i det enskilda fallet och med hänvisning till resultatet av den biometriska verifieringen – kan besluta på ett visst sätt i ett ärende, eller en viss situation i den faktiska verksamheten. Den utredningsåtgärd som den nya lagen möjliggör i form av biometrisk verifiering ska som vi ser det kunna användas just på det sättet. Vilken betydelse som den misslyckade verifieringen ska få i ett enskilt fall ska emellertid överlåtas till myndigheterna; ett beslut ska som vi ser det alltså inte kunna grunda sig enbart på en hänvisning till en bestämmelse i den nya lagen som reglerar konsekvenser av en misslyckad verifiering. I detta sammanhang kan vi konstatera att befintliga möjligheter till biometrisk verifiering i bland annat folkbokföringslagen och utlänningslagen inte heller är kopplade till någon uttrycklig konsekvens; beroende på ärendeslag och situation kan en misslyckad verifiering få olika följder, exempelvis att den enskilde nekas inresa eller att en ansökan om visering avslås.

Mot denna bakgrund anser vi alltså att det inte bör regleras i den nya lagen vilka konsekvenser som kan följa av att en verifiering inte visat att den påstådda identiteten är riktig.

23.8 Åtgärder för att förmå den enskilde att medverka till biometrisk verifiering enligt den nya lagen

Möjligheterna enligt den nya lagen för myndigheter att biometriskt verifiera identitet mot handlingar bör, som vi ser det, kunna användas både när det finns anledning att i ett enskilt fall misstänka identitetsmissbruk – det vill säga att en falsk eller felaktig identitet används eller att någons identitet utnyttjas – och när en myndighet vill genomföra bredare kontroller. Exempelvis skulle stickprovskontroller i ett visst ärendeslag kunna vara ett värdefullt instrument för att upptäcka identitetsmissbruk. Sådana kontroller kan också ha en avskräckande

effekt, och därmed vara ett sätt att skydda enskilda mot att deras identitet utnyttjas i olika sammanhang. För att målen att upptäcka identitetsmissbruk och skydda enskilda mot att deras identitet utnyttjas ska kunna uppnås och den nya lagen ska kunna få ett reellt genomslag är det av vikt att möjligheten till biometrisk verifiering enligt lagen inte i praktiken upplevs som illusorisk. Detta är en risk om sådana kontroller i praktiken är helt avhängiga av att den enskilde frivilligt medverkar i det enskilda fallet; för att en biometrisk verifiering ska kunna genomföras krävs att den vars identitet ska kontrolleras, på begäran, gör en handling som han eller hon innehar tillgänglig samt låter myndigheten ta fingeravtryck och/eller ansiktsbild. Vi kan notera att i förarbetena till de förstärkta möjligheter till identitetskontroll som införts i folkbokföringslagen lyfte remissinstanserna sådana risker. Regeringen ansåg emellertid att även med beaktande av detta behövdes en skärpning av regelverket.[21] Några särskilda bestämmelser som syftar till att förmå den enskilde att medverka infördes inte i folkbokföringslagen.

Det är alltså som vi ser det av vikt att det finns möjlighet för myndigheter att vidta åtgärder som syftar till att förmå den enskilde att medverka till en biometrisk verifiering för att den nya lagen inte i praktiken ska bli verkningslös. I avsnitt 21.5.3 har vi bedömt att det inte bör övervägas att ge myndigheter en möjlighet att vidta regelrätta tvångsåtgärder – exempelvis i form av kroppsvisitation – i sådant syfte. I stället anser vi att det i den nya lagen bör införas en särskild möjlighet för myndigheter att i vissa fall förelägga den enskilde att medverka. I avsnitt 23.8.1–23.8.6 redogör vi för våra bedömningar och förslag i detta avseende.

23.8.1 Begränsning till handläggningen av ett ärende

Vår bedömning

En möjlighet att förmå någon att medverka till en biometrisk verifiering med stöd av den nya lagen bör endast kunna avse fall när en begäran om verifiering har ställts vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde.

[21] Prop. 2021/22:217, s. 44 och 47.

De möjligheter att biometriskt verifiera identitet med stöd av den nya lagen som vi föreslagit tar sikte dels på handläggningen av ärenden som omfattas av förvaltningslagens tillämpningsområde, dels på situationer när myndigheter i annat fall genomför identitetskontroller (se avsnitt 23.6.3) En inledande fråga är om eventuella bestämmelser som gör det möjligt att förmå den enskilde att medverka till att en biometrisk verifiering med stöd av den nya lagen genomförs bör avse båda dessa situationer. Åtgärder för att få den enskilde att medverka – exempelvis i form av ett föreläggande – används normalt sett inom ramen för ett ärende av något slag, i syfte att komplettera utredningen på något sätt så att ett beslut kan fattas. Ett föreläggande – eventuellt i kombination med vite – kan också användas i syfte att mottagaren ska följa ett myndighetsbeslut eller av annan anledning vidta en åtgärd. Sådana förelägganden är vanliga på miljörättens område och inom plan- och bygglagstiftningen. Ofta motiveras sådana åtgärder från myndigheternas sida av hänsyn till det allmännas eller privatas intressen av olika slag.

När det gäller situationen att en myndighet genomför identitetskontroller kan vi konstatera att biometrisk verifiering med stöd av den nya lagen i princip uteslutande kommer att användas när personen i fråga fysiskt möter en representant för myndigheten, vanligen i dess faktiska verksamhet. Det kan vidare normalt antas vara fråga om att den enskilde vill ha tillgång till något, exempelvis en myndighetslokal, vård eller ett provgenomförande. Det är alltså som utgångspunkt inte fråga om att myndigheten har ett intresse av att förmå den enskilde att följa ett visst beslut eller vidta någon annan åtgärd. Det saknas som vi ser det redan av dessa anledningar skäl för att i den nya lagen införa en särskild möjlighet att förmå den enskilde att medverka till en biometrisk verifiering av hans eller hennes identitet i sådana situationer. Det är som vi ser det inte heller möjligt att – på något förutsebart sätt – knyta en på förhand angiven konsekvens till utebliven medverkan i dessa situationer. Om den enskilde inte följer en begäran om biometrisk verifiering i samband med att myndigheten, i annat fall än vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde, genomför identitetskontroller i sin verksamhet kan detta också leda till mer omedelbara konsekvenser än vid handläggningen av ett ärende, exempelvis genom att den enskilde på plats nekas tillträde.

För att främja att en begäran om biometrisk verifiering enligt den nya lagen faktiskt kan genomföras bör myndigheten emellertid givetvis också, i ett första steg, försöka bistå den vars identitet ska verifieras med råd eller stöd, som ett led i den serviceskyldighet som följer av 6 § förvaltningslagen, exempelvis om hur en sådan mobilapplikation som vi beskriver i avsnitt 27.4 används för att ta upp biometriska underlag. Detta bör också vara enklare att göra i samband med en biometrisk verifiering som görs med den enskilde närvarande på plats.

Mot denna bakgrund anser vi att en möjlighet att förmå den enskilde att medverka till en biometrisk verifiering endast bör kunna avse fall när en begäran om verifiering har framställts vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde.

23.8.2 En särskild bestämmelse om föreläggande ska införas

Vårt förslag

Den nya lagen ska innehålla en särskild bestämmelse som reglerar när en myndighet får förelägga någon att medverka till en biometrisk verifiering enligt lagen.

I förarbetena till den stärkta identitetskontroll som införts i folkbokföringslagen anfördes bland annat att en sådan kontroll inte är avsedd att användas i en slutlig handling på samma sätt som vid utfärdande av ett pass, och att den biometriska kontrollen i samband med identitetskontrollen i stället får ses som en självständig åtgärd inom ramen för ett pågående ärende.[22] Vi anser att den biometriska verifiering som den nya lagen ska möjliggöra vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde bör uppfattas på samma sätt. Denna typ av utredningsåtgärd syftar som vi ser det helt och hållet till att bekräfta att den som förekommer i ett ärende är den som han eller hon påstår sig vara (se dock även avsnitt 23.8.4, avseende vem ett föreläggande ska kunna rikta sig till). Att en myndighet säkert kan veta vem som har gjort en framställan är enligt vår mening många gånger av grundläggande betydelse för att den ska kunna

[22] Prop. 2021/22:217, s. 56.

prövas i sak på ett korrekt sätt. En framställan som har gjorts i någon annans identitet kan, som vi uppfattar det, också anses brista på ett grundläggande sätt genom att det saknas en faktisk viljeyttring från personen med den identitet som anges i framställan.

För att främja att en biometrisk verifiering enligt den nya lagen faktiskt kan genomföras – vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde – anser vi att en myndighet, som ett led i den serviceskyldighet som följer av 6 § förvaltningslagen, i ett första steg naturligtvis bör försöka avhjälpa bristen genom att bistå den vars identitet ska verifieras med råd eller stöd. Personen skulle exempelvis kunna behöva information om vilka handlingar som kan användas eller hur en sådan mobilapplikation som vi beskriver i avsnitt 27.4 används för att ta upp biometriska underlag. Sådan vägledning bör kunna ges direkt i applikationen, och inte kräva att en handläggare på myndigheten aktivt hjälper den enskilde; som vi pekar på i avsnitt 27.4.1 är det av vikt att en mobilapplikation utformas på ett användarvänligt sätt, för att minimera sådana problem. Anledningen till att en begäran om biometrisk verifiering inte har följts kan också tänkas vara att den helt enkelt har förbisetts av den enskilde; att begäran inte har följts behöver givetvis inte betyda att den enskilde försöker vilseleda myndigheten om sin identitet. Särskilt för den som tidigare inte behövt verifiera sin identitet biometriskt kan en sådan begäran komma att missas, eller missuppfattas. I sådana fall är det av vikt att myndigheten fullgör sin serviceskyldighet på ett ändamålsenligt sätt.

Om det inte är möjligt att genom råd och stöd avhjälpa bristande medverkan på frivillig väg anser vi däremot att en myndighet ska kunna använda ett föreläggande för att förmå den enskilde att medverka så att den biometriska verifieringen kan genomföras i ett visst ärende. En möjlighet att kunna förelägga den enskilde att medverka kan också ha en avskräckande och handlingsdirigerande effekt, det vill säga enbart vetskapen om att myndigheten kan förelägga den enskilde kan förmå honom eller henne att medverka utan att ett föreläggande behöver meddelas.

Vi kan konstatera att 20 § förvaltningslagen innehåller uttryckligt stöd för myndigheter att förelägga en part att avhjälpa brister i en framställan i ett ärende, om bristen är sådan att den medför att framställningen inte kan läggas till grund för en prövning i sak.[23] Av 23 §

[23] Prop. 2016/17:180, s. 309.

förvaltningslagen följer vidare att en myndighet ska se till att ett ärende blir utrett i den omfattning som dess beskaffenhet kräver, och om det behövs ska myndigheten genom frågor och påpekanden verka för att parten förtydligar eller kompletterar framställningen. Det är alltså fråga om att se till att prövningen i sak kan göras på ett så komplett underlag som möjligt, inte att avhjälpa formella brister i framställningen. I förarbetena till sistnämnda bestämmelse anfördes bland annat att beslutsmyndigheten har det yttersta ansvaret för att underlaget i ett förvaltningsärende är sådant att det leder till ett materiellt riktigt beslut. Den enskilde har enligt bestämmelsens andra stycke en skyldighet att medverka i utredningen. Om han eller hon inte fullgör sin skyldighet att ge in åberopad utredning anges i författningskommentaren att en myndighet, med stöd av bestämmelsen och inom ramen för sitt utredningsansvar, kan förelägga den enskilde parten att se till att allt relevant material som åberopas ges in.[24]

Förvaltningslagen gäller för en myndighets ärendehandläggning, om avvikande bestämmelser inte finns i annan författning. Detta framgår av 4 §. Det kan tyckas att ovan nämnda bestämmelser ger myndigheter ett tillräckligt – uttryckligt och indirekt – stöd för att förelägga den enskilde att medverka till en biometrisk verifiering enligt den nya lagen. Vi kan notera att i förarbetena till 23 § förvaltningslagen anfördes bland annat att en allmän bestämmelse om myndigheters utredningsansvar ansågs minska behovet av särskilda bestämmelser om detta i specialförfattningar.25 Vi anser dock att det bör preciseras i den nya lagen under vilka förutsättningar en myndighet ska få förelägga någon i syfte att en biometrisk verifiering enligt lagen ska kunna genomföras vid handläggningen av ett ärende. Detta med hänsyn till att vi nedan bedömer dels att ett föreläggande endast ska kunna riktas till den som inlett ärendet, dels att ett föreläggande endast ska få omfatta att mottagaren vidtar vissa specifika åtgärder, som syftar till att den biometriska verifieringen kan genomföras. Det framstår vidare som lämpligt att den nya lagen – som i sig reglerar en specifik *utredningsåtgärd* – innehåller en särskild bestämmelse om föreläggande; ovan nämnda bestämmelser i förvaltningslagen är däremot tillämpliga i ärendet som sådant. Vi anser sammantaget att en föreläggandebestämmelse i den nya lagen främjar en tydlighet i tillämpningen, såväl

[24] Prop. 2016/17:180, s. 309.
[25] Prop. 2016/17:180, s. 149.

för myndigheter som för enskilda som kan bli föremål för en begäran om verifiering av identitet.

Mot denna bakgrund anser vi att en särskild bestämmelse ska införas i den nya lagen som reglerar när en myndighet får förelägga en person att, vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde, medverka till att biometriskt verifiera sin identitet. En sådan bestämmelse kommer, om biometrisk verifiering med stöd av den nya lagen har ansetts nödvändig, att tillämpas i stället för förvaltningslagens bestämmelser avseende föreläggande, eftersom förvaltningslagen enligt 4 § är subsidiär.

23.8.3 Förutsättningar för att meddela ett föreläggande

Vårt förslag

Ett föreläggande enligt den nya lagen ska få meddelas om en begäran från en myndighet om att biometriskt verifiera identiteten inte har följts, och det inte har kommit fram omständigheter som talar mot att ett föreläggande meddelas. Föreläggandet ska syfta endast till att en biometrisk verifiering av identitet ska kunna genomföras.

Syftet med ett föreläggande enligt den nya lagen är som vi ser det uteslutande att förmå den vars identitet behöver verifieras biometriskt att följa en myndighets tidigare begäran med stöd av den nya lagen om detta. En grundförutsättning för ett föreläggande är därmed att en sådan begäran *inte har följts*. Anledningen till detta kan, som vi pekat på i avsnitt 23.8.2, dock variera och behöver inte i sig indikera att den enskilde har uppsåt eller vilja att vilseleda, eller medvetet inte vill rätta sig efter begäran. Vi anser att det inte ska krävas att myndigheten visar på någon särskild omständighet som talar i sådan riktning, för att ett föreläggande ska få meddelas, utan föreläggandet ska ses som ett medel att få den enskilde att följa en tidigare begäran, oavsett anledningen till att den inte följts.

Med detta sagt kan det dock tänkas att det kommit fram omständigheter som innebär att ändamålet med den ursprungliga begäran har förfallit. En sådan omständighet kan vara att myndigheten konstaterar att identiteten har kunnat verifierats på ett tillräckligt säkert

sätt på annan väg, exempelvis genom att den enskilde på eget initiativ har sökt upp myndigheten på plats. I sådana fall kan det ifrågasättas om kravet på att den biometriska verifieringen ska vara nödvändig (se avsnitt 21.5) överhuvudtaget är uppfyllt, och därmed också behovet av ett föreläggande. Det kan även ha kommit fram att den enskilde av någon anledning helt saknar möjlighet att medverka till en biometrisk verifiering enligt den nya lagen, till exempel på grund av att han eller hon saknar en relevant handling och inte kan, eller vill, få en sådan utfärdad inom överskådlig tid. Däremot anser vi att den omständigheten att myndigheten tidigare har beslutat i ärenden som rör den enskilde inte ensamt bör medföra att ett föreläggande inte kan meddelas; det kan därefter ha framkommit omständigheter som ger anledning att nu närmare utreda om den påstådda identiteten är riktig, genom en biometrisk verifiering mot en handling. En bedömning av om det finns omständigheter som talar mot att ett föreläggande meddelas får göras av myndigheten i det enskilda fallet. Avsikten är dock inte att det ska krävas några mer ingående överväganden utan skälet till den enskildes bristande medverkan bör hänföra sig till omständigheter som är relativt enkla att objektivt konstatera. Vi anser att den omständigheten att ett föreläggande – och därmed indirekt en biometrisk verifiering – kan upplevas som betungande för den enskilde inte ensamt ska leda till att ett föreläggande inte meddelas.

Det ska inte krävas att den enskilde gör gällande en viss omständighet för att den ska kunna beaktas; samtliga omständigheter som kommit till myndighetens kännedom bör kunna beaktas.

Bedömningen av om det finns omständigheter som talar mot att förelägga den enskilde att medverka till att en biometrisk verifiering av hans eller hennes identitet kan genomföras skulle visserligen kunna anses rymmas inom en fakultativt utformad bestämmelse; vi föreslår inte att en myndighet är skyldig att utfärda ett föreläggande. Ett föreläggande ska inte heller meddelas om den enskilde saknar faktisk och rättslig möjlighet att följa det. Vi bedömer emellertid att det är lämpligt att en sådan de facto, om än indirekt, förutsättning kommer till uttryck i den aktuella bestämmelsen i den nya lagen. Vi anser därför att det i en bestämmelse om föreläggande ska anges att ett föreläggande får meddelas *om det inte kommit fram omständigheter som talar mot det*.

Vidare syftar en möjlighet att förelägga någon enligt den nya lagen enbart till att biometrisk verifiering mot en handling ska kunna genomföras. Vi anser därför att ett föreläggande enligt den nya lagen endast ska kunna omfatta åtgärder som uppnår detta syfte. Föreläggandet ska alltså inte få användas för att kontrollera någons identitet på ett mer generellt sätt. Detta ska tydliggöras genom att det i den bestämmelse vi föreslår anges att om en begäran att biometriskt verifiera identitet inte har följts får den enskilde föreläggas att vidta vissa åtgärder, *för att en biometrisk verifiering av identitet ska kunna genomföras*. I avsnitt 23.8.5 lämnar vi förslag om vilka åtgärder ett föreläggande ska kunna omfatta.

23.8.4 Vem ett föreläggande ska kunna rikta sig till

Vårt förslag

Ett föreläggande enligt den nya lagen ska kunna riktas till den som har inlett det ärende som föranledde begäran om biometrisk verifiering.

Frågan är vem ett föreläggande ska kunna rikta sig till. Vi kan konstatera att bestämmelserna i 20 och 23 §§ förvaltningslagen riktar sig till den som inlett ärendet och till den som är part i ärendet. Som vi redogjort för i avsnitt 23.6.4 är tanken emellertid att den nya lagen ska kunna tillämpas även i förhållande till andra än dessa personkategorier, till exempel för att kunna biometriskt verifiera en extern uppgiftslämnares identitet, under förutsättning att det sker vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde och det är nödvändigt.

Att ett föreläggande om att medverka till biometrisk verifiering av identitet med stöd av den nya lagen ska kunna rikta sig till den som har inlett ärendet där begäran om verifiering har framställts framstår enligt vår mening som självklart. Behovet av att kunna verifiera identitet biometriskt i syfte att motverka identitetsmissbruk gör sig i första hand gällande avseende den som ansöker om något, eller som genom en anmälan eller en annan framställan har vänt sig till en myndighet; den personen har något direkt att vinna på att utnyttja någon annans identitet eller använda en falsk identitet, som ger honom eller

henne rätt till exempelvis en ekonomisk förmån på felaktiga grunder. Det är också identiteten hos den som inlett ett ärende som är av intresse för att i ett tidigt skede kunna konstatera om det alls finns förutsättningar för att pröva en framställan i sak. Myndigheter ska med hänsyn till detta kunna rikta ett föreläggande om att medverka så att en biometrisk verifiering av identitet kan genomföras till den som har inlett det aktuella ärendet.

I vissa fall inleder myndigheten ett ärende, exempelvis för att utreda om en beviljad socialförsäkringsförmån ska återkallas eller i syfte att utreda misstänkta fel i folkbokföringen. Under vårt arbete har även återkallelse av ett godkännande som deklarationsombud nämnts som exempel på ärenden där det kan finnas behov av att genomföra en biometrisk verifiering av identitet med stöd av den nya lagen. Vi är inte av någon annan uppfattning. Däremot anser vi inte att ett föreläggande att medverka till biometrisk verifiering med stöd av den nya lagen bör kunna riktas mot den som är part i ett sådant ärende, som inletts på initiativ av myndigheten. I ärenden som inletts på myndighetens initiativ och som kan leda till ett negativt beslut för den enskilde ligger normalt sett bevisbördan för att det finns grund för beslutet på myndigheten. Den enskilde har därför normalt sett inte något intresse av att medverka till att komplettera utredningen på sätt som innebär att myndigheten kan fatta beslut i ärendet, snarare tvärtom. I förarbetena till 23 § förvaltningslagen erinras också om att bestämmelsen inte innebär något tvång för parter att ge in utredning som talar till deras nackdel.[26] För att en myndighet ska få begära att den enskilde biometriskt verifierar sin identitet med stöd av den nya lagen förutsätts, som vi redogjort för i avsnitt 23.6.3, att det är nödvändigt. I ett initiativärende innebär det i praktiken att myndigheten har bedömt att biometrisk verifiering är nödvändig för att man ska kunna besluta i ärendet. Om den enskilde inte medverkar till verifieringen kommer det därför i många fall att innebära att myndigheten inte kan anses ha uppfyllt sin bevisbörda. Att förena föreläggandet med en konsekvens som innebär att ärendet avgörs på befintligt underlag skulle därmed inte tjäna något syfte. Som vi återkommer till i avsnitt 23.8.6 behöver ett föreläggande kunna förenas med en konsekvens; i annat fall blir det i praktiken endast fråga om en ytterligare begäran.

[26] Prop. 2016/17:180, s. 150 och 309.

När det gäller andra aktörer som kan förekomma i ett ärende än de som inlett ärendet anser vi att behovet av att kunna meddela ett föreläggande i syfte att verifiera identitet med hjälp av biometriska uppgifter inte är lika framträdande. Detta med hänsyn till att det normalt kan antas saknas ett samband mellan deras roll i ärendet och en möjlighet till någon form av vinning genom att vilseleda myndigheten om identiteten. Ett föreläggande som riktar sig till annan än den som inlett ärendet skulle enligt vår mening inte heller vara möjligt att förena med en konsekvens som innebär att framställan inte tas upp till prövning i sak eller prövas på befintligt underlag, om föreläggandet inte följs. Exempelvis är det som vi ser det uteslutet att låta bristande medverkan från en extern uppgiftslämnare eller någon annan aktör i ett ärende leda till att en framställan avvisas; i värsta fall skulle mottagaren av föreläggandet – till skillnad från den som inlett ärendet – kunna ha ett intresse av att ärendet avslutas på detta sätt, och därmed ett direkt incitament att inte följa föreläggandet. Som vi återkommer till i avsnitt 23.8.6 är det inte heller lämpligt att förena ett föreläggande med vite. Identiteten hos andra personer som förekommer i ett ärende kan som vi ser det normalt endast indirekt anses ha betydelse för handläggningen av ärendet. Att andra än den som inlett ärendet inte följer en begäran om att biometriskt verifiera sin identitet enligt den nya lagen får därför i stället beaktas vid handläggningen av ärendet på annat sätt, exempelvis genom att bevisvärdet av uppgifter som lämnats av en sådan aktör påverkas negativt.

Med hänsyn till det ovan anförda anser vi att ett föreläggande ska kunna rikta sig endast till *den som har inlett det ärende* i vilket begäran om att biometrisk verifiera identitet med stöd av den nya lagen har aktualiserats. Detta ska tydliggöras i den bestämmelse vi föreslår ska införas i lagen.

23.8.5 Åtgärder som den enskilde kan föreläggas att vidta

Vårt förslag

Den enskilde ska endast kunna föreläggas att göra en handling tillgänglig och låta myndigheten ta fingeravtryck och ansiktsbild.

Som vi anfört inledningsvis i avsnitt 23.6.4 förutsätts dels att den vars identitet ska kontrolleras gör en handling tillgänglig, dels att han eller hon på begäran låter myndigheten ta biometriska underlag som kan användas för den biometriska jämförelsen. Ett föreläggande som meddelas med stöd av den nya lagen bör därför få omfatta i vart fall dessa åtgärder.

När det gäller att göra en handling tillgänglig kan vi konstatera att utgångspunkten måste vara att den enskilde har en reell möjlighet att rätta sig efter ett föreläggande, i synnerhet om följden annars blir att myndigheten beslutar att inte ta upp en framställan till prövning eller avslår en framställan. Vid en begäran om biometrisk verifiering av identitet – vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde – med stöd av den nya lagen, skulle den som är föremål för kontrollen exempelvis kunna göra gällande att han eller hon inte har en sådan handling som avses i avsnitt 23.6.2 och inte heller har möjlighet att få en sådan handling utfärdad, och därför inte heller kan göra handlingen tillgänglig. Det kan antas vara svårt för myndigheten att motbevisa ett sådant påstående, eftersom det saknas möjlighet att kontrollera innehav av en handling mot exempelvis ett register; att en handling har utfärdats innebär inte nödvändigtvis att den enskilde också innehar handlingen vid tidpunkten för en begäran att biometriskt verifiera identitet. Ett föreläggande om att göra en handling tillgänglig skulle därmed indirekt innebära ett krav på den enskilde att han eller hon ansöker om en viss typ av handling, vilket kan innefatta såväl ett integritetsintrång som kostnader. Det kan också ta tid att få en handling utfärdad. Det ska dock här erinras om att en begäran om att biometriskt verifiera identitet med stöd av den nya lagen, enligt vårt förslag i avsnitt 23.6.4, endast ska kunna riktas mot den som *innehar* en sådan typ av handling som anges i avsnitt 23.6.2. Detta innebär att ett föreläggande om att göra en sådan handling tillgänglig inte innefattar att den som saknar en handling ska ansöka om att få en utfärdad utan endast att en handling som den enskilde faktiskt innehar ska göras tillgänglig så att en jämförelse kan göras mot de biometriska underlag som är lagrade i den.

Det skulle därmed kunna hävdas att den enskilde i praktiken kan undgå en begäran om biometrisk verifiering genom att helt enkelt göra gällande att han eller hon inte innehar en handling som kan användas för detta. Hur ett sådant påstående bör hanteras av en myndighet i det enskilda fallet är inte möjligt att närmare reglera, med hänsyn till

de varierande ärendeslag som den nya lagen ska kunna tillämpas i. Det kan dock tänkas att ytterligare utredningsåtgärder vidtas i ärendet, i vart fall om myndigheten misstänker att någon form av identitetsmissbruk är för handen och att den enskilde därför vill undvika att medverka till en biometrisk verifiering. Endast ett påstående om att man inte innehar någon handling som kan användas för biometrisk verifiering hindrar som vi ser det inte heller att ett föreläggande enligt den nya lagen meddelas. Huruvida den omständigheten att föreläggandet inte följs även faktiskt bör leda till den konsekvens som anges i föreläggandet (se avsnitt 23.8.6), får myndigheten ta ställning till utifrån omständigheterna i det enskilda fallet. Trovärdigheten och tillförlitligheten i en invändning om att den enskilde inte innehar någon handling skulle då kunna vara en faktor som vägs in.

Det behöver som vi ser det inte anges särskilt att ett föreläggande ska få innefatta ett krav på att den enskilde inställer sig personligen. Vi har i avsnitt 10.2.3 bedömt att utökade möjligheter för myndigheter att kräva personlig inställelse kan vara en viktig komponent i att kunna verifiera identitet med hjälp av biometriska uppgifter. Vi föreslår däremot inte någon bestämmelse som innebär en fristående möjlighet för myndigheter att kräva personlig inställelse utan det ska endast få förekomma som ett led i att biometrisk verifiering av identitet med stöd av den nya lagen ska kunna genomföras. Även om vi bedömt att det inte bör regleras på vilket sätt biometriska underlag ska tas upp vid biometrisk verifiering enligt den nya lagen kan vi konstatera att detta – med hänsyn till vilka tekniska möjligheter som en myndighet har att tillgå vid ett visst tillfälle – kan komma att förutsätta att det görs i samband med personlig inställelse. Även i fall där den enskilde gör gällande att han eller hon inte har möjlighet att använda en mobilapplikation för verifiering av identiteten på distans, eller det kommer fram att den handling som ska användas för jämförelsen har ett skadat lagringsmedium, men att biometriska uppgifter kan tas fram ur en synlig ansiktsbild på handlingen (se avsnitt 20.2.4), kan biometrisk verifiering förutsätta personlig inställelse. Som vi anfört i avsnitt 23.6.4 kan ett krav på personlig inställelse därför komma att ingå i skyldigheten att göra en handling tillgänglig.

Sammantaget anser vi att den enskilde endast ska kunna föreläggas att göra en handling tillgänglig och låta myndigheten ta fingeravtryck och ansiktsbild. Detta ska tydliggöras i den bestämmelse om föreläggande som vi föreslår ska införas i den nya lagen.

23.8.6 Konsekvenser av att ett föreläggande inte följs

Vårt förslag och vår bedömning

Ett föreläggande enligt den nya lagen ska innehålla en upplysning om vad följden av att det inte följs kan bli.

Ett föreläggande bör inte kunna förenas med vite. Det bör inte heller införas en bestämmelse i den nya lagen om att ett föreläggande ska förenas med en tidsfrist.

För att ett föreläggande om att medverka till en biometrisk verifiering enligt den nya lagen ska få någon reell effekt behöver det kunna förenas med en konsekvens om det inte följs. I annat fall skulle ett föreläggande i praktiken inte skilja sig mot den initiala begäran om att biometriskt verifiera identiteten, annat än till utformningen av begäran. Ett föreläggande som inte är kopplat till någon form av konsekvens skulle enligt vår mening då närmast ses som en påminnelse till den enskilde, inte som ett reellt påtryckningsmedel. Det kan med fog antas att den som medvetet valt att inte följa en begäran om biometrisk verifiering enligt den nya lagen inte heller skulle följa ett föreläggande som inte kan medföra en konsekvens. Ett föreläggande skulle därför i många fall endast medföra en ökad administrativ börda för myndigheten i stället för en effektiv utredningsåtgärd.

Frågan är vilka konsekvenser som kan tänkas vara aktuella vid användningen av ett föreläggande med stöd av den nya lagen. Det förekommer att myndigheter har möjlighet att förena ett föreläggande med vite. Vite skulle, vid tillämpningen av den nya lagen, kunna utgöra ett fristående sätt – som inte är knutet till utgången i ärendet – att få den enskilde att följa ett föreläggande. Ett föreläggande som kan förenas med vite skulle potentiellt kunna riktas även till andra personer än den som har inlett ett ärende. Vi kan emellertid konstatera att vitesföreläggande används i första hand för att få mottagaren att följa ett visst lagakraftvunnet beslut i sak. Vitesförelägganden används bland annat inom miljörätten och inom plan- och bygglagstiftningen, se exempelvis 26 kap. 11 och 14 §§ miljöbalken. Det kan även vara fråga om att den enskilde inte har fullgjort en skyldighet att på eget initiativ aktivt vidta en åtgärd som följer direkt av lag och som syftar till att upprätthålla ett bredare samhällsintresse – exempelvis att folkbokföringen är korrekt – och där skyldigheten alltså inte är

en följd av en myndighets bedömning i det enskilda fallet. Ett sådant exempel är Skatteverkets möjlighet att med stöd av 31 § folkbokföringslagen förelägga någon att fullgöra en anmälningsskyldighet enligt lagen. Om ett sådant föreläggande inte följs får det förenas med vite, enligt 37 §.

Ett centralt argument för att kunna använda vite är effektivitet, då det skapar ett mycket tydligt incitament för mottagaren att följa ett föreläggande. Samtidigt kan vite innebära betydande ekonomiska konsekvenser, vilket ställer höga krav på att det ska vara proportionerligt och riktat till rätt adressat. Oftast krävs delgivning, vilket kan göra förfarandet omständligt och tidskrävande för myndigheten. Detta måste som vi ser det vägas mot vad som ska uppnås med vitet. Just den ekonomiska aspekten talar som vi ser det mot att ett föreläggande enligt den nya lagen bör kunna förenas med vite. Det kan nämligen med fog antas att ett antal av de ärendeslag i vilka det kan finnas ett intresse för myndigheterna att använda biometrisk verifiering av identitet är av sådant slag att den enskilde befinner sig i en ekonomiskt utsatt situation, exempelvis ärenden om sjukpenning eller bostadsbidrag. Att då förena ett föreläggande enligt den nya lagen med vite kan enligt vår mening framstå inte bara som oproportionerligt utan som kontraproduktivt. Syftet med den nya lagen är inte heller att säkerställa regelefterlevnad. Detta skiljer sig från exempelvis miljö- och bygglagstiftning.

Vid en sammantagen bedömning av dessa omständigheter anser vi att ett föreläggande enligt den nya lagen inte bör kunna förenas med vite. I stället skulle en konsekvens i form av att ärendet inte tas upp till prövning i sak, det vill säga att framställan avvisas, kunna bli aktuell, på liknande sätt som anges bland annat i 20 § förvaltningslagen. Att i ett ärende som omfattas av förvaltningslagens tillämpningsområde kunna verifiera att den identitet som en viss framställan är gjord i är riktig kan vara av betydelse för att myndigheten ska kunna pröva ärendet i sak på ett korrekt sätt. Uppgifter om identitet kan anses vara en förutsättning för att myndigheten, i ett inledande skede, ska kunna ta ställning till om den som gjort framställan är saklegitimerad och därmed har rätt att inleda ärendet, det vill säga om han eller hon kan anses vara berörd av en fråga på ett sådant sätt att myndigheten är skyldig att ta upp en framställning till saklig bedömning.[27]

[27] Prop. 2016/17:180, s. 305 och 132 f.

Att uppgifter om identitet saknas är naturligtvis en brist av sådant slag att den många gånger medför att ett ärende inte kan prövas i sak. Framställan skulle då även kunna anses ofullständig i den mening som avses i 20 § förvaltningslagen. Den nya lagen syftar emellertid till att verifiera de identitetsuppgifter som faktiskt har lämnats; det är därmed tveksamt om det går att säga att framställan är ofullständig eller oklar på det sätt som avses i den aktuella bestämmelsen. Att en myndighet bedömt att det är nödvändigt att biometriskt verifiera identiteten i ett ärende kan enligt vår mening därför inte automatiskt leda till slutsatsen att den omständigheten att en sådan kontroll inte genomförts är en brist av sådant slag att framställan inte kan prövas i sak; som vi redogjort för i avsnitt 21.5 kan nödvändighetskriteriet ta sikte både på omständigheter i det enskilda fallet och faktorer som är mer generella. I sistnämnda fall – exempelvis om en stickprovskontroll genomförs – kan det vara svårt att hävda att en utebliven biometrisk verifiering innebär att det inte är möjligt att pröva ärendet i sak. Den omständigheten att den biometriska verifieringen inte kunnat genomföras visar inte att den påstådda identiteten inte är riktig, utan det kan endast konstateras att det inte har gått att biometriskt verifiera *att* den är riktig. Det kan med fog antas att identitetsuppgifter som enskilda lämnar till myndigheter i olika ärendeslag i mycket stor utsträckning är riktiga, även om identitetsmissbruk förekommer på olika sätt i Sverige (se vår redogörelse i kapitel 9). Att den påstådda identiteten inte biometriskt har kunnat verifierats behöver alltså inte betyda att uppgifterna objektivt sett inte är korrekta. Det aktuella ärendeslaget i sig behöver inte heller nödvändigtvis vara sådant att identiteten är av avgörande betydelse, även om det krav på att en biometrisk verifiering endast ska få genomföras om det är nödvändigt som vi föreslagit i avsnitt 21.5 kan anses tala för detta.

Ovanstående talar enligt vår mening starkt mot att det skulle vara möjligt att i den nya lagen ange att ett ärende alltid ska kunna avvisas eller avslås om ett föreläggande enligt lagen inte följs av den enskilde. En generell möjlighet för myndigheter att avvisa en framställan endast på grund av att den enskilde inte följt ett föreläggande enligt den nya lagen skulle riskera att på ett icke ändamålsenligt och oproportionerligt sätt utvidga den möjlighet att avvisa en framställan som följer av 20 § förvaltningslagen, som uttryckligen förutsätter att bristen som föreläggandet avser är sådan att den medför att framställan inte kan läggas till grund för en prövning i sak. Även om identiteten normalt

kan sägas vara av betydelse för att ett ärende ska kunna prövas i sak är det – mot bakgrund av det ovan anförda – som vi ser det inte möjligt att *generellt* säga att utebliven biometrisk verifiering utgör en sådan brist; det bör i många fall vara fullt möjligt att – på det sätt som i dag normalt sker – pröva en ansökan i sak på ett korrekt sätt utan en sådan kontroll, med utgångspunkt i de identitetsuppgifter som den enskilde lämnat.

Utöver ovan nämnda konsekvenser har vi inte identifierat någon konkret åtgärd som generellt sett kan antas vara aktuell att förena ett föreläggande med, vid handläggningen av det stora antal ärendeslag som den nya lagen ska kunna tillämpas i. Även om vi alltså anser att den nya lagen inte bör innehålla en bestämmelse som uttryckligen preciserar vilken eller vilka konsekvenser som kan följa av att ett föreläggande inte följs, anser vi att det ska framgå av lagen *att* ett föreläggande ska innehålla en upplysning om den konsekvens som myndigheten – i det enskilda fallet – vill kunna göra gällande vid utebliven medverkan. För att enbart den enskildes bristande medverkan att följa föreläggandet ska kunna medföra en viss konsekvens – exempelvis att myndigheten inte tar upp framställan till prövning i sak – ska alltså förutsättas att detta anges redan i föreläggandet. På detta sätt främjas enligt vår mening en tydlighet och förutsebarhet i tillämpningen för den som föreläggandet riktar sig till. Ett krav på att en konsekvens ska anges i föreläggandet motverkar samtidigt effektivt att skrivelser som i praktiken inte utgör ett påtryckningsmedel utan endast en påminnelse om att medverka till en biometrisk verifiering används. Vi anser att det är av vikt att förelägganden inte används slentrianmässigt.

En ordning av nämnda slag överlåter till myndigheterna att själva ta ställning till vilken konsekvens som kan bli aktuell i det enskilda fallet. Andra konsekvenser än de vi redogjort för ovan kan då komma att aktualiseras. Vi ser emellertid inte att detta skulle utgöra några problem ur rättssäkerhetssynpunkt. Det får antas att myndigheterna använder sig av konsekvenser som på ett reellt sätt påverkar den enskilde. Risken är annars stor att han eller hon ändå inte följer föreläggandet. Förelägganden kan som vi ser det främst antas få betydelse i enskilda ärenden där myndigheten av olika skäl har ställt en begäran om biometrisk verifiering på grund av att det finns anledning att misstänka att det förekommer identitetsmissbruk, då det i sådana fall bör vara enklare att bedöma att den biometriska verifieringen är av sådan

betydelse för handläggningen av ärendet att det annars inte kan prövas i sak. Detta ska inte uppfattas som att det alltid ska krävas en konkret misstanke om identitetsmissbruk för att ett föreläggande ska få användas. I samband med en stickprovskontroll som avser en större mängd personer kan det å andra sidan antas vara svårare att dra en sådan slutsats. I sistnämnda fall kan behovet av att med hjälp av ett föreläggande tvinga fram medverkan till en biometrisk verifiering emellertid många gånger antas vara mindre än när det utifrån omständigheterna i ett enskilt fall har bedömts nödvändigt med en sådan kontroll. Vi anser därför att ett krav på att föreläggandet ska innehålla en upplysning om vad följden av att det inte följs kan bli, inte motverkar syftet med en möjlighet att förelägga den enskilde.

Det är i och för sig naturligt att en särskild tidsfrist sätts ut i ett föreläggande. I annat fall blir det både för myndigheten och den enskilde svårt att bedöma när en prövning av om ett föreläggande har följts eller inte kan göras. Det finns dock inte några vägande skäl som talar för att den bestämmelse om föreläggande som vi föreslår behöver tyngas med en uttrycklig reglering om krav på en sådan särskild frist.[28]

23.9 Rätt att meddela föreskrifter

Vårt förslag

Den nya lagen ska innehålla en bestämmelse som anger att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter med stöd av 8 kap. 7 § regeringsformen om tillämpningen av lagen.

Vi har i avsnitt 23.6 lämnat förslag som dels preciserar vilka typer av handlingar som ska få användas för att biometriskt verifiera identitet med stöd av den nya lagen, dels anger i vilka situationer sådana kontroller ska få användas. Förslagen bygger på de överväganden vi har gjort i tidigare kapitel och är avgränsade på ett, som vi ser det, ändamålsenligt sätt som främjar en tydlighet och förutsebarhet. Det kan dock tänkas att förutsättningarna för biometrisk verifiering av iden-

[28] Jfr prop. 2016/17:180, s. 136.

titet av olika anledningar kan behöva ytterligare preciseras i samband med eller efter ett införande av den nya lagen.

När det gäller vilka typer av handlingar som ska få användas är det till exempel inte säkert att samtliga hemlandspass eller identitetskort som är utfärdade av behöriga myndigheter är lämpliga, exempelvis på grund av att det är känt att en viss specifik handling – exempelvis ett hemlandspass från ett visst land – utfärdas på ett sätt som inte är tillförlitligt ur identitetshänseende. Det kan bland annat tänkas att hemlandspass med en viss serie har utfärdats i samband med en statskupp eller krigstillstånd. En viss flexibilitet i tillämpningen kan därför behöva möjliggöras. En föreskrift som eventuellt preciserar vilka hemlandspass och identitetskort som ska få användas vid biometrisk verifiering enligt den nya lagen bör enligt vår mening med fördel kunna införas i förordning eller i myndighetsföreskrifter. Detsamma gäller en eventuell begränsning av de situationer då biometrisk verifiering ska få användas. Det kan exempelvis vara fråga om att ett visst ärendeslag behöver undantas av någon anledning. Vi kan konstatera att en möjlighet att i föreskrift begränsa exempelvis vilka handlingar som godtas visserligen kan leda till att den nya lagen tillämpas olika av olika myndigheter, med sämre förutsebarhet för enskilda. Sådana skillnader i tillämpningen kan samtidigt vara angelägna, utifrån olika myndigheters verksamhet och de ärendeslag som myndigheten handlägger. Dessa omständigheter bör beaktas vid utformningen av eventuella föreskrifter, antingen i förordning eller genom myndighetsföreskrifter.

Föreskrifter av nämnda slag, som till exempel begränsar i vilka ärendeslag en enskild är skyldig att medverka till en biometrisk verifiering, kan som vi ser det svårligen betraktas som betungande för den enskilde eller något som medför ett integritetsintrång, utöver vad som följer av de bestämmelser vi föreslår. De skulle endast indirekt rikta sig till enskilda; exempelvis skulle en enskild som endast har en handling som eventuellt inte kommer att kunna användas kunna känna sig tvungen att ansöka om att få någon annan godtagbar handling utfärdad, vilket kan medföra en kostnad. Föreskrifterna skulle däremot kunna påverka myndigheters arbete med att kontrollera identitet med hjälp av biometriska uppgifter med stöd av den nya lagen. Även med hänsyn till detta anser vi att de inte avser, eller utgör ett ingrepp i, enskildas ekonomiska förhållanden i den mening som avses i 8 kap. 2 § första stycket 1 och 2 regeringsformen (RF). Enligt

vår bedömning talar i stället mycket för att de är att anse som sådana verkställighetsföreskrifter som avses i 8 kap. 7 § första stycket 1 RF. I vart fall bedömer vi att det är fråga om sådana föreskrifter som faller under regeringens så kallade restkompetens enligt 8 kap. 7 § första stycket 2 RF.[29] Av 8 kap. 11 § RF följer en rätt för regeringen att bemyndiga en myndighet att meddela sådana föreskrifter. Det är därför inte nödvändigt att införa en särskild bestämmelse om föreskriftsrätten i den nya lagen. Föreskrifterna är inte heller av sådant slag att de kan anses påverka grunderna för kommunernas organisation eller deras verksamhetsformer i den mening som avses i 8 kap. 2 § första stycket 3 RF. De bedöms inte heller ha en sådan effekt eller materiell innebörd att de skulle påverka kommunernas befogenheter eller åliggande i övrigt på ett sätt som kräver att de meddelas genom ett bemyndigande i den nya lagen.

Oaktat detta kan det ibland finnas anledning att i en lag upplysa om att regleringen av en viss fråga inte är uttömmande, utan förutsätts bli kompletterad med föreskrifter på lägre nivå. En sådan information kan vara särskilt angelägen om en tillämpare får en felaktig uppfattning genom att bara läsa lagbestämmelserna i ämnet och man därigenom riskerar att bestämmelserna tillämpas fel.[30] Det kan enligt vår bedömning visserligen inte förutsättas att den nya lagen kommer att behöva kompletteras med föreskrifter av ovan angivna slag. Däremot ska lagen kunna tillämpas av en mycket bred krets av myndigheter och tillämpningen innebär att känsliga personuppgifter behöver behandlas, vilket medför ett visst intrång i skyddet för den personliga integriteten. Mot denna bakgrund anser vi att det kan finnas ett värde i att en upplysningsbestämmelse införs i den nya lagen, för att tydliggöra för tillämparen att det kan finnas ytterligare föreskrifter om tillämpningen av den nya lagen.

[29] Jfr prop. 1973:90 *med förslag till ny regeringsform och ny riksdagsförordning*, s. 210.
[30] Gröna boken, *Riktlinjer för författningsskrivning*, Ds 2014:1, s. 90.

24 Dataskydd

24.1 Inledning

Införande av en generell möjlighet för myndigheter att verifiera identitet biometriskt mot handlingar kräver utvärdering av behovet av reglering av dataskyddsrättslig karaktär. I detta kapitel föreslår vi att nya bestämmelser om personuppgiftsbehandling ska införas i den nya lagen om biometrisk verifiering av identitet (avsnitt 24.2). Vi tar vidare ställning till frågor om bland annat bestämmelsernas tillämpningsområde (avsnitt 24.4), personuppgiftsansvar (avsnitt 24.6) och enskildas rättigheter (avsnitt 24.11).

24.2 Bestämmelser om behandling av personuppgifter ska införas i den nya lagen

Vårt förslag

Den nya lagen om biometrisk verifiering av identitet ska innehålla bestämmelser om behandling av personuppgifter.

Utöver den generella dataskyddsregleringen i form av dataskyddsförordningen[1] och dataskyddslagen[2] finns det i svensk rätt ett stort antal specialförfattningar, så kallade registerförfattningar, som reglerar myndigheters behandling av personuppgifter. Registerförfattningarna utgör ett komplement till den generella regleringen och förekommer både i form av lag och förordning. Syftet med författningarna är att anpassa regleringen till särskilda behov som myndigheter har i sina respektive verksamheter och att göra avvägningar mellan behovet

[1] Europaparlamentets och rådets förordning (EU) 2016/679.
[2] Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

av effektivitet i berörd verksamhet och behovet av skydd för den enskildes personliga integritet.[3]

En generell möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar, i enlighet med våra förslag, innebär utökade sådana möjligheter för vissa myndigheter men framför allt att ett stort antal myndigheter som i dag inte kan verifiera identitet biometriskt får möjlighet att göra det, i de situationer vi föreslagit i avsnitt 23.6.3.

För det stora flertalet av de myndigheter som berörs av våra förslag är de verksamhets- eller ärendespecifika bestämmelser om personuppgiftsbehandling som finns i nationell rätt – och som blir tillämpliga vid behandling av personuppgifter i samband med handläggningen av ett ärende eller vid en identitetskontroll inom ramen för verksamheten – inte utformade med hänsyn till att myndigheten ska få behandla biometriska underlag och biometriska uppgifter. Dataskyddsförordningen och dataskyddslagen ger visserligen myndigheter möjlighet att under vissa förutsättningar behandla biometriska uppgifter. Vi anser dock att det finns ett behov av att särskilt reglera vad som ska gälla vid personuppgiftsbehandling i samband med biometrisk verifiering av identitet mot en handling, med stöd av den nya lag vi föreslår. Detta för att tydliggöra under vilka förutsättningar berörda myndigheter får behandla personuppgifter med stöd av den nya lagen och för att begränsa det integritetsintrång verifieringen innebär för de enskilda vars identitet kontrolleras biometriskt. Bestämmelser som är anpassade för den personuppgiftsbehandling som behöver utföras vid biometrisk verifiering mot handlingar, med stöd av den nya lagen, medför enligt vår mening att det blir tydligare vad som gäller i det avseendet och personuppgiftsbehandlingen blir mer förutsebar.

Mot den här bakgrunden bedömer vi att det behövs kompletterande bestämmelser om behandling av personuppgifter vid införande av en generell möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar.

Utredningen skulle teoretiskt sett kunna se över befintliga myndighets- eller verksamhetsspecifika regelverk avseende personuppgiftsbehandling och vid behov anpassa dessa till sådan behandling som krävs för biometrisk verifiering av identitet mot handlingar med stöd av den nya lagen. Som exempel kan nämnas att 114 kap. socialförsäk-

[3] *Utlänningsdatalag*, prop. 2015/16:65, s. 21.

ringsbalken – som tillämpas av Försäkringskassan och Pensionsmyndigheten under vissa förutsättningar – skulle kunna kompletteras med bestämmelser om behandling av personuppgifter i syfte att verifiera identitet biometriskt. Med tanke på det stora antalet myndigheter som genom våra förslag – om de genomförs – kommer att få möjlighet att verifiera identitet biometriskt framstår det dock som ett orimligt tidskrävande tillvägagångssätt, både inom ramen för det här uppdraget och vid eventuella framtida justeringar av regelverket; att justera befintliga registerförfattningar, som har utformats utifrån de specifika verksamheter de är tillämpliga i, utifrån ett behov av en generell möjlighet till behandling av biometriska uppgifter framstår enligt vår mening inte som lagtekniskt lämpligt. Det är enligt vår bedömning att föredra att reglera sådan behandling av personuppgifter i en särskild författning. Att samla bestämmelserna har också fördelen att regelverket avseende biometrisk verifiering av identitet mot handlingar blir självständigt och därmed lättare att överblicka, vilket skapar en tydlighet för enskilda om under vilka förutsättningar personuppgifter – framför allt biometriska underlag och biometriska uppgifter – om dem får behandlas av en myndighet i syfte att verifiera deras identitet biometriskt.

Mot den här bakgrunden anser vi att de nya, kompletterande bestämmelser om behandling av personuppgifter som vi bedömer behövs ska placeras i den nya lag om biometrisk verifiering av identitet som vi i avsnitt 23.2 har föreslagit ska införas.

24.3 De nya bestämmelserna ska komplettera den allmänna dataskyddslagstiftningen

Vårt förslag

Den nya lagen ska innehålla en bestämmelse som klargör att den kompletterar dataskyddsförordningen. Dataskyddslagen och föreskrifter som har meddelats i anslutning till den lagen ska gälla vid behandling av personuppgifter med stöd av den nya lagen, om inte något annat följer av den nya lagen eller av föreskrifter som har meddelats i anslutning till den.

Dataskyddsförordningen är direkt tillämplig i svensk rätt och ska tillämpas av myndigheter på samma sätt som om den vore lag antagen av Sveriges riksdag. Förordningen gäller alltså oavsett om det i den nya lag som vi föreslår införs en bestämmelse som hänvisar till den eller inte. Vi anser emellertid att det bör införas en upplysningsbestämmelse som syftar till att tydliggöra att lagen innehåller kompletterande bestämmelser till dataskyddsförordningen. En sådan bestämmelse tydliggör den nya lagens förhållande till dataskyddsförordningen och klargör att lagen inte kan tillämpas fristående, utan ska tillämpas tillsammans med förordningen. Hänvisningen till dataskyddsförordningen bör vara dynamisk, vilket innebär att hänvisningen avser förordningen i dess vid varje tidpunkt gällande lydelse. Vi anser att denna hänvisningsteknik är lämpligast, eftersom den nya lagen annars kan komma att behöva ändras vid varje eventuell ändring av dataskyddsförordningen. Bestämmelsen bör därför utformas på samma sätt som i andra sektorspecifika registerförfattningar som kompletterar dataskyddsförordningen, exempelvis 3 § domstolsdatalagen (2015:728).

I svensk rätt har generella kompletterande bestämmelser till dataskyddsförordningen antagits genom dataskyddslagen. Dataskyddslagens bestämmelser är subsidiära i förhållande till annan nationell dataskyddsreglering; eventuella specialbestämmelser i andra författningar om behandling av personuppgifter ska alltså tillämpas framför de allmänna bestämmelserna i dataskyddslagen. Detta följer direkt av 1 kap. 6 § dataskyddslagen och det behövs därför egentligen inte någon materiell bestämmelse för att specialbestämmelser i den nya lagen ska ges företräde framför de generella bestämmelserna i dataskyddslagen. För att det ska vara tydligt hur den nya lagen förhåller sig till dataskyddslagen föreslår vi dock att en bestämmelse ska införas i lagen som tydliggör att dataskyddslagen och föreskrifter som har meddelats i anslutning till den lagen ska gälla vid behandling av personuppgifter med stöd av den nya lagen. Detta gäller dock endast om inte annat följer av den nya lagen eller föreskrifter som har meddelats i anslutning till den. Sådana tydliggörande bestämmelser är även vanligt förekommande i andra registerförfattningar. Exempel på sådana bestämmelser är 4 § domstolsdatalagen och 5 § beskattningsdatalagen (2026:125).

Det kan i detta sammanhang emellertid noteras att behovet av att tillämpa dataskyddslagen, i avsaknad av reglering i den nya lagen

om biometrisk verifiering, kan antas vara begränsat. Den nya lagen kommer att reglera endast sådan behandling av personuppgifter som utförs i syfte att verifiera en persons identitet biometriskt med stöd av lagen (se avsnitt 24.5) och i väsentliga avseenden ange förutsättningarna för personuppgiftsbehandlingen. Det nya regelverket kommer dock inte att vara komplett i bemärkelsen att det innehåller avvikande bestämmelser som blir tillämpliga i stället för dataskyddslagen avseende samtliga de frågor som regleras i den lagen. Som exempel kan nämnas bestämmelserna om tillsynsmyndigheten i 6 kap. och om skadestånd och överklagande i 7 kap.

24.4 Tillämpningsområde för bestämmelser om personuppgiftsbehandling

Vårt förslag

De nya bestämmelserna ska tillämpas vid behandling av personuppgifter som utförs i syfte att biometriskt verifiera identitet med stöd av den nya lagen.

Vid genomförande av våra förslag kan ett mycket stort antal myndigheter komma att behandla personuppgifter i samband med biometrisk verifiering av identitet mot en handling med stöd av den nya lagen. För flertalet av dessa myndigheter finns det myndighets- eller verksamhetsspecifika registerförfattningar som blir tillämpliga vid handläggningen av ett ärende eller när identitetskontroller genomförs inom ramen för verksamheten. Registerförfattningar är ofta uppbyggda så att det finns en inledande bestämmelse som anger författningens tillämpningsområde, till exempel att lagen gäller vid behandling av personuppgifter inom socialtjänsten[4] eller i Transportstyrelsens verksamhet på vägtrafikområdet som rör fordon, behörigheter, tillstånd och tillsyn.[5] När en myndighet behandlar personuppgifter i syfte att verifiera en persons identitet kommer det, enligt vår bedömning, oftast att ske inom ramen för handläggningen av ett ärende i myndighetens verksamhet. Om till exempel Försäkringskassan behandlar personuppgifter för att verifiera sökandens identitet vid hand-

[4] Se 1 § lagen (2001:454) om behandling av personuppgifter inom socialtjänsten.
[5] Se 1 kap. 2 § vägtrafikdatalagen (2019:369).

läggningen av ett ärende om sjukpenning ska Försäkringskassan – som utgångspunkt – tillämpa det regelverk för behandling av personuppgifter som finns i 114 kap. socialförsäkringsbalken. Vid behandling av personuppgifter för att verifiera identitet i samband med handläggningen av ett ärende om ekonomiskt bistånd ska socialtjänsten – som utgångspunkt – tillämpa lagen om behandling av personuppgifter inom socialtjänsten.

De bestämmelser om personuppgiftsbehandling som i dag är tillämpliga vid handläggningen av olika ärenden är vanligen specifika för myndigheten eller verksamheten i fråga och i och med det anpassade för sådan behandling av personuppgifter som normalt sett förekommer hos myndigheten eller i verksamheten; för att åter ta Försäkringskassan som exempel får myndigheten behandla personuppgifter om det är nödvändigt bland annat för att tillgodose behovet av det underlag som krävs för att den registrerades rättigheter i fråga om förmåner ska kunna bedömas (114 kap. 8 § 1 socialförsäkringsbalken). Känsliga personuppgifter får som huvudregel behandlas om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggning av ett ärende (114 kap. 11 § första stycket). Enligt 6 § lagen om behandling av personuppgifter inom socialtjänsten får personuppgifter behandlas bara om behandlingen är nödvändig för att arbetsuppgifter inom socialtjänsten ska kunna utföras. Socialtjänsten får behandla känsliga personuppgifter endast om uppgifterna har lämnats i ett ärende eller är nödvändiga för verksamheten (7 §). Det finns alltså redan i dag bestämmelser som tar sikte på Försäkringskassans och socialtjänstens möjligheter att behandla personuppgifter i den verksamheten där behovet av att verifiera en persons identitet biometriskt kommer att finnas. Detsamma gäller för många andra av de myndigheter som enligt våra överväganden bör ha möjlighet att verifiera en persons identitet biometriskt mot handlingar.

Generellt sett är myndighets- eller verksamhetsspecifika regelverk avseende personuppgiftsbehandling dock sällan utformade med utgångspunkten att myndigheten i fråga ska behandla biometriska uppgifter i syfte att verifiera en persons identitet, vilket i normalfallet kräver särskilda överväganden. För att säkerställa skyddet för enskildas integritet och tydliggöra under vilka förutsättningar myndigheter får behandla framför allt biometriska underlag och biometriska uppgifter för att verifiera identitet anser vi att de nya bestämmelser som

vi föreslår ska tillämpas när en myndighet behandlar personuppgifter i syfte att biometriskt verifiera identitet med stöd av den nya lagen.

Ett sådant tillämpningsområde för de nya bestämmelserna innebär att den aktuella myndigheten inledningsvis kommer att tillämpa de bestämmelser om personuppgiftsbehandling som vanligen gäller vid handläggningen av ärendet i fråga eller i den aktuella situationen. Det nya regelverket blir tillämpligt först när det finns förutsättningar för att genomföra en biometrisk verifiering med stöd av lagen och myndigheten väljer att nyttja denna möjlighet; som vi anfört i kapitel 23 anser vi att möjligheten att använda biometrisk verifiering mot handlingar med stöd av den nya lagen ska ses som en specifik utredningsåtgärd, som en myndighet ska kunna vidta i de situationer som vi föreslagit i avsnitt 23.6.3. För den behandling av personuppgifter som i övrigt sker inom ramen för det aktuella ärendet eller den aktuella verksamheten gäller alltså särskild tillämplig registerförfattning eller, i avsaknad av sådan, allmänna dataskyddsbestämmelser.

Metoden att låta syftet med behandlingen avgöra när bestämmelser om personuppgiftsbehandling – i det här fallet i den nya lagen – blir tillämpliga används bland annat i brottsdatalagen (2018:1177), se 1 kap. 2 §. Det är enligt vår bedömning inte nödvändigt att avgöra den exakta tidpunkten för när syftet med personuppgiftsbehandlingen övergår till att vara just biometrisk verifiering mot en handling. Detta eftersom myndigheten i fråga som utgångspunkt har stöd för den behandling av alfanumeriska personuppgifter som utförs inom ramen för ärendehandläggningen eller vid identitetskontroller inom ramen för myndighetens verksamhet. Det är framför allt när myndigheten behandlar biometriska underlag och biometriska uppgifter för kontroll mot en handling i enlighet med det regelverk vi föreslår som det är väsentligt att de nya bestämmelserna tillämpas.

24.5 Förhållandet till befintliga registerförfattningar

Vår bedömning

Det följer av principen om lex specialis att de nya bestämmelserna om personuppgiftsbehandling vid biometrisk verifiering av identitet ska tillämpas i stället för myndighets- eller verksamhetsspecifik registerförfattning när en myndighet behandlar personuppgifter i syfte att verifiera identitet biometriskt med stöd av lagen.

Det är, som vi nämnt ovan, inte möjligt eller lämpligt att inom ramen för vårt uppdrag göra någon inventering av samtliga registerförfattningar som kan vara tillämpliga för de myndigheter som kan tänkas komma att nyttja en möjlighet att verifiera identitet biometriskt mot handlingar med stöd av det regelverk vi föreslår. Det ligger i sakens natur att registerförfattningsbeståndet aldrig kan bli ”färdigt” eftersom den offentliga verksamheten genomgår ständiga förändringar.[6] För vissa myndigheter saknas myndighets- och verksamhetsspecifika bestämmelser om personuppgiftsbehandling; i dessa fall tillämpas dataskyddsförordningen och dataskyddslagen.

Vi har under arbetets gång övervägt om biometrisk verifiering av identitet mot en handling, i enlighet med våra förslag, bör förutsätta förenlighet med de bestämmelser om behandling av personuppgifter i lag eller förordning som ska tillämpas vid handläggningen av det aktuella ärendet eller i den verksamhet i vilken identitetskontroller genomförs som föranleder biometrisk verifiering. Det kan hävdas att det framstår som mindre lämpligt att en myndighet som får behandla biometriska uppgifter endast i vissa specifika situationer enligt myndighets- eller verksamhetsspecifikt regelverk ska tillåtas att behandla sådana uppgifter i andra situationer, med stöd av det regelverk vi föreslår. De eventuella begränsningar som finns i myndighets- eller verksamhetsspecifikt regelverk skulle i så fall, på sätt och vis, åsidosättas och behandling som inte är tillåten enligt detta regelverk i den aktuella verksamheten eller vid handläggning av det aktuella ärendet skulle vara tillåten när en biometrisk verifiering mot en handling genomförs med stöd av det regelverk vi föreslår. Våra förslag ska emellertid inte uppfattas på detta sätt, av följande skäl.

[6] *Myndighetsdatalag*, SOU 2015:39, s. 105.

Det är visserligen fråga om en generell möjlighet till biometrisk verifiering av identitet som ska kunna användas i princip av alla myndigheter i alla olika slags ärenden som omfattas av tillämpningsområdet för förvaltningslagen och i situationer där identitetskontroller i annat fall genomförs inom ramen för myndighetens verksamhet. Samtidigt ger det regelverk vi föreslår inte en generell rätt för myndigheter att behandla biometriska underlag och biometriska uppgifter, utan det handlar om en specifik utredningsåtgärd som ska få vidtas endast när vissa förutsättningar är uppfyllda. Förslagen påverkar inte heller befintliga möjligheter till biometrisk verifiering mot handlingar (se avsnitt 23.3). Vidare ska de biometriska underlag och de biometriska uppgifter som används vid den biometriska verifieringen förstöras omedelbart efter att kontrollen har genomförts (se avsnitt 24.9) och personuppgifter ska få behandlas, med stöd av den nya lagen, *endast* för att en biometrisk verifiering ska kunna genomföras (se avsnitt 24.8). Det kan också förutsättas att den myndighet som verifierar identitet biometriskt med stöd av lagen har rättsligt stöd, till exempel i en myndighets- eller verksamhetsspecifik registerförfattning, för att behandla de personuppgifter utöver biometriska underlag och biometriska uppgifter som behöver behandlas för att verifieringen ska kunna genomföras; biometrisk verifiering av identitet med stöd av den nya lagen syftar endast till att bekräfta att de uppgifter om identitet – och eventuellt identitetsbeteckning – som den som kontrolleras redan har lämnat till myndigheten.

Det bör vidare beaktas att flertalet befintliga registerförfattningar helt saknar bestämmelser som syftar till att reglera behandling av biometriska uppgifter. I de fall det finns en reglering avseende känsliga personuppgifter tar den många gånger sikte på behandling av andra känsliga personuppgifter, som till exempel uppgifter om hälsa eller sexuell läggning. I dessa fall kan det finnas stöd i myndighets- eller verksamhetsspecifik reglering att behandla känsliga personuppgifter i form av biometriska uppgifter, även om detta inte var avsikten vid utformningen av regelverket. För det fall biometrisk verifiering av identitet, i enlighet med våra förslag, skulle förutsätta förenlighet med myndighets- eller verksamhetsspecifik reglering skulle det därmed kunna resultera i att myndigheter som i dag aldrig behandlar biometriska uppgifter får möjlighet att verifiera identitet biometriskt, medan myndigheter som redan har vissa uttryckliga och begränsade möjligheter att behandla biometriska uppgifter i sin verksamhet inte

kan använda den generella möjligheten att verifiera identitet biometriskt mot en handling, i andra situationer än de som redan är reglerade för myndigheten i fråga. En sådan konsekvens är, enligt vår mening, inte önskvärd. De myndigheter som redan i dag har rättsligt stöd i myndighets- eller verksamhetsspecifik reglering för att behandla biometriska uppgifter har av lagstiftaren bedömts ha behov av sådan behandling i sin verksamhet i vissa situationer. Därmed bör de rimligen omfattas av en sådan generell möjlighet att verifiera identitet biometriskt mot en handling som vi föreslår.

Med hänsyn till dessa omständigheter anser vi att en generell möjlighet att biometriskt verifiera identitet mot handlingar bör vara tillgänglig för en myndighet oavsett vad som gäller i det myndighets- eller verksamhetsspecifika regelverk avseende personuppgiftsbehandling som är tillämpligt i övrigt vid handläggningen av det aktuella ärendet eller i den aktuella situationen. I enlighet med det tillämpningsområde för nya bestämmelser om personuppgiftsbehandling som vi föreslår i avsnitt 24.4 ska den myndighet som verifierar identitet biometriskt med stöd av den nya lagen därmed tillämpa bestämmelserna i den lagen vid behandling av personuppgifter som utförs i syfte att verifiera identitet med stöd av lagen.

När en myndighet bedömer att förutsättningarna för att genomföra en biometrisk verifiering med stöd av den nya lagen är uppfyllda och myndigheten behandlar personuppgifter *i syfte att* verifiera en persons identitet med stöd av lagen blir bestämmelserna om personuppgiftsbehandling i den nya lagen därmed tillämpliga. Detta följer, som vi ser det, av principen om lex specialis, det vill säga att en lag som reglerar något specifikt ska ges företräde framför en lag som reglerar allmänna frågor (lex generalis). Den av oss föreslagna lagen om biometrisk verifiering av identitet är, enligt vår bedömning, att betrakta som lex specialis i förhållande till mer generella registerförfattningar som tar sikte på all behandling av personuppgifter i en viss typ verksamhet eller hos en viss myndighet.[7] Att bestämmelserna i den nya lagen ska tillämpas i stället för myndighets- eller verksamhetsspecifika registerförfattningar vid biometrisk verifiering med stöd av lagen behöver enligt vår bedömning därmed inte komma till uttryck i den nya lagen – det följer som sagt direkt av principen om lex specialis.

[7] Se till exempel 2 och 3 §§ utlänningsdatalagen (2016:27) och 1 kap. 1 § lagen (2020:421) om Rättsmedicinalverkets behandling av personuppgifter.

24.6 Personuppgiftsansvar

Vårt förslag

Den myndighet som bestämmer att en biometrisk verifiering av identitet ska genomföras med stöd av den nya lagen ska vara personuppgiftsansvarig för den behandling av personuppgifter som utförs med anledning av det.

Den som är personuppgiftsansvarig har ansvar för att behandlingen av personuppgifter utförs i enlighet med gällande dataskyddsreglering. Den personuppgiftsansvarige ska till exempel ansvara för och kunna visa att de grundläggande principerna för behandling av personuppgifter i dataskyddsförordningen följs. Det framgår av artikel 5 i förordningen. Den personuppgiftsansvarige ska också, enligt artikel 24, genomföra lämpliga tekniska och organisatoriska åtgärder – med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter – för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Begreppet personuppgiftsansvarig är därför ett centralt begrepp.

Med personuppgiftsansvarig avses en fysisk eller juridisk person, myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Som utgångspunkt är det alltså den aktör som bestämmer ändamålen och medlem för den behandling av personuppgifter som utförs som är ansvarig i enlighet med dataskyddsförordningen. Vem som ska anses göra det står dock inte alltid klart, och ställningstagande till vem som är personuppgiftsansvarig kan kräva bedömningar till exempel av vem som har faktiskt inflytande över behandlingen och hur avtalsförhållandena mellan berörda parter ser ut. Framför allt för den enskilde vars uppgifter behandlas kan det i vissa fall vara svårt att veta vilken aktör som är personuppgiftsansvarig för en viss behandling. Aktuella omständigheter kan också medföra att det är fråga om ett gemensamt personuppgiftsansvar, enligt artikel 26 i dataskyddsförordningen. Europeiska dataskyddsstyrelsen har gett ut riktlinjer angående begreppen personuppgiftsansvarig och person-

uppgiftsbiträde som kan användas för vägledning.[8] De innehåller bland annat exempel på när en aktör bör anses vara personuppgiftsansvarig respektive personuppgiftsbiträde.

Om ändamålen och medlen bestäms av unionsrätten eller medlemsstaternas nationella rätt är det dock, enligt artikel 4.7 i dataskyddsförordningen, möjligt för lagstiftaren att reglera vem som är personuppgiftsansvarig. Vidare har EU-domstolen i mål C-638/23, *Amt der Tiroler Landesregierung* (punkt 38), uttalat att den omständigheten att den nationella lagstiftaren direkt utser en enhet som personuppgiftsansvarig bidrar till att uppnå de rättssäkerhetsmål som eftersträvas med dataskyddsförordningen, genom att göra det möjligt för fysiska personer vars personuppgifter är föremål för behandling att enkelt identifiera den enhet som ansvarar för att deras rättigheter enligt förordningen iakttas.

Vi anser att personuppgiftsansvaret för behandling av personuppgifter vid biometrisk verifiering av identitet mot en handling med stöd av den nya lagen bör regleras i nationell rätt. Detta inte minst med hänsyn till att sådana kontroller – enligt våra överväganden i kapitel 27, vilket vi återkommer till nedan – i första hand bör kunna göras på distans, med hjälp av olika tekniska system. Det kan då vara svårare att avgöra vem som behandlar personuppgifter och därmed är ansvarig. Genom att det regleras i den nya lagen blir det tydligt vem som är personuppgiftsansvarig vid sådan behandling. Det är att föredra för de enskilda, som inte behöver analysera och ta ställning till vem som ska anses vara personuppgiftsansvarig för en viss behandling. Det är också att föredra generellt sett, både för de myndigheter som behandlar personuppgifter och för tillsynsmyndigheten, att det är tydligt vem som är personuppgiftsansvarig.

Som huvudregel gäller att den som utför själva behandlingen av personuppgifter också ska vara personuppgiftsansvarig.[9] Det saknas enligt vår mening som utgångspunkt anledning att frångå denna huvudregel. Ett gemensamt personuppgiftsansvar är enligt vår bedömning inte lämpligt, även om genomförandet av en verifiering kan komma att medföra att både den myndighet som bestämt att verifieringen ska genomföras och en annan aktör som tillhandahåller ett tekniskt system för verifiering behandlar personuppgifter. Frågan

[8] Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, version 2.1, 7 juli 2021.
[9] Se bland annat prop. 2015/16:65, s. 55 f. och *Domstolsdatalag,* prop. 2014/15:148, s. 32 ff.

är emellertid när behandlingen kan anses utföras av den verifierande myndigheten, det vill säga den myndighet som vill genomföra en verifiering med stöd av lagen. Utformningen av den tekniska lösningen för ett system för att biometriskt verifiera identitet mot handlingar kan vara av betydelse i detta avseende.

Som vi återkommer till i kapitel 27 finns det olika tänkbara tekniska lösningar för att möjliggöra biometrisk verifiering av identitet mot handlingar. En myndighet skulle kunna välja att ta fram eller införskaffa egna system, men skulle också kunna anlita en annan aktör för tillhandahållande av de system som behövs för verifiering, exempelvis en sådan mobilapplikation och ett sådant backend-system som vi redogör för i avsnitt 27.4. Den aktör som tar fram och ansvarar för dessa tekniska system skulle kunna vara antingen en privat aktör eller en annan myndighet. I det senare fallet skulle man kunna tänka sig att till exempel Polismyndigheten eller Digg (Myndigheten för digital förvaltning) tar fram en myndighetsgemensam mobilapplikation som, under vissa villkor, är tillgänglig för de myndigheter som vill nyttja den, samt tar fram det backend-system som behövs för att genomföra en biometrisk jämförelse och för kommunikationen mellan myndigheterna och mobilapplikationen. Ansvaret för de tekniska system där personuppgifter faktiskt bearbetas i samband med biometrisk verifiering med stöd av den nya lagen behöver alltså inte ligga hos den myndighet som vill genomföra en sådan kontroll. Detta bör som vi ser det dock inte påverka personuppgiftsansvaret. Vi kan här konstatera att i förarbetena till utlänningsdatalagen instämde regeringen i Datainspektionens (nuvarande Integritetsskyddsmyndigheten) uppfattning att det förhållandet att Migrationsverket var tekniskt ansvarig för de system som användes för behandling av personuppgifter enligt utlännings- och medborgarskapslagstiftningen inte bör vara avgörande för frågan om placeringen av personuppgiftsansvaret.[10] Vi delar den bedömningen och anser – oavsett val av teknisk lösning och oavsett vilken aktör som ansvarar för eller tillhandahåller de tekniska system eller programvaror som används för verifieringen – att den myndighet som handlägger det aktuella ärendet eller genomför den aktuella identitetskontrollen som föranlett verifiering av identiteten, ska vara personuppgiftsansvarig för behandlingen. Det är den myndigheten som bestämmer ändamålen och medlen för den behandling av personuppgifter som utförs, och som enligt vår

[10] Prop. 2015/16:65, s. 55 f.

mening har bäst förutsättningar att säkerställa att behandlingen utförs i enlighet med tillämpliga bestämmelser om personuppgiftsbehandling. För det fall en privat aktör anlitas för tillhandahållande av ett tekniskt system som en tjänst framstår det som än viktigare att den myndighet som nyttjar tjänsten är personuppgiftsansvarig, för att säkerställa att personuppgiftsbehandlingen är förenlig med dataskyddsförordningen och nationell rätt.

I detta sammanhang kan en jämförelse göras med den reglering av personuppgiftsansvar som framgår av EU-kommissionens förslag till Europaparlamentets och rådets förordning om inrättande av en applikation för elektronisk inlämning av reseuppgifter.[11] Av artikel 7 i förslaget framgår att personuppgiftsansvaret för uppgifter som behandlas i en gemensam backend-tjänst för validering ska ligga hos eu-Lisa, som är Europeiska unionens byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa, och som ska ansvara för utvecklingen och driften av tjänsten. Det är inte möjligt för oss att på samma sätt, på förhand, peka ut en viss tekniskt ansvarig aktör som personuppgiftsansvarig för den behandling av uppgifter som kan behöva utföras i en sådan mobilapplikation och ett sådant backend-system som vi beskriver i avsnitt 27.4. Det är inte säkert att våra förslag kommer att implementeras på ett sådant sätt överhuvudtaget. Att i den nya lagen ange att en tekniskt ansvarig aktör ska vara personuppgiftsansvarig riskerar därför att helt sakna betydelse, och framstår därför inte heller som lämpligt. Den ordning avseende personuppgiftsansvar som föreslagits av kommissionen för EU:s digitala reseapplikation utgör som vi ser det inte heller något hinder mot att personuppgiftsansvaret anges på det sätt vi föreslår, inom ramen för den nya lagen.

Mot den här bakgrunden bedömer vi att den myndighet som väljer att verifiera en persons identitet biometriskt mot en handling med stöd av det regelverk vi föreslår ska ansvara för att behandlingen utförs i enlighet med gällande dataskyddsreglering. Vi föreslår därför att den myndighet som bestämmer att en biometrisk verifiering av identitet ska genomföras med stöd av den nya lagen ska vara personuppgiftsansvarig för den behandling av personuppgifter som utförs med anledning av det. Med detta uttryckssätt kommer den myndighet som bestämmer att en biometrisk verifiering av identitet ska genomföras att vara personuppgiftsansvarig även för behandling av

[11] COM(2024) 670 final.

personuppgifter som eventuellt utförs av andra aktörer med anledning av verifieringen, till exempel i ett sådant backend-system som vi beskriver i avsnitt 27.4. Det ankommer på den verifierande myndigheten att – i egenskap av personuppgiftsansvarig – på lämpligt sätt säkerställa att biometriska underlag och biometriska uppgifter som används för verifiering enligt den nya lagen omedelbart förstörs när kontrollen har genomförts, i enlighet med den bestämmelse som vi föreslår i avsnitt 24.9.

24.7 Personuppgiftsbiträde

Vår bedömning

Möjligheten för myndigheter att anlita personuppgiftsbiträde för att biometrisk verifiera personers identitet med stöd av den nya lagen behöver inte regleras särskilt.

Personuppgiftsbiträden regleras i artikel 28 i dataskyddsförordningen. Om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas. Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. När personuppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett så kallat biträdesavtal. Ett sådant avtal syftar till att säkerställa bland annat att båda parter följer dataskyddsförordningen och skyddar de registrerades personuppgifter.

För det fall personuppgiftsansvaret inte har reglerats särskilt i unionsrätten eller nationell rätt är den som anlitar någon annan för att behandla personuppgifter, till exempel för att lagra och sprida eller för att samla in och bearbeta personuppgifterna, normalt att anse som personuppgiftsansvarig och den anlitade som personuppgiftsbiträde. Det gäller även om det är det anlitade företaget och inte uppdragsgivaren som har kunskapen om hur man bäst behandlar

personuppgifter, till exempel hur man lagrar, samlar in, sprider och bearbetar dem, och har resurserna för att göra det. Uppdragsgivaren har då nämligen bestämt medlen för att behandla personuppgifterna just genom att anlita ett företag som kan använda vissa metoder. Det kan handla om att lägga ut it-drift på entreprenad eller om att anlita ett företag för att samla in personuppgifter inom ramen för en marknadsundersökning.[12] Vid ett införande av den lag vi föreslår skulle det kunna röra sig om utveckling och drift av den mobilapplikation och det backend-system som kan behövas för att biometrisk verifiering mot handlingar ska kunna genomföras på distans, på det sätt vi redogör för i avsnitt 27.4. Den aktör som eventuellt sköter sådana it-system behandlar då inte några personuppgifter för egen räkning utan på uppdrag av den myndighet som genomför kontrollen.

Den aktör som pekats ut som personuppgiftsansvarig i unionsrätten eller i nationell rätt kan också anlita ett personuppgiftsbiträde. Personuppgiftsbiträdet kan vara en annan myndighet eller en privat aktör. Enligt 14 § lagen (2001:99) om den officiella statistiken är en statistikansvarig myndighet – som utgångspunkt – personuppgiftsansvarig för behandling av personuppgifter för framställning av statistik, men kan också vara personuppgiftsbiträde åt en annan statistikansvarig myndighet. Företaget AB Svenska Pass levererar pass och identitetskort både till Polismyndigheten och Skatteverket. I promemorian *Passdatalag – en ny lag som kompletterarar EU:s dataskyddsförordning* uttalades att vem som anlitas för att till exempel tillverka pass varierar över tid och att det måste vara upp till de personuppgiftsansvariga och inte lagstiftaren att bedöma vem som är att anses som biträde och se till att nödvändiga avtal finns. Bedömningen gjordes att vem som är personuppgiftsbiträde inte bör regleras.[13] Även i propositionen *Framtidens dataskydd vid Skatteverket, Tullverket och Kronofogdemyndigheten* gjordes bedömningen att det inte finns något behov av att införa bestämmelser om personuppgiftsbiträden, eftersom dataskyddsförordningen på ett detaljerat sätt reglerar vad som gäller när personuppgiftsansvariga anlitar personuppgiftsbiträden. [14]

Mot denna bakgrund anser vi att möjligheten för myndigheter att anlita personuppgiftsbiträde för biometrisk verifiering av iden-

[12] Se Öman, Dataskyddsförordningen (GDPR) m.m., JUNOV Version 3A, 2025-09-11, kommentaren till artikel 4.7, under rubriken *När annan anlitas för behandlingen*.
[13] Ds 2019:5, s. 106 f.
[14] Prop. 2025/26:88, s. 120 f.

titet med stöd av den nya lagen inte behöver regleras särskilt. I det avseendet är det tillräckligt att den generella dataskyddsregleringen blir tillämplig.

24.8 Ändamål för personuppgiftsbehandling

Vårt förslag

Personuppgifter – inklusive känsliga personuppgifter – ska få behandlas endast för att en biometrisk verifiering av identitet med stöd av den nya lagen ska kunna genomföras.

Enligt artikel 5.1 b i dataskyddsförordningen får personuppgifter samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Den personuppgiftsansvarige måste bestämma ändamålen för behandlingen senast när personuppgifterna samlas in. Att ändamålen ska vara *särskilda* innebär att en alltför allmänt hållen ändamålsangivelse inte godtas; om inte ändamålet har en viss grad av precision kan man knappast bedöma om personuppgifterna är adekvata och relevanta eller om för många personuppgifter behandlas. Går det inte att avgöra vilka personuppgifter som behövs för att ändamålet ska kunna uppfyllas lär ändamålet inte vara särskilt utan allmänt. Ändamålsbestämningen avgör alltså vilka personuppgifter som får behandlas.[15]

Dataskyddsförordningen ställer inga krav på att ändamålen ska vara fastställda i författning, men det finns inte heller någonting som hindrar att det görs. Registerförfattningar som reglerar personuppgiftsbehandling hos en viss myndighet eller i en viss verksamhet innehåller vanligen bestämmelser om ändamål, för att tydliggöra för vilka ändamål personuppgifter får behandlas. Ändamålsbestämmelser kan vara relativt detaljerade, som till exempel 11–13 §§ utlänningsdatalagen, och innehålla särskilda ändamål för behandling av känsliga personuppgifter, som till exempel 14 och 15 §§ samma lag. Det finns emellertid även mer generella ändamålsbestämmelser, som till exempel 6 § domstolsdatalagen (2015:728), som anger att personuppgifter får

[15] Se Öman, *Dataskyddsförordningen (GDPR) m.m.*, JUNO Version 3A, 2025-09-11, kommentaren till artikel 5.1 b.

behandlas om det behövs för handläggningen av mål och ärenden. I propositionen *Framtidens dataskydd vid Skatteverket, Tullverket och Kronofogdemyndigheten*, föreslogs brett formulerade och flexibla ändamålsbestämmelser som anger att berörda myndigheter ska få behandla personuppgifter om det är nödvändigt för att utföra verksamhet inom de föreslagna dataskyddslagarnas respektive materiella tillämpningsområde. Regeringen bedömde att en sådan bestämmelse är tillräckligt preciserad, tydlig och förutsägbar i den aktuella situationen. Nämnda ändamålsbestämmelser har genomförts genom att nya registerförfattningar har trätt i kraft den 2 april 2026, se exempelvis 7 § beskattningsdatalagen.[16]

Vi bedömer att det finns ett värde med en ändamålsbestämmelse som tydliggör och begränsar under vilka förutsättningar en myndighet får behandla personuppgifter med stöd av den föreslagna lagen om biometrisk verifiering av identitet. Som vi tidigare påpekat syftar de bestämmelser om personuppgiftsbehandling som vi nu överväger inte till att reglera all behandling hos en viss myndighet, i en viss typ av verksamhet eller vid handläggningen av en viss typ av ärenden. I stället är det fråga om att reglera den relativt begränsade personuppgiftsbehandling som behöver utföras vid en biometrisk verifiering av identitet med stöd av den nya lagen. En ändamålsbestämmelse behöver således inte formuleras med beaktande av att den ska möjliggöra all sådan behandling av personuppgifter som krävs för att myndigheterna ska kunna bedriva sin verksamhet på ett ändamålsenligt sätt.

Det är vanligt att ändamålsbestämmelser anger att personuppgifter får behandlas om det *behövs* eller är *nödvändigt* för de ändamål som specificeras i bestämmelsen. Som vi redogjort för i avsnitt 21.5.1 har de båda uttryckssätten samma innebörd i dataskyddshänseende.[17] Vidare har vi i avsnitt 23.6.3 föreslagit att biometrisk verifiering av identitet mot en handling ska få genomföras om en sådan kontroll är nödvändig, dels vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde, dels, i annat fall, när en myndighet inom ramen för sin verksamhet genomför identitetskontroller. Den bestämmelse vi föreslår som reglerar under vilka förutsättningar en myndighet ska få genomföra en biometrisk veri-

[16] Prop. 2025/26:88 s. 130 ff.
[17] *Behandling av personuppgifter vid Institutet för arbetsmarknads- och utbildningspolitisk utvärdering*, prop. 2011/12:176, s. 30.

fiering med stöd av den nya lagen innefattar således ett rekvisit som vanligen finns i ändamålsbestämmelser, nämligen att behandlingen i fråga ska vara nödvändig för att få genomföras. Med hänsyn till att detta rekvisit framgår redan av den bestämmelse som reglerar de materiella förutsättningarna för att få genomföra en biometrisk verifiering med stöd av lagen behöver det inte anges i ändamålsbestämmelsen att behandlingen ska vara nödvändig. Behandlingen av personuppgifter – däribland biometriska uppgifter – är helt nödvändig för att den utredningsåtgärd i form av biometrisk verifiering av identitet som den nya lagen möjliggör ska kunna genomföras. Behandlingen behöver därför inte vara avhängig av att något annat rekvisit ska vara uppfyllt för att den ska vara tillåten.

Den så kallade finalitetsprincipen i artikel 5.1 b i dataskyddsförordningen innebär att insamlade uppgifter inte senare får behandlas på ett sätt som är oförenligt med angivna ändamål. Eftersom de bestämmelser om behandling av personuppgifter som vi föreslår kompletterar dataskyddsförordningen blir finalitetsprincipen tillämplig vid behandling i enlighet med den nya lagen, om ändamålen inte anges uttömmande på så sätt att personuppgifter får behandlas *endast* för de angivna ändamålen. Med hänsyn till att det regelverk vi föreslår syftar enbart till att ge myndigheter möjlighet att verifiera identitet biometriskt mot handlingar, och till att skydda den som kontrolleras mot att hans eller hennes personliga integritet då kränks (se avsnitt 23.2.2), anser vi att det saknas skäl för att tillåta behandling av personuppgifter i andra situationer, även om behandlingen skulle kunna anses vara förenlig med angivna ändamål. Vidare ska biometriska underlag och biometriska uppgifter, enligt våra förslag i avsnitt 24.9, förstöras omedelbart när en kontroll har genomförts, vilket innebär att det i praktiken finns mycket begränsade möjligheter att alls behandla insamlade personuppgifter för andra ändamål än biometrisk verifiering i enlighet med den nya lagen.

Mot den här bakgrunden föreslår vi att personuppgifter – inklusive känsliga personuppgifter – ska få behandlas med stöd av den nya lagen endast för att en biometrisk verifiering av identitet med stöd av lagen ska kunna genomföras. Genom en sådan ändamålsbestämmelse blir det möjligt för myndigheter att behandla personuppgifter i den omfattning det behövs för att en biometrisk verifiering mot en handling ska kunna genomföras, samtidigt som regelverket inte ger rättsligt stöd för behandling av personuppgifter för andra syften eller

för behandling av andra personuppgifter än sådana som behövs för en verifiering enligt lagen.

24.9 Efterföljande behandling av biometriska underlag och biometriska uppgifter

Vårt förslag

När en biometrisk verifiering av identitet mot en handling har genomförts ska den ansiktsbild och de fingeravtryck som har tagits för kontrollen omedelbart förstöras. Detsamma ska gälla för de biometriska uppgifter som har tagits fram i samband med kontrollen.

Vi har i avsnitt 20.6 redogjort för vår bedömning att ansiktsbild och fingeravtryck som har tagits upp i syfte att biometrisk verifiera identitet mot en handling bör förstöras omedelbart efter att kontrollen har genomförts. Vi har också bedömt att det samma bör gälla för de biometriska uppgifter som tagits fram ur ansiktsbilden och fingeravtrycken samt ur underlagen i den handling mot vilken verifieringen genomförts. Det saknas anledning att göra en annan bedömning här.

Vi föreslår därför att när en biometrisk verifiering av identitet har genomförts med stöd av det regelverk vi föreslår, ska den ansiktsbild och de fingeravtryck som tagits för kontrollen omedelbart förstöras, liksom de biometriska uppgifter som tagits fram i samband med kontrollen. Sistnämnda uppgifter avser de som tagits fram ur såväl de biometriska underlag som finns lagrade i eller på handlingen (även en synlig ansiktsbild) som den ansiktsbild och/eller de fingeravtryck som tagits av den enskilde i samband med kontrollen.

Vi vill i detta sammanhang tydliggöra att det inte är fråga om en sådan avvikande bestämmelse som avses i 10 § tredje stycket arkivlagen (1990:782) och alltså inte om gallring av allmänna handlingar, utan om reglering av längsta tillåtna tid för behandling av aktuella typer av personuppgifter i syfte att begränsa intrånget i den personliga integriteten.[18]

[18] Jfr *Framtidens dataskydd – Vid Skatteverket, Tullverket och Kronofogden*, SOU 2023:100, Del 1, s. 847 ff.

24.10 Tillgång till personuppgifter

Vårt förslag

Tillgången till personuppgifter ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

En fysisk person som utför arbete under den personuppgiftsansvariges överinseende och som får tillgång till personuppgifter får, som utgångspunkt, endast behandla dessa på instruktion från den personuppgiftsansvarige. Detta framgår av artikel 29 i dataskyddsförordningen. Den personuppgiftsansvarige ska, enligt artikel 32.4, vidta åtgärder för att säkerställa att personuppgifter inte behandlas utöver vad den personuppgiftsansvarige har gett instruktioner om. Den personuppgiftsansvarige har alltså ett ansvar för att anställda inte behandlar personuppgifter utöver vad den personuppgiftsansvarige har bedömt lämpligt.

Utgångspunkten är att personuppgifter inte ska spridas till fler än vad som är nödvändigt med hänsyn till ändamålet med behandlingen (jfr artikel 5.1 f i dataskyddsförordningen). Vilken spridning av personuppgifter som en viss behandling innebär har av naturliga skäl stor inverkan på integritetsriskerna med behandlingen. Att begränsa tillgången till personuppgifter är en åtgärd som syftar till att säkerställa den registrerades grundläggande rättigheter och intressen. Skyldigheten för personuppgiftsansvariga att på olika sätt begränsa tillgången till personuppgifter följer alltså redan av dataskyddsförordningen.[19] Det har därför i vissa lagstiftningsärenden bedömts inte finnas skäl att införa ytterligare krav i lag.[20]

En bestämmelse i den nya lagen som anger att tillgången till personuppgifter ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter klargör att den myndighet som verifierar en persons identitet biometriskt mot en handling har ett ansvar för att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att personuppgifter inte sprids utanför den krets av personer som behöver ha tillgång till dessa för att kunna utföra sina arbetsuppgifter. Innebörden av bestämmelsen är att det ska finnas ett berättigat behov av åtkomst till personuppgifterna.

[19] *Utbetalningsmyndigheten*, prop. 2022/23:34, s. 136.
[20] A.a., s. 136 samt hänvisningar där.

En bestämmelse av aktuellt slag får naturligtvis större betydelse i en situation där regelverket tar sikte på all personuppgiftsbehandling hos en viss myndighet eller i en viss verksamhet; den som är anställd vid myndigheten ska i sådant fall inte ges obegränsad tillgång till alla personuppgifter som behandlas vid myndigheten, exempelvis i ett eller flera olika ärendehanteringssystem. Vi anser dock att en bestämmelse som begränsar tillgången till personuppgifter har ett värde även i den nu aktuella situationen, genom att den tydliggör att endast de medarbetare vid respektive myndighet som behöver tillgång till aktuella personuppgifter bör ha tillgång till dem. En sådan bestämmelse ligger också i linje med vad som anges i artikel 11.6 och 11.7 i EU:s id-kortsförordning[21]; endast vederbörligen bemyndigad personal vid behöriga nationella myndigheter och unionsbyråer ska ha tillgång till den ansiktsbild och de fingeravtryck som har lagrats i lagringsmedium på identitetskort och uppehållstillståndshandlingar och endast vederbörligen bemyndigad personal hos privata aktörer ska ha tillgång till ansiktsbilden, vid en kontroll av identiteten.[22] En bestämmelse som begränsar tillgången till personuppgifter begränsar också indirekt kretsen av personer vid myndigheterna som kan genomföra en biometrisk verifiering med stöd av den nya lagen. Det får visserligen förutsättas att myndigheter generellt sett säkerställer att endast personal vid myndigheten med nödvändig kompetens och behörighet är bemyndigad att utföra olika arbetsuppgifter. I avsnitt 23.6 har vi emellertid föreslagit att den nya lagen ska kunna användas också när myndigheten genomför identitetskontroller i sin verksamhet i annat fall än vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde. I sådana fall kan en större krets av personer hos myndigheten antas komma att kunna tillämpa den nya lagen än vid handläggning av ett ärende. Det kan därför även med hänsyn till detta vara lämpligt att det i den nya lagen tydliggörs att tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter.

[21] Rådets förordning (EU) 2025/1208 av den 12 juni 2025.
[22] Tillgång till innehavarens fingeravtryck som lagrats i lagringsmediet får inte ges till privata aktörer, se artikel 11.6 och 11.7 i förordningen.

24.11 Enskildas rättigheter

Vår bedömning

Den nya lagen bör inte innehålla några undantag från registrerades rättigheter enligt artiklarna 13 och 15–19 i dataskyddsförordningen.

Kapitel III i dataskyddsförordningen innehåller en omfattande reglering av den registrerades rättigheter. Det finns bestämmelser om bland annat information och tillgång till uppgifter (artikel 13–15), rättelse och radering (artikel 16–20) samt rätt att göra invändningar (artikel 21). Dataskyddsförordningen innehåller också flera direkt tillämpliga undantag från de rättigheter som föreskrivs.

Enligt artikel 23.1 i dataskyddsförordningen finns det en generell möjlighet att i nationell rätt begränsa tillämpningsområdet för bestämmelserna om den registrerades rättigheter. Sådana begränsningar måste göras med respekt för andemeningen i de grundläggande rättigheterna och friheterna och vara en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa vissa angivna viktiga intressen. Fråga är om det finns behov av att, i det regelverk vi föreslår, införa särskilda regler om begränsningar av enskildas rättigheter enligt dataskyddsförordningen.

24.11.1 Information och tillgång till personuppgifter

Principerna i dataskyddsförordningen om rättvis och öppen behandling kräver att den registrerade informeras om att behandling sker och syftet med den (se skäl 60). Artikel 13 innehåller bestämmelser om den information som den personuppgiftsansvarige självmant ska lämna till den registrerade i det fall personuppgifterna samlas in från den registrerade själv. Det handlar bland annat om identitet och kontaktuppgifter för den personuppgiftsansvarige (punkt 1 a) och ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen (punkt 1 c). Den registrerade ska också få information bland annat om den period under vilken personuppgifterna kommer att lagras (punkt 2 a) och rätten att ge in klagomål till en tillsynsmyndighet (punkt 2 d).

Vid en biometrisk verifiering av identitet mot en handling, i enlighet med våra förslag, kommer de personuppgifter som behövs för verifieringen att samlas in från den enskilde och artikel 13 i dataskyddsförordningen blir tillämplig. Vi ser inga hinder för den verifierande myndigheten att uppfylla skyldigheten att informera den enskilde i enlighet med artikel 13 och dataskyddsförordningen i övrigt, till exempel artikel 12 om klar och tydlig information. Vi ser inte heller något behov av ytterligare reglering avseende skyldighet för den personuppgiftsansvarige att lämna information för att säkerställa enskilda skydd mot att deras personliga integritet kränks vid den personuppgiftsbehandling som föranleds av en biometrisk verifiering.

Artikel 14 reglerar vilken information som ska tillhandahållas om personuppgifterna inte har erhållits från den registrerade och aktualiseras inte vid tillämpning av den nya lag som vi föreslår.

Den registrerades rätt till tillgång, som ofta benämns rätten till registerutdrag, regleras i artikel 15. Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och viss i bestämmelsen specificerad information, såsom ändamålen med behandlingen och rätten att ge in klagomål till en tillsynsmyndighet (punkt 1). Rätten till registerutdrag innebär även bland annat att den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling (punkt 3). Vid en biometrisk verifiering av identitet med stöd av den nya lagen kommer biometriska underlag och biometriska uppgifter att behandlas endast momentant. Sådana uppgifter ska inte sparas eller lagras utan förstöras omedelbart efter att kontrollen har genomförts (se avsnitt 24.9). Även den behandling av övriga personuppgifter – som till exempel namn och födelsedatum – som sker i samband med en biometrisk verifiering med stöd av lagen är tillfällig. Om dessa personuppgifter däremot fortsatt behandlas av den myndighet som verifierat personens identitet, till exempel i ett ärendehanteringssystem, efter att kontrollen har genomförts uppkommer en annan fråga. Uppgifterna får då som utgångspunkt anses behandlas med stöd av myndighets- eller verksamhetsspecifik registerförfattning eller – i avsaknad av sådant regelverk – med stöd av dataskyddsförordningen och dataskyddslagen. För det fall en person som har varit föremål för en begäran om biometrisk verifiering med stöd av den nya lagen begär ett så kallat

registerutdrag från den myndighet som bestämt att kontrollen ska genomföras handlar det därmed snarare om generell information om uppgifter som behandlas i myndighetens verksamhet än om uppgifter som behandlats med stöd av den nya lagen. Oavsett synsätt i detta avseende ser vi inget behov av att göra undantag från den registrerades rättigheter enligt artikel 15.

24.11.2 Rättelse och radering

Som vi varit inne på i avsnitt 24.11.1 är den behandling av personuppgifter som kommer att utföras med stöd av lagen om biometrisk verifiering av identitet tillfällig. Därmed kommer det som utgångspunkt inte att finnas några uppgifter som behandlas med stöd av den nya lagen att rätta eller radera enligt artikel 16 och 17. Det kommer som utgångspunkt inte heller att finnas några personuppgifter vars behandling kan begränsas enligt artikel 18 och alltså ingen att underrätta enligt artikel 19. För det fall den registrerade vill att den myndighet som begärt att hans eller hennes identitet ska verifieras biometriskt, ska rätta eller radera personuppgifter, eller begränsa behandlingen av dem, kommer det sannolikt att handla om personuppgifter som behandlas med stöd av myndighets- eller verksamhetsspecifikt regelverk, eller med stöd av dataskyddsförordningen eller dataskyddslagen.

Vi bedömer att ingen av de rättigheter som regleras i artikel 16–19 kommer att utgöra hinder för att biometrisk verifiering av identitet ska kunna genomföras med stöd av den nya lagen på ett ändamålsenligt sätt. Det finns därmed inget behov av att göra undantag från den registrerades rättigheter enligt artikel 16–19.

24.11.3 Rätten att göra invändningar

Vårt förslag

Artikel 21.1 i dataskyddsförordningen om rätten att göra invändningar ska inte gälla vid sådan behandling av personuppgifter som är tillåten enligt den nya lagen eller föreskrifter som har meddelats i anslutning till lagen.

Den registrerade ska, enligt artikel 21.1 i dataskyddsförordningen, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på artikel 6.1 e eller f, det vill säga som ett led i myndighetsutövning, för att utföra en uppgift av allmänt intresse eller efter en intresseavvägning. Följden av att en invändning görs är att den personuppgiftsansvarige inte längre får behandla personuppgifterna, såvida inte denne kan påvisa tvingande, berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

Den personuppgiftsbehandling som kommer att utföras vid biometrisk verifiering av identitet enligt den nya lagen kommer att ske i syfte att utföra en uppgift av allmänt intresse, och i vissa fall som ett led i myndighetsutövning (se avsnitt 21.7.1). Det innebär att bestämmelsen om rätten att göra invändningar i artikel 21 gäller vid behandling av personuppgifter enligt lagen. Som vi redogjort för inledningsvis i avsnitt 24.11 har medlemsstaterna emellertid möjlighet att begränsa rätten att göra invändningar enligt artikel 23.1 i dataskyddsförordningen under vissa förutsättningar.

Vid införandet av dataskyddslagen bedömde regeringen att det inte var lämpligt att inskränka rätten att göra invändningar mot myndigheters behandling av personuppgifter genom ett generellt undantag i dataskyddslagen. Sådana undantag skulle i stället övervägas på sektorsspecifik nivå.[23] Det är relativt vanligt med begränsning av rätten att göra invändningar i myndighets- eller verksamhetsspecifika registerförfattningar. Utlänningsdatalagen innehåller till exempel en sådan bestämmelse (se 18 b §) liksom socialförsäkringsbalken (se 114 kap. 6 §). Ett huvudsakligt skäl till detta är att det ansetts vara av stor betydelse att personuppgifter får behandlas i myndigheternas verksamheter oberoende av den registrerades inställning. Vidare har bedömningen gjorts att den personuppgiftsansvarige närmast undantagslöst skulle kunna påvisa skäl för fortsatt behandling som väger tyngre än den registrerades intressen i det enskilda fallet.[24] Att den registrerade har möjlighet att invända mot behandlingen har dock bedömts kunna påverka effektiviteten i myndigheternas verksamhet.[25]

[23] *Ny dataskyddslag*, prop. 2017/18:105, s. 105 f.
[24] *Anpassning av utlänningsdatalagen till EU:s dataskyddsförordning*, prop. 2017/18:254, s. 44 f.
[25] Jfr *Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning*, prop. 2017/18:95, s. 85.

Även vad gäller rätten att göra invändningar bör det enligt vår mening beaktas att den behandling av personuppgifter som kommer att utföras av en myndighet med stöd av den nya lagen är momentan. Vid invändning mot behandlingen är det som utgångspunkt därför inte fråga om huruvida personuppgifter fortsatt ska få behandlas i till exempel ett ärendehanteringssystem hos socialtjänsten eller Försäkringskassan, vilket är den situation som rätten att göra invändningar enligt artikel 21.1 i dataskyddsförordningen tar sikte på. Detta eftersom några personuppgifter inte kommer att behandlas av myndigheteten, med stöd av den nya lagen, vid tidpunkten för invändningen. För det fall en person väljer att medverka till en biometrisk verifiering – genom att låta myndigheten ta upp biometriska underlag – och därefter invänder mot behandlingen av personuppgifter blir frågan i stället snarare om den biometriska verifieringen kan genomföras. Med hänsyn till ordalydelsen i artikel 21.1 – ”inte längre behandla” – bör det enligt vår mening inte heller vara möjligt att med åberopande av nämnda bestämmelse invända mot en framtida behandling av personuppgifter. Sammantaget talar dessa omständigheter starkt mot att artikel 21.1 i praktiken kan göras gällande i samband med en biometrisk verifiering av identitet med stöd av den nya lagen. Detta talar visserligen mot ett behov av att i den nya lagen alls reglera rätten att göra invändningar enligt artikel 21.1 i dataskyddsförordningen.

Enskilda, som av olika anledningar inte vill medverka till en biometrisk verifiering, skulle dock kunna tänkas invända mot behandlingen med stöd av artikel 21.1 för att försvåra och förhala verifieringsprocessen. Vidare finns det ett tydligt behov för myndigheter att kunna behandla personuppgifter i samband med biometrisk verifiering av identitet i enlighet med den nya lagen, oberoende av den registrerades inställning. En myndighet, som bedömt att det är nödvändigt med en biometrisk verifiering av identitet enligt lagen, bör enligt vår mening också regelmässigt kunna påvisa skäl för fortsatt behandling som väger tyngre än den registrerades intressen i det enskilda fallet. För att fullt ut säkerställa att en myndighet kan behandla relevanta personuppgifter vid biometrisk verifiering av identitet med stöd av den nya lagen – utan fördröjning och ökad administration – anser vi att det bör anges i lagen att den registrerade inte har någon rätt att motsätta sig sådan personuppgiftsbehandling som är tillåten enligt lagen. En sådan begränsning får anses utgöra en nödvändig och proportionell åtgärd i syfte att säkerställa ett viktigt mål av allmänt

intresse som erkänns av unionen och är därmed tillåten enligt artikel 23.1 i dataskyddsförordningen.

24.12 Åtkomst och utlämnande av uppgifter

Vår bedömning

Den nya lagen bör inte innehålla bestämmelser om direktåtkomst eller elektroniskt utlämnande.

Dataskyddsförordningen saknar bestämmelser som uttryckligen reglerar formen för ett utlämnande av personuppgifter. Om ett utlämnande i sig är tillåtet är det därför normalt upp till den myndighet som lämnar ut uppgifterna att avgöra på vilket sätt detta ska göras. Den personuppgiftsansvarige ska emellertid säkerställa en lämplig säkerhetsnivå i förhållande till de risker som ett elektroniskt utlämnande kan medföra. Formerna eller sätten för det elektroniska informationsutbytet mellan myndigheter kan se olika ut.

Vi har i avsnitt 18.6 tagit ställning till frågor om utlämnande och direktåtkomst i relation till ett identitetsindex. Vi bedömde där att vid införande av ett index bör elektroniskt utlämnande av uppgifter från indexet generellt sett vara tillåtet, medan direktåtkomst inte bör kunna medges. Fråga är om det finns ett behov av att reglera elektroniskt utlämnande eller direktåtkomst vad gäller biometrisk verifiering av identitet mot handlingar i enlighet med våra förslag. I detta sammanhang kan det påpekas att direktåtkomst är en form av elektroniskt utlämnande (se även avsnitt 18.6.2).

Det kan vid en biometrisk verifiering av identitet med stöd av den nya lagen finnas ett behov av att personuppgifter hanteras inte bara av den verifierande myndigheten, utan även av en tekniskt ansvarig aktör som tillhandahåller ett sådant system för verifiering som utvecklats och/eller förvaltas av denne, som vi beskriver i avsnitt 27.4. Det kan diskuteras om det överhuvudtaget är ett *utlämnande* av personuppgifter i dataskyddsförordningens mening när en verifierande myndighet skickar personuppgifter till ett tekniskt system, som tillhandahålls av en tekniskt ansvarig aktör, för att möjliggöra en verifiering med stöd av den nya lagen. Samma fråga gör sig även gällande när en tekniskt ansvarig aktör gör uppgifter tillgängliga för

en verifierande myndighet. För det fall bedömningen görs att det inte är ett utlämnande i aktuella situationer saknas det redan av den anledning skäl att införa bestämmelser om direktåtkomst eller elektroniskt utlämnande i den nya lagen. Om det däremot skulle anses vara fråga om ett utlämnande av personuppgifter i dessa situationer gör vi följande bedömning.

Vi har i avsnitt 24.4 föreslagit att de nya bestämmelserna om personuppgiftsbehandling ska tillämpas vid behandling av personuppgifter som utförs *i syfte att verifiera en persons identitet biometriskt* med stöd av den nya lagen. Det innebär att dessa bestämmelser blir tillämpliga när en verifierande myndighet behandlar personuppgifter – till exempel genom att lämna ut dem – i syfte att en persons identitet ska kunna verifieras biometriskt med stöd av lagen. Utan bestämmelser om direktåtkomst och elektroniskt utlämnande i den nya lagen blir det därmed upp till den verifierande myndigheten att avgöra på vilket sätt uppgifterna ska komma den tekniskt ansvarige aktören till del i den aktuella situationen, och vice versa. Med hänsyn till det begränsade ändamål för vilket personuppgifter enligt vårt förslag ska få behandlas med stöd av den nya lagen (se avsnitt 24.8) bedömer vi att detta är en rimlig ordning. För det fall våra förslag implementeras genom en sådan teknisk lösning som vi beskriver i avsnitt 27.4 kan vi konstatera att de personuppgifter som behandlas vid en biometrisk verifiering behöver göras tillgängliga i elektronisk form; systemet kan i annat fall inte användas. Någon bedömning för den verifierande myndigheten är det då i realiteten inte fråga om. Detta kan som vi ser det dock inte anses olämpligt, och bör inte ses som någon utökad risk i fråga om personuppgiftsbehandling, jämfört med vad som gäller enligt olika registerförfattningar som reglerar ärendeslag eller verksamheter där biometrisk verifiering enligt den nya lagen kan bli aktuell. Som exempel kan nämnas att det i 14 § folkbokföringsdatalagen (2026:126) anges att personuppgifter får lämnas ut elektroniskt om det inte är olämpligt. Enligt förarbetena till bestämmelsen avses med elektroniskt utlämnande såväl utlämnande genom direktåtkomst som annat elektroniskt utlämnande, till exempel utlämnande genom e-post. Bedömningen av om utlämnandet är olämpligt ska ske med beaktande av eventuella bestämmelser om sekretess, vad syftet med utlämnandet är, vem mottagaren är, vilka uppgifter det rör sig om samt om nödvändiga säkerhetsåtgärder är vidtagna. Elektroniskt utlämnande på andra sätt än genom direktåtkomst till andra offentliga

aktörer bör som utgångspunkt anses vara lämpligt. Vid utlämnande genom direktåtkomst är större restriktivitet påkallad.[26] En motsvarande bestämmelse finns i 15 § beskattningsdatalagen (2026:125), 14 § tulldatalagen (2026:127) och 15 § kronofogdedatalagen (2026:128). Enligt både 16 § domstolsdatalagen (2015:728) och 19 § kustbevakningsdatalagen (2019:429) får personuppgifter lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

En rättslig möjlighet att verifiera identitet biometriskt mot handlingar bygger inte på skapandet av en ny databas eller ett nytt register innehållande sökbara personuppgifter för framtida bruk, vilket däremot är fallet för ett identitetsindex. Tanken är inte heller att personuppgifter ska sparas i de tekniska system som behövs för biometrisk verifiering av identitet enligt den nya lagen; i den mån alfanumeriska uppgifter som kommit fram i samband med en verifiering behöver sparas får det ske i verifierande myndigheters befintliga ärendehanteringssystem. Som vi återkommer till i avsnitt 25.3.3 skyddas uppgifterna som lämnas till en tekniskt ansvarig aktör också av sekretess hos denne, och i kapitel 28 beskriver vi de åtgärder i fråga om informations- och cybersäkerhet som behöver beaktas vid implementeringen av en sådan teknisk lösning som vi beskriver i avsnitt 27.4. I avsnitt 29.4 bedömer vi även att privata aktörer inte bör ansvara för en myndighetsgemensam teknisk lösning; en tekniskt ansvarig aktör kommer därför – utifrån vår bedömning – att vara en myndighet.

Dessa omständigheter talar enligt vår mening samtliga mot att tillgängliggörande i elektronisk form av de personuppgifter som behövs vid biometrisk verifiering av identitet enligt den nya lagen skulle vara olämpligt, på det sätt som avses i ovan nämnda registerförfattningar. Vi kan i detta sammanhang även lyfta fram att det, som vi ser det, inte kommer att bli aktuellt med direktåtkomst för att en tekniskt ansvarig aktör ska få tillgång till de uppgifter som behövs för genomförandet av en verifiering; den verifierande myndigheten kommer i stället att initiera en verifieringsbegäran och i samband med det lämna de uppgifter den tekniskt ansvarige aktören behöver (se avsnitt 27.4.1). Inte heller framstår det som troligt att direktåtkomst behövs vad gäller en verifierande myndighets tillgång till uppgifter hos en tekniskt ansvarig aktör; resultatet av en genomförd verifiering samt tillhörande uppgifter bör i stället lämnas till den verifierande myndigheten när dessa uppgifter finns tillgängliga.

[26] Prop. 2025/26:88, s. 216.

Processen liknar därmed mer en så kallad fråga-svar-tjänst. Det är, enligt vår mening, dock inte uteslutet att en myndighetsgemensam teknisk lösning utformas på ett sådant sätt att en verifierande myndighet får direktåtkomst till enbart information om de verifieringar som denna myndighet har bestämt ska genomföras.

Mot den här bakgrunden bedömer vi att den nya lagen inte bör innehålla bestämmelser om direktåtkomst eller elektroniskt utlämnande.

25 Sekretess

25.1 Inledning

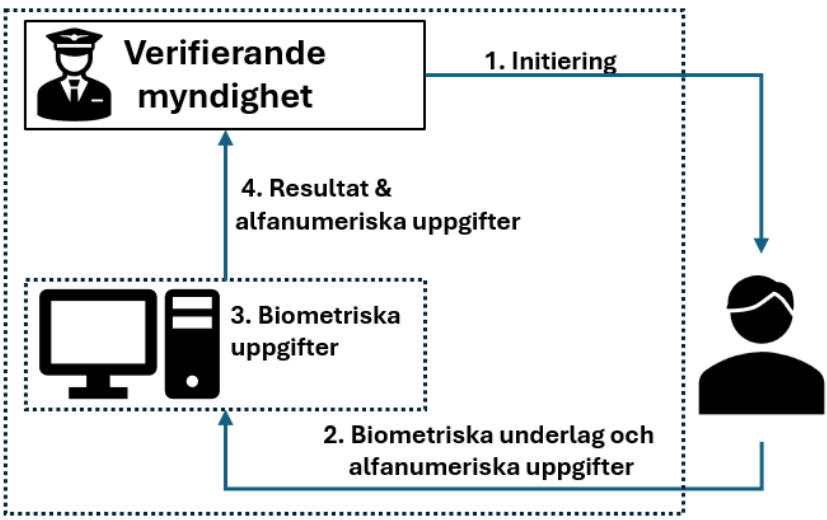
Införande av en generell möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar förutsätter en utvärdering av behovet av kompletterande reglering av sekretesskydd för de uppgifter om enskildas personliga förhållanden som behöver behandlas vid sådana kontroller. Det som behöver säkerställas är, som vi ser det, att våra författningsförslag kan genomföras utan hinder av sekretess och med tillräckligt skydd för aktuella uppgifter. Som vi pekar på i kapitel 27 kan våra författningsförslag komma att implementeras tekniskt på olika sätt, men vi redogör i nämnda kapitel för två huvudsakliga alternativ: en verifieringsprocess som bygger på användning av tekniska system som den myndighet som vill genomföra en verifiering med stöd av lagen (den verifierande myndigheten) ansvarar för, eller en teknisk lösning som bygger på myndighetsgemensamma komponenter i form av en mobilapplikation och ett backend-system som har utvecklats och/eller förvaltas av en tekniskt ansvarig aktör. Den senare skulle, som utgångspunkt, kunna vara såväl en annan myndighet som en enskild aktör. Vi utgår vid våra överväganden i detta kapitel från dessa två huvudsakliga verifieringsmodeller och tekniska lösningar, utan att ta ställning till vilka som faktiskt bör användas vid implementering av våra förslag.

Detta kapitel tar som sagt sikte på frågor om sekretess. Huruvida de uppgifter som förekommer i samband med en biometrisk verifiering med stöd av den nya lagen ingår i en allmän handling anser vi i första hand är en fråga för rättstillämparen; sådana överväganden kan kräva en bedömning av bland annat var uppgifterna ska anses förvarade i den mening som avses i 2 kap. tryckfrihetsförordningen (TF) och är som vi ser det inte av central betydelse i detta sammanhang. Vissa observationer görs dock i relevanta delar nedan.

25.2 Sekretess vid användning av den verifierande myndighetens system

Med en verifieringsprocess som bygger på att den verifierande myndigheten använder sådana tekniska lösningar – såväl hårdvara som mjukvara – som den själv har tagit fram eller upphandlat och ansvarar för, kommer samtliga uppgifter om enskilda som behövs för verifieringen att finnas hos den myndigheten. Flödet av uppgifter kan illustreras av figuren nedan.

Figur 25.1 Översikt av uppgiftsflöde



Alfanumeriska uppgifter om den vars identitet ska verifieras biometriskt kommer som utgångspunkt att finnas tillgängliga för den verifierande myndigheten i samband med att begäran om biometrisk verifiering initieras, vanligtvis i ett ärendehanteringssystem (1). Alfanumeriska uppgifter kommer också, tillsammans med biometriska underlag, att läsas in från den handling som används för verifieringen (2). De biometriska uppgifter som tas fram ur en ansiktsbild eller fingeravtryck kommer att behöva hanteras av den verifierande myndigheten i verifieringsprocessen (3), samt resultatet av den biometriska jämförelsen (4). Fråga är om det – genom befintliga sekretessbestämmelser eller på annat sätt – finns ett tillräckligt och ändamålsenligt skydd för dessa uppgifter hos den verifierande myndigheten.

25.2.1 Alfanumeriska uppgifter

Vår bedömning

Alfanumeriska uppgifter om enskilda som behövs för biometrisk verifiering av identitet enligt den nya lagen skyddas av bestämmelser om sekretess som är tillämpliga i den aktuella verksamheten hos den verifierande myndigheten. Det saknas därför behov av kompletterande sekretessbestämmelser.

En biometrisk verifiering med stöd av den nya lagen utgör som vi ser det en utredningsåtgärd som vidtas antingen vid handläggningen av ett ärende som omfattas av förvaltningslagens (2017:900) tillämpningsområde eller vid identitetskontroller i annat fall, inom ramen för myndighetens verksamhet. Det kan antas att alfanumeriska uppgifter av de slag som nämnts ovan, i samband med dessa situationer, registreras i ett ärendehanteringssystem eller antecknas på något annat sätt hos den verifierande myndigheten, oavsett om identiteten ska verifieras biometriskt; uppgifterna kommer vanligtvis att ha lämnats av den enskilde till myndigheten i samband med att ärendet inleddes eller att en identitetskontroll genomförs. I sistnämnda situation är det dock inte säkert att uppgifter om den person som kontrolleras dokumenteras av myndigheten. Uppgifter kan dock komma att registreras i ett datasystem eller antecknas på något annat sätt i samband med att en identitetskontroll genomförs som innebär att de ingår i en allmän handling hos myndigheten. Nämnda typer av alfanumeriska uppgifter behöver alltså normalt behandlas hos myndigheten i aktuella situationer, oberoende av om en biometrisk verifiering genomförs eller inte, bland annat för att ett ärende ska kunna hanteras på ett korrekt sätt. Vi föreslår därför inte heller att alfanumeriska uppgifter ska förstöras omedelbart när en kontroll har genomförts, på samma sätt som för biometriska underlag och biometriska uppgifter (se avsnitt 24.9).

Eftersom det är fråga om uppgifter av ett slag som – oavsett om en biometrisk verifiering genomförs – normalt redan hanteras av den verifierande myndigheten måste utgångspunkten, enligt vår mening, vara att det finns befintliga sekretessbestämmelser som blir tillämpliga i ärendehandläggningen eller i den faktiska verksamheten hos myndigheten. Som exempel kan nämnas 26 kap. 1 § offentlighets-

och sekretesslagen (2009:400) som anger att sekretess gäller *inom socialtjänsten* och 22 kap. 1 § som anger att sekretess gäller *i verksamhet som avser folkbokföringen*. För det fall en myndighet har ett behov av att verifiera identitet biometriskt enligt den nya lagen kan det därmed antas att de sekretessbestämmelser som är tillämpliga hos myndigheten eller i den aktuella verksamheten utgör ett tillräckligt skydd även för sådana alfanumeriska uppgifter om enskildas personliga förhållanden som behövs för att en verifiering ska kunna genomföras; uppgifterna behövs även i övrigt för handläggningen av det aktuella ärendet eller i den aktuella verksamheten.

Det finns alltså – som utgångspunkt – redan ett tillfredsställande sekretesskydd för denna typ av uppgifter, som till exempel namn och födelsetid. Det faktum *att* en biometrisk verifiering har genomförts och resultatet av den kan, enligt vår mening, inte heller anses vara en sådan känslig uppgift som behöver ett annat sekretesskydd än andra alfanumeriska uppgifter om den enskilde som hanteras av myndigheten. Detsamma gäller i de fall då en verifiering inte har kunnat genomföras av någon anledning. Detta med hänsyn till att en biometrisk verifiering enligt den nya lagen inte förutsätter att det finns omständigheter som gör att det finns anledning att misstänka identitetsmissbruk i ett enskilt fall (se avsnitt 23.6.3) och att det inte går att härleda något om anledningen till begäran om verifiering genom uppgifterna; att en biometrisk verifiering har genomförts avslöjar i princip inte något mer än att personen i fråga förekommer i ett ärende hos myndigheten eller har varit i kontakt med myndigheten på något annat sätt som har föranlett en identitetskontroll.

Styrkan på den sekretess som gäller för de aktuella uppgifterna kommer med detta synsätt att variera, beroende på i vilket ärendeslag och hos vilken myndighet de förekommer. Det är som vi ser det också en ändamålsenlig effekt.

Mot denna bakgrund saknas det enligt vår bedömning ett behov av kompletterande sekretessbestämmelser för att skydda alfanumeriska uppgifter som hanteras av den verifierande myndigheten vid en biometrisk verifiering med stöd av den nya lagen, som utförs med hjälp av tekniska system som myndigheten själv har tagit fram eller upphandlat och ansvarar för.

Verifiering på uppdrag av den verifierande myndigheten

Statens servicecenter är en statlig myndighet som erbjuder vägledning och service till enskilda för vissa myndigheters räkning. Statens servicecenter kan ingå serviceavtal med olika myndigheter om att för deras räkning utföra uppgifter enligt lagen (2019:212) om viss gemensam offentlig service. Statens servicecenter har redan i dag ingått serviceavtal med bland annat Skatteverket, Migrationsverket och Försäkringskassan. För Skatteverket och Migrationsverket är det bland annat fråga om att ta upp biometriska underlag och genomföra identitetskontroller, exempelvis i folkbokföringsärenden. Den myndighet som ansvarar för en viss förvaltningsuppgift har det rättsliga ansvaret för sina ärenden även efter att myndigheten ingått ett serviceavtal. Ärendehanteringen anses alltså ske inom ramen för den ursprungligt ansvariga myndighetens verksamhet även om vissa uppgifter de facto utförs av Statens servicecenter, och det rättsliga ansvaret för ärendehanteringen ligger inte på Statens servicecenter utan på till exempel Skatteverket.[1]

Om den verifierande myndigheten har ingått ett serviceavtal med Statens servicecenter om att utföra viss verksamhet för förstnämnda myndighets räkning, och en biometrisk verifiering av identitet genomförs inom ramen för detta uppdrag, kommer motsvarande sekretess som hos den verifierande myndigheten att gälla hos Statens servicecenter. Detta framgår av 40 kap. 7 c § offentlighets- och sekretesslagen. I förarbetena till bestämmelsen påpekades att de uppgifter som hanteras i de samverkande myndigheternas verksamhet generellt rör enskildas personliga och ekonomiska förhållanden och ofta kan antas vara av känslig art. Det fick därför inte finnas någon risk att situationer uppkommer då en handling lämnas ut av myndigheten som ansvarar för servicekontoret, trots att den skulle anses omfattas av sekretess hos den myndighet som ansvarar för det ärende som handlingen avser.[2] Bestämmelsen innebär alltså att uppgifter om enskilda får samma skydd hos Statens servicecenter som hos den verifierande myndigheten. Vi har ovan bedömt att det saknas ett behov av kompletterande sekretessbestämmelser för att skydda de alfanumeriska uppgifter om enskilda som kan förekomma hos den verifierande myn-

[1] *Samlad struktur för tillhandahållande av lokal statlig service,* prop. 2018/19:47, s. 14.
[2] A.a., s. 23 f.

digheten vid en kontroll med stöd av den nya lagen. Samma bedömning kan därmed göras avseende uppgifter hos Statens servicecenter.

25.2.2 Biometriska underlag och biometriska uppgifter

Vårt förslag

Sekretess ska gälla för uppgift i form av fingeravtryck eller ansiktsbild som har tagits upp med stöd av den nya lagen, och biometrisk uppgift som har tagits fram ur fingeravtrycket eller ansiktsbilden.

Bestämmelsen ska placeras i en ny paragraf i 40 kap. offentlighets- och sekretesslagen. En ny rubrik, *Biometrisk verifiering*, ska införas innan den nya bestämmelsen.

Den tystnadsplikt som följer av sekretessbestämmelsen ska inskränka rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Vid en biometrisk verifiering av identitet med stöd av den nya lagen behöver av naturliga skäl biometriska underlag och biometriska uppgifter som kan tas fram ur dem behandlas. Med hänsyn till uppgifternas karaktär är det enligt vår mening av stor vikt att det finns ett tydligt och tillräckligt skydd för uppgifterna som innebär att de inte obehörigen kan spridas.

Vi kan konstatera att enligt våra förslag i avsnitt 24.9 ska nämnda uppgifter förstöras omedelbart efter att en biometrisk verifiering enligt den nya lagen har genomförts. Varken de biometriska underlagen eller de biometriska uppgifterna ska alltså få lagras hos den verifierande myndigheten. I flera tidigare lagstiftningsärenden har en sådan ordning ansetts medföra att uppgifterna inte ingår i en allmän handling, med hänsyn till att de inte anses upprättade enligt 2 kap. 10 § TF, eftersom de varken expedieras eller tas om hand för arkivering. Som en följd av detta ansågs frågan om sekretess inte heller aktualiseras.[3] Vi är visserligen inte av någon annan uppfattning än att uppgifterna, som utgångspunkt, inte kommer att ingå i en allmän

[3] Jfr *Ökad säkerhet i pass m.m.*, prop. 2004/05:119, s. 43 ff., *Stärkt kontroll och kvalitet i folkbokföringen*, prop. 2021/22:217, s. 55 f., *Biometri – för en effektivare brottsbekämpning*, SOU 2023:32, s. 449 ff. och *Folkbokföringsverksamhet, biometri och brottsbekämpning*, SOU 2025:75, s. 441 f.

handling hos den verifierande myndigheten. Det är dock viktigt att hålla i minnet att sekretess innebär såväl handlingssekretess som tystnadsplikt, och gäller inte bara för uppgifter i allmänna handlingar utan även för uppgifter som finns hos en myndighet i sådana handlingar som ännu inte blivit allmänna (se 3 kap. 1 § offentlighets- och sekretesslagen). Förbud att röja eller utnyttja en uppgift enligt offentlighets- och sekretesslagen gäller, enligt 2 kap. 1 § första stycket, för myndigheter. Enligt bestämmelsens andra stycke gäller förbudet också för en person som fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet på grund av anställning eller uppdrag hos myndigheten, på grund av tjänsteplikt eller på annan liknande grund. Befattningshavare får alltså inte låta någon annan ta del av en hemlig uppgift vare sig det sker genom att allmän handling företes eller att någon får ta del av en handling som inte är allmän, eller att till exempel ett hemligt föremål förevisas för någon.[4] Att de biometriska underlag och biometriska uppgifter som förekommer hos den verifierande myndigheten, i samband med en kontroll med stöd av den nya lagen, inte är allmänna handlingar leder alltså inte ensamt till slutsatsen att det saknas ett behov av en sekretessbestämmelse som kan skydda uppgifterna.

Det behövs en kompletterande sekretessbestämmelse

Med undantag för ett fåtal myndigheter som redan i dag har rättsligt stöd för behandling av biometriska underlag och biometriska uppgifter – däribland Migrationsverket och Skatteverket – är det fråga om typer av uppgifter som i nuläget normalt inte förekommer i de ärendeslag där biometrisk verifiering med stöd av den nya lagen kan komma att aktualiseras, eller i myndigheternas verksamhet överhuvudtaget. I de fall sådana uppgifter i dagsläget inte förekommer hos den verifierande myndigheten är det därför inte säkert att tillämpliga sekretessbestämmelser ger ett tillräckligt skydd för denna typ av uppgifter; sekretessregelverket är helt enkelt inte utformat med hänsyn till att sådana uppgifter ska hanteras i ärendeslaget eller verksamheten. Detta talar som vi ser det tydligt för att det finns behov av en kompletterande sekretessbestämmelse.

[4] Prop. 1979/80:2, *med förslag till sekretesslag m.m.,* del A, s. 119.

De biometriska underlagen och de biometriska uppgifter som tas fram ur dessa ska – med utgångspunkt i våra förslag – endast hanteras momentant i samband med att verifieringen genomförs. Det kan vidare förutsättas att hanteringen sköts maskinellt; en biometrisk jämförelse behöver alltid göras med hjälp av datorstödda algoritmer och funktioner. Dessa tekniska aspekter talar därför i sig mot att det skulle finnas någon konkret risk för att uppgifterna faktiskt kan spridas på ett obehörigt sätt, och därmed mot ett behov av en sekretessbestämmelse som uppnår detta. Det är som vi ser det emellertid inte lämpligt att göra skyddet för biometriska underlag och biometriska uppgifter avhängigt av den tekniska lösningen, och ett antagande att handläggare vid den verifierande myndigheten i praktiken inte tar del av sådana uppgifter. Det kan mycket väl vara så att tekniska system som finns hos en viss verifierande myndighet är utformade just för att göra detta möjligt, exempelvis för att en företrädare för myndigheten ska kunna göra en manuell granskning, utöver den maskinella jämförelsen. Även om en teknisk spärr byggs in i systemen som syftar till att hindra eller begränsa tillgång till de biometriska underlagen och de biometriska uppgifterna, kan det inte fullt ut säkerställas att sådana spärrar ändå inte kringgås på teknisk väg. I betänkandet *Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering* lyftes, i fråga om utkontraktering av it-drift, fram att ”det finns inga nu kända säkerhetsåtgärder som gör det helt, både i teori och praktik, omöjligt för en tjänsteleverantör att ta del av uppgifterna. De tekniska säkerhetsåtgärderna medför alltså endast att det blir mer osannolikt att tjänsteleverantören tar del av uppgifterna i jämförelse med vad som skulle ha varit fallet om åtgärderna inte hade vidtagits.”[5] Vi anser att det är mycket viktigt att det, om personal på den verifierande myndigheten – behörigen eller obehörigen – får tillgång till uppgifter av nu aktuellt slag, i vart fall finns ett tillräckligt rättsligt skydd mot att uppgifterna sprids. Detta inte minst med hänsyn till att biometriska underlag kan vara särskilt värdefulla uppgifter för en extern antagonist, till exempel en hackare eller en fientlig stat, att få tillgång till, då de skulle kunna användas exempelvis för att framställa falska handlingar av olika slag.

Vid en sammantagen bedömning anser vi att det behöver införas en bestämmelse om sekretess som skyddar ansiktsbilder och fingeravtryck som tagits upp med stöd av den nya lagen, och de biometriska

[5] SOU 2021:1, s. 282.

uppgifter som har tagits fram ur dessa. Med uttrycket *tagits upp med stöd av lagen* omfattas såväl de biometriska underlag som tagits upp från den person vars identitet ska verifieras som de biometriska underlag som lästs in från ett lagringsmedium i eller en synlig ansiktsbild på den handling som används för verifieringen. Vidare saknar det betydelse för bestämmelsens tillämpning om de biometriska underlagen tas upp vid personlig inställelse eller på distans, till exempel genom att den enskilde använder en mobilapplikation.

Eftersom uppgifterna inte ska få lagras efter kontrollen eller användas i något annat syfte än att genomföra en biometrisk verifiering enligt den nya lagen anser vi att det helt saknas ett insynsintresse – till skillnad från exempelvis vad som gäller för folkbokföringsverksamheten – som motiverar att annat än absolut sekretess ska gälla för uppgifterna. Behovet av insyn gör sig, som vi ser det, i första hand gällande i det ärendeslag eller i den verksamhet i vilket den biometriska kontrollen genomförs. Att uppgifterna är av sådant slag att obehörig spridning av dem kan medföra ett intrång i den enskildes integritet (jfr avsnitt 21.7.3) talar i samma riktning. Vi anser alltså att bestämmelsen ska utformas utan något skaderekvisit.

Sekretessen ska, enligt vår bedömning, gälla oavsett i vilken situation en biometrisk verifiering med stöd av den nya lagen genomförs, och utan hänsyn till om uppgifterna förekommer hos den verifierande myndigheten eller hos någon annan, företrädesvis en tekniskt ansvarig aktör som är en myndighet (se avsnitt 25.3). Bestämmelsen bör därför utformas så att sekretess gäller för uppgift i form av fingeravtryck eller ansiktsbild som tagits upp med stöd av den nya lagen, och de biometriska uppgifter som tagits fram ur fingeravtrycket eller ansiktsbilden. Tillämpningen knyts därmed till användning i sig av biometrisk verifiering enligt den nya lagen, inte till en viss myndighets verksamhet eller ett visst ärendeslag.

Eftersom vi ovan bedömt att uppgifterna sannolikt inte kommer att ingå i en allmän handling behöver det inte anges någon längsta tid som sekretessen ska gälla.

Bestämmelsens placering

Frågan är var i offentlighets- och sekretesslagen en bestämmelse med ovan föreslagna lydelse bör placeras. Ett alternativ skulle kunna vara 21 kap., som innehåller bestämmelser om sekretess som tar sikte på uppgift om enskilds personliga förhållanden, oavsett i vilket sammanhang uppgiften förekommer. De uppgifter om biometriska underlag och biometriska uppgifter som ska skyddas av den nu aktuella bestämmelsen kommer emellertid att förekomma endast i en specifik situation, nämligen vid biometrisk verifiering enligt den nya lagen, även om den kan tillämpas av en bred krets av myndigheter. Vi anser därför att bestämmelsen inte bör placeras i 21 kap.

I stället anser vi att den lämpligen bör införas efter 40 kap. 5 §, som reglerar sekretess för uppgifter i verksamhet för enbart teknisk bearbetning eller teknisk lagring (vi återkommer i avsnitt 25.3 till sistnämnda bestämmelse); beroende på vilken teknisk lösning som används – utifrån de två tekniska huvudalternativ som vi beskriver i avsnitt 27.3 och 27.4 – kan antingen bestämmelsen i 40 kap. 5 § eller den bestämmelse som vi nu föreslår komma att bli tillämplig. Att placera dem i anslutning till varandra framstår därför som ändamålsenligt. Lydelsen av rubriken på 40 kap. – *Sekretess till skydd för enskild hos övriga myndigheter och i övriga verksamheter* – talar enligt vår mening inte heller mot en sådan placering. För att tydliggöra att den nya bestämmelsen avser biometrisk verifiering anser vi att en rubrik med den ordalydelsen ska införas innan bestämmelsen.

Inskränkt meddelarfrihet

Den rätt att meddela och offentliggöra uppgifter (meddelarfrihet) som framgår av 1 kap. 1 § och 7 § första stycket TF samt 1 kap. 1 § första stycket och 10 § första stycket yttrandefrihetsgrundlagen innebär en rätt att lämna uppgifter, även sådana som omfattas av sekretess eller tystnadsplikt, för offentliggörande i tryckt skrift, program eller genom tekniska upptagningar. Tanken med meddelarfriheten är att samhällsdebatten inte ska berövas uppgifter som är mycket betydelsefulla från allmän synpunkt av den anledningen att uppgifterna är sekretessbelagda av hänsyn till ett intresse som just i det aktuella sammanhanget väger mindre tungt. Som grundprincip gäller att stor återhållsamhet bör iakttas vid prövningen av om undantag

från meddelarfrihet ska göras i ett enskilt fall. Den aktuella sekretessbestämmelsens konstruktion kan ge viss vägledning; när det är fråga om bestämmelser om absolut sekretess kan det finnas större anledning att överväga undantag från meddelarfriheten än i andra fall.[6]

Vi har ovan föreslagit att de biometriska underlag och biometriska uppgifter som tas fram med stöd av den nya lagen ska skyddas med absolut sekretess, bland annat med hänsyn till att vi bedömer att det saknas ett insynsintresse avseende dessa uppgifter. Att en myndighet väljer att genomföra en biometrisk verifiering med stöd av den nya lagen, i vissa typsituationer eller i ett enskilt fall, skulle visserligen kunna vara av intresse för allmänheten. Vi har emellertid svårt att se att de biometriska underlagen och de biometriska uppgifterna i sig är betydelsefulla från allmän synpunkt.

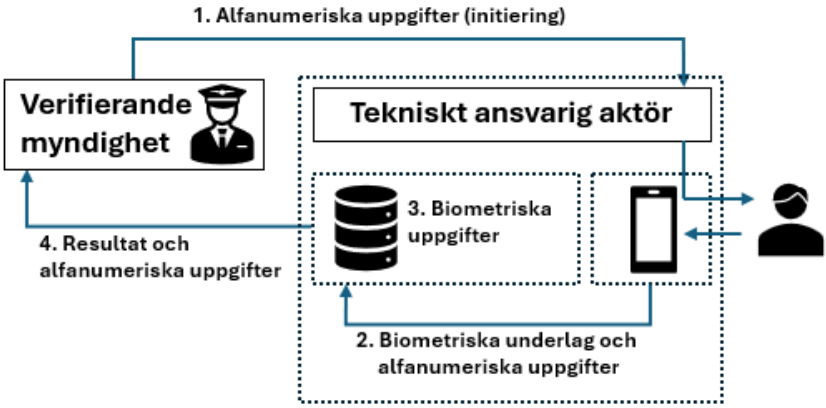
Vid en sammantagen bedömning anser vi att den tystnadsplikt som följer av den föreslagna sekretessbestämmelsen ska inskränka rätten att meddela och offentliggöra uppgifter.

25.3 Sekretess vid användning av myndighetsgemensamma system

Om biometrisk verifiering av identitet enligt den nya lagen genomförs med hjälp av en teknisk lösning som bygger på myndighetsgemensamma komponenter i form av ett backend-system och en mobilapplikation som har utvecklats och förvaltas av en tekniskt ansvarig aktör, kommer de uppgifter om enskilda som behövs för verifieringen att finnas dels hos den verifierande myndigheten, dels hos den tekniskt ansvarige aktören. Flödet av uppgifter i ett sådant system kan illustreras av följande figur.

[6] Prop. 1979/80:2, Del A, s. 104 f.

Figur 25.2 Översikt av uppgiftsflöde



Alfanumeriska uppgifter om den vars identitet ska verifieras biometriskt behöver lämnas ut till den tekniskt ansvarige aktören (1). Mobilapplikationen läser därefter in alfanumeriska uppgifter och biometriska underlag från handlingen, och en ansiktsbild tas upp med hjälp av applikationen (2). De alfanumeriska uppgifterna och de biometriska uppgifter som tas fram ur ansiktsbilden (3) kommer alltså att finnas hos den tekniskt ansvarige aktören. Den verifierande myndigheten behöver därefter få del av resultatet av den biometriska jämförelsen och alfanumeriska uppgifter om identitet och identitetsbeteckning (4).

I detta avsnitt tar vi ställning till om det finns ett tillräckligt skydd för dessa uppgifter hos den tekniskt ansvarige aktören, och om det finns stöd för att lämna uppgifter mellan denne och den verifierande myndigheten. Av central betydelse för bedömningen är om ett backend-system och en mobilapplikation av sådant slag vi redogör för i avsnitt 27.4 utgör en funktion för teknisk bearbetning av uppgifter, i den mening som avses bland annat i 10 kap. 2 a § och 40 kap. 5 § offentlighets- och sekretesslagen.

25.3.1 Särskilt om teknisk bearbetning

Vår bedömning

En tekniskt ansvarig aktörs befattning med uppgifter i ett backendsystem och i en mobilapplikation, som denne tillhandahåller i syfte att en biometrisk verifiering enligt den nya lagen ska kunna genomföras, bör ses som teknisk bearbetning av uppgifter för den verifierande myndighetens räkning.

Vi kan konstatera att det saknas en legaldefinition av begreppet *teknisk bearbetning*. I 10 kap. 2 a § och 40 kap. 5 § offentlighets- och sekretesslagen, som nämnts ovan, förekommer även begreppet *teknisk lagring*. Med hänsyn till att inga uppgifter ska lagras av den tekniskt ansvarige aktören vid en biometrisk verifiering med stöd av den nya lagen kommer vi dock här att begränsa oss till att belysa vad som avses med teknisk bearbetning.

Begreppet teknisk bearbetning är ett funktionsbaserat och teknikneutralt begrepp, som avgränsas genom en kombination av materiella och funktionella rekvisit. Vilka typer av funktioner som kan utgöra teknisk bearbetning kan komma att förändras över tid med anledning av den tekniska utvecklingen. Exempel på vad som kan omfattas är överföring av information från ett medium till ett annat, överföring från en pappershandling till magnetband eller framkallning av fotografi, men även teknisk infrastruktur eller en teknisk plattform för it-drift kan omfattas, samt tillhandahållande av en it-baserad funktion, exempelvis en applikation eller en standardiserad eller anpassad digital tjänst.[7] I vägledning från eSam (ett medlemsdrivet program för samverkan mellan myndigheter) anges att enligt deras uppfattning finns det ett relativt stort utrymme avseende vilka it-tjänster som kan innefattas i begreppet teknisk bearbetning.[8]

Centralt för att det ska vara fråga om teknisk bearbetning enligt ovan nämnda bestämmelser är att befattningen med uppgifterna *endast* ska vara teknisk, utan ett eget innehållsmässigt inflytande eller självständigt ändamål hos den som utför bearbetningen; nämnda rekvisit framgår direkt av såväl 10 kap. 2 a § och 40 kap. 5 § offentlighets-

[7] Se Regeringens proposition om *nya grundlagsbestämmelser angående allmänna handlingars offentlighet*, prop. 1975/76:160, s. 137 och *Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter*, prop. 2019/20:201, s. 6 och 22.
[8] *Utkontraktering – sekretess och dataskydd*, ES2023-06, s. 17.

och sekretesslagen som av 1 § lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (tystnadspliktslagen). Det är inte tillräckligt att en viss åtgärd *kan* beskrivas som teknisk utan den får inte kombineras med andra moment som innebär saklig bearbetning eller egen användning av uppgifterna. Om den aktör som bearbetar uppgifterna exempelvis använder dem för statistik, utveckling eller andra egna ändamål faller verksamheten utanför begreppet. Av Högsta förvaltningsdomstolens avgörande HFD 2018 ref. 48 framgår även bland annat att för att rekvisitet ska vara uppfyllt krävs att det ska finnas såväl tekniska som administrativa begränsningar för den egna personalens tillgång till uppgifterna så att dessa inte är tillgängliga i läsbart skick (jfr även RÅ 1994 ref. 64, där central datalagring godtogs eftersom den som tekniskt lagrade uppgifterna saknade dispositionsrätt till informationen). Bearbetningen ska vidare ske för *någon annans räkning*. Det förutsätter ett uppdragsförhållande. Detta uppdrag kan följa av en överenskommelse eller framgå av en författning. Vidare förutsätts att det är uppdragsgivande myndighet som rättsligt kan anses förfoga över uppgifterna.[9] Den som ska bearbeta uppgifterna tekniskt får alltså inte ha ett självständigt förfogande eller egen rättslig kontroll över informationen.

Med utgångspunkt i det ovan anförda anser vi att en tekniskt ansvarig aktörs befattning med uppgifter i ett gemensamt backend-system och en mobilapplikation bör ses som endast teknisk bearbetning av uppgifter för den verifierande myndighetens räkning. Vi bygger vår bedömning på följande skäl.

Att det i ett sådant system som vi beskriver i avsnitt 27.4 är fråga om bearbetning av teknisk natur får som vi ser det anses givet; det är en helt maskinell bearbetning, även om upptagningen av ansiktsbilden och läsningen av den handling som används för verifieringen förutsätter vissa manuella åtgärder av den enskilde. Den tekniskt ansvarige aktören ska däremot inte utföra några manuella jämförelser eller annan bearbetning av uppgifterna utan vi förutsätter att det görs helt och hållet i backend-systemet och/eller i mobilapplikationen, på det sätt som vi beskriver i nyss nämnda avsnitt.

När det gäller kravet på att bearbetning ska ske för någon annans räkning är vår utgångspunkt att en tekniskt ansvarig aktör inte ska

[9] *Säker och kostnadseffektiv id-drift – förslag till varaktiga former för samordnad statlig it-drift*, SOU 2021:97, s. 259.

kunna använda uppgifterna för egen del. Det får förutsättas att tekniska system och it-drift som tillhandahålls av aktören utformas på ett sådant sätt att det finns nödvändiga tekniska och administrativa begränsningar för att upprätthålla kravet på att det inte ska finnas ett självständigt förfogande eller egen rättslig kontroll över informationen. Att ansiktsbild och alfanumeriska uppgifter tas upp med hjälp av mobilapplikationen på den enskildes enhet, och det därmed skulle kunna hävdas att uppgifterna inte kan anses som utlämnade till den tekniskt ansvarige aktören från den verifierande myndigheten eftersom de aldrig har funnits hos den sistnämnda, utgör som vi ser det inte hinder mot att det kan vara fråga om teknisk bearbetning för den verifierande myndighetens räkning, och leder inte heller till slutsatsen att den tekniskt ansvarige aktören, endast av den anledningen, anses självständigt kunna förfoga över uppgifterna.

När det gäller biometriska underlag och biometriska uppgifter ska dessa – enligt våra förslag i avsnitt 24.9 – förstöras omedelbart efter att kontrollen har genomförts, vilket indirekt medför att de inte får eller kan användas eller lagras av den tekniskt ansvarige aktören för egen räkning. Inte heller de alfanumeriska uppgifterna som förekommer vid en biometrisk verifiering enligt den nya lagen ska få användas eller lagras av den tekniskt ansvarige aktören. Att den tekniskt ansvarige aktören saknar en egen förfogandemöjlighet över uppgifterna följer enligt vår mening även av att det är den verifierande myndigheten som är att se som rättsligt ansvarig för den biometriska verifieringen. Som vi anfört i avsnitt 24.6 är det den myndigheten som bestämmer såväl ändamål som medlen för den behandling av personuppgifter som utförs vid en biometrisk verifiering med stöd av den nya lagen. Det är också den myndigheten som tar ställning till om en sådan utredningsåtgärd alls är nödvändig. Att det är den verifierande myndigheten som är rättsligt ansvarig för verifieringsprocessen och uppgifterna bör som vi ser det också kunna tydliggöras för den vars identitet ska verifieras genom att det i mobilapplikationen – på liknande sätt som vid användning av mobilt BankID – anges att det är den verifierande myndigheten som har initierat begäran, inte den tekniskt ansvarige aktören.

Redan att det är den verifierande myndigheten som, i det enskilda fallet, bestämmer att en biometrisk verifiering ska genomföras, och att verifieringen därefter *utförs* med hjälp av system som en tekniskt ansvarig aktör tillhandahåller, bör enligt vår mening kunna anses visa

att det är fråga om ett uppdragsförhållande, på det sätt som förutsätts för att det ska vara fråga om teknisk bearbetning i den mening som avses bland annat i 40 kap. 5 §§ offentlighets- och sekretesslagen. Uppdragsförhållandet bör som vi ser det även kunna klargöras på förhand genom att det framgår av instruktionen för den myndighet som i ett senare skede eventuellt får ansvar för att tillhandahålla en myndighetsgemensam teknisk lösning. Ett särskilt uppdragsavtal mellan den verifierande myndigheten och en tekniskt ansvarig aktör skulle också kunna upprättas, i likhet med de serviceavtal som kan upprättas mellan Statens servicecenter och myndigheter, enligt lagen om viss gemensam offentlig service.

25.3.2 Utlämnande av uppgifter till en tekniskt ansvarig aktör

Vår bedömning

En myndighet som vill verifiera identitet biometriskt med stöd av den nya lagen bör, som utgångspunkt, kunna lämna ut de uppgifter som behövs för att kontrollen ska kunna genomföras till en annan myndighet eller till en privat aktör, enligt 10 kap. 2 a § offentlighets- och sekretesslagen. En bedömning behöver dock göras innan ett sådant utlämnande faktiskt görs.

De alfanumeriska uppgifter som kan behövas för att initiera verifieringsprocessen behöver lämnas ut till den tekniskt ansvarige aktören (se avsnitt 27.4.1). Eftersom sådana uppgifter i många fall omfattas av sekretess (se avsnitt 25.2.1), krävs att det finns en tillämplig sekretessbrytande bestämmelse för att så ska få ske; en uppgift som omfattas av sekretess och som görs tillgänglig för en tjänsteleverantör för teknisk bearbetning eller teknisk lagring betraktas som utlämnad eller röjd i offentlighets- och sekretesslagens mening.[10] För det fall de biometriska underlag som tas upp med hjälp av en mobiltelefon från den enskilde och från handlingen, och de biometriska uppgifter som tas fram ur dem, bedöms vara förvarade hos och därmed även utlämnade från den verifierande myndigheten, kommer dessa upp-

[10] *Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring av uppgifter*, prop. 2022/23:97, s. 7.

gifter – utifrån vårt förslag i avsnitt 25.2.2 – också att omfattas av sekretess.

Utlämnande enligt 10 kap. 2 a § offentlighets- och sekretesslagen

Den sekretessbrytande bestämmelse som, utifrån bedömningen i föregående avsnitt, bör kunna vara tillämplig är 10 kap. 2 a § offentlighets- och sekretesslagen, som anger att sekretess inte hindrar att en uppgift lämnas till en enskild eller till en annan myndighet som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut. Att en uppgift inte får lämnas ut om det med hänsyn till omständigheterna är olämpligt innebär, enligt förarbetena till bestämmelsen, att en myndighet, innan en uppgift lämnas ut, ska pröva om det finns skäl som talar mot att den lämnas ut. Omständigheter som ska beaktas är som utgångspunkt sådana som har koppling till den utlämnande myndigheten och till uppgiftsmottagaren likväl som till de uppgifter som är eller kan bli föremål för utlämnande. Det ska göras en allsidig prövning av alla omständigheter som är relevanta i det enskilda fallet. Omständigheter som kan ha betydelse är exempelvis vilken typ av uppgifter det rör sig om, vilka intressen som ligger till grund för sekretessen och uppgifternas omfattning. En omständighet som med viss tyngd kan tala mot ett utlämnande är att det är fråga om uppgifter av särskilt känsligt slag, exempelvis uppgifter av synnerlig betydelse för rikets säkerhet när det gäller totalförsvaret. Det bör även beaktas vilka åtgärder som uppgiftsmottagaren vidtar för att skydda uppgifterna och om denne omfattas av en lag- eller avtalsreglerad tystnadsplikt.[11]

De uppgifter som kan behöva lämnas ut till en tekniskt ansvarig aktör kan även omfatta känsliga personuppgifter i form av biometriska uppgifter. Dessa får anses särskilt skyddsvärda. Det måste samtidigt beaktas att de är helt nödvändiga för att en biometrisk verifiering enligt den nya lagen ska kunna genomföras, och i synnerhet att de – enligt våra förslag i avsnitt 24.9 – ska förstöras omedelbart efter kontrollen. När det gäller de alfanumeriska uppgifter som behöver lämnas ut till en tekniskt ansvarig aktör kan de enligt vår mening normalt

[11] Prop. 2022/23:97, s. 17.

sett inte anses skyddsvärda på ett sätt som gör att det är olämpligt att lämna ut dem med stöd av 10 kap. 2 a § offentlighets- och sekretesslagen; de kan i vart fall inte anses ha synnerlig betydelse för rikets säkerhet när det gäller totalförsvaret. En tekniskt ansvarig aktör ska inte på något sätt kunna ta del av någon av uppgifterna som har lämnats ut på ett sätt som innebär att de kan användas för egen del, utan de ska endast tekniskt bearbetas, momentant och maskinellt. Som vi återkommer till i avsnitt 25.3.3 och 25.3.4 kommer samtliga uppgifter som lämnas ut för teknisk bearbetning också att omfattas av tystnadsplikt i form av absolut sekretess, enligt 40 kap. 5 § offentlighets- och sekretesslagen eller, om den tekniskt ansvarige aktören är ett privat företag, av 4 § tystnadspliktslagen. I förarbetena till tystnadspliktslagen påtalas visserligen att riskerna med en utkontraktering inte alltid elimineras eller ens minimeras med hjälp av bestämmelsen i tystnadspliktslagen.[12] I sin vägledning anför eSam emellertid att man uppfattar att det straffrättsliga ansvar som anställda har enligt en lagstadgad tystnadsplikt ändå bör ha viss tyngd vid olämplighetsbedömningen.[13]

De särskilda intressen som ligger bakom utlämnandet kan, som vi nämnt, också beaktas. Utlämnandet behövs för att kunna genomföra en biometrisk verifiering enligt den nya lagen, som syftar till att ge myndigheter utökade möjligheter att motverka identitetsmissbruk, vilket utgör ett viktigt allmänt intresse (se bland annat avsnitt 21.7.3). Det bör även finnas möjlighet att genom avtal – särskilt för det fall den tekniskt ansvarige aktören är ett privat företag – närmare reglera villkoren för dennes befattning med uppgifterna, på det sätt som vi pekat på i föregående avsnitt. Även skyddsåtgärder av informationssäkerhetsslag bör kunna regleras, för att säkerställa ett tillräckligt skydd även i sådana hänseenden (se kapitel 28).

Sammantaget anser vi att det – som utgångspunkt – inte är olämpligt för en verifierande myndighet att med stöd av bestämmelsen i 10 kap. 2 a § offentlighets- och sekretesslagen lämna ut de uppgifter som behövs för att en biometrisk verifiering ska kunna genomföras till en tekniskt ansvarig aktör. En bedömning måste emellertid göras utifrån de förhållanden som gör sig gällande för den tekniskt ansvarige aktör som får ansvar för att tillhandahålla ett backend-system och en mobilapplikation, oavsett om det är en myndighet eller en privat

[12] Prop. 2019/20:201, s. 12.
[13] eSam, *Utkontraktering – sekretess och dataskydd*, s. 29.

aktör. Det bör lyftas fram att avsikten inte är att den verifierande myndigheten ska göra en sådan bedömning i varje enskilt fall, utan att nödvändiga ställningstaganden görs på förhand, i samband med att en viss teknisk aktör utses. Nödvändiga begränsningar i hur uppgifterna får användas kan då också regleras i avtal.

25.3.3 Skydd för uppgifter hos en tekniskt ansvarig aktör

Vår bedömning

Uppgifter om enskilda som behövs för biometrisk verifiering enligt den nya lagen och som förekommer hos en tekniskt ansvarig aktör skyddas bland annat av befintliga bestämmelser om sekretess och tystnadsplikt avseende teknisk bearbetning. Det saknas därför behov av kompletterande bestämmelser om sekretess eller tystnadsplikt.

Med utgångspunkt i vår bedömning i avsnitt 25.3.1 kommer de uppgifter som förekommer i ett backend-system och i en mobilapplikation, i syfte att en biometrisk verifiering med stöd av den nya lagen ska kunna genomföras, att omfattas av bestämmelsen i 40 kap. 5 § offentlighets- och sekretesslagen, om den tekniskt ansvarige aktören är en myndighet. Bestämmelsen anger att sekretess gäller för uppgift om en enskilds personliga eller ekonomiska förhållanden i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning. Om den tekniskt ansvarige aktören är ett privat företag gäller i stället 4 § tystnadspliktslagen, som innehåller ett motsvarande skydd. I båda fallen är det fråga om absolut sekretess respektive tystnadsplikt. Dessa bestämmelser omfattar såväl de alfanumeriska uppgifter som de uppgifter i form av biometriska underlag och biometriska uppgifter som behöver hanteras vid en biometrisk verifiering med stöd av den nya lagen.

Nämnda bestämmelser innehåller som vi ser det ett tillräckligt skydd för uppgifterna hos den teknisk ansvarige aktören. Det saknas därför ett behov av någon kompletterande sekretessbestämmelse. När det gäller de ansiktsbilder och fingeravtryck som tagits upp med stöd av den nya lagen, och de biometriska uppgifter som tagits fram ur dessa, har vi dessutom i avsnitt 25.2.2 föreslagit att en ny bestäm-

melse ska införas, som anger att sekretess gäller för dessa uppgifter, utan någon skadeprövning. Den föreslagna bestämmelsen är utformad på så sätt att tillämpningen knyts till användning av biometrisk verifiering enligt den nya lagen i sig, inte till en viss verksamhet eller ett visst ärendeslag. Bestämmelsen bör därför kunna omfatta även uppgifter av nyss nämnda slag som förekommer hos den tekniskt ansvarige aktören, om denne är en myndighet. Detta talar ytterligare mot att en kompletterande bestämmelse om sekretess behöver införas.

25.3.4 Utlämnande av uppgifter från en tekniskt ansvarig aktör till den verifierande myndigheten

Vår bedömning

Det finns inga hinder mot att den verifierande myndigheten får ta del av uppgifter som är hänförliga till en genomförd biometrisk jämförelse från den tekniskt ansvarige aktören.

De uppgifter som förekommer hos den tekniskt ansvarige aktören i samband med verifieringsprocessen kommer, som vi redogjort för i föregående avsnitt, att omfattas av absolut sekretess. När det gäller de alfanumeriska uppgifterna kommer sekretessen därmed i de flesta fall att vara strängare än för motsvarande typer av uppgifter hos den verifierande myndigheten, i det ärendeslag eller den verksamhet som verifieringen genomförs i. Att den verifierande myndigheten skulle vara förhindrad att ta del av uppgifterna efter bearbetningen med hänsyn till sekretess – enbart på grund av att dessa uppgifter har befunnit sig hos den tekniskt ansvarige aktören för myndighetens räkning – är enligt vår mening svårt att förena med syftet med bestämmelserna om teknisk bearbetning i såväl offentlighets- och sekretesslagen som 2 kap. TF. Bestämmelserna i 40 kap. 5 § offentlighets- och sekretesslagen och 4 § tystnadspliktslagen måste rimligtvis syfta till att skydda uppgifterna, under tiden de är föremål för teknisk bearbetning, i förhållande till *andra* än den myndighet för vars räkning den tekniska bearbetningen görs. Något skyddsintresse i förhållande till sistnämnda myndighet har vi svårt att se. I förarbetena till bestämmelsens föregångare finns vidare uttalanden som talar för att den myndighet som endast tekniskt bearbetar uppgifter får lämna ut uppgifter till upp-

dragsgivare i enlighet med myndighetens åtagande enligt uppdraget.[14] Under alla omständigheter kan det svårligen vara fråga om att den tekniskt ansvarige aktören obehörigen röjer några uppgifter, i förhållande till den verifierande myndigheten enligt 4 § tystnadspliktslagen.

Redan det ovan anförda talar, som vi ser det, för att det saknas hinder mot att den verifierande myndigheten tar del av uppgifter från den tekniskt ansvarige aktören, som är hänförliga till en biometrisk jämförelse som genomförts på uppdrag av myndigheten. Som vi redogjort för i avsnitt 25.3.1 anser vi vidare att den verifierande myndigheten har rättslig rådighet och ansvar för de uppgifter som behövs för att en biometrisk verifiering med hjälp av den nya lagen ska kunna genomföras; upptagningen och den tekniska bearbetningen av uppgifterna utförs för den verifierande myndighetens räkning, på uppdrag av denna. Det skulle därför enligt vår mening närmast kunna ses som ett *återlämnande* av uppgifterna till den verifierande myndigheten. Vi kan vidare notera att i praxis avseende rätt att ta del av allmänna handlingar har en handling som finns hos ett privaträttsligt subjekt ansetts vara förvarad hos den uppdragsgivande myndigheten när handlingen har mottagits eller upprättats för myndighetens räkning, trots att den aldrig har kommit in till eller funnits hos myndigheten (se Högsta förvaltningsdomstolen avgöranden RÅ 1984 2:49, RÅ 1989 ref. 29, RÅ 1996 ref. 25 och HFD 2017 ref. 15). Motsvarande synsätt bör enligt vår mening kunna göras gällande avseende uppgifter som finns hos en tekniskt ansvarig aktör endast för teknisk bearbetning, i ett backend-system och en mobilapplikation som denne tillhandahåller. Med en sådan utgångspunkt skulle det kunna hävdas att det inte ens är fråga om ett *överlämnande* av uppgifter från den tekniskt ansvarige aktören, eftersom uppgifterna hela tiden får anses – åtminstone rättsligt – ha befunnit sig hos den verifierande myndigheten.

Om bedömningen ändå görs att den tekniskt ansvarige aktören behöver *lämna ut* uppgifter om resultatet av den biometriska jämförelsen och alfanumeriska uppgifter – bland annat om identitet och identitetsbeteckning – till den verifierande myndigheten, anser vi att detta kan göras med stöd av den sekretessbrytande bestämmelsen i 10 kap. 2 § offentlighets- och sekretesslagen, under förutsättning att den tekniskt ansvarige aktören är en myndighet. I avsnitt 29.4 bedömer vi att privata aktörer *inte* bör ansvara för en myndighets-

[14] Prop. 1979/80:2, Del A, s. 21 och 272.

gemensam teknisk lösning. Enligt 10 kap. 2 § offentlighets- och sekretesslagen hindrar sekretess inte att en uppgift lämnas till en enskild eller till en annan myndighet, under förutsättning att det är nödvändigt för att den utlämnande myndigheten, i detta fall den tekniskt ansvarige aktören, ska kunna fullgöra sin verksamhet. Bestämmelsen ska visserligen tillämpas restriktivt och avsikten är inte att man av rena effektivitetsskäl ska kunna bryta sekretessen. I en verifieringsprocess av det slag som vi beskriver i avsnitt 27.4 och som nu är aktuell bedömer vi emellertid att det är helt nödvändigt att den tekniskt ansvarige aktören kan lämna ut ovan nämnda uppgifter efter att den biometriska jämförelsen har genomförts i de system som denne ansvarar för, till den verifierande myndigheten. Att kunna lämna ut uppgifterna till den myndigheten är en förutsättning för att en tekniskt ansvarig aktör ska kunna fullgöra uppdraget från den verifierande myndigheten, och därmed för den verksamhet som följer av uppdraget.

Mot denna bakgrund anser vi att det saknas hinder mot att den verifierande myndigheten får del av uppgifter från den tekniskt ansvarige aktören, som är hänförliga till en genomförd biometrisk jämförelse. Om den tekniskt ansvarige aktören är en myndighet kan uppgifterna – om de anses förvarade hos denne – lämnas ut till den verifierande myndigheten med stöd av 10 kap. 2 § offentlighets- och sekretesslagen. Om den tekniskt ansvarige aktören är ett företag eller en annan enskild utgör lagen om tystnadsplikt inte hinder mot att uppgifter lämnas till den verifierande myndigheten.

25.4 Sammanfattande slutsatser

Vår bedömning

Det saknas hinder som kan hänföras till sekretess mot att implementera våra förslag. Genom befintliga bestämmelser om sekretess och den bestämmelse vi föreslår i avsnitt 25.2.2 kommer de uppgifter som behövs för biometrisk verifiering att skyddas, både om verifieringen genomförs med hjälp av tekniska system som den verifierande myndigheten ansvarar för, och om den genomförs med hjälp av en teknisk lösning som bygger på myndighetsgemensamma komponenter i form av en mobilapplikation och ett backend-system som förvaltas av en tekniskt ansvarig aktör.

Ytterligare överväganden bör emellertid göras innan ett visst tekniskt system implementeras, för att säkerställa att de uppgifter som behövs för biometrisk verifiering med stöd av den nya lagen skyddas. Detta i synnerhet om en annan teknisk lösning än de som beskrivs i kapitel 27 används.

Syftet med detta kapitel är att identifiera eventuella hinder som kan hänföras till sekretess mot att implementera våra förslag. I detta ligger att ta ställning till om det finns ett tillräckligt skydd för de uppgifter som används för en biometrisk verifiering med stöd av den nya lagen. Vi har utgått från de två verifieringsprocesser som vi enligt den tekniska analysen i kapitel 27 anser utgör huvudalternativ. Som vi redogjort för i avsnitt 25.2.1 och 25.3 bedömer vi att det kommer att finnas ett tillräckligt skydd för de alfanumeriska uppgifter som kan förekomma hos den verifierande myndigheten och eventuellt hos en tekniskt ansvarig aktör. Vi har därför inte identifierat något behov av kompletterande bestämmelser om sekretess för alfanumeriska uppgifter, förutsatt att någon av de tekniska lösningar som vi beskriver används.

När det gäller biometriska underlag och de biometriska uppgifter som tas fram ur dem har vi däremot bedömt att en ny sekretessbestämmelse ska införas i 40 kap. offentlighets- och sekretesslagen, i syfte att säkerställa att sådana uppgifter inte obehörigen röjs, oavsett hos vilken myndighet de förekommer. I avsnitt 25.3.4 har vi även konstaterat att vi inte ser något hinder hänförligt till sekretess mot att den verifierande myndigheten får del av uppgifter från den tekniskt ansvarige aktören som är hänförliga till en genomförd biometrisk jämförelse.

Sammantaget anser vi därför dels att det saknas hinder som kan hänföras till sekretess mot att implementera våra förslag, dels att det finns ett tillräckligt skydd för de uppgifter som behövs för biometrisk verifiering av identitet enligt den nya lagen.

Med detta sagt kan vi konstatera att i vart fall bedömningarna avseende en verifieringsprocess som bygger på myndighetsgemensamma komponenter – i form av ett backend-system och en mobilapplikation – som har utvecklats och förvaltas av en tekniskt ansvarig aktör, innehåller ett visst mått av osäkerhet. Även om vi i avsnitt 27.4 beskriver relativt detaljerat hur ett sådant system tekniskt kan implementeras, kan andra lösningar väljas, som skulle kunna påverka be-

hovet av både sekretessbestämmelser och sekretessbrytande bestämmelser. Det är enligt vår mening inte möjligt att inom ramen för detta betänkande uttömmande beskriva samtliga tänkbara situationer och tekniska lösningar. Detta är i hög grad beroende av den tekniska utvecklingen. Med utgångspunkt i en verifieringsprocess som bygger på system som den verifierande myndigheten helt förfogar över, har vi emellertid svårt att se att våra överväganden i avsnitt 25.2 inte skulle vara tillräckliga för att våra författningsförslag ska kunna tillämpas på avsett sätt.

Med en teknisk lösning som innebär att information ska hanteras av andra aktörer än den verifierande myndigheten bör det – oavsett de överväganden som vi gjort i avsnitt 25.3 – göras ytterligare överväganden avseende sekretess, innan en sådan teknisk lösning implementeras. Exempelvis kan det finnas anledning att ta ställning till om det är möjligt att kryptera uppgifterna på ett sätt som innebär att mottagaren saknar teknisk kapacitet att forcera krypteringen; när en uppgift skyddas av en kryptografisk funktion som hindrar att mottagaren tar del av uppgiftens informationsbärande innehåll, bör den inte betraktas som obehörigen röjd enligt offentlighets- och sekretesslagen.[15] Det kan emellertid många gånger vara svårt att säkerställa en sådan total kryptering. Krav på att en tekniskt ansvarig aktör implementerar sådana tekniska funktioner kan behöva regleras i avtal. Det kan vidare finnas behov av att analysera risker för att uppgifterna överförs till tredje land. Även var uppgifterna hanteras geografiskt kan ha betydelse för bland annat bedömningen av om det är möjligt att tillämpa den sekretessbrytande bestämmelsen i 10 kap. 2 a § offentlighets- och sekretesslagen; en viss geografisk lokalisering hos en tekniskt ansvarig aktör kan vara olämplig avseende vissa känsliga uppgifter. Utifrån de särskilda faktorer som en teknisk lösning för med sig kan det alltså vara nödvändigt att överväga om ytterligare bestämmelser om sekretess behövs, eller om en tystnadsplikt behöver regleras i avtal, om den tekniskt ansvarige aktören är ett privat företag. Sådana överväganden – som är beroende av utformningen av en eventuell teknisk lösning – faller som vi ser det utanför vårt uppdrag.

[15] eSam, *Utkontraktering – sekretess och dataskydd*, s. 25.

26 Processuella frågor

26.1 Inledning

Rätten till domstolsprövning och annan rättslig prövning är grundläggande i en rättsstat för att enskilda bland annat ska kunna skydda sig mot och få gottgörelse för överträdelser av grundläggande fri- och rättigheter, och försvara sig i straffrättsliga förfaranden. Vi kan konstatera att överklagande av myndigheters beslut regleras på ett generellt plan i förvaltningslagen (2017:900). Det finns dock specialbestämmelser som tillämpas i stället för eller som ett komplement till förvaltningslagen i många författningar på olika rättsområden, till exempel 113 kap. socialförsäkringsbalken och 38–41 §§ folkbokföringslagen (1991:481). Vidare innehåller 7 kap. lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning bestämmelser om överklagande avseende behandling av personuppgifter, som ska tillämpas om inte annan lag eller förordning innehåller någon bestämmelse som avviker från lagen.

I det här kapitlet tar vi ställning till om det finns ett behov av kompletterande eller avvikande processuella regler i något avseende – i förhållande till befintliga regelverk – med anledning av våra förslag om en ny lag om biometrisk verifiering av identitet.

26.2 Rätten att överklaga enligt förvaltningslagen

Enligt 41 § förvaltningslagen får ett beslut överklagas om beslutet kan antas påverka någons situation på ett inte obetydligt sätt. Vidare får ett beslut, enligt 42 § förvaltningslagen, överklagas av den som beslutet angår, om det har gått honom eller henne emot. Beslut överklagas, enligt 40 § förvaltningslagen, till allmän förvaltningsdomstol.

26.2.1 Beslut

Det som är avgörande för om ett ställningstagande från en myndighet ska betraktas som ett förvaltningsbeslut är om det innefattar att uttalande varigenom myndigheten vill påverka förvaltningsorgans eller enskildas handlade, det vill säga om det är avsett att vara handlingsdirigerande. Det är alltså uttalandets syfte och innehåll som avgör dess karaktär av förvaltningsbeslut, inte dess yttre form. I praxis har förhållandevis låga krav ställts upp för att ett ställningstagande ska anses utgöra ett förvaltningsbeslut, och i vissa fall är detta endast underförstått.[1]

26.2.2 Antas påverka någons situation

En förutsättning för att ett beslut ska anses överklagbart enligt 41 § förvaltningslagen är att det kan antas påverka någons situation på ett visst sätt. Detta stämmer väl överens med vad som tidigare gällt enligt de allmänna förvaltningsrättsliga principer som följer av praxis. Ledning för hur kravet ska tolkas kan således hittas även i tidigare avgöranden i fråga om överklagbarhet.

Prövningen av om ett visst beslut ska anses överklagbart enligt bestämmelsen utgår från en objektiv bedömning av om omständigheterna i det enskilda fallet är sådana att kravet på påverkan ska anses uppfyllt. Uttrycket *påverka någons situation* tar sikte på beslutets faktiska verkningar (se bland annat RÅ 2003 ref. 87). Uttrycket avser emellertid även andra tänkbara varianter (jfr RÅ 2007 ref. 7 och RÅ 2010 ref. 9). Frågan om ett beslut är överklagbart ska alltså inte avgöras i förhållande till den som beslutet riktats till, det vill säga adressaten. Frågan ska i stället avgöras utifrån om beslutet till sin karaktär är sådant att det bör kunna angripas (HFD 2019 ref. 21). Även beslut som saknar egentliga rättsverkningar kan vara överklagbara om beslutet har utformats på ett sätt som kan leda till att det får konsekvenser enligt sitt innehåll. Högsta förvaltningsdomstolen har i flera avgöranden bekräftat det principiella förhållningssättet att det för överklagbarhet inte krävs rättsverkningar i egentlig mening, utan att det är de faktiska konsekvenserna för den som påverkas av

[1] Se Lundmark och Säfsten, *Förvaltningslagen, En kommentar*, JUNO Version 2, 2025-12-15, kommentaren till 41 §, under rubriken *För överklagbarhet krävs ett beslut*.

ett beslut som är avgörande vid bedömningen av ett besluts överklagbarhet.[2]

26.2.3 På ett inte obetydligt sätt

Att ett beslut endast i mycket begränsad mån påverkar en enskild är inte tillräckligt för att beslutet ska vara överklagbart; beslutets påverkan får inte vara obetydlig. Enligt förarbetena till förvaltningslagen innebär kravet på att det ska kunna antas att ett beslut påverkar någons situation på ett inte obetydligt sätt att det måste vara fråga om en viss grad av sannolik påverkan för att ett beslut ska få överklagas.[3]

26.3 Förvaltningsbeslut

En biometrisk verifiering med stöd av den nya lagen förutsätter – i ett första steg – att den myndighet som vill verifiera en persons identitet (den verifierande myndigheten) tar ställning till om villkoren för verifiering är uppfyllda (se avsnitt 23.6). Om så anses vara fallet kan myndigheten begära att personen, på angivna sätt, medverkar till att genomföra en biometrisk verifiering (se avsnitt 23.6.4). Om personen medverkar till den biometriska verifieringen kommer den verifierande myndigheten att ta del av uppgifter i den handling som används för verifieringen samt ta fingeravtryck och/eller ansiktsbild av personen för att kontrollera att dessa motsvarar dem som finns i eller på handlingen. Om personen inte följer en begäran om biometrisk verifiering ska myndigheten, under vissa förutsättningar, få förelägga personen att göra det och ska i föreläggandet ange följden av att det inte följs (se avsnitt 23.8).

Fråga är, enligt vår bedömning, om rätten att överklaga en begäran eller ett föreläggande om biometrisk verifiering ska följa regelverket i förvaltningslagen eller om särskilda överklaganderegler bör införas i den nya lagen.

[2] Se Lundmark och Säfsten, *Förvaltningslagen, En kommentar*, JUNO Version 2, 2025-12-15, kommentaren till 41 §, under rubriken *Beslutet måste kunna antas påverka någons situation.*
[3] *En modern och rättssäker förvaltning – ny förvaltningslag*, prop. 2016/17:180, s. 332.

26.3.1 Biometrisk verifiering vid handläggningen av ett ärende

Vårt förslag

En begäran om biometrisk verifiering vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde ska få överklagas endast i samband med talan mot beslut som innebär att ärendet avgörs. Detsamma ska gälla för ett föreläggande som meddelats med stöd av den nya lagen.

Begäran

En biometrisk verifiering av identitet med stöd av den nya lagen ska, enligt vår bedömning, betraktas som en utredningsåtgärd som vidtas inom ramen för det aktuella ärendet eller den aktuella verksamheten. Med hänsyn till detta bör en myndighets begäran om biometrisk verifiering som utgångspunkt inte betraktas som ett överklagbart beslut enligt 41 § förvaltningslagen, då själva begäran om verifiering inte kan antas påverka någons situation på ett inte obetydligt sätt. Detsamma bör, som vi ser det, anses gälla själva upptagningen av biometriska underlag och den efterföljande kontrollen av om dessa motsvarar dem som finns i eller på den handling som används för verifieringen. Att kontrollen innebär ett visst ingrepp i den personliga integriteten förändrar inte bedömningen; det kan som vi ser det inte i sig anses påverka den enskilde på det sätt som avses i 41 § förvaltningslagen. Inte heller får själva jämförelsen av uppgifter eller resultatet av verifieringen, enligt vår mening, i sig någon sådan påverkan på den enskildes situation att det kan anses vara fråga om ett överklagbart beslut enligt förvaltningslagen.

Det är, enligt våra förslag, emellertid fråga om ett stort antal myndigheter som kan komma att använda sig av möjligheten att verifiera identitet biometriskt med stöd av den nya lagen i en stor mängd olika ärendeslag samt vid identitetskontroller i olika situationer, inom ramen för olika myndigheters verksamhet. Det är därför mycket svårt att förutse alla tänkbara situationer i vilka en biometrisk verifiering kan komma att begäras och det kan, enligt vår mening, inte uteslutas att redan en begäran om biometrisk verifiering med stöd av den nya lagen i något sammanhang skulle kunna antas påverka någons situation på ett inte obetydligt sätt. En sådan begäran från en myndighet

skulle därmed – potentiellt sett – kunna utgöra ett överklagbart beslut enligt 41 § förvaltningslagen. Nämnda bestämmelse ger uttryck för de principer som kommit till uttryck genom Högsta förvaltningsdomstolens praxis, som innebär att det är ett besluts faktiska verkningar som är i grunden avgörande för bedömningen av beslutets överklagbarhet; ytterst är det praxis från denna domstol kring bestämmelsen som i det enskilda fallet blir vägledande för bedömningen i sak.[4] I avsaknad av särskilda bestämmelser om överklagande i den nya lagen om biometrisk verifiering av identitet skulle det därmed bli upp till den verifierande myndigheten – och i förlängningen de allmänna förvaltningsdomstolarna – att ta ställning till om och så fall under vilka förutsättningar en begäran från en myndighet om en biometrisk verifiering kan anses utgöra ett överklagbart beslut.

Som vi ser det är det emellertid framför allt myndighetens agerande med anledning av resultatet av en verifiering – fail/pass eller ett jämförelsevärde – eller av en utebliven verifiering, på grund av bristande medverkan från den enskilde eller tekniska problem, som potentiellt sett kan påverka den enskildes situation på ett inte obetydligt sätt. Om resultatet av verifieringen leder till fortsatta utredningsåtgärder är det, enligt vår mening, som utgångspunkt inte heller fråga om påverkan på ett inte obetydligt sätt. Om resultatet av den biometriska verifieringen eller en utebliven verifiering däremot leder till att myndigheten av den anledningen beslutar att avvisa eller avslå den enskildes framställan är det emellertid rimligt att utgå från att det är fråga om ett överklagbart avvisnings- eller avslagsbeslut.

Med hänsyn till framför allt den biometriska verifieringens karaktär som utredningsåtgärd bedömer vi att rätten att överklaga en begäran bör begränsas under tiden det aktuella ärendet handläggs. Först när ärendet har avgjorts slutligt bör det finnas en möjlighet för den enskilde att få till stånd en domstolsprövning. Enligt huvudregeln i 34 § förvaltningsprocesslagen (1971:291) är endast beslut genom vilket domstolen slutgiltigt avgör målet överklagbara, till skillnad från vad som gäller för förvaltningsmyndigheter. Syftet med att begränsa rätten att överklaga beslut under beredningen av ett mål i förvaltningsdomstol är att det slutliga avgörandet inte ska fördröjas i onödan. Detta ändamål gör sig, enligt vår mening, gällande även vid biometrisk verifiering av identitet vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde. Som vi redogjort för ovan

[4] Prop. 2016/17:180, s. 332 f.

anser vi dessutom att det i första hand är när resultatet av den biometriska verifieringen eller en utebliven verifiering leder till avvisning av eller avslag på en framställan som myndighetens beslut kan antas påverka någons situation på ett inte obetydligt sätt. En begränsning av rätten att överklaga en begäran om biometrisk verifiering särskilt – alltså under handläggningen av det aktuella ärendet – kommer därmed som utgångspunkt inte att innebära en begränsning av rätten att överklaga enligt förvaltningslagen. I de fall en begränsning av rätten att överklaga en begäran enligt den nya lagen även innebär en begränsning av rätten att överklaga enligt förvaltningslagen bedömer vi att det är motiverat med hänsyn till att ärendets slutliga avgörande inte bör fördröjas av en domstolsprocess.

Det kan i detta sammanhang påpekas att en myndighet som begärt en biometrisk verifiering inte är skyldig att förelägga den enskilde att genomföra verifieringen och, enligt våra förslag, inte heller ska få förelägga den enskilde om det kommit fram omständigheter som talar mot ett föreläggande. Att den enskilde väljer att inte följa en begäran om biometrisk verifiering vid handläggningen av ett ärende enligt förvaltningslagen behöver alltså inte nödvändigtvis få några direkta konsekvenser för den enskilde.

Mot den här bakgrunden bedömer vi att det ska anges i den nya lagen att en begäran om biometrisk verifiering vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde ska få överklagas endast i samband med talan mot beslut som innebär att ärendet avgörs. Vid överklagande i samband med det slutliga beslutet i ärendet är det egentligen inte fråga om ett överklagande av begäran om verifiering; det som överklagas är avgörandet i ärendet, men till stöd för yrkandena som förts fram avseende detta kan invändningar avseende begäran om verifieringen anföras.[5]

De ovan anförda begränsningarna skulle också i praktiken kunna uppnås genom att det i den nya lagen anges att en begäran om att biometriskt verifiera identiteten, eller ett föreläggande om detta, inte alls får överklagas. En sådan bestämmelse skulle inte hindra att den enskilde – vid överklagande av ett beslut i ärendet i sig – anför omständigheter som avser begäran om verifiering av identitet enligt den nya lagen. Vi anser emellertid att bestämmelsen i den nya lagen inte bör utformas som ett överklagandeförbud, med hänsyn till att det

[5] Jfr von Essen, *Förvaltningsprocesslagen m.m.*, JUNO Version 9 A, kommentaren till 34 §, under rubriken *Första stycket – Överklagbarhet domstolsbeslut*, *Huvudregeln*.

skulle kunna felaktigt ge intryck av att den enskilde inte heller i samband med ett överklagande av ett slutligt beslut i ärendet får invända mot en begäran om biometrisk verifiering med stöd av den nya lagen. En bestämmelse som anger att överklagande får göras endast i samband med talan mot beslut som innebär att ärendet avgörs är också den utformning som används i andra författningar.

Föreläggande

Ett föreläggande om biometrisk verifiering av identitet ska, enligt vårt förslag i avsnitt 23.8, endast få meddelas vid handläggningen av ärenden som omfattas av förvaltningslagens tillämpningsområde. Ett föreläggande utgör därmed en åtgärd vid handläggningen av det aktuella ärendet. Det kan därför – på liknande sätt som vid en begäran – övervägas om det ska vara möjligt att överklaga ett föreläggande särskilt eller om talan mot det ska kunna föras först i samband med att talan förs mot ett beslut som avgjort ärendet.

Som vi varit inne på ovan är huvudregeln i 34 § förvaltningsprocesslagen att endast beslut genom vilket domstolen slutgiltigt avgör ett mål är överklagbara. Enligt bestämmelsen får dock talan föras särskilt i vissa uppräknade situationer, däribland när rätten förelagt någon att medverka på annat sätt än genom inställelse inför rätten och underlåtenheten att iakttaga föreläggandet kan medföra särskild påföljd för honom (första stycket 4). Med *särskild påföljd* avses främst vite, hämtning och exekutiv handräckning, men man kan även tänka sig att andra sanktioner ska anses utgöra särskild påföljd. Däremot utgör ett ”hot” innebärande att målet ändå avgörs om föreläggandet inte följs ingen särskild påföljd. Är ett föreläggande inte förenat med någon konsekvens – det vill säga saknar särskild påföljd – och riktar sig mot part kan underlåtenhet att följa föreläggandet visserligen tillräknas honom eller henne i bevishänseende, men några andra följder får det inte, vare sig det i föreläggandet angetts eller inte att målet kan komma att avgöras även om parten inte hör av sig. Med hänsyn till detta är det naturligt att sådana förelägganden inte får överklagas särskilt. Vidare har av praktiska skäl ansetts att förelägganden för någon att *inställa sig* inför rätten inte ska vara överklagbara ens då de är sanktionerade. Övriga *sanktionerade förelägganden* för någon

att medverka kan däremot överklagas särskilt enligt förvaltningsprocesslagen.[6]

Vi har i avsnitt 23.8.6 föreslagit att ett föreläggande ska innehålla en upplysning om vad följden av att det inte följs kan bli samt bedömt att ett föreläggande inte bör kunna förenas med vite. Vidare har vi i avsnitt 21.5.3 bedömt att en rätt att vidta tvångsåtgärder för att möjliggöra biometrisk verifiering av identitet inte bör övervägas inom ramen för utredningen. Det kommer därmed, som vi ser det, inte att bli aktuellt med sanktionerade förelägganden med stöd av den nya lagen.

Ett föreläggande om biometrisk verifiering med stöd av den nya lagen kan dock komma att meddelas vid äventyr av att den framställan som inlett det aktuella ärendet avvisas eller avslås, det vill säga om en begärd verifiering inte genomförs kan myndigheten komma att avvisa eller avslå framställan. Vid en sådan följd av att föreläggandet inte följs är det enligt vår mening inte orimligt att anse att det kan antas påverka den enskildes situation på ett inte obetydligt sätt, i den mening som avses i 41 § förvaltningslagen, vilket innebär att det i så fall skulle kunna vara fråga om ett överklagbart beslut. En begränsning i den nya lagen av rätten att överklaga ett föreläggande skulle i vissa fall därmed kunna innebära en begränsning av rätten att överklaga enligt förvaltningslagen. Vi anser dock att det är motiverat att den enskilde, även i de fall ett föreläggande hade bedömts vara överklagbart enligt förvaltningslagen, har möjlighet att föra talan mot föreläggandet först i samband med ett eventuellt överklagande av det beslut som avgör ärendet. Den faktiska påverkan på den enskildes situation kommer i praktiken inte att gå att bedöma fullt ut innan det står klart om och i så fall vilka åtgärder myndigheten vidtar med anledning av en genomförd eller utebliven verifiering och vilken betydelse detta får vid avgörandet av ärendet. Att låta ett föreläggande om att medverka till en biometrisk verifiering enligt den nya lagen vara överklagbart särskilt samtidigt som begäran i sig – enligt våra förslag ovan – inte ska vara det, framstår enligt vår mening som en motsägelsefull ordning.

Mot den här bakgrunden bedömer vi att ett föreläggande som meddelats med stöd av den nya lagen ska få överklagas endast i samband med talan mot beslut som innebär att ärendet avgörs.

[6] Se von Essen, *Förvaltningsprocesslagen m.m.*, JUNO Version 9A, 2026-02-25, kommentaren till 34 §, under rubriken *Första stycket – Överklagbarhet domstolsbeslut, Undantag.*

26.3.2 Biometrisk verifiering vid genomförande av identitetskontroller

Vår bedömning

Rätten att överklaga en begäran om biometrisk verifiering när en myndighet, i annat fall än vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde, genomför identitetskontroller inom ramen för sin verksamhet bör inte regleras särskilt i den nya lagen. Det innebär att bestämmelserna om överklagande i förvaltningslagen blir tillämpliga vid ställningstagande till om en sådan begäran får överklagas i det enskilda fallet.

Vid biometrisk verifiering av identitet med stöd av den nya lagen när en myndighet, i annat fall än vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde, genomför identitetskontroller ska den enskilde, enligt våra förslag, inte kunna föreläggas att genomföra en verifiering (se avsnitt 23.8.1). Det är därmed endast aktuellt att ta ställning till om rätten att överklaga en begäran om biometrisk verifiering i sådana situationer ska regleras särskilt i den nya lagen.

Den omständigheten att en domstolsprocess kan komma att fördröja ett ärendes slutliga avgörande gör sig inte gällande i den nu aktuella situationen på samma sätt som vid handläggningen av ett ärende enligt förvaltningslagen. Detta eftersom en begäran om biometrisk verifiering vid genomförandet av en identitetskontroll som utgångspunkt kommer att framställas direkt till den enskilde, när denne träffar en representant för myndigheten. En genomförd verifiering kan till exempel leda till att en person nekas tillträde till myndighetens lokaler. Så kan vara fallet både om den genomförda verifieringen visar att personen i fråga är den han eller hon utger sig för att vara eller om personens påstådda identitet inte kan bekräftas genom verifieringen. En utebliven verifiering – på grund av att den enskilde inte medverkar eller tekniska problem – skulle också kunna få konsekvensen att den enskilde till exempel nekas tillträde till myndighetens lokaler, eftersom myndigheten då inte kunnat kontrollera biometriskt om den enskilde är den han eller hon påstår sig vara.

För det fall en myndighet fattar ett beslut med anledning av en genomförd eller utebliven biometrisk verifiering vid en identitets-

kontroll kommer det, som vi ser det, i stor utsträckning vara fråga om beslut som fattas direkt i anslutning till verifieringen, och som verkställs direkt. Ett eventuellt överklagande av en begäran kommer således som utgångspunkt att hanteras tillsammans med ett överklagande av ett beslut som fattats med anledning av verifieringen; begäran om verifiering och beslutet sammanfaller i dessa fall tidsmässigt. Det saknas därför som vi ser det behov av att föreskriva att en begäran inte får överklagas särskilt, utan endast i samband med att talan förs mot ett annat beslut. Dessutom är det svårt att, i författningstext, koppla rätten till överklagande till att talan förs mot vissa andra, specifika beslut på ett tydligt och förutsägbart sätt. Till skillnad från vid handläggningen av ett ärende då någon form av beslut som innebär att ärendet avgörs i princip alltid fattas, är det inte säkert att den verifierande myndigheten överhuvudtaget fattar något formellt beslut. I vart fall kommer beslutet sällan att dokumenteras skriftligt, på det sätt som görs vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde.

Det är, enligt vår bedömning, inte heller motiverat med ett överklagandeförbud. En begäran om biometrisk verifiering vid en identitetskontroll, i annat fall än vid handläggningen av ett ärende enligt förvaltningslagen, skulle under vissa förutsättningar kunna anses ha en inte obetydlig påverkan på den enskilde. Om så är fallet bör den enskilde ha en rätt till domstolsprövning.

Vidare överklagas den typ av beslut som potentiellt sett kan fattas med anledning av identitetskontroller, såvitt vi känner till, mycket sällan i dagsläget. Vad gäller exempelvis situationen att en person nekas tillträde till en myndighets lokaler har ändamålet med en domstolsprövning dessutom, som utgångspunkt, förfallit när ärendet kan tas upp till prövning av en domstol. Vi anser dock att det bör finnas en möjlighet att få till stånd en domstolsprövning av en begäran om biometrisk verifiering vid identitetskontroller, eventuellt i samband med att talan mot ett beslut som fattats med anledning av verifieringen, om förutsättningarna för överklagande enligt 41 och 42 §§ förvaltningslagen är uppfyllda. För det fall ett beslut som fattats med anledning av en genomförd eller utebliven verifiering överklagas kan, som vi påpekat ovan (se avsnitt 26.3.1), den enskilde till stöd för yrkandena som förts fram för ett sådant överklagande anföra invändningar avseende begäran om verifiering. Sådana invändningar kan avse

såväl att en begäran i sig har ställts som utfallet av en genomförd verifiering.

Mot den här bakgrunden bedömer vi att rätten att överklaga en begäran om biometrisk verifiering när en myndighet, i annat fall än vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde, genomför identitetskontroller inom ramen för sin verksamhet inte bör regleras särskilt i den nya lagen. Det innebär alltså att bestämmelserna i förvaltningslagen blir tillämpliga vid ställningstagande till om en sådan begäran är ett överklagbart beslut i det enskilda fallet.

26.4 Beslut enligt regelverket om dataskydd

Dataskyddsförordningen[7] innehåller i artikel 78 och 79 bestämmelser om rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde och mot tillsynsmyndighetens beslut. Vidare finns det bestämmelser om överklagande i 7 kap. dataskyddslagen. I samtliga fall krävs det enligt lagen prövningstillstånd vid överklagande till kammarrätten. Regleringen är strukturerad så att överklagande av personuppgiftsansvariga myndigheters beslut regleras i 2 § och överklagande av tillsynsmyndighetens beslut i 3 och 3 a §§. I 4 § regleras överklagande av vissa andra beslut. Slutligen finns det i 5 § ett överklagandeförbud avseende andra beslut.

26.4.1 Personuppgiftsansvariga myndigheters beslut

Enligt artikel 79.1 i dataskyddsförordningen ska varje registrerad som anser att hans eller hennes rättigheter enligt förordningen har åsidosatts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med förordningen ha rätt till ett effektivt rättsmedel. I förarbetena till dataskyddslagen bedömdes att rätten att överklaga en myndighets beslut om personuppgiftsbehandling bör omfatta beslut som en personuppgiftsansvarig myndighet fattar med anledning av att en registrerad utövar sina rättigheter enligt kapitel III i dataskyddsförordningen.[8] I 7 kap. 2 § dataskyddslagen anges att beslut enligt artiklarna 12.5 och 15–21 som har med-

[7] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.
[8] *Ny dataskyddslag*, prop. 2017/18:105, s. 151.

delats av en myndighet i egenskap av personuppgiftsansvarig får överklagas till allmän förvaltningsdomstol. Bestämmelsen innebär att om den personuppgiftsansvarige är en myndighet får beslut som myndigheten fattar enligt dataskyddsförordningen med anledning av att en registrerad utövar sin rätt till information och tillgång till personuppgifter, rättelse, radering, begränsning, invändning och dataportabilitet överklagas till allmän förvaltningsdomstol.

Det har ansetts att den registrerades rätt till ett effektivt rättsmedel mot den personuppgiftsansvarige eller personuppgiftsbiträdet i Sverige tillgodoses genom möjligheten att föra talan om skadestånd i allmän domstol.[9] Även andra former av fullgörelsetalan, till exempel yrkande om förbud att behandla personuppgifter eller åläggande att lämna ett registerutdrag, med eller utan vite, lär vara möjliga i allmän domstol.[10]

26.4.2 Tillsynsmyndighetens beslut

Enligt artikel 78.1 i dataskyddsförordningen ska varje fysisk eller juridisk person ha rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut rörande dem som meddelats av en tillsynsmyndighet. Genom bestämmelsen i 7 kap. 3 § dataskyddslagen klargörs att Integritetsskyddsmyndighetens beslut om sanktionsavgifter riktade till myndigheter får överklagas. I 7 kap. 3 a § dataskyddslagen stadgas att tillsynsmyndighetens beslut att avslå en begäran om besked om handläggningen av ett klagomål får överklagas. Det samma gäller en begäran som anses ha avslagits på grund av att tillsynsmyndigheten inte har lämnat ett besked eller meddelat ett beslut inom två veckor från den dag då begäran kom in till myndigheten.

26.4.3 Vissa andra beslut

Av 7 kap. 4 § dataskyddslagen framgår att beslut i vissa enskilda fall får överklagas. Det handlar om beslut i enskilda fall om att personuppgiftsansvariga som inte omfattas av föreskrifter om arkiv får behandla personuppgifter för arkivändamål av allmänt intresse samt om

[9] *Ny dataskyddslag, Kompletterande bestämmelser till EU:s dataskyddsförordning,* SOU 2017:39, s. 302 ff.
[10] Öman, *Dataskyddsförordningen (GDPR) m.m.*, JUNO Version 3A, 2025-09-11, kommentaren till artikel 79.

att andra än myndigheter får behandla personuppgifter som rör lagöverträdelser.

26.4.4 Behov saknas av särskilda överklagandebestämmelser

Vår bedömning

Det saknas behov av särskilda bestämmelser om överklagande av dataskyddsrättsliga beslut i den nya lagen.

Mot bakgrund av redogörelsen för regelverket avseende överklagande av dataskyddsrättsliga beslut i avsnitt 26.4.1–26.4.3 bedömer vi att det inte behövs särskilda bestämmelser om överklagande av sådana beslut i den nya lagen. Befintligt regelverk säkerställer enligt vår bedömning såväl enskildas rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde som rätten till ett effektivt rättsmedel mot tillsynsmyndighetens beslut. Vidare anser vi att det inte finns något behov av att begränsa rätten till överklagande, i förhållande till vad som gäller enligt dataskyddslagen. Enligt vårt förslag i avsnitt 24.11.3 ska rätten att göra invändningar inte gälla vid sådan behandling av personuppgifter som är tillåten enligt den ny lagen; detta för att säkerställa att en verifierande myndighet kan behandla relevanta personuppgifter vid verifiering med stöd av lagen utan fördröjning och ökad administration. En rätt att i övrigt överklaga dataskyddsrättsliga beslut i enlighet med regelverket i dataskyddslagen medför, som vi ser det, inga sådana hinder för den verifierande myndigheten att det är motiverat med en begränsning av överklaganderätten.

27 Tekniska frågor

27.1 Inledning

Som framgår av våra direktiv kan begränsningar när det gäller tekniska lösningar vara av betydelse för vilket system för säkrare verifiering av identitet som kan vara lämpligt, proportionerligt och ändamålsenligt att föreslå och införa. Vårt uppdrag omfattar därför bland annat att ta ställning till vilka tekniska lösningar som kan komma att behövas för säkrare verifiering av identitet. Det övergripande syftet med en teknisk analys måste som vi ser det emellertid vara att kunna ta ställning till om några direkta tekniska hinder mot att införa det rättsliga ramverk som vi föreslår kan identifieras; givetvis måste det gå att konstatera att en utökad möjlighet för myndigheter att biometriskt verifiera identitet kan användas i praktiken och inte bara blir en pappersprodukt. Att på lämpligt sätt belysa frågor av teknisk natur är också av vikt för att, i möjligaste mån, kunna uppskatta kostnader för utveckling och förvaltning av de tekniska system som kan behövas, vilket vi återkommer till i konsekvensanalysen i kapitel 30.

Den tekniska analysen bör som vi ser det däremot inte utmynna i några direkta förslag om vilken eller vilka specifika tekniska system eller komponenter som ska användas eller hur dessa i så fall ska implementeras i praktiken. Detta är enligt vår mening inte möjligt, med hänsyn till att den tekniska utvecklingen på området för biometrisk verifiering förändras i mycket snabb takt, exempelvis vad gäller möjlighet att använda och upptäcka så kallade deepfakes och ökad processorkraft i mobilenheter. I vilken utsträckning det är möjligt och lämpligt att exempelvis använda AI-modeller och utföra mer komplexa beräkningar – till exempel för att jämföra biometriska upp-

gifter – lokalt på mobilenheten påverkas av denna utveckling.[1] Sådana komponenter som vi beskriver i avsnitt 27.4.2 tillhandahålls inte sällan av privata aktörer på marknaden och skulle kunna upphandlas och inkorporeras i ett system för att biometriskt verifiera identitet mot handlingar; exempelvis kan nödvändiga moduler för att genomföra biometriska jämförelser vara komplexa att utveckla och därmed mer kostnadseffektiva att köpa in. Vilka sådana lösningar som finns att tillgå kan dock antas variera över tid. Vi kan vidare konstatera att det såväl på EU-nivå som nationellt pågår lagstiftningsprojekt avseende elektronisk identifiering, e-legitimation och den europeiska digitala identitetsplånboken, vars implementering skulle kunna få betydelse för hur exempelvis en mobilapplikation för att biometriskt verifiera identitet mot handlingar utformas, för att användarupplevelsen ska vara så smidig som möjlig.

Även om vårt uppdrag omfattar att kartlägga vilket tekniskt stöd som kan behövas för att införa ett system för att stärka verifiering av identitet med hjälp av biometriska uppgifter anser vi alltså att det varken är möjligt eller lämpligt att lämna förslag om vilken teknisk lösning som ska eller bör användas för att implementera en viss del av systemet. Det skulle som vi ser det bland annat riskera att peka ut system eller leverantörer som inte är relevanta vid den tidpunkt våra förslag eventuellt träder i kraft. Vi kan här också notera att tidigare betänkanden i vilka förslag har lämnats som bland annat möjliggör biometrisk verifiering mot handlingar i vissa ärendeslag – se exempelvis *Om folkbokföring, samordningsnummer och identitetsnummer* (SOU 2021:57) och *Vissa åtgärder för stärkt återvändandeverksamhet och utlänningskontroll* (SOU 2024:80) – inte har innehållit några överväganden av hur de rättsliga möjligheterna bör implementeras tekniskt, annat än på en synnerligen översiktlig nivå, i samband med konsekvensanalysen. Vi begränsar oss därför i avsnitt 27.6 till en bedömning av vilken teknisk modell som vi anser i första hand bör övervägas, utifrån de för- och nackdelar som vi belyser i avsnitt 27.3 och 27.4.

De särskilda tekniska frågor som kan behöva belysas närmare är hur en verifieringsprocess kan tänkas utformas. Två huvudalternativ är då aktuella. I det första utförs verifiering på plats, vid personlig

[1] I del 9, avsnitt 3.5, till Internationella civila luftfartsorganisationens (ICAO) dokument om maskinläsbara resehandlingar (9303) lyfts särskilt fram att det är erkänt att implementeringen av de flesta biometriska tekniker är föremål för ytterligare utveckling, och att med tanke på den snabba tekniska förändringen måste alla specifikationer (inklusive de i dokument 9303) ta hänsyn till och erkänna att det kommer att ske förändringar till följd av tekniska förbättringar.

inställelse, med hjälp av tekniska system som den verifierande myndigheten (se avsnitt 25.1) ansvarar för, på det sätt som redan görs av exempelvis Migrationsverket och Skatteverket; en sådan ordning har den fördelen att den nya lag som vi i kapitel 23 har föreslagit ska införas skulle kunna få ett snabbare genomslag. Detta alternativ redogör vi för i avsnitt 27.3.

Med hänsyn till att den nya lag som vi föreslår ska kunna tillämpas av ett stort antal myndigheter kan det emellertid vara av stort värde att samordna tekniska resurser och att tillämpa en så enhetlig teknisk modell och verifieringsprocess som möjligt. Vikten av ett sammanhållet ansvar för utvecklande och förvaltning av en myndighetsgemensam teknisk lösning har lyfts fram av flera myndigheter under vårt arbete. För att uppnå sådana mål och möjliggöra biometrisk verifiering på distans bör även ett alternativ som utgår från en teknisk lösning som bygger på användning av en myndighetsgemensam mobilapplikation och ett backend-system närmare belysas (se avsnitt 27.4). Det kan för respektive modell även finnas ett behov av att i vart fall på ett övergripande plan beskriva nödvändiga systemtekniska komponenter.

En särskild fråga som har lyfts under vårt arbete är om teknisk bearbetning av biometriska underlag som tas upp vid verifieringen – såväl från den enskilde som från den handling som används för kontrollen – och jämförelsen av biometriska uppgifter som tas fram ur dem bör göras i huvudsak i mobilapplikationen eller i backend-systemet, för det fall en sådan teknisk lösning implementeras. Detta kan påverka risker kopplade till informationssäkerhet, kontroll över verifieringsprocessen samt kapacitetsbehov och krav på robusthet i systemen. För att kunna beskriva nämnda verifieringsprocesser kan en översikt av relevanta tekniska standarder för de handlingar som enligt våra förslag i avsnitt 23.6.2 ska få användas för biometrisk verifiering vara av värde. En sådan översikt finns i avsnitt 27.2. I avsnitt 27.5 gör vi en kort internationell utblick. Avslutningsvis finns våra sammanfattande slutsatser i avsnitt 27.6.

27.2 Tekniska standarder för uppgifter i handlingar

De handlingar som vi har föreslagit ska kunna användas för biometrisk verifiering av identitet med stöd av den nya lagen innehåller olika uppgifter om innehavaren, såväl tryckta synligt på handlingen som digitalt i ett lagringsmedium i form av ett RFID-chip[2], vilket är en särskild teknik för att överföra data trådlöst över korta avstånd. Ofta används i stället begreppet NFC[3], vilket är en vidareutveckling av RF-tekniken som gör det möjligt att utbyta data i båda riktningarna. Vi kommer i detta kapitel att använda begreppet NFC-chip.

Vilka uppgifter som ska och får finnas synliga på en handling och lagras i ett NFC-chip på handlingen följer vissa standarder. Utformningen av hemlandspass och identitetskort som utfärdas av behöriga myndigheter i EU:s medlemsstater, och uppehållstillståndskort som utfärdas av svenska myndigheter, regleras närmare i relevanta EU-förordningar. I bilagorna till EU:s passförordning[4] och förordningen om en enhetlig utformning av uppehållstillstånd[5] anges att handlingarna ska utformas i enlighet med specifikationerna i ICAO:s (International Civil Aviation Organization) dokument 9303 om maskinläsbara resehandlingar. För nationella identitetskort som utfärdas av behöriga myndigheter i medlemsstaterna framgår detta av artikel 3 i EU:s id-kortsförordning[6]. Som vi noterat i avsnitt 21.2 regleras det statliga identitetskort utan resefunktion som föreslagits i promemorian *Ett statligt identitetskort* inte av EU:s id-kortsförordning. Av förslagen i promemorian framgår inte att utformningen av ett sådant identitetskort ska skilja sig från det med resefunktion, förutom att det förstnämnda inte ska innehålla en uppgift om medborgarskap. Det är enligt vår mening oklart om det endast avser de synliga uppgifterna. Vi kan dock notera att det statliga identitetskortet, enligt förslagen, ska innehålla uppgifter om innehavaren. Vilka uppgifter om innehavaren som ska framgå av det nya kortet ska enligt förslagen regleras på lägre nivå än lag.[7] Enligt 2 kap. 1 § förslag till förordning om statligt identitetskort ska det, utöver vissa andra uppgifter, finnas uppgifter om person- eller samordningsnummer på

[2] Radio Frequency Identification.
[3] Near Field Communication.
[4] Rådets förordning (EG) nr 1030/2002 av den 13 juni 2002.
[5] Rådets förordning (EG) nr 2252/2004 av den 13 december 2004.
[6] Rådets förordning (EU) 2025/1208 av den 12 juni 2025.
[7] Ju 2026/01595, s. 65 f.

kortet.[8] Såvitt vi kan bedöma ska även det statliga identitetskortet utan resefunktion utformas i enlighet med vad som följer av EU:s id-kortsförordning – det vill säga ICAO:s dokument 9303 – med undantag för att handlingen inte ska innehålla uppgift om medborgarskap.

Dokument 9303 från ICAO utgör den internationella standarden för utformning, innehåll och teknisk struktur för resehandlingar. Standarden syftar till att säkerställa en global interoperabilitet, hög säkerhet och tillförlitlig verifiering av både handlingen och dess innehavare. En grundläggande princip i ICAO:s dokument 9303 är att uppgifter om identitet, dokumentnummer och särskilda eventuella nationella identitetsbeteckningar – för svensk del person- och samordningsnummer – ska finnas tryckta på handlingen och digitalt lagrade i ett NFC-chip (eMRTD[9]). Vi kan, utifrån information från företrädare för Migrationsverket, notera att uppehållstillståndskort som utfärdas av svenska myndigheter däremot inte innehåller Migrationsverkets individnummer eller person- eller samordningsnummer, varken synligt eller lagrat digitalt i NFC-chippet. En ansiktsbild ska dock vara synlig på handlingen och lagras i NFC-chippet.

Att uppgifterna finns både synliga och digitalt lagrade möjliggör manuell kontroll, optisk maskinläsning och elektronisk verifiering av handlingens och uppgifternas äkthet. Handlingen ska även ha en maskinläsbar zon (MRZ). Detta är en standardiserad textzon som kan avläsas optiskt av en maskin och som innehåller ett definierat urval av uppgifter, bland annat identitetsuppgifter, utfärdande stat och giltighetstid. MRZ utgör också den primära källan för att etablera åtkomst till NFC-chippet, genom så kallad Basic Access Control (BAC) eller, i nyare passhandlingar, Password Authenticated Connection Establishment (PACE). I chippet lagras den synliga informationen på ett strukturerat sätt, i datagrupper. De i detta sammanhang centrala datagrupperna är DG1 och DG2. DG1 innehåller de maskinläsbara identitetsuppgifterna i digital form och används för att säkerställa att uppgifterna i chippet överensstämmer med de som är tryckta på handlingen och därmed att den inte har manipulerats. DG2 innehåller biometriska underlag i form av en digital ansiktsbild av innehavaren; bilden lagras i ett standardiserat format och ska motsvara den bild av innehavaren som finns synligt tryckt på handlingen, vilket skapar en koppling mellan okulär och digital kontroll. Härutöver

[8] A.a., s. 28.
[9] Electronic Machine-Readable Travel Document.

finns i datagrupp DG3 biometriska underlag i form av digitala fingeravtrycksbilder. Det bör här lyftas fram är att det är biometriska *underlag* som lagras i NFC-chippet, inte de biometriska uppgifter som kan tas fram ur dem, som används för en datorstödd jämförelse i samband med verifiering av identitet. Att extraheringen av biometriska uppgifter görs vid den tidpunkten återspeglar en medveten designprincip i dokument 9303 om interoperabilitet, där NFC-chippet fungerar som bärare av referensdata och bearbetning av sådan data sker externt. I NFC-chippet lagras även ett SOD (Security Object Document), som används för att kontrollera handlingens äkthet.

Vid de överväganden som görs i följande avsnitt kommer vi endast att belysa processer som utgår från att verifieringen görs mot en handling som är utformad i enlighet med ICAO 9303-standarden.

27.3 En verifieringsprocess som bygger på egna tekniska system

En verifieringsprocess som bygger på att den verifierande myndigheten använder sådana tekniska lösningar – såväl hårdvara som mjukvara – som den själv har tagit fram eller upphandlat och ansvarar för skulle som vi ser det kunna utgöra ett realistiskt alternativ, i vart fall om verifieringen inte ska utföras på distans. Att varje myndighet som vill tillämpa den nya lagen själv tar fram eller upphandlar en teknisk lösning som möjliggör verifiering på distans ser vi däremot inte som realistiskt. Migrationsverket, Polismyndigheten och Skatteverket genomför redan i dag biometriska kontroller mot handlingar i olika ärendeslag. Befintliga tekniska lösningar som dessa myndigheter förfogar över skulle enligt vår mening kunna användas även vid tillämpning av den nya lag som vi föreslår, även om det kan förväntas att det skulle kräva viss anpassning och integrering för att de tekniska systemen ska kunna användas för kontroller också i andra ärendeslag än nuvarande.

Om den verifierande myndigheten – på liknande sätt som bland annat Skatteverket – träffar avtal med Statens servicecenter om att sistnämnda myndighet ska utföra uppgifter enligt lagen (2019:212) om viss gemensam offentlig service för förstnämnda myndighets räkning (se avsnitt 25.2.1), skulle som utgångspunkt utrustning som finns på servicekontoren kunna användas. På servicekontoren erbjuds

enskilda vägledning och service av flera myndigheter: Skatteverket, Försäkringskassan, Pensionsmyndigheten, Migrationsverket och Arbetsförmedlingen. Vi kan konstatera att sedan den 3 juni 2024 kan biometriska jämförelser vid Skatteverkets identitetskontroll göras på de servicekontor som Statens servicecenter ansvarar för, med stöd av nyss nämnda lag. Identitetshandlingar granskas också maskinellt. En verifieringsprocess som utgår från att biometrisk verifiering mot handlingar – för i vart fall nämnda myndigheter – genomförs vid personlig inställelse och med hjälp av den utrustning som finns på servicekontoren, skulle kunna vara ett möjligt alternativ. Som lyftes fram i betänkandet *Registrering av EES-medborgare* skulle en fråga i så fall vara om det är lämpligt att Skatteverkets upphandlade utrustning och programvara för identitetskontroll (inklusive biometrisk kontroll av fotografi) även används för biometrisk verifiering av identitet som kan komma att genomföras i ett ärendeslag som handläggs av en annan myndighet än Skatteverket.[10] Vi vill emellertid understryka att detta är i första hand en ekonomisk fråga, som vi inte avser att ta ställning till i detta sammanhang. Något principiellt eller rättsligt hinder mot att myndigheter – på motsvarande sätt som Skatteverket – i egen regi upphandlar eller utvecklar nödvändiga tekniska system som sedan används av Statens servicecenter för den verifierande myndighetens räkning kan vi däremot inte se. Det kan dock ta viss tid att implementera en sådan lösning, vilket innebär att kretsen av myndigheter som kan utnyttja den generella möjlighet att biometriskt verifiera identitet mot handlingar som vi föreslår i vart fall initialt blir begränsad i praktiken.

En verifieringsprocess som bygger på att den genomförs med hjälp av särskilda tekniska system som myndigheten själv förfogar över – på det sätt som exempelvis görs vid identitetskontroller enligt folkbokföringslagen (1991:481) och utlänningslagen (2005:716) – är som utgångpunkt begränsad på så sätt att den inte möjliggör en kontroll på distans. Detta utgör som vi ser det en väsentlig begränsning. Å andra sidan kan varken en synlig ansiktsbild eller fingeravtryck användas vid verifiering på distans, i en sådan verifieringsprocess som vi beskriver i avsnitt 27.4.

[10] SOU 2026:9, s. 146.

27.3.1 Översikt av de olika stegen i verifieringsprocessen

En verifieringsprocess av nu beskrivet slag omfattar av naturliga skäl färre tekniska steg än den modell och process som vi beskriver i mer detalj i avsnitt 27.4, som innefattar även ett backend-system, och där de biometriska underlag och alfanumeriska uppgifter som tas upp med hjälp av en mobilapplikation kan behöva överföras till backend-systemet. De centrala stegen är dock principiellt samma, men utförs på olika sätt.

Initiering av verifieringsprocessen kan lämpligen göras genom att företrädaren för myndigheten muntligen instruerar den enskilde hur processen går till och att han eller hon anmodas att ta fram den handling som ska användas för verifieringen. De delar av processen som i den modell som vi beskriver i avsnitt 27.4 utförs med hjälp av en mobilapplikation kan i stället genomföras med särskild utrustning som finns hos den verifierande myndigheten. Med hjälp av en kamera och/eller fingeravtrycksläsare kan biometriska underlag tas upp, och en särskild chipläsare läser in relevant information från handlingen och kontrollerar dess äkthet. En sådan liveness-check och andra åtgärder för att motverka manipulation som behöver göras vid verifiering på distans och som vi återkommer till i avsnitt 27.4.1 är givetvis inte aktuella vid verifiering vid personlig inställelse. Guidning av den enskilde så att korrekta biometriska underlag tas upp görs i första hand av företrädaren för myndigheten, inte av en mobilapplikation. Den biometriska jämförelsen görs lokalt i den programvara som myndigheten förfogar över och resultatet av jämförelsen (Pass/Fail eller ett jämförelsevärde) kan direkt visas för företrädaren för myndigheten, som omedelbart kan kontrollera resultatet och vidta relevanta åtgärder. Överföring av resultatet till myndighetens ärendesystem kan vid verifiering på plats göras manuellt av handläggaren, utan ett behov av något särskilt gränssnitt.

27.3.2 Nödvändiga systemkomponenter och särskilda risker

Med hänsyn till att bland annat Skatteverket redan i nuläget genomför biometrisk verifiering av identitet mot handlingar med hjälp av utrustning och programvara som myndigheten har upphandlat anser vi att det saknas behov av att i detta sammanhang närmare redogöra för vilka systemkomponenter som kan vara nödvändiga inom ramen

för en sådan teknisk lösning, för att kunna konstatera att våra förslag kan genomföras. I relevanta delar hänvisas till avsnitt 27.4.1.

Vid en verifieringsprocess av det slag vi beskrivit i detta avsnitt, som görs på plats och med teknisk utrustning som finns antingen i den verifierande myndighetens lokaler eller hos någon annan aktör, exempelvis Statens servicecenter, blir utgångspunkten att processen inte kan antas medföra motsvarande systemtekniska utmaningar som vi återkommer till i avsnitt 27.4, som blir aktuella i ett myndighetsgemensamt system med en mobilapplikation och ett backend-system. Även om det kan antas att uppdateringar av framför allt programvara för att genomföra biometriska jämförelser behöver göras, torde däremot inte någon central serverstruktur som ställer krav på driftsäkerhet och skalbarhet krävas. Känsliga personuppgifter behöver inte heller överföras till ett backend-system, vilket minskar risken för att de sprids som resultat av ett cyberangrepp eller annat angrepp. Verifieringsprocessen blir inte heller avhängig av en stabil nätverksuppkoppling, vilket är en förutsättning vid verifiering på distans, eller av krav på att kunna hantera en heterogen klientmiljö i form av olika mobilenheter och operativsystem i dessa. En verifieringsprocess som genomförs på plats, med utrustning och tekniska system som den verifierande myndigheten förfogar över, innebär som vi ser det också att en kontrollerad exekveringsmiljö kan uppnås. Detta motverkar effektivt risken för eventuell manipulation av såväl de biometriska underlagen som resultatet av den biometriska jämförelsen, jämfört med om detta sker i en mobilapplikation och/eller i ett backend-system av det slag vi beskriver i avsnitt 27.4.

27.4 En verifieringsprocess som bygger på ett system med myndighetsgemensamma komponenter

Vid biometrisk verifiering av identitet mot handlingar vid en gränskontroll eller en inre utlänningskontroll är det naturligt att kontrollen görs på plats och med tekniska system som Migrationsverket eller Polismyndigheten förfogar över. Biometrisk verifiering som görs enligt folkbokföringslagen är kopplad till en identitetskontroll som genomförs på plats. En möjlighet att biometriskt verifiera identitet med stöd av den nya lagen på distans kan som vi ser det emellertid få en betydande effekt på den nya lagens genomslag i praktiken, mot

bakgrund av att allt fler ärendeslag inleds på digital väg, och att myndigheten ofta kommunicerar med den enskilde på det sättet. I Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter* lyftes fram att den största risken för identitetsrelaterade välfärdsbrott är relaterad just till att en e-legitimation som används för ansökan om en förmån inte hör ihop med personen som han eller hon utger sig för att vara.[11] Att på distans kunna göra en sådan koppling genom en biometrisk verifiering enligt den nya lagen skulle, som vi ser det, vara av stor betydelse, En teknisk lösning som möjliggör detta behöver därför belysas närmare. Som vi nämnt redan inledningsvis i avsnitt 27.1 anser vi att en sådan lösning bör bygga på myndighetsgemensamma system i form av en mobilapplikation och ett centralt backend-system.

Vi kan i detta sammanhang konstatera att en verifieringsprocess som genomförs på distans och bygger på en sådan teknisk modell som vi beskriver i detta avsnitt i sig har vissa begränsningar. För det första är det – som vi pekat på i avsnitt 20.2.4 – inte möjligt att på distans använda en synlig ansiktsbild på den handling som används för den biometriska jämförelsen, eftersom myndigheten inte på något enkelt sätt kan säkerställa att ansiktsbilden faktiskt härrör från handlingen och inte från någon annan källa; risken för manipulation framstår i sådana fall som alltför hög. Vidare kan, vilket vi redogjort för i avsnitt 20.2.3, biometriska underlag i form av fingeravtryck inte heller användas vid verifiering på distans. Dessa begränsningar talar som vi ser det emellertid inte med någon nämnvärd styrka mot att överväga en teknisk modell som möjliggör en verifieringsprocess på distans. Detta med hänsyn till att det är fullt möjligt att genomföra en biometrisk verifiering med endast en ansiktsbild som jämförelseunderlag, och att den synliga ansiktsbilden i första hand bör ses som en reservmetod, i de fall NFC-chippet av någon anledning inte går att använda. Verifiering som genomförs på distans innebär slutligen också att den verifierande myndigheten har en lägre grad av kontroll över processen än om den enskilde finns på plats.

Det saknas som vi ser det i princip hinder mot att en verifieringsprocess som utformas på det sätt och med de komponenter som vi redogör för i detta avsnitt används även i situationer när den vars identitet behöver verifieras biometriskt antingen befinner sig hos

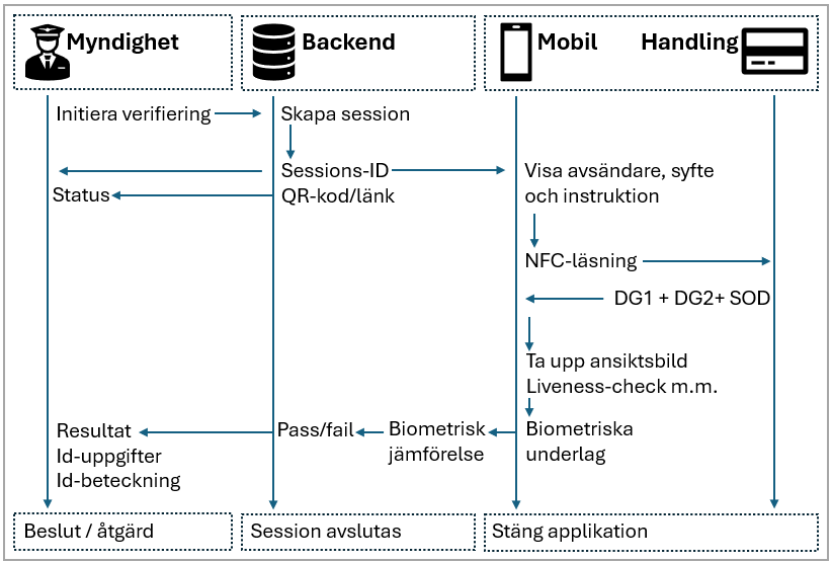
[11] RiR 2024:12, s. 68.

myndigheten eller kontrolleras direkt av en företrädare för myndigheten någon annanstans.

27.4.1 Närmare om verifieringsprocessen

En verifieringsprocess av nu aktuellt slag skulle schematiskt kunna åskådliggöras med nedanstående figur. De olika stegen beskrivs närmare i texten nedan. Vi lyfter i samband med detta, där det är relevant, även för- och nackdelar med att förlägga ett visst steg i mobilapplikationen respektive backend-systemet. Vi återkommer i avsnitt 27.6 till en mer samlad bedömning av vilka alternativ som vi anser är lämpligast; figuren nedan utgår dock från att huvuddelen av verifieringslogiken placeras i ett myndighetsgemensamt backend-system.

Figur 27.1 Översikt av verifieringsprocessen



Steg 1: Initiering av verifieringen

Den myndighet som vill biometriskt verifiera en persons identitet initierar en verifieringsbegäran, som skickas till ett myndighetsgemensamt backend-system. Backend-systemet skapar ett sessions-ID och förmedlar en verifieringsinstruktion till personen vars identitet ska

verifieras. Vi bedömer att något centralt register för att säkerställa att verifieringen startas i rätt individs mobilapplikation inte är nödvändigt. En jämförelse kan göras med hur mobilt BankID fungerar.

Ett mobilt BankID utfärdas av en bank till den som har ett personnummer och knyts vid skapandet till en specifik enhet (mobiltelefon) och applikation som installeras på denna. I ett centralt register lagras uppgifter om bland annat vilka aktiva BankID som är utfärdade för ett personnummer. Registret och det backend-system som används förvaltas av Finansiell ID-Teknik BID AB, inte av den bank som har utfärdat ett mobilt BankID eller de privata aktörer som använder BankID för legitimering av en person i en viss process eller ett visst ärende. Legitimeringen kan i det enskilda fallet initieras på olika sätt. Den aktör som vill genomföra en legitimering kan starta sessionen i bakgrunden utifrån angivande av personnummer. Så sker exempelvis vid kontakt med en bank när kunden ringer upp kundtjänst och i samband med det anger sitt personnummer. Sessionen kan också initieras utan användning av personnummer, genom att den enskilde aktivt skannar en QR-kod eller öppnar en djuplänk, som i sin tur öppnar mobilt BankID-applikationen på hans eller hennes mobiltelefon. Oavsett vilken modell som används för att initiera sessionen krävs anrop mot det centrala register och backend-system som förvaltas av Finansiell ID-Teknik BID AB; en kontroll görs av vilka aktiva BankID som är utfärdade för det aktuella personnumret och en order skapas av systemet.[12]

Ett system för att biometriskt verifiera identitet mot handlingar, med hjälp av en mobilapplikation, bör enligt vår mening inte bygga på ett centralt register och en modell där enskilda måste förregistrera sig på det sätt som gäller för exempelvis BankID. En sådan lösning skulle som vi ser det medföra dels en ökad teknisk komplexitet, dels sådana särskilda rättsliga överväganden som följer enligt dataskyddsförordningen avseende register som innehåller personuppgifter. Det skulle även kräva noggranna överväganden kring vilken eller vilka myndigheter som skulle ansvara för att förvalta systemet. I stället anser vi att en så fristående och enkel teknisk lösning som möjligt, för att starta en begäran om att verifiera identitet med hjälp av biometriska uppgifter mot handlingar, bör eftersträvas. För att kunna knyta en verifieringsbegäran till rätt individ krävs endast att den kan

[12] För en detaljerad beskrivning av den praktiska legitimeringsprocessen för mobilt BankID, se https://developers.bankid.com/, senast besökt den 7 juli 2026.

knytas till en viss unik, pågående session, inte till en identitet som lagrats i ett centralt register. Det viktiga är att endast den avsedda individen kan fullfölja verifieringen och att resultatet av den på ett säkert sätt kan skickas till den myndighet som initierat begäran. Detta kan uppnås på olika sätt, vilka dock förutsätter viss aktiv medverkan från den enskilde och som därmed kan upplevas som mindre smidiga för användaren än när sessionen startas i bakgrunden av myndigheten.

En modell som vi bedömer uppfyller krav på enkelhet, minimal hantering av personuppgifter och skalbarhet kan principiellt utformas som så att myndigheten skapar en verifieringssession i backend-systemet, som inte adresseras till en viss individ utan kopplas till ett slumpmässigt och kortlivat sessions-ID. Ett sessions-ID kan lämpligen utformas som ett sådant UUID som vi beskrivit i avsnitt 11.3.3. Sessionen aktiveras därefter av den vars identitet ska verifieras i hans eller hennes mobilapplikation genom att personen antingen skannar en QR-kod eller öppnar en djuplänk som har genererats av backend-systemet. QR-koden kan presenteras för den enskilde antingen vid personlig inställelse eller via den verifierande myndighetens hemsida (”Mina sidor”), och en länk kan levereras till användaren genom SMS eller e-post eller till en digital brevlåda som till exempel Kivra. En QR-kod kan även skickas med fysiskt brev.

Som vi ser det möjliggör detta en säker och integritetsbevarande process. Vissa säkerhetsmässiga aspekter som bör beaktas kan emellertid särskilt lyftas fram i detta sammanhang.

En angripare skulle kunna försöka manipulera verifieringsprocessen genom att kapa eller återanvända en verifieringsbegäran, genomföra verifiering mot ”fel” individ eller återspela tidigare giltiga verifieringar. När det gäller *kapning av en verifieringsbegäran* kan det ske genom att en länk eller QR-kod fotograferas av och skickas vidare till någon annan person än den vars identitet ska verifieras. Konsekvensen blir att verifieringen utförs korrekt men av fel person. För att motverka denna typ av attack bör kort livslängd för sessions-ID tillämpas, och ett visst sessions-ID bör bara kunna användas en gång. Verifiering med personlig inställelse vid myndigheten är naturligtvis också en effektiv åtgärd, men även andra bindningar till en viss kontext, exempelvis genom kontroll av ip-nummer, kan användas. Vid en *återspelning* (replay attack) kan en angripare försöka använda en tidigare genomförd verifiering genom att ett tidigare giltigt verifieringsresultat skickas till myndigheten. En effektiv åtgärd för att mot-

verka sådana attacker är att backend-systemet kontinuerligt kontrollerar status på ett sessions-ID, genom att det anges som exempelvis ”Skapat”, ”Aktivt”, ”Genomfört” och ”Utgånget”. En *falsk verifiering* kan genomföras genom att angriparen skapar en falsk QR-kod eller länk, i syfte att imitera en giltig verifieringsbegäran från en myndighet och förmå någon att genomföra en verifiering mot en skadlig applikation eller webbsida, för att stjäla biometriska underlag och biometriska uppgifter från – eller kapa identiteten för – den som utsätts för attacken.

Även om det alltså finns möjliga sätt att angripa en verifieringsprocess som utformas enligt ovan beskrivna modell anser vi att en robust konstruerad teknisk lösning effektivt kan motverka sådana hot. Informationssäkerhetsmässiga faktorer utgör därför inte, som vi ser det, något hinder mot att tillämpa den beskrivna modellen för att initiera en verifieringsbegäran och koppla denna till en viss användares mobilapplikation (se även avsnitt 28.2.4).

Steg 2: Inläsning av relevanta uppgifter från handlingen

Mobilapplikationen visar viss information för användaren som namn på den verifierande myndigheten, syfte och instruktioner. Applikationen läser också optiskt av MRZ-fältet och samtidigt det NFC-chip som finns i handlingen som används för den biometriska jämförelsen. Relevanta uppgifter som läses från NFC-chippet är identitetsuppgifter och andra alfanumeriska uppgifter (DG1), biometriska underlag (DG2) samt SOD, som innehåller en digital signatur med handlingens data. Biometriska underlag i form av fingeravtryck som är lagrade i handlingen (DG3) behöver däremot inte läsas in.

Steg 3: Äkthetskontroll av handlingen och dess innehåll

En kryptografisk verifiering görs av dokumentets äkthet, för att verifiera att handlingen är utfärdad av rätt stat och att uppgifterna i den är oförändrade, och för att kunna få åtkomst till den information som är lagrad i NFC-chippet. Verifieringen görs med hjälp av nationella och internationella certifikat som tillhandahålls av betrodda dokumentutfärdare (CSCA[13]), till exempel Polismyndigheten i Sverige.

[13] Country Signing Certification Authority.

Äkthetskontrollen kan göras antingen i backend-systemet eller helt lokalt i mobilapplikationen. I förstnämnda situation – som under vårt arbete är det som har förordats – hanteras data ur SOD och kontrollen mot CSCA centralt; certifikaten hämtas från en centralt underhållen trust store. En fördel med en sådan modell är en mer enhetlig verifieringslogik – i synnerhet om även den efterföljande biometriska jämförelsen görs i backend-systemet – och att det är enklare att hantera uppdateringar av CSCA-certifikaten, då dessa inte behöver uppdateras i mobilapplikationen, antingen genom en schemalagd uppdatering eller i samband med att verifiering sker i ett enskilt fall. Samtidigt innebär en äkthetskontroll som görs i backend-systemet ett behov av en mer kontinuerlig kommunikation mellan mobilapplikationen och systemet under verifieringsprocessen. Vi ser emellertid inte detta som något avgörande som talar mot en sådan ordning; någon form av kommunikation kommer alltid att vara nödvändig i något steg av verifieringsprocessen och mobilapplikationen bör – om ett avbrott inträffar – kunna meddela användaren detta på lämpligt sätt så att ett nytt försök kan genomföras.

Steg 4: Upptagning av biometriska underlag (ansiktsbild)

Personen använder därefter applikationen för att ta en ansiktsbild av sig själv. För att säkerställa att bilden är matchningsbar och korrekt bör ett flertal kontroller utföras, bland annat en så kallad livenesscheck för att säkerställa att bilden avser en levande, närvarande person, att bilden verkligen kommer från kamerans bildsensor samt att bilden överförs i oförvanskat skick. Vägledande för vilka kontroller som kan behöva implementeras är avsnitt 5.1 i ISO/IEC 30107-3, som är en internationell standard för skydd mot så kallad spoofing vid ansiktsigenkänning. Kontroller behöver göras av att ansiktet är centrerat på rätt sätt, att bildkvaliteten är tillräcklig och att delar av ansiktet inte är täckt, exempelvis av glasögon eller hår. Applikationen behöver kunna guida användaren rätt.

I vart fall liveness-checken bör enligt vår mening som utgångspunkt ske helt och hållet i mobilapplikationen. I annat fall skulle en kontinuerlig kommunikation behöva upprätthållas mellan applikationen och backend-systemet. När det gäller kontroller för att säkerställa att ansiktsbilden är korrekt i övrigt skulle denna logik däremot kunna

förläggas i backend-systemet, för att i högre grad främja att ett enhetligt jämförelseunderlag alltid tas fram och används. Detta kan främja en högre träffsäkerhet vid den biometriska jämförelsen. Att i stället genomföra kontroller av sistnämnda slag i mobilapplikationen innebär vissa risker. I likhet med mobilt BankID kommer applikationen att kunna installeras och köras på hårdvara av olika slag. Kvaliteten på kameran i användarens enhet och tillgång till NFC-läsare kan då variera. Även CPU/GPU-resurser kan skilja sig åt betydligt. Att inom ramen för ett gemensamt och kraftfullare backend-system kunna utföra nödvändig behandling och kontroll av ansiktsbilden som tagits upp med en mobilkamera kan därför vara av vikt för att säkerställa att ett korrekt och över tid enhetligt formaterat jämförelseunderlag används. Om kontrollerna ska göras i mobilapplikationen ställs högre krav på vilka mobilenheter som kan användas, utformningen av mobilapplikationen ur prestandasynpunkt och användarvänlighet. För att på ett säkert sätt kunna hantera en heterogen verifieringsmiljö kan det vid utveckling och drift av systemet i större utsträckning krävas personal som har särskild kompetens och erfarenhet av olika mobilplattformar. Vi kan emellertid också se en vinst i att nu aktuella kontroller av de biometriska underlagen helt görs i mobilapplikationen, genom att det avlastar backend-systemet, bland annat genom att onödiga anrop till systemet undviks. Återkoppling till den enskilde för det fall ansiktsbilden behöver korrigeras och tas upp på nytt kan också göras snabbare om kontrollen görs direkt i mobilapplikationen.

En hybrid-modell, där vissa kvalitetskontroller och viss presentationsattackdetektion (PAD) görs i mobilapplikationen, men den slutliga kontrollen görs i backend-systemet, skulle enligt vår mening också kunna utgöra ett alternativ.

Steg 5: Extraktion och jämförelse av biometriska uppgifter

De biometriska underlag som hämtats genom kameran i mobilapplikationen och ur NFC-chippet på handlingen används därefter för att ta fram biometriska uppgifter som används för den biometriska jämförelsen. Dessa delar kan vara förhållandevis resurskrävande; inte minst den biometriska jämförelsen kan kräva viss processorkraft. Under vårt arbete har förordats att dessa delar av verifieringsproces-

sen alltid bör hanteras i backend-systemet. Det finns som vi ser det argument som talar både för och emot detta.

Ett system för säkrare verifiering av identitet av det slag vi föreslår kan – i verifieringsprocessen – visserligen tänkas möta liknande utmaningar som de utfärdare av e-legitimationer som använder sig av biometriska jämförelser. Det skulle därför vara rimligt att den tekniska lösning som kan komma att användas för att implementera våra förslag som lägst bör motsvara kraven i det svenska tillitsramverket för svensk e-legitimation, som återspeglar den praxis som gäller för motsvarande funktioner i eIDAS-ramverket. Vi är inte av någon annan uppfattning än att framtagningen av biometriska uppgifter och den biometriska jämförelsen, inom ramen för en sådan teknisk lösning som vi beskriver i detta avsnitt, bör genomföras på ett sätt som så långt som möjligt följer dessa rekommendationer, vilka syftar till att säkerställa en tillförlitlig verifieringsprocess. Något uttryckligt krav på att de nu aktuella momenten ska utföras inom ramen för ett centralt backend-system kan vi emellertid inte utläsa av ICAO:s dokument 9303 eller andra standarder. Enligt vår mening framstår det även som rimligt att kraven på att kontrollera verifieringsprocessens olika steg är högre vid skapandet av en e-legitimation – som är en bestående digital identitetshandling – än vid biometrisk verifiering av identitet med stöd av den nya lagen, vilket utgör en särskild utredningsåtgärd; effekterna av att verifieringsprocessen skulle manipuleras i ett enskilt fall är därmed betydligt mer begränsade. Om verifieringen görs på plats, men med hjälp av en mobilapplikation, är det också möjligt för företrädaren för den verifierande myndigheten att direkt kontrollera att upptagning av ansiktsbilden görs på rätt sätt och att mobilapplikationen inte på annat sätt manipuleras.

Med detta sagt är frågan emellertid om det utifrån nuvarande teknik – och med beaktande av andra relevanta faktorer – är lämpligt att placera funktionalitet för att ta fram biometriska uppgifter och genomföra den biometriska jämförelsen i en mobilapplikation.

Som nämnts ovan är funktioner av nämnda slag, särskilt den biometriska jämförelsen, beräkningsintensiva processer. De kan involvera tillämpning av avancerade matematiska modeller och maskininlärning. Den biometriska analysen av de biometriska underlagen bör som utgångspunkt göras på flera nivåer. Algoritmerna och teknikerna måste vara tillförlitliga och testade så att risken för så kallade falska positiva utslag hålls mycket låg. Moderna mobiltelefoner

innehåller vanligtvis förhållandevis kraftfull hårdvara, som i många fall är fullt kapabel att utföra denna typ av beräkningar i en applikation på telefonen. Det kan emellertid inte förutsättas att alla enskilda vars identitet kan behöva verifieras biometriskt också har tillgång till en mobilenhet som uppfyller de hårdvarukrav som kan vara aktuella; som jämförelse kan vi notera att vid biometrisk verifiering av identitet med hjälp av en sådan mobilapplikation som Storbritanniens inrikesministerium har tagit fram inom ramen för identitetsplattformen för digitala offentliga tjänster – GOV.UK One Login (se avsnitt 27.5) – krävs att en iPhone 8 eller en Android-telefon utrustad med Android 10 eller nyare används.[14] I ett backend-system – vilket generellt sett kan antas vara kraftfullare än en mobilenhet – kan dessa funktioner göras mer komplexa och därmed mer träffsäkra. Detta minskar risken för både falska positiva och falska negativa resultat av jämförelsen. En centraliserad modell – som kan kräva att många samtidiga beräkningsintensiva anrop hanteras – ställer emellertid större krav på robusthet, tillgänglighet och skalbarhet. Detta kan medföra större kostnader för framför allt den hårdvara som behövs, jämfört med om hårdvaran i praktiken utgörs av den enskildes mobilenhet.

Om såväl framtagning av biometriska uppgifter som den biometriska jämförelsen görs i backend-systemet kan en högre grad av kontroll av exekveringsmiljön uppnås. Det minskar risken för manipulation av processen och möjliggör en mer enhetlig styrning och kontroll av de komponenter och algoritmer som används; samma modell och samma parametrar används för alla användare, oberoende av vilken typ av mobilenhet användaren har. Detta främjar även en enhetlig kvalitet i resultaten och förenklar uppdateringar som kan behöva göras av dessa för verifieringsprocessen centrala komponenter. Exempelvis kan förbättringar i matchningsmodeller eller ändringar i tröskelvärden införas snabbare och oberoende av att användarna uppdaterar mobilapplikationen.

En tydlig fördel med att extraktion av biometriska uppgifter och den biometriska jämförelsen genomförs endast i mobilapplikationen är att uppgifterna då skulle behandlas helt lokalt, på en enhet som den enskilde förfogar över. Känsliga personuppgifter behöver inte heller överföras till ett backend-system, vilket ligger i linje med principen om uppgiftsminimering i dataskyddsförordningen. En centraliserad

[14] https://www.gov.uk/guidance/using-the-govuk-id-check-app, senast besökt den 7 juli 2026.

hantering av biometriska jämförelser ökar också risken för en central attackyta. Vidare kan användarupplevelsen antas vara bättre om mindre information behöver överföras till backend-systemet, genom minskad nätverkslatens. Detta kan dock antas medföra minimal påverkan i normalfallet. Med en övervägande ”lokal” modell skulle den verifierande myndighetens insyn i och kontroll av verifieringsprocessen minska, med en ökad risk för att processen utsätts för angrepp av olika slag, exempelvis genom så kallad jailbreaking[15] (se mer om detta i avsnitt 28.2.4). Detta eftersom den biometriska jämförelsen behöver utföras i en klientmiljö som kan variera stort, både vad gäller mobiloperativsystem och hårdvara. Kraven på särskild teknisk kompetens om en sådan miljö hos den aktör som är ansvarig för backend-systemet skulle också öka.

Steg 6: Överföring av resultatet av den biometriska jämförelsen

Resultatet av den biometriska jämförelsen behöver göras tillgängligt för den myndighet som begärt att den enskilde ska verifiera sin identitet biometriskt. Resultatet, i form av Pass/Fail eller ett jämförelsevärde, och relevanta DG1-uppgifter i form av identitetsuppgifter och identitetsbeteckning, förs över antingen direkt från eller via backend-systemet, beroende på var den biometriska jämförelsen har genomförts tekniskt. Det kan här noteras att uppehållstillståndskort som har utfärdats av svenska myndigheter inte innehåller uppgifter om Migrationsverkets individnummer (se avsnitt 19.3.3). Den uppgiften kommer alltså inte att göras tillgänglig för myndigheten som har begärt verifieringen, om ett sådant kort används för verifieringen. Mobilapplikationen behöver även på lämpligt sätt notifiera den enskilde om att verifieringen har genomförts på ett korrekt sätt.

Eftersom verifieringsresultatet kan behöva kopplas till en specifik individ och ett specifikt ärende hos den verifierande myndigheten krävs standardiserade gränssnitt mellan ett backend-system och myndighetens egna ärendesystem. Utan en sådan standardisering finns en risk för ökad komplexitet och varierande implementeringar mellan myndigheter.

[15] Jailbreaking innebär att man tar bort de digitala begränsningar som en tillverkare har lagt in i enhetens operativsystem.

27.4.2 Nödvändiga systemkomponenter

Som vi noterat inledningsvis i avsnitt 27.1 anser vi att det inom ramen för detta betänkande inte är möjligt att på detaljnivå föreslå hur de tekniska modeller för biometrisk verifiering som vi beskriver bör eller ska implementeras. Det kan emellertid vara av värde att på ett övergripande plan åskådliggöra vilka systemkomponenter som kan vara nödvändiga i vart fall i en verifieringsprocess som bygger på ett system med myndighetsgemensamma komponenter, för att identifiera eventuella problem eller risker. I detta avsnitt lämnar vi därför en sådan översikt.

Mobilapplikationen

Ett system som bygger på biometrisk verifiering mot handlingar är i sig dokumentcentrerat. Handlingarna fungerar som tillitsankare i en sådan verifieringsprocess. Även om huvuddelen av verifieringslogiken bör förläggas till ett backend-system (se avsnitt 27.6) är utformningen av mobilapplikationen av central betydelse; den behöver kunna läsa av handlingen och utföra en NFC-baserad dokumentverifiering, om äkthetskontrollen ska utföras i applikationen. En utmaning ligger oavsett i att göra mobilapplikationen smidig och intuitiv att använda för den person vars identitet ska verifieras. Den måste också innehålla teknik som skyddar mot och motverkar så kallade presentation attacks, exempelvis att en bild, en mask eller någon annan teknisk attack används i syfte att använda ett annat jämförelseunderlag än de biometriska kännetecken som tillhör personen som ska verifieras. Även skydd mot manipulering av mobilapplikationen som sådan måste säkerställas. Mobilapplikationen behöver enligt vår mening i vart fall bestå av följande typer av tekniska moduler.

En *UI-modul*, det vill säga användargränssnittet, som visar vilken myndighet som har begärt verifieringen och syftet med begäran och som kan vägleda den enskilde genom verifieringsprocessen på ett intuitivt sätt. Användargränssnittet bör utformas så att användaren, det vill säga den verifierande myndigheten, väljer om verifiering av identitet i det enskilda fallet ska genomföras på distans eller på plats. I syfte att sköta kommunikationen med backend-systemet, det vill säga hantera sessions-ID samt ta emot en verifieringsbegäran och skicka biometriska underlag och relevanta alfanumeriska uppgifter

till systemet, behövs en *sessions- och säkerhetsmodul.* Vidare behövs en *NFC- och dokumentmodul* som hanterar läsning av MRZ-fältet för att härleda nycklar för BAC eller PACE-autentisering, och läsning av NFC-chippet (DG1, DG2 och SOD). Modulen behöver även, om detta inte görs i backend-systemet, kunna utföra en passiv autentisering för att verifiera att uppgifterna som hämtas är oförändrade och att handlingen är utfärdad av rätt stat. Detta kräver att DS-certifikatet läses in, och tillgång till ett CSCA-certifikat, vilket kan levereras med applikationen, för det fall en sådan lösning väljs.

Utöver dessa komponenter förutsätts att mobilapplikationen innehåller en *biometrimodul*, som används för att ta upp biometriska underlag från handlingen och från användaren med hjälp av kameran på telefonen. Modulen behöver, tillsammans med UI-modulen, kunna styra användaren, exempelvis genom att ange att han eller hon ska titta framåt eller vrida huvudet, och genomföra liveness-check för att upptäcka manipuleringsförsök i form av fotografier på papper, deepfakes eller masker.

Backend-systemet

Ett backend-system, vilket fungerar som en länk mellan mobilapplikationen och den verifierande myndigheten och eventuella ärendehanteringssystem som myndigheten använder, behöver – med utgångspunkten att huvuddelen av verifieringslogiken i form av att ta fram biometriska uppgifter ur de biometriska underlagen och att genomföra den biometriska jämförelsen placeras i systemet – bestå av flera olika tekniska komponenter. Utöver de som beskrivs nedan krävs även tekniska system som stöd för såväl verifieringsprocessen som underhåll och drift. Bland annat bör det finns ett system för risk- och bedrägerihantering, som kan upptäcka mönster som till exempel onormalt många misslyckade verifieringsförsök från en viss mobilenhet eller att verifiering görs från ovanliga tidszoner. Vidare krävs en portal för att hantera anslutna myndigheter, loggar, statistik och för att administrera trösklar för när en matchning ska anses lyckad. Personuppgifter, däribland biometriska uppgifter, ska inte sparas utan loggar bör endast omfatta skapade sessioner och annan liknande information.

De särskilda tekniska komponenter som ett myndighetsgemensamt backend-system kan förväntas behöva innehålla är för det första en *central servermodul* med ett gränssnitt för att ta emot en begäran om att starta en verifiering, hantera skapande av sessions-ID och skicka detta till myndigheten och till mobilapplikationen, samt hantering av status för sessionen. Systemet behöver bland annat kontrollera att svaret från mobilapplikationen kommer från rätt session och att det kommer inom ett givet tidsfönster för att motverka exempelvis så kallade replay-attacker, vilket innebär att en angripare fångar upp giltig information (exempelvis en inloggning) och spelar upp den igen för att få obehörig åtkomst. Modulen levererar även ett svar till myndigheten – genom att exponera detta genom ett lämpligt gränssnitt – som innefattar om verifieringen lyckades, eventuellt med angivande av matchningsresultat, identitetsuppgifter och identitetsbeteckning för att kunna manuellt kontrollera uppgifterna och jämföra dem med de som den enskilde lämnat om sin identitet, exempelvis i en ansökan. En *modul för certifikatshantering* (trust store) behöver också finnas, som kan säkerställa att uppdaterade certifikat (CSCA-certifikat och DS-certifikat) är tillgängliga för de handlingar som ska kunna användas för den biometriska verifieringen. Certifikaten kan antingen lagras i modulen och hämtas efterhand, eller uppdateras direkt till mobilapplikationen hos användaren. Även en *attributmodul*, som hanterar vilka uppgifter som får lämnas ut till den myndighet som begär verifieringen samt hanterar trösklar för när en lyckad matchning ska anses ha genomförts, behöver som vi ser det finnas.

Om logik för extrahering av biometriska uppgifter ur de biometriska underlagen, och den biometriska jämförelsen, ska utföras i backend-system förutsätts även att det innehåller en *biometrimodul*. Modulen kan även utföra viss ytterligare förbehandling av de biometriska underlagen, utöver vad som gjorts i mobilapplikationen. Framtagning av de biometriska uppgifterna (mall) och matchning görs med hjälp av särskilda modeller – exempelvis ResNet-baserade[16] modeller – som utgår från djupinlärning och som har tränats på stora ansiktsdatamängder. Utifrån en-mot-en-jämförelsen av de biometriska uppgifterna räknar modulen ut ett jämförelseresultat, samt Pass/Fail, utifrån satta tröskelvärden.

[16] En ResNet-baserad modell (Residual Network) är en typ av djupinlärningsarkitektur inom artificiell intelligens, specifikt använd för datorseende (computer vision) och bildanalys.

Gränssnitt mot den verifierande myndighetens system

Det kan även behöva utvecklas gemensamma gränssnitt som hanterar kontakten med backend-systemet, dels när en verifieringssession startas, dels för att hämta in resultatet av den biometriska jämförelsen och identitetsuppgifter och föra in dessa uppgifter i den verifierande myndighetens egna system, exempelvis ett ärendehanteringssystem. Hur sådana gemensamma gränssnitt bör utformas är som vi ser det beroende av hur befintliga ärendehanteringssystem och andra tekniska system hos olika myndigheter är uppbyggda, och vilket behov den enskilda myndigheten har av att biometriskt verifiera identitet mot handlingar på distans. Med hänsyn till att myndigheters befintliga system kan skilja sig åt betydligt är det inte möjligt att inom ramen för detta betänkande närmare beskriva hur kopplingen till backend-systemet bör lösas tekniskt. Som vi återkommer till i avsnitt 27.6 är det emellertid av vikt att dessa komponenter utformas på ett standardiserat sätt.

27.4.3 Särskilt om koppling till en svensk identitetsbeteckning och till Migrationsverkets individnummer

Vår bedömning

Det bör inom ramen för denna utredning inte övervägas att införa ett särskilt register för att koppla samman en utländsk identitetshandling, eller ett uppehållstillståndskort som har utfärdats av svenska myndigheter, med en svensk identitetsbeteckning eller Migrationsverkets individnummer.

För att kunna använda en handling för att biometriskt verifiera identitet behöver en koppling kunna etableras mellan den påstådda identiteten och handlingen. Eftersom flera individer kan ha samma identitet – utifrån hur vi definierat begreppet i detta betänkande i avsnitt 3.2 och 23.5.2 – kan det ifrågasättas om det är tillräckligt att verifieringen görs mot en handling som är utfärdad för en viss identitet, eller om det måste gå att säkerställa att den är utfärdad till den *individ* som förekommer i ett visst ärende eller som den verifierande myndigheten möter i samband med en identitetskontroll i annat fall, exempelvis genom att handlingen innehåller ett person- eller samordningsnum-

mer som är unikt och som kan kontrolleras. Utifrån den process som vi beskrivit i avsnitt 27.4.1 bör backend-systemet – efter genomförd verifiering – skicka dels resultatet av den biometriska jämförelsen, dels identitetsuppgifter och eventuell identitetsbeteckning som lästs av från handlingen av mobilapplikationen till myndigheten. På det sättet kan myndigheten bekräfta att handlingen som använts också är utfärdad för rätt individ, inte bara i rätt identitet.

Vi har i avsnitt 23.6.2 föreslagit att bland annat hemlandspass och identitetskort som har utfärdats av utländska myndigheter, som utgångspunkt, bör kunna användas för att biometriskt verifiera identiteten. Till skillnad från sådana handlingar som utfärdas av svenska myndigheter innehåller de inte en svensk identitetsbeteckning, och ett uppehållstillståndskort innehåller inte heller det unika individnummer som tilldelas av Migrationsverket. Vid en verifiering mot dessa typer av handlingar kommer backend-systemet inte att kunna göra en unik beteckning tillgänglig i svaret till den verifierande myndigheten, utan endast uppgifter om innehavarens identitet.

Detta kan leda till att den biometriska verifieringen inte anses tillförlitlig, på så sätt att verifieringen inte bekräftar att personen är den individ som har ett visst personnummer, samordningsnummer eller individnummer. Exempelvis kan person A – som är tysk medborgare – ansöka om en förmån, men utge sig för att vara den tyske medborgaren B. De båda personerna A och B har samma identitetsuppgifter (namn, födelsetid och medborgarskap), men av naturliga skäl olika personnummer om de har ett sådant. Om A vid en begäran om att verifiera sin identitet biometriskt använder sig av sitt tyska pass kommer utnyttjandet av B:s identitet inte att upptäckas, eftersom backend-systemet inte returnerar en unik identitetsbeteckning från handlingen i samband med verifieringen. Myndigheten skulle därför på något annat sätt behöva kunna koppla handlingen till den identitet som förekommer i ärendet, för att säkerställa att handlingen som används för verifieringen avser rätt person. Detta förutsätter emellertid att uppgifter som möjliggör en koppling – exempelvis ett dokumentnummer – får behandlas i myndighetens verksamhet, och att sådana uppgifter sedan tidigare har registrerats. Ett problem är också att en uppgift som utgår från exempelvis ett dokumentnummer snabbt kan bli inaktuellt, när personen förnyar handlingen. Tidigare registrerade uppgifter om handlingar har därmed en begränsad användning om de inte kontinuerligt uppdateras, vilket i sin tur förutsätter att

den enskilde på eget initiativ kontaktar svenska myndigheter för att uppdatera uppgifterna. En uppgift som används för att koppla samman en utländsk handling eller ett uppehållstillståndskort med en svensk identitetsbeteckning eller Migrationsverkets individnummer måste också vara åtkomlig för samtliga myndigheter som, enligt våra förslag i avsnitt 23.5, ska få använda handlingar för biometrisk verifiering av identitet. Detta förutsätter någon form av centralt register, i likhet med det kopplingsregister som Skatteverket för några år sedan lämnade förslag om avseende en koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar.[17]

Ett system av ovan beskrivet slag skulle enligt vår bedömning vara komplext att genomföra, både praktiskt och juridiskt. Eftersom det sannolikt också skulle kräva den enskildes aktiva medverkan är risken uppenbar att tillförlitligheten i ett eventuellt register inte går att upprätthålla och att det skulle få en begränsad nytta i praktiken. Vidare anser vi att det kan ifrågasättas om avsaknaden av en kopplingsmöjlighet utgör en mer framträdande risk i praktiken. För det första förutsätts att den person vars identitet utnyttjas och den person som genomför identitetsbedrägeriet har samma identitet. Redan detta begränsar betydligt möjligheten att utnyttja någon annans identitet, jämfört med om en biometrisk verifiering inte kan användas. Till detta kommer att vi i avsnitt 19.4 bedömt att myndigheter bör kunna välja vilken eller vilka handlingar som i ett enskilt ärende används för verifiering, och att det finns anledning att i första hand kräva att handlingar som är utfärdade av svenska myndigheter görs tillgängliga, när detta är möjligt. Ett krav på att i första hand använda en handling utfärdad av svenska myndigheter, som innehåller en identitetsbeteckning, kan visserligen antas vara svårt att upprätthålla i det enskilda fallet, i synnerhet om en biometrisk verifiering görs på distans. Det får emellertid ankomma på myndigheten som vill verifiera identiteten att vidta de utredningsåtgärder som kan krävas i det enskilda fallet, för att motverka risker av ovan nämnda slag.

Vid en sammantagen bedömning av det ovan anförda anser vi att det – i vart fall inom ramen för denna utredning – inte bör övervägas att införa ett register för att koppla samman en utländsk identitetshandling eller ett uppehållstillståndskort med en svensk identitetsbeteckning eller Migrationsverkets individnummer.

[17] Skatteverket, *Fördjupad utredning rörande koppling mellan utländska eID-handlingar och svenska identitetsbeteckningar*, den 21 januari 2019, dnr 20227351-19/113.

27.5 Internationell utblick – GOV.UK One Login

I detta sammanhang kan det vara av intresse att kort belysa den plattform för digitala offentliga tjänster – vilken bygger bland annat på biometrisk verifiering av identitet mot handlingar – som har implementerats av brittiska myndigheter: GOV.UK One Login. Plattformen drivs av myndigheten Government Digital Service (GDS) i nära samverkan med bland annat Storbritanniens inrikesministerium och syftar till att skapa en enhetlig och återanvändbar digital identitet för medborgare och invånare.

Vid verifiering med hjälp av GOV.UK One Login tillåts i första hand användning av biometriska passhandlingar och nationella identitetskort (i den mån de uppfyller relevanta tekniska krav), brittiska körkort samt biometriska uppehållstillståndskort såsom Biometric Residence Permit och Biometric Residence Card. Dessa typer av handlingar motsvarar som vi ser det i allt väsentligt de typer som vi i avsnitt 23.6.2 har föreslagit ska kunna användas för biometrisk verifiering, med undantag för körkort. Urvalet av handlingstyperna i det brittiska systemet härrör enligt vår bedömning från de övergripande kriterier som vi också beaktat, nämligen tillförlitlighet i utfärdandet, maskinell verifierbarhet och ett mål att omfatta en så bred personkrets som möjligt. Körkort saknar i regel motsvarande kryptografiska skydd som numera finns i passhandlingar och nationella identitetskort, men accepteras trots detta i GOV.UK One Login, med hänsyn till dess höga utbredning i befolkningen.

Den biometriska komponenten i systemet utgörs huvudsakligen av biometriska jämförelser av uppgifter som tas fram ur en ansiktsbild, vilken extraheras från den aktuella handlingen (antingen via avläsning av ett NFC-chip eller optisk avläsning av den synliga ansiktsbilden), och uppgifter som tas fram genom en live-upptagning som genereras genom användarens mobilkamera. Upptagningen innefattar en liveness-kontroll. Även om de tekniska metoderna inte är offentliga, är det enligt vår bedömning rimligt att anta att de följer etablerade branschstandarder och relevanta internationella standarder, bland annat ICAO:s dokument 9303, för att motverka olika former av attacker, exempelvis genom analys av rörelser, reflektioner eller tredimensionella egenskaper, på det sätt vi beskrivit ovan. I likhet med den möjliga verifieringsprocess som vi beskrivit i avsnitt 27.4 spelar

mobilapplikationen – som kan laddas ner i antingen Apple App Store eller Google Play Store – en betydelsefull roll.

Verifieringsprocessen initieras typiskt inom ramen för en specifik myndighetstjänst, varefter användaren dirigeras till GOV.UK One Login och därifrån vidare till mobilapplikationen via en sessionsbunden länk, ofta i form av en QR-kod eller en djuplänk (jfr avsnitt 27.4.1). Denna koppling säkerställer att den information som samlas in i mobilapplikationen entydigt kan knytas till rätt användare och rätt ärende. Det har inte varit möjligt att finna någon säker information avseende om den biometriska jämförelsen av de underlag som tagits upp i mobilapplikationen och de som är lagrade i en viss handling görs i applikationen eller i ett backend-system. Av information som beskriver hur man använder applikationen för att verifiera sin identitet framgår emellertid bland annat att när användaren har skannat sitt ansikte med appen och informationen har skickats in, slutförs verifieringen av identitet på den GOV.UK-tjänst som användaren vill logga in i.[18] Det skulle enligt vår mening kunna tala för att den biometriska jämförelsen inte görs i mobilapplikationen utan i ett backend-system. Resultatet av verifieringsprocessen är inte en överföring av biometriska uppgifter till den myndighet som den enskilde interagerar med, utan backend-systemet skapar ett identitetsintyg som innehåller uppgifter om att en viss identitet har verifierats till en viss tillitsnivå, samt i förekommande fall ett begränsat urval av personuppgifter såsom namn och födelsedatum.

27.6 Sammanfattande slutsatser

Vår bedömning

Våra förslag kan implementeras dels med hjälp av tekniska system som den verifierande myndigheten ansvarar för, dels med en teknisk lösning som bygger på myndighetsgemensamma komponenter i form av en mobilapplikation och ett backend-system.

Det bör som utgångspunkt överlåtas till den verifierande myndigheten att avgöra vilken teknisk modell som bör användas. Sistnämnda modell bör dock övervägas i första hand, eftersom den

[18] https://www.gov.uk/guidance/proving-your-identity-with-the-govuk-one-login-app#how-to-finish-proving-your-identity, senast besökt den 7 juli 2026.

gör det möjligt att biometriskt verifiera identitet såväl på distans som på plats. Tyngdpunkten för verifieringslogiken bör då finnas i backend-systemet.

I avsnitt 27.3 och 27.4 har vi beskrivit de två huvudalternativ som vi anser bör vara aktuella för att tekniskt kunna implementera våra förslag om en utökad möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar. Utifrån den tekniska analysen i dessa avsnitt bedömer vi att våra förslag kan implementeras genom båda alternativen. Som vi varit inne på i inledningen till avsnitt 27.3 och 27.4 finns det emellertid för- och nackdelar med respektive verifieringsprocess som beskrivs i nämnda avsnitt.

När det gäller en process som bygger på användning av tekniska system som den verifierande myndigheten ansvarar för är en uppenbar begränsning att verifiering endast kan göras när den enskilde befinner sig på plats, inte på distans. Samtidigt gör detta att den verifierande myndigheten har en större insyn och kontroll över processen, jämfört med om den genomförs helt på distans. Exempelvis behöver system för att upptäcka manipulation av en mobilapplikation eller av upptagningen av biometriska underlag inte utvecklas, och en serverstruktur för att hantera ett backend-system – med krav på robusthet och kontinuerlig drift samt hantering av många samtidiga verifieringar – är inte en förutsättning för att kunna genomföra en biometrisk verifiering. Att ta fram en teknisk lösning som bygger på myndighetsgemensamma komponenter i form av en mobilapplikation och ett backend-system kan – som lyfts av företrädare för Skatteverket under vårt arbete – innebära en implementeringstid om minst 12 till 24 månader. Även om en verifieringsprocess som bygger på tekniska system som den verifierande myndigheten ansvarar för kan kräva tid för bland annat upphandling av nödvändiga tekniska komponenter och programvara, bör en sådan process kunna medföra att våra förslag snabbare kan implementeras. Detta särskilt om befintliga system – exempelvis de som Skatteverket förvaltar och som används på Statens servicecenter i dag – kan utnyttjas.

En sådan verifieringsprocess som vi beskrivit i avsnitt 27.4 innebär också – för det fall huvuddelen av verifieringslogiken förläggs till ett backend-system – att biometriska underlag och andra uppgifter behöver överföras och hanteras centralt, vilket medför särskilda risker för den personliga integriteten; det bör emellertid beaktas att

uppgifterna inte ska lagras i backend-systemet utan endast finns där momentant, för den tekniska bearbetning som krävs för att genomföra verifieringen. Motsvarande risker gör sig – som vi ser det – inte gällande om verifieringsprocessen genomförs på plats, med hjälp av system som den verifierande myndigheten har tagit fram och förfogar över.

Nämnda risker, vilka i första hand är hänförliga till om verifieringsprocessen byggs på en sådan teknisk lösning som vi beskrivit i avsnitt 27.4, bör som vi ser det dock inte överdrivas, utan borde kunna hanteras genom att de tekniska systemen utformas med detta i åtanke. Vi saknar anledning att utgå från annat än att systemen utformas på ett sätt som uppnår tillräckligt skydd mot intrång, manipulation av sessionshantering och överbelastningsattacker. Det är viktigt att säkerställa riktighet, spårbarhet och skydd mot obehörig åtkomst. Infrastrukturen behöver byggas robust med en hög uthållighet så att fel i enskilda komponenter, nätverkstjänster eller system inte leder till avbrott eller störningar. Hur detta i detalj bör implementeras är emellertid inte möjligt för oss att bedöma eller lämna förslag om. Som pekats på under vårt arbete och som vi återkommer till i kapitel 29 kan en viktig del i att motverka risker hänförliga till informations- och cybersäkerhet i ett system av det slag vi beskrivit i avsnitt 27.4 vara att säkerställa att det finns en tydlig offentlig rådighet över hur lösningen utvecklas och förvaltas, och att ansvaret samlas inom en och samma myndighet. Även om en viss myndighet pekas ut bör den samarbeta med andra aktörer som har särskild kompetens inom området informations- och cybersäkerhet och som kan bidra med råd och stöd i framtagandet av infrastrukturen samt vid upphandling av drift, system och komponenter. I säkerhetsarbetet kopplat till riskanalyser och säkerhetsåtgärder behöver även underleverantörer och deras eventuella underleverantörer ingå, i syfte att upprätthålla nödvändig säkerhet i hela systemet. Uppföljning och tester bör ske genom återkommande säkerhetsgranskningar, revisioner och penetrationstester. Detta kan göras genom stöd från myndigheter med särskild kompetens på området, men det kan även upphandlas på marknaden.

Med utgångspunkten att risker av ovan nämnda slag hanteras på ett ändamålsenligt sätt, anser vi att en teknisk lösning som bygger på myndighetsgemensamma komponenter i form av en mobilapplikation och ett backend-system i första hand bör övervägas. Detta med hänsyn till att endast den verifieringsprocess vi har beskrivit i av-

snitt 27.4 gör det möjligt att genomföra en biometrisk verifiering av identitet mot handlingar på distans. Vi bedömer att detta har en helt avgörande betydelse för vilket faktiskt genomslag som våra förslag kan komma att få i praktiken. Särskilt i ärendeslag som rör socialförsäkringsförmåner – vilka är utsatta för omfattande bedrägerier och där ansökan oftast görs på distans – är detta av betydelse. Vi kan i detta sammanhang notera att det alternativ som vi beskrivit i avsnitt 27.4, enligt vår mening, i väsentliga delar uppvisar stora likheter med det brittiska system och den verifieringsprocess som vi redogjort för i avsnitt 27.5. Det brittiska systemet är visserligen ett bredare system för identitetsförvaltning och verifieringsprocessen är av naturliga skäl, ur teknisk synvinkel, därför inte identisk med den process, och de systemkomponenter, som vi beskriver i avsnitt 27.4. I väsentliga delar uppvisar det enligt vår mening emellertid stora likheter; användning av en mobilapplikation för att ta upp biometriska underlag från den enskilde och ur den handling som ska användas för verifieringen, och ett backend-system som har koppling till applikationen och till de myndigheter som vill verifiera identitet. Att den tekniska lösning och verifieringsprocess som vi förordar ligger i linje med ett etablerat system för att biometriskt verifiera identitet talar enligt vår mening för att det också är tekniskt möjligt att genomföra, om ett sådant system för säkrare verifiering som vi föreslår införs i Sverige.

Även med hänsyn till detta saknas naturligtvis hinder mot att den i avsnitt 27.3 beskrivna verifieringsprocessen används som ett komplement, och den kan som vi ser det ha ett värde dels under tiden som en myndighetsgemensam lösning utvecklas, dels i situationer då biometrisk verifiering av olika anledningar genomförs på plats.

En teknisk lösning för verifieringsprocessen som bygger på myndighetsgemensamma komponenter i form av en mobilapplikation och ett backend-system kan kräva särskilda överväganden kring i vilken av dessa delar av systemet som vissa centrala funktioner bör läggas. Vi har i avsnitt 27.4.1 – avseende steg 3 och 5 i den beskriva verifieringsprocessen – lyft fram omständigheter som vi anser bör särskilt beaktas. I nedanstående tabell ges en översikt av de för- och nackdelar med att samla centrala funktioner i backend-systemet respektive i mobilapplikationen som vi har identifierat.

Tabell 27.1 Systemarkitekturmässiga för- och nackdelar

Aspekt	Mobilapplikation	Backend-system
Latens och prestanda	Låg latens och direkt återkoppling	Högre latens på grund av ökad nätverkskommunikation
Dataskyddsaspekter	Biometriska uppgifter lämnar inte mobilenheten	Överföring av biometriska underlag och andra uppgifter över nätverk ger större exponering
Komplexitet	Högre komplexitet på klientsidan som kan kräva uppdateringar	Komplexitet
Versionshantering	Kräver att mobilapplikationen är uppdaterad	Kan uppdateras direkt, utan åtgärd från användarna
Processorkrav	Förutsätter att mobilenheten är tillräckligt kraftfull	Processorkrav
Risk för angrepp	Högre risk, mindre kontroll	Risk för angrepp
Jämförelsemodell	Begränsad av mobilenhetens hårdvara	Mer avancerade algoritmer kan användas
Kontrollmöjligheter	Sämre, heterogen klientmiljö	Större enhetlighet i jämförelseunderlag och resultat

Att samla de centrala funktionerna, i synnerhet den biometriska jämförelsen, i mobilapplikationen har främst fördelar ur dataskyddshänseende, då känsliga personuppgifter endast behöver behandlas lokalt, i en mobilenhet som den enskilde förfogar över. En sådan lösning kan också innebära vissa tekniska och ekonomiska fördelar, genom ett minskat behov av att utveckla och förvalta ett kraftfullt och skalbart backend-system. Användarupplevelsen kan komma att upplevas som smidigare eftersom behovet av kommunikation med backend-systemet minskar, och därmed eventuella fördröjningar på grund av nätverkslatens. Vidare skulle – om all verifieringslogik samlas i mobilapplikationen – en förenklad modell för biometrisk verifiering kunna användas när den enskilde befinner sig på plats hos myndigheten eller när identiteten kontrolleras direkt av en företrädare för myndigheten någon annanstans; initiering av processen skulle kunna genomföras av handläggaren, och resultatet av den biometriska jämförelsen kan visas direkt för honom eller henne, utan kommunikation med ett backend-system.

Det finns enligt vår mening dock starka skäl för att genomföra dels extraktion av biometriska uppgifter, dels den biometriska jämförelsen i ett backend-system. Detta har också framhållits av experter

i utredningen; ett annat synsätt skulle enligt företrädare för Skatteverket gå emot befintliga system- och säkerhetsarkitektoniska principer hos den myndigheten. Vi kan även notera att det brittiska system som beskrivits i avsnitt 27.5 synes bygga på en sådan fördelning av verifieringslogiken. Om framtagning av de biometriska uppgifterna sker i backend-systemet behöver sådana uppgifter inte överföras från mobilapplikationen. Med huvuddelen av verifieringslogiken koncentrerad till backend-systemet möjliggörs en större kontroll över processen och en enhetlighet i hur kontrollerna genomförs. Detta har som vi ser det avgörande betydelse för möjligheten att motverka olika former av angrepp mot verifieringsprocessen, och därmed resultatet av den. Uppdatering av centrala funktioner, i takt med att exempelvis relevanta algoritmer utvecklas, kan också implementeras snabbare, utan att vara avhängig av att användarna uppdaterar mobilapplikationen. Kraftfullare hårdvara, som kan främja ett mer träffsäkert resultat, kan också användas. Detta kan vara av vikt för att minska antalet felaktiga träffar och bidra till att upprätthålla tillförlitligheten till verifieringsprocessen.

Med särskilt beaktande av främjandet av en kontrollerad exekveringsmiljö anser vi sammantaget att tyngdpunkten för verifieringslogiken – det vill säga i vart fall extraktion av biometriska uppgifter och den biometriska jämförelsen – bör samlas i backend-systemet. Ytterligare överväganden och utvärdering i samband med att en viss teknisk lösning tas fram, utifrån då tillgänglig teknik och med beaktande av eventuella särskilda risker i fråga om informationssäkerhet, cybersäkerhet och skydd för den personliga integriteten som kan identifieras utifrån vald teknisk implementering, kan dock behövas.

En fråga som har lyfts under vårt arbete är om det ska vara obligatoriskt för de verifierande myndigheterna att använda en specifik teknisk modell, företrädesvis någon av de två alternativ vi redogjort för i detta kapitel, vid biometrisk verifiering av identitet med stöd av den nya lagen. Redan med hänsyn till att vi – utifrån de svårigheter i fråga om bland annat den tekniska utvecklingen som vi pekat på i inledningen till detta kapitel – inte avser att lämna några författningsförslag om hur våra förslag bör tekniskt implementeras, saknas anledning, och som vi ser det möjlighet, att lämna förslag om obligatorisk användning av en specifik teknisk modell eller lösning. En sådan eventuell skyldighet bör i stället utredas och utvärderas när en viss teknisk modell för att implementera våra förslag har kommit på plats. Till

detta kommer att vi i kapitel 23 har kommit fram till att biometrisk verifiering med stöd av den nya lagen inte ska vara en skyldighet för myndigheter. Det är därför inte heller lämpligt att i författning reglera att myndigheterna då skulle vara skyldiga att använda en viss teknisk lösning.

28 Informations- och cybersäkerhet samt säkerhetsskydd

28.1 Inledning

I kapitel 27 har vi gjort en teknisk analys av de två tekniska modeller som vi ser som huvudalternativ för att implementera våra förslag om en generell möjlighet för myndigheter att använda biometriska uppgifter i handlingar för att verifiera identitet. Vi har i nämnda kapitel konstaterat att en verifieringsprocess som bygger på myndighetsgemensamma komponenter i form ett backend-system och en mobilapplikation kan ställa krav på bland annat prestanda, robusthet och skalbarhet. Med hänsyn till att information om enskilda kommer att behöva finnas i ett sådant system – och skickas mellan den verifierande myndigheten och en tekniskt ansvarig aktör – måste systemen och dess förvaltning utformas så att nödvändiga krav på informations- och cybersäkerhet beaktas; av våra direktiv framgår att vi ska identifiera och analysera risker kopplade till dessa frågor samt lämna förslag för att hantera riskerna.

Det är som vi ser det inte möjligt att lämna detaljerade förslag om vilka tekniska och andra åtgärder som de verifierande myndigheterna och en eventuell tekniskt ansvarig aktör kan behöva vidta, eftersom det i hög grad kan förväntas variera beroende på olika myndigheters verksamheter och hur våra förslag tekniskt implementeras.

I svensk rätt och på EU-nivå finns flera regelverk som ställer krav på informations- och cybersäkerhet utifrån olika syften och förutsättningar, samt på arbete med säkerhetsskydd. Det är svårt att på förhand bedöma i vilken utsträckning dessa kan komma att bli tillämpliga med anledning av våra förslag, då detta är beroende av vald teknisk lösning och vilket faktiskt genomslag våra författningsförslag får. I detta kapitel redogör vi översiktligt för relevanta regelverk och läm-

nar i det sammanhanget även vissa överväganden kring deras eventuella tillämplighet, och lyfter, med utgångspunkt i regelverken och i de två tekniska modeller vi beskrivit i kapitel 27, fram särskilda risker och möjliga åtgärder som vi identifierat. Som vi anfört i kapitel 27 bör det understrykas att en översyn måste göras, utifrån vald teknisk lösning, i samband med att våra förslag eventuellt implementeras, och då utifrån de särskilda krav som framgår av de olika regelverk som kan komma att vara tillämpliga.

28.2 Informations- och cybersäkerhet

Begreppen informationssäkerhet och cybersäkerhet kan i många delar anses vara överlappande. De har dock olika fokus. Informationssäkerhet handlar om att skydda information, oavsett form, ur olika aspekter. Tre principer kan sägas vara i fokus: *konfidentialitet*, nämligen att endast behöriga har åtkomst till informationen, *riktighet* avseende att informationen är fullständig och att endast behöriga kan ändra den och *tillgänglighet*, det vill säga att behöriga har åtkomst till informationen när den behövs.[1] Informationssäkerhet kan främjas genom styrdokument, klassificering av information, fysisk säkerhet – exempelvis tillgång till dokumentskåp – och tillräckliga backup-system, för att se till att information inte går förlorad. Cybersäkerhet är som vi ser det snävare och har ett mer tekniskt fokus och innebär att skydda nätverks- och informationssystem, deras användare och andra berörda personer från cyberincidenter och cyberhot. Det kan exempelvis handla om att skydda datorer, servrar, nätverk och applikationer mot hot som virus och exploatering av sårbarheter i systemet. Detta kan främjas genom exempelvis penetrationstestning, en robust och säker nätverksstruktur, analys av loggar, användarautentisering och säker kod.[2]

Som nämnts inledningsvis finns flera regelverk som ställer krav på informations- och cybersäkerhet utifrån olika syften och förutsättningar. Europaparlamentet och rådet har antagit två direktiv som är centrala på detta område: NIS2-direktivet[3] och CER-direktivet.[4] Det

[1] eSam, *Vägledning Utkontraktering – sekretess och dataskydd*, ES2023-06, s. 52.
[2] Se bland annat *Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem*, SOU 2021:63, s. 150 ff.
[3] Europaparlamentets och rådets direktiv (EU) 2022/2555.
[4] Europaparlamentets och rådets direktiv (EU) 2022/2557.

förstnämnda direktivet har införts i svensk lagstiftning genom cybersäkerhetslagen (2025:1506), tillsammans med vissa ytterligare författningsändringar. Vi redogör för dessa regelverk nedan. I säkerhetsskyddslagen (2018:585) med tillhörande förordning finns också regler i fråga om informationssäkerhet som gäller för verksamhetsutövare av säkerhetskänslig verksamhet. Även dataskyddsförordningen[5] innehåller bestämmelser som rör informationssäkerhet vid behandling av personuppgifter.

28.2.1 Cybersäkerhetslagen (NIS2-direktivet)

NIS2-direktivet, som huvudsakligen införts i Sverige genom cybersäkerhetslagen, ställer krav på säkerhet i nätverks- och informationssystem. Syftet med lagen är att uppnå en hög nivå av cybersäkerhet i samhället. Det är endast vissa verksamhetsutövare som omfattas av kraven i cybersäkerhetslagen.

Av 2 kap. 2 § cybersäkerhetslagen framgår att en verksamhetsutövare så snart det kan ske ska anmäla sig till den myndighet som regeringen bestämmer; denna myndighet är enligt 23 § cybersäkerhetsförordningen (2025:1507) Försvarets radioanstalt. Det ankommer på den enskilde verksamhetsutövaren att – utifrån de kriterier som anges i cybersäkerhetslagen – själv ta ställning till om man omfattas av lagen. Myndigheten för civilt försvar har utfärdat en *Vägledning för anmälan och identifiering av verksamhetsutövare som omfattas av cybersäkerhetslagen*. Bedömningen ska göras utifrån vilken typ av verksamhet som bedrivs, verksamhetens storlek samt om särskilda regler eller undantag gäller. Myndigheten för civilt försvar gör inte någon bedömning av om en viss verksamhetsutövare omfattas.

Det är alltså är upp till den verifierande myndigheten, eller en tekniskt ansvarig aktör, att ta ställning till om man omfattas av cybersäkerhetslagen. Det framstår därför inte som lämpligt att inom ramen för detta betänkande föregå en sådan bedömning och närmare ta ställning till om de verifierande myndigheterna eller en tekniskt ansvarig aktör kan komma att omfattas. Oaktat detta anser vi att det kan finnas anledning att i detta sammanhang – med utgångspunkt i våra förslag och de tekniska lösningar som vi beskrivit i kapitel 27 – lyfta fram

[5] Europaparlamentets och rådets förordning (EU) 2016/679.

vissa omständigheter som kan vara av värde vid en sådan framtida bedömning.

Utgångspunkten är att samtliga statliga myndigheter kan omfattas av cybersäkerhetslagen, dock med vissa begränsningar; av 1 kap. 3 § lagen framgår att den gäller för en verksamhetsutövare som är en statlig myndighet med befogenhet att fatta beslut som påverkar fysiska eller juridiska personers rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital. Till exempel bör en myndighet som kan fatta beslut om tillhandahållandet av varor på inre marknaden, däribland Livsmedelsverket, anses fatta sådana beslut som avses i direktivet. Även verksamhetsutövare som är regioner, kommuner och kommunalförbund kan omfattas av lagen.

Utifrån ordalydelsen av nämnda bestämmelse kan det tänkas att relativt många av de myndigheter som ska kunna tillämpa den nya lagen om biometrisk verifiering också kan komma att omfattas av cybersäkerhetslagen; de fattar beslut av slag som åtminstone indirekt påverkar exempelvis möjligheten för en individ att studera, arbeta eller etablera sig i en annan medlemsstat, med följden att dessa skulle anses omfattas av 1 kap. 3 § cybersäkerhetslagen. I förarbetena synes regeringen emellertid ha ansett att en tolkning, som utgår från den indirekta effekten av exempelvis ett anställningsbeslut, skulle vara alltför extensiv.[6] Syftet är att den nya lagen om biometrisk verifiering av identitet ska kunna tillämpas av en bred krets av myndigheter, som bedriver verksamhet av högst varierande slag. Det är enligt vår mening därför också mycket svårt att på förhand dra någon säker slutsats om vilka av de verifierande myndigheterna som skulle kunna omfattas av bestämmelsen i 1 kap. 3 § cybersäkerhetslagen. Exempelvis fattar Försäkringskassan beslut om socialförsäkringsförmåner som har sin grund i EU-rätten och som även direkt kan anses påverka enskildas möjlighet till fri rörlighet. En myndighet bör som vi ser det däremot inte omfattas av 1 kap. 3 § cybersäkerhetslagen *endast* med anledning av att den biometriskt verifierar identitet med stöd av den nya lagen, utan detta styrs av verksamheten i sig och de beslut som fattas i den. Inte heller att myndigheten använder egna system för att biometriskt verifiera identitet med stöd av den nya lagen, på det sätt vi har beskrivit i avsnitt 27.3, bör leda till någon annan slutsats.

[6] *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag*, prop. 2025/26:28, s. 58.

Vi kan vidare konstatera att cybersäkerhetslagen, enligt bestämmelsen i 1 kap. 5 §, är tillämplig på sådana verksamhetsutövare – däribland aktörer inom offentlig förvaltning (se 1 kap. 4 § 1 lagen) – som träffas av de särskilda kriterier som anges i punkterna i bestämmelsen; i *offentlig förvaltning* ingår framför allt statliga myndigheter.[7] För det första omfattas verksamhetsutövare som är ensamma leverantörer i Sverige av en tjänst som är väsentlig för att upprätthålla en kritisk samhällelig eller ekonomisk verksamhet (första punkten); av förarbetena till bestämmelsen framgår att det rör sig om tjänster där ett avbrott i tjänsten hindrar genomförandet av ekonomisk verksamhet, genererar omfattande förluster, undergräver användarnas förtroenden och medför allvarliga konsekvenser för landets och unionens ekonomi.[8] En verksamhetsutövare omfattas också av cybersäkerhetslagen om en störning av den tjänst som denne tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa eller medföra betydande systemrisker (andra punkten). Enligt tredje punkten omfattas en verksamhetsutövare som har särskild betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst eller för andra sektorer som är beroende av verksamhetsutövaren. Enligt fjärde punkten omfattas verksamhetsutövare som tillhandahåller betrodda tjänster; enligt 1 kap. 2 § 3 cybersäkerhetslagen avses med betrodda tjänster samma som i eIDAS-förordningen[9]. Det kan röra sig om skapande eller validerande av elektroniska underskrifter eller elektroniska stämplar, exempelvis när någon godkänner en betalning via Swish med mobilt BankID eller godkänner sin deklaration via Skatteverkets e-tjänst.[10]

Ett sådant centralt informationssystem som vi beskrivit i avsnitt 27.4 och som möjliggör biometrisk verifiering av identitet skulle, enligt vår bedömning, under vissa förutsättningar kunna betraktas som väsentligt för att upprätthålla en kritisk samhällelig eller ekonomisk verksamhet, på det sätt som avses i 1 kap. 5 § 1 cybersäkerhetslagen. Det torde dock, som vi ser det, förutsätta att tillämpningen av den nya lagen utvecklas så att biometrisk verifiering i praktiken utgör ett krav och en förutsättning för tillgång till olika centrala funktioner i samhället – exempelvis tillgång till socialförsäkringsförmåner

[7] *Nya regler om cybersäkerhet*, SOU 2024:18, s. 129.
[8] Jfr prop. 2025/26:28, s. 54 och *Informationssäkerhet för samhällsviktiga och digitala tjänster*, prop. 2017/18:205, s. 34.
[9] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014.
[10] https://www.pts.se/internet-och-telefoni/betrodda-tjanster/, senast besökt den 20 maj 2026.

av olika slag, fysiskt tillträde till myndighetslokaler eller tillgång till vård. Det är inte möjligt för oss att förutse utfallet och tillämpningen av den nya lagen. Att den nya lagen syftar till att ge myndigheter en *möjlighet* att biometriskt verifiera identitet mot handlingar bör dock beaktas; avsikten är inte att det ska vara en skyldighet. Ett avbrott i ett system som möjliggör biometrisk verifiering skulle visserligen kunna fördröja handläggningen av ett ärende, om myndigheten anser att verifieringen är nödvändig, men skulle som vi ser det sannolikt endast påverka enskilda ärenden, inte en större krets av personer eller samhällsfunktioner på något mer omedelbart sätt. Biometrisk verifiering enligt den nya lagen utgör en utredningsåtgärd och – enligt våra förslag – inte ensamt en materiell förutsättning för att besluta i ett ärende. Eventuella konsekvenser av att identiteten inte kan verifieras biometriskt i ett visst ärendeslag eller ärende ankommer på den verifierande myndigheten att ta ställning till. Sammantaget kan detta anses tala mot att ett avbrott i möjligheten att biometriskt verifiera identitet med stöd av den nya lagen får sådana effekter som anges i 5 § 2 cybersäkerhetslagen. Möjligheten att exempelvis tillhandahålla vård kan inte heller anses begränsad på grund av ett tillfälligt avbrott i ett system för att biometriskt verifiera identitet med stöd av den nya lagen.

De omständigheter som vi lyft fram ovan talar som vi ser det även mot att en tekniskt ansvarig aktör kan anses ha en sådan särskild betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst eller för andra sektorer som är beroende av verksamhetsutövaren, på det sätt som avses i 1 kap. 5 § 3 cybersäkerhetslagen. Vi anser vidare att det är svårt att betrakta ett myndighetsgemensamt system för biometrisk verifiering som en sådan betrodd tjänst som avses i 1 kap. 5 § 4 cybersäkerhetslagen, eller som en allmänt tillgänglig elektronisk kommunikationstjänst enligt 1 kap. 6 §. Däremot är det som vi ser det inte otänkbart att en tekniskt ansvarig aktör kan anses omfattas enligt 1 kap. 7 §, för det fall systemet för biometrisk verifiering av identitet med stöd av den nya lagen betraktas som en sådan it-tjänst som anges i bestämmelsen, exempelvis en datacentraltjänst eller en utlokaliserad driftstjänst. Som vi nämnt ovan är detta emellertid beroende av utfallet och tillämpningen av den nya lagen, och hur verifieringsprocessen implementeras tekniskt.

Det finns således flera omständigheter hänförliga till den nya lag om biometrisk verifiering som vi föreslår – i första hand för en tek-

niskt ansvarig aktör – som kan få betydelse vid bedömningen av om en viss verksamhetsutövare omfattas av cybersäkerhetslagen, enligt ovan nämnda bestämmelser. Vi kan också konstatera att enligt 1 kap. 8 § cybersäkerhetslagen kan regeringen bestämma att även andra statliga myndigheter än de som omfattas av nämnda bestämmelser ska omfattas av lagen. En verifierande myndighet eller en tekniskt ansvarig aktör kan givetvis omfattas av cybersäkerhetslagen också av andra skäl än sådana som är hänförliga till den nya lagen, utifrån den verksamhet som aktören i fråga bedriver; som utgångspunkt omfattas då hela verksamheten, inte bara den del som är skälet till att verksamhetsutövaren omfattas av cybersäkerhetslagen.

28.2.2 CER-direktivet

Det övergripdanande syftet med CER-direktivet är att stärka kritiska entiteters motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster på den inre marknaden. Genomförandet av direktivet i svensk rätt pågår; regeringen föreslog i lagrådsremissen *En ny lag för ökad motståndskraft hos kritiska verksamhetsutövare* en ny lag om motståndskraft hos kritiska verksamhetsutövare.[11] En kritisk verksamhetsutövare ska enligt förslagen i lagrådsremissen vidta lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft. Detta inbegriper åtgärder som är nödvändiga för att bland annat säkerställa ett tillfredställande fysiskt skydd av lokaler och kritisk infrastruktur, reagera på, stå emot och begränsa konsekvenserna av incidenter, med vederbörlig hänsyn till genomförandet av risk- och krishanteringsförfaraden och protokoll samt varningsrutiner, och säkerställa en ändamålsenlig hantering av personalsäkerhet, såsom fastställande av åtkomsträttigheter till lokaler och genomförande av bakgrundskontroller, kritisk infrastruktur och känslig information (se 3 kap. 3 § i förslaget till en ny lag om motståndskraft hos kritiska verksamhetsutövare).[12]

Regelverket ska tillämpas på enskilda och offentliga verksamhetsutövare som tillhandahåller en sådan samhällsviktig tjänst som omfattas av bilagan till CER-direktivet. Till skillnad från cybersäkerhetslagen – där myndigheterna själva behöver anmäla sig om man omfattas

[11] Lagrådsremissen *En ny lag för ökad motståndskraft hos kritiska verksamhetsutövare* den 21 maj 2026, s. 25 ff.
[12] A.a., s. 204.

av regelverket – är det enligt den föreslagna lagen den eller de myndigheter som regeringen bestämmer som ska besluta om att en viss verksamhetsutövare ska omfattas av regelverket.

För att en verksamhetsutövare ska identifieras som kritisk ska, enligt den föreslagna lagen, fyra särskilda kriterier vara uppfyllda: (1) verksamhetsutövaren ska tillhandahålla en eller flera samhällsviktiga tjänster som omfattas av bilagan till CER-direktivet, (2) omfattas av någon av kategorierna i bilagan till CER-direktivet eller vara en statlig myndighet som regeringen i övrigt bestämmer ska kunna omfattas av lagen, (3) bedriva verksamhet i och ha kritisk infrastruktur belägen i Sverige och (4) en incident ska få *betydande störande effekt* för tillhandahållandet av tjänsten. Med samhällsviktig tjänst avses enligt 2 kap. 2 § i den föreslagna lagen en tjänst som är avgörande för att upprätthålla centrala samhällsfunktioner, ekonomisk verksamhet, folkhälsa, allmän säkerhet eller miljön och som omfattas av bilagan till CER-direktivet, i den ursprungliga lydelsen. Av förslagen till en ny lag framgår att regeringen eller den myndighet regeringen bestämmer ska få meddela föreskrifter om när en störande effekt är betydande. Vid bedömningen ska, enligt artikel 7.1 i CER-direktivet, beaktas bland annat antalet användare som är beroende av den samhällsviktiga tjänst som den berörda verksamhetsutövaren tillhandahåller, vilken effekt incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet, miljön, den allmänna säkerheten och tryggheten eller befolkningens hälsa och verksamhetsutövarens betydelse för upprätthållandet av en tillräcklig nivå på den samhällsviktiga tjänsten, med beaktande av tillgången till alternativa sätt för att erbjuda den samhällsviktiga tjänsten.

Som framgår av det ovan anförda är det tillsynsmyndigheten som ska ta ställning till om en viss myndighet omfattas av CER-direktivets tillämpningsområde. Det framstår därför inte som lämpligt eller möjligt att inom ramen för detta betänkande närmare ta ställning till om de verifierande myndigheterna eller en tekniskt ansvarig aktör kan komma att omfattas. Med detta sagt anser vi emellertid att de omständigheter som vi lyft fram i avsnitt 28.2.1 avseende om en tekniskt ansvarig aktör kan anses omfattas av cybersäkerhetslagen gör sig gällande även för CER-direktivets tillämpning; det skulle som vi ser det kunna ifrågasättas dels om tillhandahållande av ett backend-system och en mobilapplikation utgör en samhällsviktig tjänst enligt bilagan till CER-direktivet, dels om en incident skulle få en betydande störande

effekt för verksamhetsutövarens tillhandahållande av en sådan tjänst. En myndighet torde enligt vår uppfattning normalt inte heller omfattas av CER-direktivet *endast* med anledning av att den – antingen med hjälp av egna eller myndighetsgemensamma system – biometriskt verifierar identitet med stöd av den nya lagen.

28.2.3 Dataskyddsförordningen

Informationssäkerhet utgör en del av de centrala principerna också i dataskyddsförordningen. I artikel 25 föreskrivs om inbyggt dataskydd och dataskydd som standard, vilket utgör en del i den personuppgiftsansvariges skyldighet att genomföra lämpliga tekniska och organisatoriska åtgärder. Inbyggt dataskydd innebär att den personuppgiftsansvariga ska ta hänsyn till integritetsskyddsreglerna redan när it-system och rutiner utformas. Syftet med säkerhetsåtgärderna är att skydda de registrerades rättigheter och säkerställa att skyddet av deras personuppgifter byggs in i behandlingen. För att betraktas som lämpliga bör åtgärderna vara utformade så att de uppfyller principerna om lagrings- och uppgiftsminimering. Dataskydd som standard innebär att inställningarna för en produkt, ett system eller en tjänst ska vara dataskyddsvänliga. Av artikel 32 följer även ett ansvar att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Åtgärderna kan till exempel inbegripa kryptering av personuppgifter, tillgänglighet och motståndskraft hos systemen och ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

28.2.4 Vissa särskilda risker och åtgärder för att motverka dem

Om en myndighet som vill biometriskt verifiera identitet med stöd av den nya lagen använder en sådan myndighetsgemensam teknisk lösning som vi har beskrivit i avsnitt 27.4, uppkommer som vi ser det inte några särskilda informations- eller cybersäkerhetsrisker hos den verifierande myndigheten som kan hänföras till denna utredningsåtgärd. Det förutsätts dock att myndigheten, inom ramen för sitt systematiska informations- och cybersäkerhetsarbete, identifierar och hante-

rar de risker som uppkommer vid användningen av en sådan lösning. Den verifierande myndigheten har även – i egenskap av personuppgiftsansvarig enligt våra förslag i avsnitt 24.6 – att iaktta de principer om inbyggt dataskydd och dataskydd som standard som följer av dataskyddsförordningen. Riskerna i fråga om informations- och cybersäkerhet finns i dessa fall – som vi ser det – i allt väsentligt hos den tekniskt ansvarige aktören. Sådana risker kan dock även, i viss utsträckning, göra sig gällande om den verifierande myndigheten använder tekniska system som den själv har tagit fram och förvaltar, på det sätt vi beskrivit i avsnitt 27.3; risker hänförliga till en mobilapplikation aktualiseras däremot inte i dessa fall.

Att ge en heltäckande beskrivning av vilka risker i fråga om informations- och cybersäkerhet som kan tänkas uppstå, och hur dessa kan och bör motverkas på bästa sätt är givetvis svårt, med hänsyn till att förutsättningarna hos den verifierande myndigheten och hos en tekniskt ansvarig aktör kan variera, och till att konkreta risker kan bero på hur de tekniska lösningarna implementeras, utifrån bästa möjliga teknik som är tillgänglig vid en viss implementeringstidpunkt. Vi vill emellertid i detta sammanhang peka på några särskilda faktorer som vi anser bör beaktas. I vissa delar har de redan lyfts fram i kapitel 27, särskilt avsnitt 27.4.1.

Kryptering bör integreras i hela verifieringsprocessen

Oavsett i vilken del av det system som vi beskrivit i avsnitt 27.4 som den huvudsakliga verifieringslogiken placeras, eller om en sådan lösning som vi beskrivit i avsnitt 27.3 väljs, som innebär att den verifierande myndigheten använder system som den själv har tagit fram och ansvarar för, är behovet av stark kryptering av informationen framträdande. För en översikt av vad begreppet kryptering innebär och hur det används i praktiken kan vi hänvisa exempelvis till betänkandet *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet*. Kort sagt innebär kryptering att i kommunikationssystem åstadkomma sekretess och/eller autenticitet (säkerställa äkthet hos information) genom att utnyttja en för de obehöriga användarna hemlighållen nyckel.[13]

[13] SOU 2017:89, s. 160 ff.

Kryptering bör enligt vår mening ses som ett viktigt tekniskt komplement till det rättsliga skydd som tillämpliga sekretessbestämmelser avser att ge, mot att uppgifter som förekommer vid en biometrisk verifiering med stöd av den nya lagen obehörigen röjs. Krypteringen bör som vi ser det som utgångspunkt omfatta hela verifieringskedjan och ses som en grundläggande skyddsåtgärd som bör integreras i systemarkitekturen.

Med hänsyn till att det system för biometrisk verifiering av identitet som vi föreslår inte ska omfatta någon lagring av uppgifter, gör sig behovet av kryptering för data i vila inte gällande på samma sätt som för ett register. I stället uppkommer ett behov av stark kryptering i första hand för de uppgifter som överförs mellan delar av systemet, i en sådan teknisk lösning som vi beskrivit i avsnitt 27.4; om den biometriska jämförelsen ska göras i backend-systemet kommer inte bara alfanumeriska uppgifter om den enskilde utan även biometriska underlag och/eller biometriska uppgifter att behöva överföras från mobilapplikationen till backend-systemet. Vid sådan överföring av uppgifter finns risk för avlyssning, manipulation av processen och replay-angrepp (se avsnitt 27.4.1 angående sådana risker i samband med att verifieringen initieras). Behovet av kryptering kan enligt vår mening särskilt aktualiseras om den vars identitet ska verifieras är ansluten till osäkra nätverk, där en så kallad man-in-the-middle-attack kan användas. Kommunikationen mellan verifieringsprocessens olika logiska delar bör som vi ser det därför skyddas med moderna transportskyddsprotokoll. Utöver att skydda tillgången till informationen behöver det säkerställas att den inte har manipulerats i samband med att den överförs. En angripare kan annars försöka modifiera biometriska uppgifter eller ändra jämförelseresultatet, utan att detta syns för den verifierande myndigheten. Kryptering bör därför kombineras med mekanismer som syftar till att säkerställa att de uppgifter som används för biometrisk verifiering med stöd av den nya lagen – däribland de alfanumeriska uppgifter om bland annat identitet som hämtas från den handling som används för kontrollen – inte har ändrats under överföringen till backend-systemet eller till den verifierande myndighetens egna system.

Även hanteringen av krypteringsnycklarna måste som vi ser det få ett starkt skydd, både tekniskt genom att dessa separeras från den krypterade information som hanteras i systemet, och genom att endast behörig personal får åtkomst till nycklarna, vilket kan inne-

fatta att behörighet till lokaler och kritisk infrastruktur begränsas på lämpligt sätt.

Särskilda risker som är hänförliga till ett backend-system

Vi har i avsnitt 27.6 bedömt att, i en teknisk modell som bygger på myndighetsgemensamma komponenter, bör tyngdpunkten för verifieringslogiken placeras i backend-systemet, även om en utvärdering behöver göras när en sådan lösning eventuellt implementeras. Backend-systemet får då en kritisk roll och kan utgöra en mer central angreppspunkt, där stora mängder biometriska uppgifter och uppgifter avseende identitet behandlas, om än under en kort tid vid varje verifieringstillfälle. Att upprätthålla tillräcklig informations- och cybersäkerhet i backend-systemet blir därför givetvis av stor betydelse.

Med centrala delar av verifieringslogiken placerad i ett backend-system – däribland den biometrisk jämförelsen – finns risker för att dessa funktioner manipuleras på ett sätt som medför att resultatet av den biometriska verifieringen inte blir tillförlitligt. En angripare kan försöka få tillgång till komponenter i systemet för att förändra jämförelseresultat, beslutslogik eller de tröskelvärden som systemet använder vid den biometriska jämförelsen. Detta kan medföra risk för att användning av falska eller utnyttjade identiteter inte upptäcks på avsett sätt. Eftersom ett backend-system kan antas behöva omfatta komplexa och beräkningsintensiva processer kan tredjepartskomponenter som utför sådana delar av verifieringsprocessen behöva användas. Detta skapar en attackyta där sårbarheter i olika gränssnitt (API:er) och komponenter som den tekniskt ansvarige aktören inte till fullo kontrollerar kan uppkomma. Ett backend-system kan även vara utsatt för risker i form av attacker som syftar till att orsaka avbrott, så kallade överbelastningsattacker; sådana angrepp kan även användas för att försöka analysera de tröskelvärden för den biometrisk jämförelsen som systemet tillämpar, för att utnyttja detta.

För att motverka risker av nu nämnda slag behöver ett backend-system utformas med utgångspunkten att ingen enskild komponent, tjänst eller användare bör ges automatisk tillgång till systemet, utan samtliga tjänster och processer bör uttryckligen autentiseras. Kommunikation även mellan systeminterna resurser och komponenter bör därför – på samma sätt som vid kommunikation mellan en mobil-

applikation och backend-systemet – ske på ett säkert och krypterat, sätt. Backend-systemet bör vidare segmenteras så att olika centrala delar som hanterar certifikat, biometriska uppgifter, jämförelsemodeller och alfanumeriska uppgifter isoleras från varandra i möjligaste mån. Det kan göras såväl logiskt som fysiskt, om det är möjligt. Syftet med sådan separation är att begränsa möjligheten för en angripare att få tillgång till och röra sig mellan flera olika delar av systemet på ett sätt som kan påverka det som helhet eller som exponerar även mer känsliga delar, exempelvis biometriska uppgifter. För att skydda ett backend-system mot överbelastningsattacker kan åtgärder i form av hastighetsbegränsning (rate limiting) – som sätter ett tak för hur många förfrågningar en användare kan göra under en viss tid – och trafikfiltrering behöva implementeras.

Det bör i detta sammanhang lyftas fram att inte bara externa angrepp måste beaktas vid utformningen av ett backend-system. Även risker relaterade till obehörig åtkomst eller manipulering av systemet som kan härledas till administratörer, utvecklare eller driftpersonal måste motverkas på lämpligt sätt. Åtkomst till systemen bör därför begränsas och kontinuerligt övervakas. Loggning av kritiska händelser samt åtkomst till delar av systemet och känsliga uppgifter kan utgöra en viktig del av detta.

Det finns även risker som inte kan hänföras till något direkt antagonistiskt agerande. Som vi har pekat på i avsnitt 27.4.1 ställer en centraliserad teknisk modell – som kan kräva att många samtidiga beräkningsintensiva anrop hanteras – särskilda krav på robusthet, tillgänglighet och nödvändig skalbarhet. Ett backend-system behöver även kunna hantera certifikats- och sessionshantering, loggning, behörighetskontroll och leverans av resultatet av en biometrisk jämförelse och alfanumeriska uppgifter till den verifierande myndigheten. Allteftersom de generella möjligheter att biometriskt verifiera identitet som vi föreslår kan komma att användas av allt fler myndigheter, kan dessa krav på systemets tekniska infrastruktur förväntas öka. Som vi noterat ovan kan backend-systemet även utsättas för överbelastningsattacker. Ett backend-system behöver därför utformas med en serverstruktur som minimerar avbrott. Ett temporärt avbrott i backendsystemet medför visserligen inte nödvändigtvis att det inte alls går att genomföra en biometrisk verifiering, endast att verifieringsprocessen fördröjs eller upplevs som mindre smidig. Ett avbrott påverkar inte heller – annat än indirekt – möjligheten för en verifierande myn-

dighet att besluta i ett ärende. Oaktat detta är det, som vi ser det, av mycket stor vikt att systemet dimensioneras och utformas på ett sätt som gör det robust och skalbart, för att tilliten till det inte ska påverkas negativt.

Vissa särskilda risker som är hänförliga till en mobilapplikation

Beroende på vilka delar av verifieringslogiken som placeras i en mobilapplikation respektive ett backend-system kommer riskerna som kan hänföras till en klientmiljö, det vill säga mobilapplikationen, att variera. Upptagning av biometriska underlag och inläsning av sådana uppgifter och alfanumeriska uppgifter från den aktuella handlingen kommer dock alltid att behöva göras i mobilapplikationen.

En central riskfaktor är att mobilenheten kan vara manipulerad eller konfigurerad på ett sätt som motverkar säkerhetsmekanismer vid insamlingen av uppgifter med hjälp av en applikation som installeras på den. Ett grundläggande krav bör givetvis vara att endast viss hårdvara och mjukvara accepteras, för att mobilapplikationen alls ska få installeras; i avsnitt 27.4.1 har vi pekat på sådana krav i den mobilapplikation som Storbritanniens inrikesministerium har tagit fram inom ramen för identitetsplattformen för digitala offentliga tjänster – GOV.UK One Login. Motsvarande krav bör enligt vår mening tillämpas för en mobilapplikation i ett sådant system som vi beskriver i avsnitt 27.4. Sammantaget bör de tekniska kraven för och utvecklingen av mobilapplikationen utformas med utgångspunkten att klientmiljön i viss utsträckning får betraktas som ”fientlig”.

Genom att mobilapplikationen och dess installation är hänförlig till klientmiljön finns en risk för att angripare försöker analysera och manipulera applikationen, genom så kallad reverse engineering. Det är därför viktigt att känsliga delar av systemet – exempelvis kryptografiska nycklar, interna konfigureringsparametrar eller tröskelvärden – inte är hårdkodade i applikationen så att dessa kan extraheras och användas för att angripa backend-systemet och därmed resultatet av den biometriska jämförelsen. Tillförlitligheten som en biometrisk verifiering ska tillföra skulle då påverkas negativt. Genom reverse engineering kan också liveness-kontrollen och sessionshantering utsättas för angrepp. En annan risk med en klientmiljö som den verifierande myndigheten inte kontrollerar är att mobilenheten kan vara

jailbreakad, vilket är en process för att ta bort tillverkarens begränsningar i syfte att ge fullständig åtkomst till operativsystemet och administrativa rättigheter. Detta kan möjliggöra installation av skadlig kod eller tillgång till även krypterade uppgifter – exempelvis biometriska uppgifter – innan de överförs till ett backend-system.

En mobilapplikation behöver mot denna bakgrund utvecklas med flera lager av tekniska skyddsåtgärder, för att kunna upprätthålla informations- och cybersäkerhetskrav.

När det gäller att motverka att applikationen manipuleras eller att mobilenheten är utsatt för jailbreaking bör funktioner som Android Play Integrity API[14] och Apple App Attest[15] användas vid utvecklingen och driftsättningen. Dessa funktioner möjliggör att backend-systemet kan verifiera att kommunikationen med systemet sker från en oförändrad applikation, på en autentisk mobilenhet. För att motverka manipulation av verifieringsprocessen, exempelvis genom replay-attacker, bör – som vi lyft fram i avsnitt 27.4.1 – kortlivade sessioner användas, vars giltighet kontinuerligt kontrolleras av backend-systemet, i kombination med bindningar till en viss kontext, exempelvis genom kontroll av ip-nummer för mobilapplikationen. Applikationen bör även kunna upptäcka onormala interaktionsmönster och användarbeteenden som tyder på att en människa inte är aktiv i verifieringsprocessen, exempelvis genom att många upprepade försök genomförs under kort tid, i syfte att försöka kringgå de tröskelvärden för när den biometriska jämförelsen ska anses ha lyckats som används av systemet.

En särskild risk utgörs av att de biometriska underlagen i form av den enskildes ansiktsbild manipuleras när dessa tas upp med hjälp av mobilkameran. För att motverka detta krävs skyddsmekanismer för att säkerställa att de biometriska underlag som används härrör från en verklig, levande och närvarande person. En angripare kan exempelvis försöka använda fotografier, videouppspelningar och masker. En utökad tillgång till och användning av deepfake-verktyg, som används för att framställa bland annat statiska och rörliga bilder av personer, bör också beaktas. För att motverka sådana risker måste en mobilapplikation – och ett backend-system – innehålla särskilda säkerhetsmekanismer för att upptäcka sådana presentationsattacker.

[14] https://developer.android.com/google/play/integrity, senast besökt den 12 maj 2026.
[15] https://developer.apple.com/documentation/devicecheck/establishing-your-app-s-integrity, senast besökt den 12 maj 2026.

En central komponent utgörs av liveness-kontrollen. Som nämnts ovan kommer den normalt att göras i mobilapplikationen, i en sådan teknisk modell som vi har beskrivit i avsnitt 27.4; om verifiering sker på plats hos myndigheten uppkommer av naturliga skäl inte något behov av en liveness-kontroll. Vägledning för hur detta ska gå till finns bland annat i de ISO-standarder som vi hänvisat till i avsnitt 27.4.1. Exakt vilka tekniska åtgärder som kan behöva vidtas är inte möjligt att redogöra för här. Mobilapplikationen bör dock innehålla funktioner som gör det möjligt att till exempel analysera hudtextur, ljusreflektioner, perspektivförändringar och mikrorörelser. Användaren kan också genom mobilapplikationens visuella gränssnitt uppmanas att röra på huvudet, blinka eller följa visuella instruktioner.

Eftersom tekniken för att utföra denna typ av angrepp hela tiden utvecklas är det som vi ser det viktigt att en viss lösning som syftar till att motverka presentationsattacker inte är statisk och knuten till tidpunkten för implementeringen av våra förslag, utan att den kontinuerligt testas, utvärderas och uppdateras.

Incidenthantering och kontinuitetsförmåga

De skyddsåtgärder som har beskrivits ovan syftar i första hand till att förebygga och försvåra medvetna angrepp mot ett system för att biometriskt verifiera identitet mot handlingar. Oaktat detta kan säkerhetsincidenter, tekniska fel och andra störningar inte helt uteslutas. Såväl en tekniskt ansvarig aktör som verifierande myndigheter bör därför säkerställa att det finns ändamålsenliga rutiner för incidenthantering, kontinuitetsplanering och återställning av verksamheten. Det bör bland annat finnas förmåga att upptäcka och analysera incidenter, begränsa deras konsekvenser samt återställa funktionalitet inom rimlig tid. Även behovet av alternativa arbetsrutiner vid längre avbrott bör beaktas.

28.2.5 Sammanfattning

Vår bedömning

Våra förslag för med sig utmaningar i fråga om informations- och cybersäkerhet, särskilt om de implementeras genom att ett myndighetsgemensamt backend-system och en gemensam mobilapplikation används.

De verifierande myndigheterna och/eller en tekniskt ansvarig aktör behöver vidta lämpliga och proportionella tekniska och organisatoriska säkerhetsåtgärder för att skydda nätverks- och informationssystem, och därmed de uppgifter om enskilda som förekommer vid biometrisk verifiering av identitet med stöd av den nya lagen.

Vi har i föregående avsnitt, och även i avsnitt 27.4, pekat på olika potentiella informations- och cybersäkerhetsrisker som vi menar kan aktualiseras om våra förslag genomförs. Vi bedömer att riskerna kan vara särskilt framträdande vid en verifieringsprocess som utgår från ett myndighetsgemensamt backend-system och en gemensam mobilapplikation. Vi har i föregående avsnitt redogjort för hur dessa risker skulle kunna mötas, och motverkas.

Som vi anfört i avsnitt 28.2.1 och 28.2.2 är det inte lämpligt eller möjligt att inom ramen för detta betänkande närmare ta ställning till om våra förslag om en ny lag om biometrisk verifiering av identitet i sig innebär att en verifierande myndighet eller en tekniskt ansvarig aktör – endast med hänsyn till tillämpningen av den nya lagen – omfattas av cybersäkerhetslagen, eller av den lag som föreslagits för att genomföra CER-direktivet. En bedömning måste göras utifrån dels vilken myndighet eller annan aktör som får ett sådant ansvar, dels tillämpningen av ett sådant system och våra förslag i praktiken. Detsamma får som vi ser det anses gälla för det fall våra förslag implementeras genom att den verifierande myndigheten använder tekniska system som den själv har tagit fram och ansvarar för; givetvis kan en verifierande myndighet också omfattas av nämnda regelverk av skäl som är hänförliga till dess verksamhet i övrigt. Oavsett vilken bedömning som görs i slutändan anser vi att det är av vikt att främst en tekniskt ansvarig aktör men även en verifierande myndighet – i linje med vad som följer av nyss nämnda regelverk, och även av dataskyddsför-

ordningen – vidtar lämpliga och proportionerliga riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot angrepp, och därmed mot att personuppgifter som förekommer vid en biometrisk verifiering av identitet med stöd av den nya lagen kommer obehöriga tillhanda. De möjliga åtgärder som vi har lyft i avsnitt 28.2.4 bör, som vi ser det, kunna vara till ledning i ett sådant arbete.

För att få en effektiv och säker informationshantering är en förutsättning att informations- och cybersäkerhetsarbetet bedrivs systematiskt. Denna grundprincip gäller som vi ser det dock all information som en verifierande myndighet eller en tekniskt ansvarig aktör hanterar vid biometrisk verifiering med stöd av den nya lagen. I betänkandet från Cybersäkerhetsutredningen, *Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem*, anfördes att åtgärder som avser informationssäkerhet enligt cybersäkerhetslagen inte kan särskiljas från informationssäkerhet i en vidare bemärkelse; skydd mot skadlig kod och användarautentisering är relevanta åtgärder även för nätverks- och informationssystem som inte är av betydelse för Sveriges säkerhet.[16]

28.3 Säkerhetsskydd

Med hänsyn till att vi föreslår möjligheter för en bred krets av myndigheter att verifiera identitet med hjälp av biometriska uppgifter, och att vi i kapitel 27 förordar en teknisk lösning som bygger på myndighetsgemensamma komponenter i form av en mobilapplikation och ett backend-system, finns som vi ser det skäl att belysa hur våra förslag förhåller sig till regelverket om säkerhetsskydd. Vi vill emellertid redan här understryka att det ankommer på varje myndighet att ta ställning till om den omfattas av säkerhetsskyddslagen, utifrån den verksamhet som myndigheten bedriver.

[16] SOU 2021:63, s. 150.

28.3.1 Allmänt om säkerhetsskydd

Bestämmelser som reglerar säkerhetsskydd finns i första hand i säkerhetsskyddslagen och säkerhetsskyddsförordningen (2021:955). Flera myndigheter, bland annat Säkerhetspolisen och Försvarsmakten, har meddelat föreskrifter avseende säkerhetsskydd som kompletterar bestämmelserna i lag och förordning.

Enligt 1 kap. 1 § säkerhetsskyddslagen gäller lagen för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. Lagen är tillämplig vid verksamhet hos staten, kommuner, landsting och enskilda oberoende av verksamhetsform. För att lagen ska vara tillämplig krävs inte att hela verksamheten kan anses utgöra säkerhetskänslig verksamhet, utan endast att verksamheten till någon del utgör det.[17] Lagens krav på säkerhetsskydd gäller för såväl militär som civil verksamhet. Den som till någon del bedriver säkerhetskänslig verksamhet är skyldig att göra en säkerhetsskyddsanalys, det vill säga utreda behovet av säkerhetsskydd. Säkerhetsskyddsanalysen ska dokumenteras. Med utgångspunkt i analysen ska verksamhetsutövaren planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomsten av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.

Av 1 kap. 2 § säkerhetsskyddslagen framgår att med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Säkerhetsskyddsklassificerade uppgifter avser uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), eller som skulle ha omfattats av sekretess enligt den lagen om den hade varit tillämplig. De bestämmelser i offentlighets- och sekretesslagen som framför allt kan vara relevanta är 15 kap. 2 § (försvarsverksamhet), 18 kap. 2 § (underrättelseverksamhet) och 15 kap. 1 § (utrikessekretess).[18]

Av 2 kap. 2–4 §§ säkerhetsskyddslagen framgår att säkerhetsskyddsåtgärder kan delas upp i informationssäkerhet, fysisk säkerhet och personalsäkerhet. Informationssäkerhet ska förebygga dels

[17] *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*, prop. 2017/18:89, s. 133.
[18] SOU 2021:1, s. 167.

att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, dels skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet. Det innebär att om ett informationssystem ska hantera säkerhetsskyddsklassificerade uppgifter ska dess säkerhetsfunktioner anpassas för att förebygga att sådana uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs. Säkerhetsåtgärderna ska dessutom i förhållande till uppgifter och informationssystem som inte utgör eller innehåller säkerhetsskyddsklassificerade uppgifter, men som har avgörande betydelse för till exempel styrning, reglering och övervakning av för Sverige viktiga samhällsfunktioner, tillgodose behov av tillgänglighet och riktighet.[19]

28.3.2 Tillhandahållande av ett myndighetsgemensamt system

Med utgångspunkten att en teknisk lösning som bygger på myndighetsgemensamma komponenter i form av en mobilapplikation och ett backend-system används för biometrisk verifiering av identitet enligt den nya lagen, uppkommer fråga om tillhandahållande av ett sådant tekniskt system i sig skulle kunna anses omfattas av säkerhetsskyddslagen. Av betydelse är om det kan anses utgöra verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd, i den mening som avses i 1 kap. 1 § säkerhetsskyddslagen.

Uttrycket *Sveriges säkerhet* tar sikte på sådant som är av grundläggande betydelse för Sverige. I detta ingår bland annat det militära och civila försvaret, den nationella ekonomin, de brottsbekämpande myndigheterna, domstolarna och sådana leveranser av exempelvis livsmedel, elkraft, dricksvatten och drivmedel som är nödvändiga för samhällets funktionalitet på nationell nivå. Samhällsviktig verksamhet kan bedömas röra Sveriges säkerhet i den mening som avses i 1 kap. 1 § säkerhetsskyddslagen. Med *samhällsviktig verksamhet* avses, enligt 6 § förordningen (2022:524) om statliga myndigheters beredskap, verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet. Vilka verksamheter som är av betydelse för att upprätthålla Sveriges säkerhet måste bedömas

[19] Prop. 2017/18:89, s. 138.

i ljuset av samhällsutvecklingen. Ett sådant exempel är hur samhällets funktionalitet de senaste åren blivit mer beroende av datasystem och mobiltelefoni.[20] Samhällsviktiga verksamheter finns ofta inom sektorerna energiförsörjning, livsmedelsförsörjning, elektroniska kommunikationer, vattenförsörjning, transporter och finansiella tjänster. Avgörande för om verksamheten kan anses röra Sveriges säkerhet bör vara om en antagonistisk handling (exempelvis spionerі, sabotage eller terroristbrott) skulle kunna medföra skadekonsekvenser på nationell nivå. Sådana skadekonsekvenser kan exempelvis vara störningar i eller bortfall av leveranser, tjänster och funktioner som är nödvändiga för samhällets funktionalitet ur ett nationellt perspektiv. Det kan röra sig om elförsörjning och centrala betalningssystem.[21] Av Myndigheten för civilt försvars *Lista med de viktigaste samhällsfunktionerna* framgår bland annat att utbetalningar av statliga ersättningar utgör en viktig samhällsfunktion; den avser förmågan att hantera fastställande och utbetalning av statliga ersättningar och försvarsförmåner, bland annat socialförsäkring, arbetslöshetsförsäkring, pension och pensionsrelaterade förmåner, och omfattar allt från handläggning till utbetalning samt information och vägledning till medborgare.[22]

Ett centralt informationssystem som möjliggör biometrisk verifiering av identitet på det sätt vi föreslår skulle som vi ser det kunna utgöra ett informationssystem i den mening som avses i 1 kap. 3 § säkerhetsskyddsförordningen, nämligen *ett system av sammansatt mjuk- och hårdvara som behandlar information.* Innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift ska verksamhetsutövaren, enligt 3 kap. 1 § förordningen, genom en särskild säkerhetsskyddsbedömning ta ställning till vilka säkerhetskrav i systemet som är motiverade och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses. Enligt 3 kap. 4 § förordningen ska verksamhetsutövaren även vidta lämpliga skyddsåtgärder för att kunna upptäcka, försvåra och hantera skadlig inverkan på informationssystemet samt obehörig avlyssning av, åtkomst till och nyttjande av informationssystemet.

Under vissa förutsättningar skulle en teknisk lösning för att biometriskt verifiera identitet som utformas på det sätt vi beskrivit i avsnitt 27.4, kunna klassificeras som en samhällsviktig verksamhet eller

[20] SOU 2021:63, s. 129.
[21] Prop. 2017/18:89, s. 44.
[22] *Lista med de viktigaste samhällsfunktionerna*, s. 12.

ha en roll i en samhällsfunktion som är viktig för Sverige. I avsnitt 28.2.1 har vi dock gjort bedömningen att ett sådant tekniskt system inte bör vara väsentligt för att upprätthålla en kritisk samhällelig eller ekonomisk verksamhet, på det sätt som avses i 5 § 1 cybersäkerhetslagen. De omständigheter vi pekat på i nämnda avsnitt kan enligt vår mening även beaktas vid den nu aktuella bedömningen. Vi anser därför att mycket talar för att ett avbrott i möjligheten att biometriskt verifiera identitet med stöd av den nya lagen inte skulle anses påverka en nationell förmåga och funktion på ett sätt som medför skada för Sveriges säkerhet, i den mening som avses i säkerhetsskyddslagen. Detta talar också mot slutsatsen att tillhandahållande av ett gemensamt backend-system och en mobilapplikation som möjliggör sådana kontroller i sig utgör sådan verksamhet som omfattas av säkerhetsskyddslagen.

Med detta sagt ankommer det, som vi anfört inledningsvis i detta avsnitt, på den myndighet som eventuellt får ansvar för ett sådant tekniskt system att ta ställning till om man av den eller annan anledning omfattas av säkerhetsskyddslagen.

28.3.3 Uppgifter som förekommer vid biometrisk verifiering

En omständighet som i Säkerhetspolisens promemoria *Vad är säkerhetskänslig verksamhet?* anses visa på att en viss verksamhetsutövare bedriver säkerhethetskänslig verksamhet är att denne hanterar säkerhetsskyddsklassificerade uppgifter.[23] Frågan är om de uppgifter som kommer att behöva hanteras vid biometrisk verifiering av identitet med stöd av den nya lagen – såväl av en verifierande myndighet som av en tekniskt ansvarig aktör – skulle kunna anses utgöra sådana uppgifter.

Vi kan konstatera att det i första hand är alfanumeriska uppgifter om identitet, identitetsbeteckningar och Migrationsverkets individnummer, samt biometriska underlag och biometriska uppgifter som är aktuella. Även vissa andra identitetsrelaterade uppgifter, exempelvis kön, kan förekomma. I avsnitt 20.5 har vi bedömt att de alfanumeriska uppgifterna är av sådant slag att de, när de förekommer i bland annat folkbokföringsverksamheten, normalt sett anses vara harmlösa och som huvudregel är offentliga. Detsamma bör gälla vid biometrisk verifiering enligt den nya lagen. Detta talar enligt vår mening mot

[23] Säkerhetspolisens promemoria från den 5 mars 2024, s. 4.

att de skulle bedömas vara säkerhetsskyddsklassificerade uppgifter. Att den verifierande myndigheten bedriver verksamhet som omfattas av säkerhetsskyddslagen och vill verifiera identitet på någon vid handläggningen av ett ärende eller i annat fall – exempelvis i samband med inpassering till en byggnad – talar som vi ser det inte i sig för att uppgifterna är att betrakta som säkerhetsskyddsklassificerade uppgifter. Detta med hänsyn till att de alfanumeriska uppgifterna normalt sett inte bör kunna härledas till den säkerhetskänsliga verksamheten eller till säkerhetsskyddsklassificerade uppgifter som kan förekomma i verksamheten; enbart att en verifiering genomförs innebär exempelvis inte att det framgår att en person vars identitet verifieras biometriskt är anställd inom Försvarsmakten. Detsamma gäller som vi ser det för de biometriska uppgifter som behandlas vid den biometriska jämförelsen. Det kan enligt vår mening även beaktas att uppgifterna endast behandlas momentant i systemet, och endast i syfte att genomföra en biometrisk verifiering. Uppgifterna ska inte heller kunna lagras av den myndighet som ansvarar för ett backend-system och en mobilapplikation. Vi kan i detta sammanhang notera att i promemorian *En extern tjänsteleverantör för biometriupptagning i migrationsverksamheten* bedömdes att personuppgifter som en extern tjänsteleverantör får tillgång till i samband med upptagning av biometriska underlag, inom ramen för ett ärende om uppehållstillstånd eller nationell visering, inte utgör säkerhetsskyddsklassificerade uppgifter. Sådan verksamhet bedömdes inte heller vara säkerhetskänslig verksamhet.[24]

Sammantaget kan vi konstatera att mycket få uppgifter ska hanteras i de tekniska systemen, oavsett om det är i system som den verifierande myndigheten själv ansvarar för eller ett gemensamt som en tekniskt ansvarig aktör tillhandahåller, att de alfanumeriska uppgifter som förekommer normalt inte omfattas av sekretess, att uppgifterna normalt sett inte bör kunna härledas till någon eventuell verksamhet som omfattas av säkerhetsskyddslagen hos den verifierande myndigheten, och att biometriska underlag och biometriska uppgifter, enligt våra förslag, omedelbart ska förstöras efter att en kontroll har genomförts. I likhet med vad vi anfört i föregående avsnitt ankommer det emellertid på varje verifierande myndighet att ta ställning till detta, utifrån den verksamhet man bedriver. De omständigheter som vi redogjort för ovan bör då kunna beaktas.

[24] Ds 2026:8, s. 186.

28.3.4 Sammanfattning

Vår bedömning

Säkerhetsskyddsåtgärder som en verifierande myndighet eller en tekniskt ansvarig aktör vidtar på grund av att denne omfattas av regelverket om säkerhetsskydd bör på lämpligt sätt beaktas även vid biometrisk verifiering av identitet med stöd av den nya lagen, eller vid tillhandahållande av ett sådant tekniskt system som beskrivs i avsnitt 27.4.

Vi har i avsnitt 28.3.2 och 28.3.3 redogjort för omständigheter som vi anser kan beaktas vid en bedömning av om en verifierande myndighet eller en tekniskt ansvarig aktör kan komma att omfattas av regelverket om säkerhetsskydd och de särskilda krav på att vidta säkerhetsskyddsåtgärder som följer av det, enbart med anledning av att myndigheten biometriskt verifierar identitet med stöd av den nya lagen eller tillhandahåller en sådan teknisk lösning som vi beskrivit i avsnitt 27.4. Bedömningen behöver göras av varje enskild myndighet, men de omständigheter vi lyft fram skulle då kunna vara till ledning.

En verifierande myndighet eller en tekniskt ansvarig aktör kan oaktat detta, av annan anledning, anses bedriva verksamhet som innebär att man omfattas av regelverket om säkerhetsskydd. Säkerhetsskyddsåtgärder som myndigheten med anledning av detta vidtar kan i sådana fall behöva beaktas, och eventuellt anpassas, på lämpligt sätt så att åtgärderna även tar i beaktande de risker som vi har lyft fram i avsnitt 28.2 och som kan uppkomma vid biometrisk verifiering med stöd av den nya lagen, eller vid tillhandahållande av ett myndighetsgemensamt system som möjliggör sådan verifiering. Bland annat kan det handla om olika åtgärder som tar sikte på att förebygga skadlig inverkan på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet. Som vi ser det bör de uppgifter som förekommer vid en biometrisk verifiering enligt den nya lagen – om verifieringen görs av en myndighet som också bedriver verksamhet som omfattas av regelverket om säkerhetsskydd – inte ges ett sämre säkerhetsskydd än motsvarande slag av uppgifter som i övrigt kan förekomma i verksamheten, även om de förstnämnda i sig inte anses utgöra säkerhetsskyddsklassificerade uppgifter. Vidare bör åtgärder som tar sikte på den fysiska säkerheten hos en viss myndighet också kunna få bety-

delse för det fall myndigheten ges ansvar för att tillhandahålla ett myndighetsgemensamt system för att biometriskt verifiera identitet. Detsamma gäller åtgärder i fråga om personalsäkerhet.

Sammantaget anser vi att det saknas hinder mot att en myndighet på olika sätt drar nytta av säkerhetsskyddsarbete som redan bedrivs av annan anledning. På så sätt kan ett konsekvent och ändamålsenligt säkerhetsskydd främjas även för nätverks- och informationssystem, och för de uppgifter om enskilda, som aktualiseras vid en implementering av våra förslag och en tillämpning av den nya lagen i praktiken.

29 Ansvarsfördelning

29.1 Inledning

En central fråga för ett system för säkrare verifiering av identitet och andra förslag för att stärka kopplingen mellan fastställd grundidentitet och verifiering av identitet är, enligt våra direktiv, vilken eller vilka myndigheter som ska ansvara för de uppgifter som behöver utföras. I samband med detta bör det belysas vilka eventuella synergieffekter som kan finnas med andra uppgifter som myndigheterna ansvarar för i dag eller kan komma att få ansvar för i takt med genomförandet av förslag som bereds. Även frågor om kostnadseffektivitet, tillgänglighet och myndigheternas möjlighet att tillhandahålla service behöver beaktas. Samtidigt är myndigheternas kapacitet att tillgodose krav på säkerhet och andra tekniska förutsättningar en viktig fråga vid övervägandena om ansvarsfördelningen.

29.2 Ansvar för biometrisk verifiering av identitet

Vår bedömning

Den verifierande myndigheten bör vara rättsligt ansvarig för de biometriska kontroller som myndigheten bestämmer ska genomföras med stöd av den nya lagen om biometrisk verifiering av identitet. Det bör därför inte övervägas att ge en eller flera myndigheter i uppdrag att bedriva verksamhet med biometrisk verifiering av identitet mot handlingar med stöd av den nya lagen.

Biometrisk verifiering av identitet är, som vi varit inne på tidigare (se avsnitt 21.5.1), att betrakta som en utredningsåtgärd som kan vidtas av den myndighet som vill verifiera identitet biometriskt med

stöd av den nya lagen (den verifierande myndigheten) antingen inom ramen för handläggningen av ett ärende som omfattas av förvaltningslagens (2017:900) tillämpningsområde eller när myndigheten, i annat fall, genomför identitetskontroller inom ramen för sin verksamhet. Med detta synsätt framstår det som naturligt att den verifierande myndigheten är rättsligt ansvarig för de biometriska verifieringar som man bestämmer ska genomföras med stöd av den nya lagen.

Det skulle också kunna övervägas att en viss myndighet får i uppdrag att bedriva verksamhet med biometrisk verifiering av identitet mot handlingar. En myndighet som vill verifiera identitet med stöd av den nya lagen skulle i sådant fall få vända sig till denna myndighet och överlåta ansvaret för att genomföra verifieringen såväl rättsligt som faktiskt. Det går här att dra paralleller till sådan verksamhet med ett identitetsindex som vi redogjort för i avsnitt 16.2.1. Till skillnad från biometrisk verifiering mot ett identitetsindex förutsätter biometrisk verifiering mot handlingar dock inte att någon aktör ansvarar för fortlöpande lagring av personuppgifter om samtliga de personer som ska kunna verifieras biometriskt. Biometrisk verifiering mot pass eller andra handlingar – i enlighet med våra förslag – kräver endast tillfällig behandling av personuppgifter, vilket innebär att det inte finns något egentligt behov av att en viss utpekad myndighet bär det rättsliga ansvaret för samtliga verifieringar som genomförs med stöd av den nya lagen.

Det är, enligt vår bedömning, den verifierande myndigheten som bäst kan ta ställning till om förutsättningarna för en biometrisk verifiering är uppfyllda och det ska, enligt våra förslag, därmed ankomma på den verifierande myndigheten att avgöra om förutsättningarna är uppfyllda. Vidare kommer det därmed i praktiken att vara den verifierande myndigheten som bestämmer ändamålen och medlen för behandlingen av personuppgifter och vi har i avsnitt 24.6 föreslagit att den verifierande myndigheten ska vara personuppgiftsansvarig. Om en annan myndighet skulle vara rättsligt ansvarig för att – på uppdrag av en verifierande myndighet – genomföra biometriska verifieringar med stöd av den nya lagen, skulle denna myndighet i princip behöva förlita sig på den verifierande myndighetens bedömning av om det finns förutsättningar för en verifiering. Det är enligt vår mening inte en ändamålsenlig eller i övrigt lämplig ordning.

Mot den här bakgrunden anser vi att den verifierande myndigheten alltid själv bör ansvara rättsligt för de biometriska verifier-

ingar som myndigheten bedömer är nödvändiga i enlighet med den nya lagen. Det bör därför inte övervägas att ge en eller flera myndigheter i uppdrag att bedriva verksamhet med biometrisk verifiering av identitet mot handlingar.

29.3 Genomförande av våra förslag förutsätter inte en myndighetsgemensam teknisk lösning

Vår bedömning

En generell möjlighet för myndigheter att verifiera identitet biometriskt mot handlingar, i enlighet med vårt förslag om en ny lag, förutsätter varken att en myndighetsgemensam teknisk lösning finns tillgänglig eller att en viss myndighet pekas ut som ansvarig för en sådan lösning.

Införande av ett identitetsindex förutsätter, som vi ser det, att en eller flera myndigheter bedriver verksamhet med ett identitetsindex (se avsnitt 16.2.1). För det fall vi hade föreslagit att ett identitetsindex ska införas hade det därmed varit naturligt att ta ställning till vilken eller vilka myndigheter som bör bedriva sådan verksamhet och lämna nödvändiga författningsförslag i detta avseende. Den nya lagen om biometrisk verifiering av identitet, i enlighet med våra förslag, förutsätter emellertid inte att en eller flera myndigheter får i uppdrag att för andra myndigheters räkning möjliggöra sådan verifiering (jfr avsnitt 29.2). Om de myndigheter som vill nyttja den rättsliga möjligheten att verifiera identitet biometriskt med stöd av den nya lagen själv skapar tekniska förutsättningar för att göra detta behöver ingen annan myndighet ansvara varken för en särskild verifieringsverksamhet eller för ett myndighetsgemensamt tekniskt system för verifiering. En generell möjlighet för myndigheter att verifiera identitet biometriskt mot handlingar, i enlighet med vårt förslag, förutsätter alltså varken att en myndighetsgemensam teknisk lösning tas fram och tillgängliggörs eller att en viss myndighet pekas ut som ansvarig för en sådan lösning.

Vidare är det inte säkert att ett uppdrag till en viss myndighet att utveckla och förvalta en myndighetsgemensam teknisk lösning kräver författningsändringar i form av till exempel tillägg i den aktuella

myndighetens instruktion; uppdraget skulle, beroende på omständigheterna, kunna lämnas endast genom ett regeringsbeslut eller i myndighetens årliga regleringsbrev, som även det beslutas av regeringen. Med hänsyn till detta, och till att det inom ramen för utredningen inte är möjligt eller lämpligt att lämna konkreta eller detaljerade förslag avseende hur våra förslag ska implementeras tekniskt (se avsnitt 27.1), lämnar vi inte några författningsförslag om vilken eller vilka myndigheter som ska ansvara för ett eventuellt myndighetsgemensamt tekniskt system och distributionen av information till de verifierande myndigheterna från detta system.

Vi avser dock att i de kommande avsnitten utvärdera om en eller flera privata aktörer bör kunna ansvara för en eventuell myndighetsgemensam teknisk lösning (avsnitt 29.4), om ansvaret för en sådan lösning bör ges till en eller flera myndigheter (avsnitt 29.5) och i sådant fall vilken eller vilka myndigheter som är bäst lämpade att vara ansvarig (avsnitt 29.6).

29.4 En eller flera privata aktörer bör inte ansvara för en myndighetsgemensam teknisk lösning

Vår bedömning

En eller flera privata aktörer bör inte ansvara för en myndighetsgemensam teknisk lösning.

Att den verifierande myndigheten, enligt vår bedömning i avsnitt 29.2, bör vara rättsligt ansvarig för de biometriska verifieringar som myndigheten bestämmer ska genomföras med stöd av den nya lagen utesluter inte att de myndigheter som så önskar ansluter sig till en myndighetsgemensam teknisk lösning av det slag vi beskrivit i avsnitt 27.4. Det utesluter inte heller nödvändigtvis att den verifierande myndigheten anlitar en privat aktör för tillhandahållande av de tekniska system som behövs för att myndigheten ska kunna genomföra biometriska verifiering av identitet med stöd av den nya lagen. Vi bedömer dock att det inte är lämpligt att låta en eller flera privata aktörer ha helhetsansvaret för den tekniska lösning som används av en eller flera verifierande myndigheter. I stället bör en verifierande myndighet som väljer att använda en egen teknisk lösning vara ansvarig för den och

en eller flera myndigheter bör ansvara för att ta fram och förvalta en eventuell myndighetsgemensam teknisk lösning. Skälen för denna bedömning är följande.

Liknande tekniska lösningar som den vi redogjort för i avsnitt 27.4 finns redan på marknaden hos privata aktörer. Det finns bland annat svenska utfärdare av e-legitimationer som använder en liknande verifieringsprocess vid utfärdande av e-legitimationer när den enskilde gör en ansökan på distans. Dessa aktörer har erfarenhet av att ta fram och erbjuda relevanta tekniska lösningar för olika delar av en verifieringsprocess, som till exempel så kallad liveness-check. En lösning som bygger på en e-legitimation skulle sannolikt även underlätta för de myndigheter som i vissa situationer vill använda biometrisk verifiering som en del av ett ansökningsförfarande. Att låta godkända leverantörer av e-legitimationer tillhandahålla en tjänst som möjliggör verifiering av identitet biometriskt mot en handling på distans skulle kunna möta behov av stark användarintegration, förutsättningar för skalbarhet och en snabb implementering. Vidare finns det, enligt vår bedömning, som utgångspunkt inga hinder från sekretessynpunkt mot att låta en privat aktör vara ansvarig för en teknisk lösning för biometrisk verifiering av identitet mot handlingar (se avsnitt 25.3). Dessa omständigheter talar för att en eller flera privata aktörer skulle kunna vara ansvariga för en myndighetsgemensam teknisk lösning.

Vi har dock i avsnitt 21.3.2 bedömt att privata aktörer, i vart fall i nuläget, inte bör omfattas av en generell möjlighet att biometriskt verifiera identitet mot handlingar. Vid denna bedömning har vi bland annat beaktat att det finns risker för den personliga integriteten och för bristande förenlighet med dataskyddsförordningen[1] med att ge privata aktörer möjlighet att verifiera identitet biometriskt. Det framstår med hänsyn till detta inte som lämpligt att låta privata aktörer ansvara för väsentliga delar av den faktiska hanteringen av biometriska uppgifter och andra personuppgifter vid sådan verifiering. Vidare finns det utmaningar från säkerhetssynpunkt – om en privat aktör ska ansvara för den tekniska lösningen – vad gäller förvaltningen av de certifikat som behövs för att en verifiering mot en handling ska kunna genomföras (se avsnitt 27.4.1 och 27.4.2). Det finns, som vi ser det, också en inte oväsentlig risk för ändamålsglidning hos en privat tillhandahållare av tekniska system, det vill säga att uppgifter efter insamlingen används för nya eller utökade syften (se avsnitt 21.3.2),

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.

även om dessa uppgifter inte på något sätt ska få användas av den tekniskt ansvarige aktören, utöver tekniskt i verifieringsprocessen. Dessa omständigheter talar i stället mot att en eller flera privata aktörer bör få ansvar för att ta fram och förvalta en myndighetsgemensam teknisk lösning.

Vid ställningstagande till om en eller flera privata aktörer bör kunna ansvara för en myndighetsgemensam teknisk lösning bör uppdragets komplexitet samt dess betydelse för säker verifiering av identitet och för en sammanhållen statlig identitetsförvaltning också beaktas. Det är, enligt vår bedömning, viktigt att det finns en tydlig offentlig rådighet över hur den tekniska lösningen används, utvecklas och förvaltas för att uppnå hög tillit till lösningen. Sådan rådighet minskar vidare risken för att information används för andra syften än de avsedda. Tydlig offentlig rådighet förutsätter god insyn från myndighetshåll i den tekniska produkten, driften av den och produktutvecklingen. Även om en myndighet som får i uppdrag att ta fram och ansvara för en myndighetsgemensam lösning kan behöva använda såväl komponenter som specialistkompetens och tekniskt stöd från privata aktörer bör helheten, som vi ser det, tillhandahållas och styras av en myndighet, eftersom det är viktigt för att säkerställa kontroll, tillit och långsiktig förvaltning. Om en privat aktör tillhandahåller hela det system för biometrisk verifiering av identitet som används av myndigheter finns det vidare en överhängande risk för att det offentliga blir beroende av den privata aktören. Vidare kan såväl systemet som sådant som tilliten till det bli lidande om den privata aktören till exempel går i konkurs eller blir uppköpt av ett annat företag.

Den nya lag vi föreslår syftar till en bred användning av biometrisk verifiering av identitet mot handlingar för myndigheter. En myndighetsgemensam teknisk lösning behöver därför vara robust och tillgängligheten god för att möta efterfrågan och möjliggöra verifiering i de situationer som lagen avser att träffa. Med hänsyn till detta och de omständigheter vi redogjort för ovan förespråkar vi att en offentlig aktör får i uppdrag att ta fram och tillhandahålla en myndighetsgemensamteknisk lösning för biometrisk verifiering mot handlingar, om en sådan blir aktuell. Vi anser alltså att en eller flera privata aktörer inte bör ansvara för en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet.

29.5 En enda myndighet bör ha huvudansvaret för en myndighetsgemensam teknisk lösning

Vår bedömning

En enda myndighet bör ha huvudansvaret för en myndighetsgemensam teknisk lösning.

Den tekniska lösning som vi redogjort för i avsnitt 27.4 bygger på myndighetsgemensamma komponenter i form av en mobilapplikation och ett backend-system. Ett uppdelat ansvar för en sådan lösning skulle kunna övervägas, så att en myndighet får i uppdrag att ta fram och säkerställa driften av en funktionell, användarvänlig mobilapplikation och en annan myndighet får ansvaret för ett robust och tillgängligt backend-system, som kan ta emot och bearbeta information från mobilapplikationen och kopplas till verifierande myndigheters system. En sådan uppdelning av ansvaret skulle innebära att flera myndigheters resurser och kompetens kan nyttjas för den gemensamma helhetslösningen. Ett uppdelat ansvar ökar dock risken för otydlighet i ansvarsfördelningen och för bristande helhetssyn. Utan god samverkan mellan inblandade myndigheter finns även en risk för ökad administration, vilket i sin tur kan orsaka längre införandetider och högre kostnader. Det finns, som vi ser det, fördelar med att hålla samman ansvar för utveckling av en mobilapplikation och ett backendsystem samt förvaltning och underhåll av dessa, eftersom de utgör nödvändiga delar av samma tekniska lösning och måste vara kompatibla. Vidare finns det ett starkt samband mellan utveckling, vidareutveckling, säkerhetsarbete, förvaltning och drift, vilket medför att en och samma myndighet bör ansvara för samtliga dessa moment.

I betänkandet *En säker och tillgänglig statlig e-legitimation* föreslogs ett delat myndighetsansvar för grundidentifiering respektive utfärdande av en statlig e-legitimation. Polismyndigheten bedömdes vara bäst lämpad att utföra uppdraget att genomföra grundidentifieringen, medan utredningen bedömde att Myndigheten för digital förvaltning (Digg) skulle tillhandahålla den statliga e-legitimationen.[2] I den efterföljande propositionen *En statlig e-legitimation* föreslog regeringen emellertid att Polismyndigheten – och i vissa fall utlandsmyndigheterna – ska ansvara för såväl grundidentifieringen som ut-

[2] SOU 2023:61, s. 172 f. och 180.

färdandet av e-legitimationen, vilket förordades av många remissinstanser.[3] Regeringen har också gett Polismyndigheten i uppdrag att utfärda en statlig e-legitimation.[4] I beslutet uttalade regeringen att samma myndighet bör ha ansvaret för både grundidentifiering och utfärdande av den statliga e-legitimationen samt att ett sammanhållet myndighetsansvar är mer kostnadseffektivt, minskar administrationen och ökar säkerheten i systemet. Argumenten för ett sammanhållet myndighetsansvar gör sig, enligt vår mening, gällande även i den nu aktuella situationen.

Mot den här bakgrunden bedömer vi att endast en myndighet bör ha det huvudsakliga ansvaret för en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet. Att en myndighet är huvudansvarig för en myndighetsgemensam lösning utesluter emellertid inte att denna myndighet samverkar med andra myndigheter för att utnyttja befintlig kompetens och uppnå en så kostnadseffektiv och funktionell lösning som möjligt.

29.6 Myndigheter som är lämpade att ansvara för en myndighetsgemensam teknisk lösning

Polismyndigheten, Migrationsverket och Skatteverket har, som vi påpekat i bland annat avsnitt 6.1, en central roll i den svenska identitetsförvaltningen genom att de ansvarar för att i vissa ärendeslag verifiera identitet för personer som vistas, eller vill vistas i Sverige, och – för det fall det kommer fram att personen inte är känd för svenska myndigheter sedan tidigare – bestämma och registrera en så kallad grundidentitet för personen. Vidare har vi bedömt att vid införande av ett identitetsindex bör en identitetsnyckel kunna skapas av dessa myndigheter. Med hänsyn till detta framstår samtliga dessa myndigheter som utgångspunkt som lämpliga för ett uppdrag att ta fram en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet mot handlingar med stöd av den nya lagen.

Vi kan i detta sammanhang notera att Försäkringskassan, enligt förordningen (2024:1005) om samordnad och säker statlig it-drift, har fått i uppdrag att samordna ett statligt tjänsteutbud för it-drift. Försäkringskassan har vidare en av de största it-avdelningarna i lan-

[3] Prop. 2025/26:250, s. 43 f.
[4] Regeringsbeslut den 27 mars 2025, dnr Ju2025/00740.

det med cirka 1 000 anställda.[5] Med hänsyn till bland annat dessa omständigheter skulle även Försäkringskassan potentiellt sett kunna vara lämplig att ansvara för en myndighetsgemensam teknisk lösning. En annan myndighet som, med anledning av dess verksamhet, bör utvärderas i sammanhanget är Digg. Diggs huvudsakliga uppgifter är att samordna och stödja den förvaltningsgemensamma digitaliseringen, ansvara för den förvaltningsgemensamma digitala infrastrukturen och bistå regeringen med underlag för den offentliga förvaltningen och samhällets digitalisering.[6]

29.6.1 Migrationsverket

Det framgår av 1 § förordningen (2019:502) med instruktion för Migrationsverket att myndigheten är förvaltningsmyndighet för frågor som rör bland annat uppehålls- och arbetstillstånd, uppehållsrätt, visering, mottagande av asylsökande inklusive boenden och medborgarskap.

Vid handläggningen av ärenden om bland annat uppehållstillstånd ankommer det på Migrationsverket att i möjligaste mån klarlägga och verifiera sökandens identitet. Migrationsverket har stor erfarenhet av att ta upp biometriska underlag, för att söka med biometriska uppgifter i framför allt EU-gemensamma system, vid handläggningen av ansökningar om uppehållstillstånd på grund av behov av internationellt skydd. Myndighetens möjlighet att använda biometriska uppgifter i verksamheten kommer också att utökas framöver. Det bör emellertid noteras att Migrationsverket i nuläget inte för något särskilt register över fotografier; fotografierna finns i stället i den centrala utlänningsdatabasen och är tillgängliga – men inte sökbara – genom myndighetens olika ärendehanteringssystem. Vidare förvaltas Migrationsverkets register över fingeravtryck i praktiken av Polismyndigheten efter en särskild överenskommelse mellan myndigheterna, som innebär att endast Polismyndigheten har tillgång till fingeravtrycken i registret.[7]

Migrationsverket erbjuder vidare digital passkontroll, under vissa förutsättningar, för personer som har ansökt om uppehållstillstånd för att arbeta, studera eller flytta till någon i Sverige. I stället för att

[5] https://www.sgit.se/uppdraget, hämtad 2026-05-19.
[6] https://www.digg.se/om-oss/vart-uppdrag, hämtad 2026-05-18.
[7] *Biometri i brottsbekämpningen*, prop. 2024/25:37, s. 130.

en kontroll av sökandens pass görs i samband med ett personligt besök på en svensk ambassad eller ett generalkonsulat, alternativt hos Migrationsverket eller Statens servicecenter, kan kontrollen göras digitalt i e-tjänsten *Digital passkontroll*. Den digitala kontrollen görs med användning av e-legitimationen Freja och Migrationsverket har ingått ett samarbetsavtal med Freja eID Group AB kring digital identitetshantering. Migrationsverkets digitala passkontroll liknar, enligt uppgift från myndigheten, på många sätt den tänkta användningen av den myndighetsgemensamma mobilapplikation som vi redogjort för i avsnitt 27.4. Vidare utfärdar Migrationsverket de uppehållstillståndskort innehållande ett lagringsmedium med biometriska underlag som, enligt våra förslag, ska få användas för biometrisk verifiering av identitet med stöd av den nya lagen.

Mot den här bakgrunden kan det konstateras att Migrationsverket har erfarenhet av och kompetens att genomföra identitetskontroller och utreda utländska medborgares identitet. Även vad gäller hantering av biometri och digital kontroll av identitetshandlingar finns det erfarenhet och kompetens hos Migrationsverket; i dessa avseende samverkar myndigheten med Polismyndigheten och Freja eID Group AB. Dessa omständigheter är, enligt vår bedömning, dock inte tillräckliga för att Migrationsverket ska vara en reell kandidat för att ansvara för en myndighetsgemensam teknisk lösning för verifiering av identitet mot handlingar. Migrationsverket saknar både ett tydligt generellt informations- och serviceuppdrag – gentemot det allmänna och andra myndigheter – och en sådan tydlig teknisk profil som skulle kunna göra myndigheten lämplig för det aktuella uppdraget. Utifrån nuvarande verksamhet, uppdrag och organisation skulle ett uppdrag för Migrationsverket att ansvara för en myndighetsgemensam lösning, som vi ser det, inte bara vara en utökning av befintlig verksamhet, utan snarare ses som en helt ny verksamhet för myndigheten.

Med hänsyn till de omständigheter vi redogjort för ovan är Migrationsverket, enligt vår mening, inte lämpligt att ansvara för att ta fram och förvalta en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet mot handlingar.

29.6.2 Försäkringskassan

Försäkringskassan är enligt förordningen (2009:1174) med instruktion för Försäkringskassan förvaltningsmyndighet för de delar av socialförsäkringen och andra förmåner och ersättningar som ska administreras av myndigheten. Verksamheten består huvudsakligen i att besluta om och betala ut sådana förmåner och ersättningar som myndigheten ansvarar för.

Försäkringskassan, som under 2025 fattade drygt 21 miljoner beslut om olika socialförsäkringsförmåner,[8] kan antas bli en stor användare av en generell möjlighet att verifiera identitet biometriskt och detta särskilt om verifiering på distans möjliggörs tekniskt. Vidare är Försäkringskassan, enligt 4 § förordningen om samordnad och säker statlig it-drift, samordnande myndighet, och har i uppdrag att samordna ett statligt tjänsteutbud för it-drift. Det finns således en stor teknisk kompetens hos Försäkringskassan och myndigheten ska bidra till en effektiv, säker och enhetlig hantering av statens it-driftstjänster. Dessa omständigheter talar för att myndigheten skulle kunna vara lämplig för att ansvara för en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet.

Försäkringskassan saknar dock erfarenhet av att ta upp biometriska underlag och göra biometriska jämförelser, då det i dagsläget inte finns rättsligt stöd för myndigheten att göra det. Försäkringskassan genomför inte heller i dag någon egentlig identitetskontroll vid handläggningen av ett ärende; autentisering sker normalt med e-legitimation, vilket innebär risk för att förmåner inte betalas ut till rätt person.[9] Försäkringskassan kan alltså i dagsläget inte anses utgöra en del av den statliga identitetsförvaltningen.

Försäkringskassan skulle som vi ser det visserligen kunna säkerställa erforderlig kompetens inom relevanta områden om myndigheten fick i uppdrag att ansvara för en myndighetsgemensam teknisk lösning. Med hänsyn till de omständigheter vi redogjort för ovan bedömer vi emellertid att myndigheten inte bör övervägas för ett sådant uppdrag.

[8] Försäkringskassans årsredovisning 2025, tabell 6, s. 16.
[9] Se Riksrevisionens rapport *Vem där – fastställande av identitet vid statliga myndigheter*, RiR 2024:12, s. 70 f.

29.6.3 Skatteverket

Skatteverkets huvuduppgifter är att ta in skatter, sköta folkbokföringen, registrera bouppteckningar och vara borgenär åt staten.[10] Enligt 2 § andra stycket förordningen (2017:154) med instruktion för Skatteverket ska uppgifterna i folkbokföringen spegla befolkningens bosättning, identitet och familjerättsliga förhållanden så att olika samhällsfunktioner får ett korrekt underlag för beslut och åtgärder.

För syftet att distribuera folkbokföringsuppgifter till samhället har Skatteverket systemet Navet, där alla offentliga aktörer kan hämta folkbokföringsuppgifter digitalt. Skatteverket är alltså ansvarig för etablering av personer som folkbokförs eller tilldelas samordningsnummer i folkbokföringsverksamheten och för kontroll av identitet i samband med det, samt har i uppdrag att försörja samhället med identitetsuppgifter och vissa andra uppgifter om personer. Vidare har Skatteverket, liksom Försäkringskassan, ett formellt ansvar för statlig it-drift, vilket framgår av 5 § förordningen om samordnad och säker statlig it-drift, och har till exempel tidigare fått i uppdrag av regeringen att leverera it-tjänster till Utbetalningsmyndigheten.[11]

Skatteverket har, under senare år, fått rättsligt stöd för att inom folkbokföringsverksamheten ta upp biometriska underlag och göra jämförelser av biometriska uppgifter. Myndigheten kommer också att få utökade möjligheter att hantera biometri, genom förslag som bereds i Regeringskansliet. Det finns därmed redan i dag kompetens inom detta område och den kan antas komma att stärkas i takt med att myndighetens verksamhet i detta avseende utvecklas.

Skatteverket har alltså ett uppdrag att förse samhället med uppgifter om de personer som är registrerade i folkbokföringsverksamheten, det vill säga folkbokförda personer och personer som tilldelats ett samordningsnummer. Det skulle kunna ses som en naturlig utökning av detta uppdrag att även låta myndigheten ansvara för en myndighetsgemensam teknisk lösning som möjliggör biometrisk verifiering av identitet för, framför allt, personer som uppger ett personnummer eller ett samordningsnummer vid kontakt med en verifierande myndighet och därmed påstår sig vara en viss person. I Skatteverkets uppdrag om informationsförsörjning ligger också ett kundperspektiv och

[10] https://www.skatteverket.se/omoss/varverksamhet/styrningochuppfoljning/dethargorskatteverket.4.7856a2b411550b99fb780008148.html, hämtad 2026-05-18.
[11] Regeringsbeslut den 16 mars 2023, dnr Fi2023/01060.

ett användarvänligt perspektiv; aspekter som framstår som viktiga framför allt vid utformningen av en mobilapplikation som ska användas av enskilda, men även vid utformningen av gemensamma gränssnitt som hanterar kontakten mellan ett backend-system och verifierande myndigheters egna system.

Mot den här bakgrunden kan det konstateras att det finns flera omständigheter som talar för att Skatteverket är lämplig att ansvara för en myndighetsgemensam teknisk lösning för verifiering av identitet mot handlingar.

29.6.4 Polismyndigheten

Polismyndigheten har en bred verksamhet, där den brottsbekämpande delen är den många vanligen tänker på. I Polismyndighetens uppdrag ingår dock även andra verksamhetsområden, bland annat utfärdande av pass och nationellt identitetskort. Framöver kommer polisen att utfärda både pass och det statliga identitetskort som föreslagits i promemorian *Ett statligt identitetskort* (Ju2026/01595) och som ska kunna innehålla en statlig e-legitimation. Även den statliga e-legitimation – *Sverige-id* – som föreslagits i propositionen *En statlig e-legitimation*, och som under en begränsad tidsperiod ska utfärdas enligt en ny lag om statlig e-legitimation och elektronisk identifiering ska utfärdas av Polismyndigheten.[12] Polismyndigheten har också fått i uppdrag av regeringen att utfärda uppgifter för personidentifiering för fysiska personer, ofta benämnda PID (personal identification data), som behövs för den europeiska digitala identitetsplånboken som Digg ansvarar för att utveckla. Ett uppdrag att ansvara för en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet mot handlingar enligt den nya lagen får anses ligga väl i linje med utfärdande av fysiska identitetshandlingar, statlig e-legitimation och PID.

Vidare har förslag lämnats om att Polismyndigheten ska ansvara för inrättandet av ett Nationellt ID-center.[13] Att erbjuda stöd och utbildning inom dokumentkunskap, biometri och metod bör utgöra ett av centrets fokusområden. Även uppdraget att ansvara för ett nationellt ID-center medför, enligt vår mening, att det finns en tydlig roll och funktion för Polismyndigheten på området biometrisk veri-

[12] Prop. 2025/26:250, s. 43.
[13] Slutredovisning av regeringsuppdrag att stärka samarbetet för att upprätthålla och sprida kompetens inom identitetsfrågor, Fi2024/02215, 2025-09-30, dnr 8-93999-2025.

fiering av identitet mot handlingar. Polismyndighetens befintliga verksamhet innebär vidare att myndigheten redan har erfarenhet av och utvecklingsresurser kring både ansiktsigenkänning och RFID-teknologi (se avsnitt 27.2), vilket är värdefullt vid biometrisk verifiering av identitet mot handlingar. Vidare är det Polismyndigheten som ansvarar för den svenska masterlistan för publika certifikat för Machine Readable Travel Document (MRTD) baserade på ICAO:s dokument 9303 (se avsnitt 27.2); sådana certifikat behövs för att kunna genomföra en biometrisk verifiering mot en handling.

Polismyndigheten anser också själv, mot bakgrund av uppdragets komplexitet och samhällskritiska karaktär, att ansvaret för utveckling och underhåll av en myndighetsgemensam teknisk lösning för biometrisk verifiering bör läggas på myndigheten. Vidare är Polismyndigheten av uppfattningen att det är möjligt att inom myndigheten utveckla en applikation och ett system för avsett ändamål som kan användas mobilt. Dock anser Polismyndigheten att den myndighet som får uppdraget också bör få frihet att utforma den tekniska lösningen. Med hänsyn till detta och det ovan anförda kan vi konstatera att det finns flera omständigheter som talar för att Polismyndigheten är lämplig att ansvara för en myndighetsgemensam teknisk lösning för verifiering av identitet mot handlingar.

29.6.5 Digg

Enligt 1 § första stycket förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning ska Digg – som från den 1 januari 2027 slås samman med Post- och telestyrelsen (PTS) och då kommer att heta Digitaliseringsmyndigheten – samordna och stödja den förvaltningsgemensamma digitaliseringen i syfte att göra den offentliga förvaltningen mer effektiv och ändamålsenlig. På Diggs webbplats uppges myndighetens huvudsakliga uppgifter vara att samordna och stödja den förvaltningsgemensamma digitaliseringen, ansvara för den förvaltningsgemensamma digitala infrastrukturen samt bistå regeringen med underlag för den offentliga förvaltningen och samhällets digitalisering. Vidare leder Digg arbetet med den statliga nationella digitala infrastrukturen som kallas för *Ena – Sveriges digitala infrastruktur*. Ena bygger på idén om att staten behöver tillhandahålla vissa grundläggande lösningar som tillgodoser de behov som

är gemensamma för offentliga aktörer i deras datadelning och digitalisering. Arbetet med den nationella digitala infrastrukturen görs i nära samverkan med andra offentliga aktörer och lösningarna inom infrastrukturen tillhandahålls av olika statliga myndigheter. Inom ramen för Ena ska Digg utveckla och tillhandahålla en sammanhållen infrastruktur för identitets- och behörighetshantering.[14] I detta avseende skapar Digg en lösning för *Samordnad identitet och behörighet*, som syftar till att en inloggning och behörigheter kan användas för tillgång till flera system. Samordnad identitet och behörighet är till för verksamheter inom välfärdsområdet, som är helt eller delvis offentligt finansierade.[15]

Digg har också i uppdrag att utveckla en statlig digital identitetsplånbok. Det är en ny tjänst som ska göra det enklare och säkrare för både människor och företag att använda digitala tjänster i Sverige och inom hela EU. För att identitetsplånboken ska bli användbar kommer många svenska myndigheter att behöva bidra med så kallade attributsintyg. Digg samarbetar exempelvis med Polismyndigheten för att den kommande statliga e-legitimationen *Sverige-id* ska kunna användas för att få tillgång till identitetsplånboken.[16] I betänkandet *En säker och tillgänglig statlig e-legitimation* gjordes bedömningen att Digg skulle ansvara för att utfärda den statliga e-legitimationen[17], medan Polismyndigheten bedömdes vara den myndighet som var bäst lämpad att genomföra grundidentifieringen inför utfärdandet.[18] Digg fick också i uppdrag av regeringen att analysera möjligheterna för och lämna förslag om framtagandet och driften av en statlig e-legitimation – ett uppdrag som skulle utföras i samarbete med Polismyndigheten och Försäkringskassan.[19] Som vi redogjort för ovan har dock Polismyndigheten därefter föreslagits få helhetsansvaret för att utfärda en statlig e-legitimation, med motiveringen att samma myndighet bör ha ansvaret för både grundidentifiering och utfärdande av den statliga e-legitimationen samt att ett sammanhållet myndighetsansvar är mer kostnadseffektivt, minskar administrationen och ökar säkerheten i

[14] Regleringsbrev för budgetår 2026 avseende Myndigheten för digital förvaltning, 2025-12-18, Fi2025/00536 och Fi2025/02358 (delvis).
[15] https://www.digg.se/digitala-tjanster/samordnad-identitet-och-behorighet/nu-gor-vi-inloggning-och-atkomst-enklare-for-hela-valfarden, hämtad den 21 maj 2026.
[16] https://www.digg.se/digitala-tjanster/digital-identitetsplanbok/diggs-roll-och-samverkan-med-andra-, hämtad den 21 maj 2026.
[17] Utredaren skulle enligt kommittédirektiv 2022:142 lämna förslag på hur en e-legitimation kunde utformas och tillhandahållas av Digg.
[18] SOU 2023:61, s. 172 f. och 180 f.
[19] Regeringsbeslut I2022/01335, 2022-06-16.

systemet. Vid ställningstagande till vilken myndighet som bör ansvara för en myndighetsgemensam teknisk lösning gör de argument som ledde till att Polismyndigheten fick helhetsansvaret för en statlig e-legitimation sig emellertid inte gällande på samma sätt, eftersom det här är fråga om en enda ansvarig myndighet (se avsnitt 29.5). Det faktum att Digg, som utgångspunkt, ansågs lämplig för utfärdande av den statliga e-legitimationen kan i stället anses tala för att myndigheten skulle kunna vara lämplig för att ta fram och förvalta en myndighetsgemensam teknisk lösning för biometrisk verifiering mot handlingar.

I detta sammanhang bör det också nämnas att Digg granskar och godkänner svenska e-legitimationer och ansvarar för den svenska eIDAS-noden som möjliggör e-legitimering över landsgränserna. Vi har visserligen bedömt att en e-legitimation – som inte i sig innehåller biometriska underlag – i vart fall inom ramen för ett sådant regelverk som vi överväger, inte bör kunna användas för att biometriskt verifiera innehavarens identitet (avsnitt 19.3.6). Den statliga e-legitimationen *Sverige-id* kommer inte heller i sig att innehålla biometriska underlag; ansiktsbild och fingeravtryck som tas i samband med ansökan ska sparas *i ett lagringsmedium i bäraren av* den statliga e-legitimationen.[20] Det har under arbetets gång emellertid förts fram önskemål från potentiella verifierande myndigheter om stark användarintegration och en möjlighet att kunna samordna till exempel en autentisering med hjälp av e-legitimation i en myndighets e-tjänster med biometrisk verifiering av identitet mot handlingar. Med en sådan målsättning kan Diggs erfarenhet av e-legitimationer och kompetens inom detta område vara värdefulla, även om myndigheten inte själv utfärdar någon e-legitimation och den biometriska verifieringen som sådan kommer att ske mot en fysisk handling.

Det övergripande målet med en myndighetsgemensam teknisk lösning är visserligen att göra det möjligt för verifierande myndigheter att kontrollera en persons identitet biometriskt, utan personlig inställelse, men den primära användaren – i vart fall av en mobilapplikation – skulle ändå kunna anses vara den enskilde vars identitet ska verifieras. Diggs ansvar för den förvaltningsgemensamma digitala infrastrukturen syftar dock huvudsakligen på system och tjänster som primärt används av myndigheter, inte av enskilda. I detta uppdrag ligger dock

[20] Se 2 kap. 5 § förslag till lag om statlig e-legitimation och elektronisk identifiering i *En statlig e-legitimation*, prop. 2025/26:250, s. 7.

en samordnande roll i förhållande till flera myndigheter. Diggs erfarenheter i detta avseende kan vara till nytta vid utveckling och förvaltning av en myndighetsgemensam teknisk lösning, eftersom samverkan med andra myndigheter kommer vara en förutsättning för att ta fram en funktionell lösning.

Mot den här bakgrunden kan det konstateras att det finns flera omständigheter som talar för att Digg kan vara lämplig att ansvara för en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet mot handlingar. I sammanhanget bör det dock påpekas att Digg inte har någon egen driftmiljö utan anlitar Försäkringskassan för detta i dagsläget. Det är, som vi ser det, en brist att Digg utifrån nuvarande förutsättningar inte kommer att kunna ansvara även för driften av en myndighetsgemensam lösning.

Det bör vidare beaktas att regeringen har beslutat att ge Digg och Post- och telestyrelsen i uppdrag att förbereda en sammanslagning, med syftet att stärka arbetet med säker och tillgänglig digital infrastruktur, AI och data. Uppdragen innebär att Diggs uppgifter överförs och inordnas i Post- och telestyrelsen och att Digg upphör som egen myndighet, Digitaliseringsmyndigheten. För att tillvarata uppbyggd kompetens och kapacitet ska utgångspunkten vara att verksamhet fortsatt bedrivs på befintliga verksamhetsorter. Den nya organisationen ska, som vi nämnt inledningsvis i detta avsnitt, vara på plats den 1 januari 2027.[21] De omständigheter som talar för att Digg – från och med 2027 Digitaliseringsmyndigheten – är lämplig att ansvara för en myndighetsgemensam teknisk lösning är, såvitt vi kan bedöma, relevanta även med hänsyn till detta. Vi vet dock inte hur den nya Digitaliseringsmyndighetens verksamhet kommer att utvecklas, och det är fråga om en betydligt mindre myndighet än både Skatteverket och Polismyndigheten, vilket innebär mer begränsade resurser.

[21] Se bland annat https://www.regeringen.se/pressmeddelanden/2026/05/digg-och-pts-blir-digitaliseringsmyndigheten/ och regeringsbeslut den 11 december 2025, dnr Fi2025/00654 och Fi2025/02303.

29.6.6 Sammantagen bedömning

Vår bedömning

Polismyndigheten är bäst lämpad att ansvara för en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet mot handlingar med stöd av den nya lagen.

Inledningsvis vill vi här påpeka att det är svårt att utifrån en hypotetisk myndighetsgemensam teknisk lösning (se avsnitt 27.4) bedöma vilken myndighet som är bäst lämpad att ansvara för lösningen. Vår bedömning görs utifrån antaganden om den tekniska lösningen. Omständigheterna kan komma att förändras eller omvärderas vid den fortsatta beredningen av våra förslag. Vidare har Regeringskansliet och regeringen bäst förutsättningar att bedöma vilken myndighet som är bäst lämpad att ta fram en myndighetsgemensam teknisk lösning vid den tidpunkt då det eventuellt blir aktuellt, med hänsyn även till omständigheter som tillkommande uppdrag för relevanta myndigheter, samt med beaktande av bästa tillgängliga teknik. Regeringen bör också bestämma hur stor frihet den myndighet som får uppdraget att ansvara för en myndighetsgemensam lösning ska få att utforma en sådan lösning och vilken funktionalitet som ska vara obligatorisk.

Med det sagt har vi i avsnitt 29.6.1 och 29.6.2 bedömt att Migrationsverket och Försäkringskassan inte är lämpliga att ansvara för en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet med stöd av den nya lagen. Fråga är därmed vilken av myndigheterna Skatteverket, Polismyndigheten och Digg – som enligt vår bedömning alla kan vara lämpliga – som kan anses vara bäst lämpad för ett sådant uppdrag.

Skatteverket har en naturlig roll i sammanhanget från perspektivet informationsförsörjning; myndigheten har i uppdrag att försörja samhället med uppgifter om personer som har ett personnummer eller ett samordningsnummer, det vill säga om en mycket stor andel av de personer vars identitet kan komma att verifieras biometriskt med stöd av den nya lagen. Det finns också en stor teknisk kompetens hos myndigheten och sedan något år tillbaka använder myndigheten biometriska uppgifter i folkbokföringsverksamheten och utvecklar kontinuerligt kompetensen inom detta område.

Det är däremot Polismyndigheten som utfärdar pass och nationellt identitetskort och som kommer att utfärda det statliga identitetskort (som ska ersätta det nationella) – handlingar vilka sannolikt kommer att användas vid majoriteten av de biometriska verifieringar som genomförs med stöd av den nya lagen. Vidare har Polismyndigheten mer omfattande erfarenhet av att använda biometriska uppgifter i olika delar av sin verksamhet – bland annat vid kontroll av såväl svenska som utländska pass i samband med gränskontroller – och därmed troligen större kompentens inom detta område än Skatteverket. Det är också av betydelse i sammanhanget att Polismyndigheten ansvarar för certifikaten för att få tillgång till information på vissa av de relevanta handlingarna, att myndigheten ska ansvara för utfärdande av PID till den digitala identitetsplånboken samt att myndigheten ska ansvara för ett nationellt ID-center. Sammantaget bedömer vi, vid en jämförelse mellan Skatteverket och Polismyndigheten, att den senare är bättre lämpad att ansvara för en myndighetsgemensam teknisk lösning. Det framstår, som vi ser det, som en mer naturlig utveckling av Polismyndighetens befintliga verksamhet att utöka denna med uppdraget att utveckla och förvalta en sådan lösning än vad det gör att låta Skatteverket få detta uppdrag, som en del av folkbokföringsverksamheten.

Diggs verksamhet är av helt annan karaktär än både Skatteverkets och Polismyndighetens, i det att myndighetens verksamhet och arbete primärt riktar sig till offentliga aktörer och leverantörer av digitala tjänster, inte direkt till enskilda individer. Det är främst Diggs tekniska kompetens och erfarenheter som innebär att myndigheten skulle kunna vara aktuell för ett uppdrag att ansvara för en myndighetsgemensam lösning. Myndighetens verksamhet som sådan avser som utgångspunkt dock inte identitetsförvaltning. Som vi nämnt ovan är det till exempel Polismyndigheten som ska utfärda den PID som behövs för den digitala identitetsplånbok som Digg ansvarar för att utveckla. Det är i det nu aktuella avseendet emellertid inte fråga om att förvalta uppgifter om personer och deras identiteter på motsvarande sätt som i ett identitetsindex (se kapitel 11–18), i folkbokföringsverksamheten, passregistret, det föreslagna pass- och identitetskortsregistret[22] eller det föreslagna registret över ärenden om statlig e-legitimation[23]. I stället handlar det om ett tekniskt system för till-

[22] Ju 2026/01595, s. 129.
[23] Prop. 2025/26:250, s. 57.

fällig behandling av personuppgifter, i form av jämförelse av uppgifter som finns i eller på vissa handlingar med uppgifter som tas upp av en verifierande myndighet från den enskilde vid det aktuella verifieringstillfället. Vidare ska den verifierande myndigheten vara personuppgiftsansvarig för den behandling som utförs med anledning av att myndigheten bestämmer att en biometrisk verifiering ska genomföras (se avsnitt 24.6) och avsikten är, som sagt, att systemet endast ska behandla personuppgifter tillfälligt; biometriska underlag och biometriska uppgifter ska enligt våra förslag förstöras omedelbart när en kontroll har genomförts (se avsnitt 24.9). Detta är, som vi ser det, omständigheter som bör beaktas vid bedömningen av vilken myndighet som är bäst lämpad att ansvara för ett myndighetsgemensamt system. Vidare finns det, enligt vår bedömning, inte skäl att ifrågasätta att Digg har kapacitet att tillgodose krav på säker hantering av personuppgifter, inklusive biometriska underlag och biometriska uppgifter, samt distribution av information till verifierande myndigheter. Digg saknar däremot i nuläget möjlighet att ansvara för driften av en myndighetsgemensam lösning, vilket lyfts fram som en nackdel av utredningens experter.

Som vi ser det är synen på en myndighetsgemensam teknisk lösning också av betydelse för vilken myndighet som bör ansvara för lösningen. Om det är fråga om en – så att säga – fristående teknisk lösning, som möjliggör tillgång till information i de handlingar som ska få användas för biometrisk verifiering, upptagning av biometriska underlag och jämförelse av biometriska uppgifter, skulle Digg kunna anses vara bäst lämpad, i vart fall om myndigheten hade haft kapacitet att även ansvara för drift. Vi anser dock att den tekniska lösningen i stället bör betraktas som en mer integrerad del av den statliga identitetsförvaltningen. Med den utgångspunkten framstår Polismyndigheten som bäst lämpad.

Sammantaget bedömer vi att Polismyndigheten får anses vara bäst lämpad att ansvara för en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet med stöd av den nya lagen, för det fall den fortsatta beredningen utmynnar i att en sådan lösning ska tas fram.

DEL 4

Avslutande del

30 Konsekvensanalys

30.1 Inledning

Enligt våra kommittédirektiv ska vi, utöver vad som följer av kommittéförordningen (1998:1474) och förordningen (2024:183) om konsekvensutredningar, redovisa de konsekvenser som våra förslag kan få för arbetet med att förebygga och i övrigt motverka brottslighet. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna ska vi även föreslå hur dessa ska finansieras.

30.2 Övergripande frågor

30.2.1 Problemet och vad våra förslag syftar till att uppnå

I våra direktiv slås fast att förutsättningarna för identitetsförvaltningen i Sverige behöver stärkas. Vi har i kapitel 9 redogjort för olika typer av identitetsmissbruk och hur detta kan drabba såväl offentliga aktörer som enskilda; problembilden beskrivs särskilt i avsnitt 9.2. En tillförlitlig identitetsförvaltning syftar både till att skapa trygghet och säkerhet för medborgarna och till att motverka missbruk och bedrägerier som drabbar alla delar av samhället. I vissa delar har lagstiftaren under senare år vidtagit åtgärder för att ge centrala myndigheter – Polismyndigheten, Migrationsverket och Skatteverket – fler och bättre verktyg för att kontrollera identitet på personer som vistas eller vill vistas i Sverige. Åtgärderna tar emellertid sikte på ett begränsat antal ärendeslag och situationer och syftar i första hand till att kontrollera identitet i samband med etablering av en identitet och utfärdande av rese- och identitetshandlingar (se kapitel 10). Som vi lyft fram i kapitel 9 framstår däremot utnyttjande av redan etablerade identiteter – där den enskilde är medveten eller omedveten om detta – som det mest framträdande problemet. Särskilt i ett samhälle där allt fler kon-

takter tas på digital väg och med hjälp av bland annat e-legitimation, kan det vara svårt för myndigheter att på ett säkert sätt kontrollera att den person som man möter är den som han eller hon påstår sig vara.

Vi har i kapitel 11–21 övervägt två huvudalternativ som vi menar kan främja en stärkt identitetsförvaltning i Sverige och säkrare verifiering av identitet: ett nytt, centralt identitetsindex respektive en generell möjlighet för myndigheter att biometriskt verifiera identitet mot olika typer av handlingar. Våra författningsförslag – som avser att implementera det sistnämnda alternativet – syftar till att komplettera befintliga möjligheter för myndigheter att kontrollera identitet, och tar sikte på deras behov av att säkert verifiera identitet i betydligt fler ärendeslag och situationer än i dag, i första hand för att motverka att identiteter utnyttjas på olika sätt. Förslagen kan enligt vår mening också ses som ett komplement till den autentisering med hjälp av e-legitimation som används bland annat vid ansökan om olika socialförsäkringsförmåner, i synnerhet om förslagen avseende ett statligt identitetskort, som ska kunna innehålla en e-legitimation, och en separat statlig e-legitimation genomförs. En autentisering med e-legitimation och en biometrisk verifiering skulle i så fall kunna göras med användande av en och samma fysiska handling, i ett sammanhållet flöde, under förutsättning att en teknisk lösning av det slag vi beskrivit i avsnitt 27.4 används, som gör det möjligt att biometriskt verifiera identitet mot handlingar på distans. Detta skulle som vi ser det kunna få betydande effekter på de problem med utnyttjande av e-legitimation som vi beskrivit i avsnitt 9.2.4.

30.2.2 Effekten av att våra förslag inte genomförs och alternativa lösningar

Omfattningen av identitetsmissbruk är – som vi pekat på i avsnitt 9.2.5 – svår att bedöma, inte minst utifrån att det kan antas finnas ett betydande mörkertal. Vi anser dock att det står klart att missbruket riktas mot en större krets samhällsaktörer och att omfattningen är på en sådan nivå att ytterligare åtgärder behövs. Större möjligheter till säkrare verifiering av identitet för myndigheter, i enlighet med våra förslag, kan som vi ser det få betydelse för att minska förekomsten av utnyttjande av identiteter, bland annat i ärenden som rör social-

försäkringsförmåner (se även avsnitt 30.4 angående konsekvenser för att förebygga och motverka brottslighet).

Effekten av förslagen är emellertid mycket svår att överblicka, då det beror inte minst på hur myndigheter väljer att utnyttja den nya lag som vi föreslår, men även på hur förslagen tekniskt implementeras i praktiken. I viss mån är genomförandet och effekten också beroende av andra förslag, bland annat om det statliga identitetskortet, som ska kunna innehålla en e-legitimation, och om en separat statlig e-legitimation. Som en följd av detta är det också svårt att jämföra effekten av våra förslag med utvecklingen och förekomsten av identitetsmissbruk i samhället om förslagen inte genomförs. Även om effekten av förslagen är svår att förutse anser vi emellertid att det står klart att ett genomförande av våra förslag har potential att förändra synen på hur identitet kontrolleras i många ärendeslag och situationer, och redan *möjligheten* för myndigheter att i stor utsträckning använda biometrisk verifiering mot handlingar kan få en avskräckande effekt. Nollalternativet framstår därför inte som ändamålsenligt.

Ett alternativ till våra förslag om en generell möjlighet för myndigheter att biometriskt verifiera identitet mot handlingar är ett system i form av ett centralt identitetsindex, av det slag vi övervägt i kapitel 11–18 och 21. Vi har i kapitel 22 dock gjort en utförlig jämförelse mellan detta alternativ och det alternativ som vi föreslår, och då valt att inte gå vidare med författningsförslag för att implementera ett system med ett identitetsindex.

En annan alternativ lösning skulle, som vi ser det, kunna innefatta att våra förslag utökas till att avse även privata aktörer, i mindre eller större omfattning. Att även privata aktörer – som kan vara utsatta för identitetsmissbruk bland annat vid köp och upptagning av lån – får möjlighet att biometriskt verifiera identitet mot handlingar, kan antas bidra till att motverka utnyttjande av identiteter i sådana syften. Vi har emellertid bedömt att detta inte är lämpligt i nuläget. Ett skäl till att vi valt att inte gå vidare med förslag avseende ett identitetsindex eller en möjlighet för privata aktörer att biometriskt verifiera identitet mot handlingar är de utökade risker för skyddet för den personliga integriteten som dessa alternativ, enligt vår mening, innebär (se avsnitt 21.3.2 och 22.11). Ett ändamål med ett system för säkrare verifiering av identitet, som tar sikte på en mycket stor personkrets, däribland barn, är att uppnå en lämplig balans mellan systemets effek-

tivitet och sådana skyddsintressen. Med hänsyn till detta anser vi att de båda alternativa lösningarna som vi nyss nämnt inte framstår som ändamålsenliga.

30.2.3 Förenlighet med EU-rätten och Sveriges internationella åtaganden

Vi har vid våra överväganden och vid utformningen av våra förslag genomgående beaktat EU-rätten, särskilt dataskyddsförordningen[1] och EU:s rättighetsstadga[2]. För våra överväganden i dessa avseenden hänvisar vi till kapitel 16, 17, 21 och 24. Våra förslag syftar i första hand till att ge myndigheter möjlighet att i fler ärendeslag och situationer än i dag verifiera identitet biometriskt för personer som vistas i Sverige. Detta innefattar EES-medborgare som vistas i landet med stöd av rätten till fri rörlighet. Vi bedömer att våra förslag inte på ett direkt sätt kommer att ha en negativ inverkan på den fria rörligheten. Däremot är det möjligt att en kontroll av identitet med stöd av våra förslag i ett visst enskilt ärende kan komma att leda till att beslut fattas i ärendet som påverkar den fria rörligheten för den enskilde. Detta innebär emellertid inte, enligt vår mening, att förslagen skulle vara oförenliga med EU-rätten.

I detta sammanhang kan även nämnas förhållandet till den reviderade eIDAS-förordningen[3], som syftar till att säkerställa att medlemsstaterna tillhandahåller en europeisk digital identitetsplånbok. Den europeiska digitala identitetsplånboken ska göra det möjligt för användaren att begära, erhålla, välja, kombinera, lagra, radera, dela och visa upp uppgifter om personidentifiering, och kunna autentisera sig gentemot bland annat förlitande parter, exempelvis för att få tillgång till offentliga tjänster i ett annat medlemsland. Plånboken är alltså ett medel för elektronisk identifiering. Med införandet av plånboken kommer ett krav för offentliga organ att acceptera andra länders plånböcker som autentiseringsmedel. Den reviderade eIDAS-förordningen ställer krav på att när offentliga aktörer kräver användande av e-legitimation för åtkomst till en nättjänst så ska de godkänna e-legitimationer som utfärdats i en annan medlemsstat. Som vi anfört i avsnitt 19.3.6 reglerar förordningen emellertid inte användningen

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016.
[2] Europeiska unionens stadga om de grundläggande rättigheterna.
[3] Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024.

av biometriska underlag eller biometriska uppgifter, och en e-legitimation som ingår i den digitala identitetsplånboken syftar alltså inte i sig till att användas för biometrisk verifiering. Biometrisk verifiering av identitet med stöd av våra förslag är, som vi ser det, en fristående utredningsåtgärd (se avsnitt 30.3) i förhållande till användningen av en sådan digital identitetsplånbok som regleras i eIDAS-förordningen. Vidare innebär biometrisk verifiering av identitet med stöd av våra förslag, enligt vår mening, inte någon begränsning av krav i förordningen på bland annat ömsesidigt erkännande i syfte att få tillgång till en nättjänst med hjälp av en e-legitimation. Vi bedömer därför att våra förslag är förenliga med den reviderade eIDAS-förordningen.

Eftersom våra förslag får påverkan på skyddet för den personliga integriteten har vi beaktat relevanta delar av Europakonventionen, särskilt artikel 8. Som vi redogjort för i avsnitt 17.5 och 21.7.3 bedömer vi att våra förslag är förenliga med nämnda artikel. Även i övrigt bedömer vi att förslagen är förenliga med Sveriges internationella åtaganden.

30.3 Konsekvenser för enskilda

I betänkandet *Ett säkert statligt ID-kort – med e-legitimation* anförde 2017 års ID-kortsutredning bland annat att enskilda som utsätts för identitetskapning och vars identitet används i bedrägliga syften ofta drabbas av allvarliga konsekvenser, både ekonomiska och känslomässiga. Utredningen bedömde att förslag som minskar denna form av brottslighet därför gynnar enskilda direkt.[4] Vi delar denna bedömning. Syftet med den nya lag om biometrisk verifiering av identitet som vi föreslår är att motverka identitetsmissbruk, vilket innefattar dels att skydda det allmänna, dels att främja att enskilda kan vara trygga i att ingen annan kan uppträda i deras identitet i olika sammanhang; i avsnitt 23.6.1 har vi redogjort för hur den nya lagen skulle kunna användas som en form av ”spärrtjänst” för enskilda. Det regelverk vi föreslår medför alltså inte bara kontrollmöjligheter för det allmänna, utan utgör också en form av skyddslagstiftning för enskilda mot att deras identitet utnyttjas av andra. Med hänsyn till de kostnader och det besvär det kan medföra för enskilda att få sin identitet

[4] SOU 2019:14, s. 379.

utnyttjad är en sådan skyddsaspekt en konsekvens som inte får glömmas bort i sammanhanget.

Många enskilda använder i dag e-legitimation i sina kontakter med myndigheter, exempelvis för att ansöka om förmåner som handläggs av Försäkringskassan eller för att logga in till olika nättjänster, som exempelvis 1177.se (Sveriges samlingsplats för information och tjänster inom hälsa och vård). Under vårt arbete har det framförts att skiljelinjen mellan användning av e-legitimation och sådan biometrisk verifiering av identitet som våra förslag ska möjliggöra inte är helt enkel att dra. Det kan vara av vikt för genomslaget av våra förslag, och hur enskilda uppfattar en begäran om att biometriskt verifiera identitet, att detta tydliggörs. Risken är annars att enskilda missuppfattar syftet med förslagen och vad som förväntas av dem när en begäran enligt den nya lagen aktualiseras.

Vi har i avsnitt 19.3.6 redogjort för att vi anser att sådan autentisering som görs med hjälp av en e-legitimation är ett sätt att visa på en *behörighet*, inte ett sätt att verifiera identitet, det vill säga kontrollera om den som använder e-legitimationen också är den som han eller hon påstår sig vara. Detta illustreras av att de problem som har uppmärksammats av bland annat Skatteverket med att e-legitimationer skapas för olika personer och sedan används av någon annan, med eller utan deras vetskap eller aktiva medverkan (se avsnitt 9.2.4). Våra förslag syftar bland annat till att kunna komplettera den autentisering som genomförs med hjälp av en e-legitimation, och syftar alltså inte till att ersätta sådana möjligheter. Biometrisk verifiering av identitet med stöd av den lag som vi föreslår är en fristående utredningsåtgärd. Vår förhoppning är emellertid att våra förslag kan implementeras så att biometrisk verifiering med stöd av den nya lagen utvecklas till att vara ett naturligt integrerat moment i en digital autentiserings- och verifieringsprocess, där en e-legitimation används i förstnämnda del och bäraren av den – exempelvis ett sådant statligt identitetskort som föreslagits – används för den biometriska verifieringen. Samma fysiska handling kommer alltså att kunna användas i olika, men sammankopplade, syften. I ett sådant flöde kan biometrisk verifiering av identitet med stöd av den nya lagen ses som det tredje steget i en trefaktorsautentisering (3FA). 3FA bygger på tre grundläggande komponenter: något användaren har (till exempel ett identitetskort), något användaren vet (exempelvis en PIN-kod) och något han eller hon är (biometriska underlag). Med en ordning av detta slag – där den bio-

metriska verifieringen ingår som en del av en sammanhållen process – bedömer vi också att negativa effekter för enskilda – i den meningen att ett krav på att biometriskt verifiera identiteten upplevs som betungande – blir mindre.

Vi lämnar inte några förslag som uttryckligen gör det möjligt för myndigheter att kräva att enskilda inställer sig personligen. Som vi redogjort för i avsnitt 23.6.4 kan en begäran enligt den nya lagen om att göra en handling tillgänglig och låta myndigheten ta upp biometriska underlag däremot i praktiken komma att innebära en sådan skyldighet, om en biometrisk verifiering inte kan genomföras på distans, på grund av tekniska eller andra skäl i det enskilda fallet. Ett de facto-krav på personlig inställelse kan medföra såväl kostnader för resor som förlorad arbetsinkomst för den enskilde.

Våra förslag medför enligt vår bedömning inte i övrigt några kostnader för enskilda. Om den enskilde saknar sådana handlingar som ska få användas för biometrisk verifiering (se avsnitt 23.6.2) skulle han eller hon visserligen kunna känna sig tvungen att skaffa en ny handling. Någon skyldighet att inneha en sådan handling uppställs däremot inte; som vi erinrat om i avsnitt 23.8.5 ska en begäran enligt den nya lagen endast kunna riktas mot den som *innehar* en sådan handling. Under alla omständigheter kan det, enligt vår bedömning, med fog antas att få personer kommer att sakna en handling som kan användas för biometrisk verifiering med stöd av våra förslag; såväl hemlandspass som identitetskort är handlingar av sådant slag att enskilda i stor utsträckning behöver dessa för att kunna agera i vardagen och för att kunna resa. När det gäller det statliga identitetskort som har föreslagits kan det dessutom antas att ett innehav av dessa kommer att främjas, genom att det föreslås att en statlig e-legitimation ska finnas på kortet.[5] Även om en begäran om biometrisk verifiering enligt våra förslag skulle kunna utgöra en utlösande faktor till att den enskilde faktiskt skaffar ett nytt pass eller identitetskort, medför det, enligt vår bedömning, inte någon *ytterligare* kostnad för den enskilde, som direkt föranleds av våra förslag.

Vi har inte lämnat några förslag som närmare reglerar vilka konsekvenser som ska kunna följa av att en biometrisk verifiering enligt den nya lagen inte visat att den påstådda identiteten är riktig, utan det ankommer som utgångspunkt på den enskilda myndigheten att bestämma detta, utifrån det aktuella ärendeslaget eller den aktuella

[5] Promemorian *Ett statligt identitetskort*, Ju 2026/01595, s. 92.

situationen. Några sådana förslag är, som vi ser det, inte möjliga att lämna, bland annat med hänsyn till den breda krets av myndigheter och situationer som förslagen ska kunna tillämpas i. Som en följd av detta är det mycket svårt att förutse vilka konsekvenser – som är direkt hänförliga till en begäran om att genomföra en biometrisk verifiering – våra förslag kan få för enskilda. Effekterna är också avhängiga av i vilken utsträckning sådana kontroller faktiskt kommer att användas av olika myndigheter.

Under vissa omständigheter kan en begäran om biometrisk verifiering av identitet, från en myndighet som handlägger ett ärende som omfattas av förvaltningslagens (2017:900) tillämpningsområde, komma att medföra att ett beslut i ärendet fördröjs. Om så blir fallet beror i stor utsträckning på när under handläggningen av ärendet begäran framställs och på den enskildes vilja och möjligheter att följa begäran. En biometrisk verifiering som genomförs direkt, exempelvis i samband med att en myndighet tar emot en ansökan från en enskild, kan enligt vår mening inte antas fördröja ärendet, annat än om verifieringen inte bekräftar den av den enskilde uppgivna identiteten; ytterligare utredningsåtgärder kan då behöva vidtas. En begäran som framställs efter manuell hantering av ärendet kan dock antas förlänga handläggningstiden och detta särskilt om den enskilde behöver inställa sig personligen för att verifieringen ska kunna genomföras. Framför allt i ärenden där automatiserade beslut vanligen fattas, exempelvis hos Försäkringskassan, kan handläggningstiden antas fördröjas om en begäran om biometrisk verifiering behöver göras manuellt eller den enskilde av någon anledning inte har möjlighet att medverka till verifieringen direkt, till exempel på distans. Det skulle kunna få effekten att utbetalning av en förmån som den enskilde har rätt till fördröjs, vilket i vissa fall kan ha stor betydelse för den enskilde. I de fall det finns oklarheter om identitet som myndigheten anser behöver utredas kan möjligheten att verifiera identitet biometriskt, i vart fall på distans, emellertid effektivisera handläggningen; den enskilde kan relativt enkelt visa att den påstådda identiteten är riktig genom en biometrisk verifiering.

Det kan också konstateras att biometriska kontroller av det slag som våra förslag ska möjliggöra, i många fall kommer att utgöra en ny företeelse i enskildas kontakter med myndigheter, i situationer där det tidigare inte genomförts någon – eller en begränsad – kontroll av identitet. Den enskilde skulle exempelvis kunna tänkas vara

oförberedd på att biometrisk verifiering av identitet används vid kontakter med en vårdgivare eller vid inpassering till en myndighetslokal, med konsekvensen att ett vårdbesök eller ett besök hos myndigheten inte kan genomföras på tänkt sätt, eller att det fördröjs. När det gäller kontakter med vården skulle det exempelvis kunna vara fråga om ett besök för en frivillig vaccinering eller en allmän hälsokontroll; akut eller annan nödvändig vård kan givetvis inte nekas. Att identitetskontroller i många fall redan görs, och kommer att göras, mot de typer av handlingar som ska få användas för biometrisk verifiering med stöd av våra förslag, motverkar emellertid sådana konsekvenser. Effekter av nämnda slag kan också antas förekomma framför allt i nära samband med att våra förslag eventuellt har trätt i kraft. Det är oavsett detta motiverat att myndigheter på ett tydligt sätt, och om möjligt på förhand, informerar enskilda om att biometrisk verifiering av identitet kan komma att användas. Negativa konsekvenser som beror på att den enskilde helt enkelt är omedveten om eller oförberedd på att en kontroll skulle komma att genomföras kan då effektivt motverkas.

Sammantaget anser vi att sådana negativa konsekvenser för enskilda som kan hänföras till bristande kunskap om den nya lagens tillämpning kan förväntas bli begränsade. De kan också antas vara övergående. Detsamma gäller som vi ser det eventuella svårigheter för enskilda att installera och använda en sådan myndighetsgemensam mobilapplikation som vi beskrivit i avsnitt 27.4. Som vi återkommer till i avsnitt 30.5.2 framstår en sådan applikation dock som ändamålsenlig från ett användarperspektiv, med hänsyn till att den enskilde, vars identitet ska verifieras, möter en och samma användargränssnitt och verifieringsprocess, oberoende av vilken myndighet det är som vill verifiera identitet biometriskt. Om varje myndighet utvecklar en egen teknisk lösning riskerar den enskilde att möta olika applikationer, flöden och instruktioner beroende på vilken myndighet som bestämt att verifieringen ska genomföras. Information till allmänheten om biometrisk verifiering av identitet är av vikt för att förbereda enskilda på att deras identitet kan komma att verifieras på detta sätt av myndigheter och för att skapa förståelse för vad sådan verifiering innebär.

Vi återkommer nedan till vilka konsekvenser för skyddet för den personliga integriteten som våra förslag kan förväntas medföra. Här kan vi emellertid konstatera att en ökad användning av biometriska

uppgifter för att verifiera identitet kan komma att innebära att enskilda upplever ett ökat integritetsintrång. Det kan då framhållas att våra förslag även syftar till att skydda enskilda mot att deras identitet utnyttjas utan deras vetskap. Vi bedömer vidare att konsekvenser som utgörs av att enskilda upplever ett obehag av att lämna biometriska underlag inte bör överdrivas, med hänsyn till att detta sker i allt större utsträckning redan i dag, även till privata aktörer. Ett sådant exempel är sådan ansiktsigenkänning och jämförelse med en identitetshandling som under vissa förutsättningar används vid förnyelse av mobilt BankID och av AirBnb – en global online-marknadsplats och applikation för korttidsuthyrning av privatbostäder – bland annat när ett konto skapas hos företaget. Med hänsyn till de skyddsåtgärder i fråga om biometriska underlag och biometriska uppgifter som vi föreslår i den nya lagen bör eventuella tveksamheter hos enskilda om hur deras uppgifter behandlas också motverkas.

30.3.1 Skyddet för den personliga integriteten

Våra förslag får konsekvenser för den personliga integriteten, genom att enskilda personer kan vara skyldiga att på begäran låta myndigheter ta fingeravtryck och ansiktsbilder för att kunna genomföra en biometrisk verifiering mot en handling. Beroende på hur det rättsliga stöd som vi föreslår implementeras tekniskt kan känsliga personuppgifter – i form av biometriska uppgifter – komma att behöva behandlas av en bred krets av myndigheter; om en sådan myndighetsgemensam teknisk lösning som vi beskrivit i avsnitt 27.4 används kommer behandlingen av känsliga personuppgifter dock att kunna koncentreras till någon eller några få myndigheter. Utöver nämnda typer av uppgifter medför våra förslag att relativt få personuppgifter behöver behandlas, och i första hand sådana som den enskilde redan har lämnat till myndigheten.

I avsnitt 21.7.3 har vi bedömt att biometrisk verifiering av identitet mot handlingar – i de situationer som vi föreslår att sådan verifiering ska få användas – medför ett visst intrång i den personliga integriteten, men att intrånget motiveras av ett starkt samhällsintresse. Vi hänvisar till de närmare överväganden som gjorts i det avsnittet, och de upprepas därför inte i detta sammanhang. Utifrån de omständigheter som vi lyft fram i nämnda avsnitt är det vår bedömning att våra

förslag utgör en motiverad och proportionerlig inskränkning av skyddet för den personliga integriteten och privatlivet som följer av bestämmelser i regeringsformen, Europakonventionen och EU:s rättighetsstadga. Den behandling av biometriska uppgifter som behöver utföras är också proportionerlig, på det sätt som avses i artikel 9.2 g i dataskyddsförordningen.

Skyddet för personuppgifter – däribland känsliga sådana – tillgodoses bland annat genom att biometriska underlag och de biometriska uppgifter som tas fram ur dessa omedelbart ska förstöras när en kontroll har genomförts. Inga sådana uppgifter ska alltså få lagras med anledning av verifieringen. I kapitel 24 har vi vidare föreslagit att den nya lagen ska innehålla särskilda bestämmelser som reglerar den personuppgiftsbehandling som behöver utföras och föreslagit ett personuppgiftsansvar som syftar till att uppnå en tydlighet i tillämpningen. Utöver den dataskyddsrättsliga regleringen föreslår vi att absolut sekretess ska gälla för fingeravtryck och ansiktsbilder som tagits upp med stöd av den nya lagen och för biometriska uppgifter som tagits fram ur dessa. Dessa åtgärder är av vikt för att säkerställa att det finns ett rättsligt skydd mot att sådana uppgifter obehörigen sprids eller används för andra syften än de som följer av våra förslag. Tillsammans med det dataskyddsrättsliga regelverket i övrigt uppnås enligt vår bedömning ett tillfredsställande skydd för den personliga integriteten.

30.3.2 Särskilt om konsekvenser för barn

Våra förslag om en generell möjlighet för myndigheter att biometriskt verifiera identitet mot vissa handlingar omfattar även barn som har fyllt sex år. Förslagen innebär att även barns personuppgifter kommer att behandlas. I enlighet med artikel 3.1 i FN:s konvention om barnets rättigheter, barnkonventionen, ska barnets bästa i första hand bedömas och beaktas vid alla åtgärder som rör barn direkt eller indirekt. Barnets bästa är emellertid inte alltid utslagsgivande utan måste vägas mot andra intressen och rättigheter. Barnets bästa kan inte heller definieras en gång för alla utan måste kopplas till det individuella barnet och barnets situation.[6]

Våra förslag innebär inte en skyldighet för myndigheter att biometriskt verifiera identitet i olika situationer, på samma sätt som ex-

[6] *Inkorporering av FN:s konvention om barnets rättigheter*, prop. 2017/18:186, s. 96.

empelvis följer av bestämmelser i utlänningslagen (2005:716). Förslagen utgår vidare från att den nya lagen endast får användas när det är nödvändigt, vilket ger myndigheter ett bedömningsutrymme i det enskilda fallet. Barnets bästa bör beaktas vid bedömningen av i vilka situationer det är lämpligt att fingeravtryck eller ansiktsbild tas med stöd av våra förslag. Vi bedömer att det i många fall när det skulle kunna vara nödvändigt att biometriskt verifiera identiteten för en vuxen person kan saknas ett motsvarande behov för ett barn. Detta följer av att i vart fall yngre barn som utgångspunkt saknar egen rättshandlingsförmåga (se avsnitt 12.4.1); det kan med fog förutsättas att en biometrisk verifiering av identitet framför allt är nödvändig i förhållande till personer som har rätt att på egen hand uppträda som part i ett ärende eller i någon annan kontakt med myndigheter. Tillräckliga uppgifter om identiteten för ett barn som saknar egen rättshandlingsförmåga kan också ofta lämnas av den som har rätt att företräda barnet, exempelvis en vårdnadshavare. Det förekommer visserligen situationer då barn som uppnått viss ålder och mognad har rätt att agera på egen hand, exempelvis i vårdsammanhang. Även med hänsyn till detta bedömer vi att konsekvenserna av våra förslag för barn som ett kollektiv kan antas bli förhållandevis begränsade.

Vid ett genomförande av våra förslag är det emellertid – med hänsyn till att den nya lagen ska kunna användas av många myndigheter, i varierande situationer – sannolikt att barn i större utsträckning än i dag kan vara skyldiga att låta myndigheter ta biometriska underlag.

En möjlighet för myndigheter att ta fingeravtryck och ansiktsbilder kan innebära negativa konsekvenser för barn. Att ta fingeravtryck utgör ett påtvingat kroppsligt ingrepp och ett intrång i den personliga integriteten. Det kan, som lyfts fram i andra sammanhang, också verka skrämmande för barn att få sina fingeravtryck tagna.[7] Vi anser emellertid – i likhet med den bedömning som gjordes i betänkandet *Folkbokföringsverksamhet, biometri och brottsbekämpning* – att det är svårt att se att integritetsintrånget skulle vara större för ett barn än för en vuxen person.[8] Precis som vid andra tillfällen när fingeravtryck och/eller ansiktsbilder tas från barn är det också viktigt att det görs på ett barnvänligt och barnanpassat sätt, med beaktande av principen om barnets bästa. Med hänsyn till att våra förslag endast avser myn-

[7] *Registrering av EES-medborgare*, SOU 2026:9, s. 197.
[8] SOU 2025:75, s. 431 f.

digheter kan vi inte utgå från annat än att detta beaktas, när de möjligheter som våra förslag ger utnyttjas.

Våra förslag syftar inte bara till att möjliggöra bättre kontroller för myndigheter utan även till att motverka att enskilda får sina identiteter utnyttjade utan deras vetskap. Som vi noterat i avsnitt 12.4.1 kan barn vara särskilt utsatta i sådana sammanhang. Upptagningen av biometriska underlag med stöd av våra förslag innebär ett kortvarigt ingrepp och kan som vi ser det vara ett sätt att tillförlitligt kunna verifiera identitet för ett barn som befinner sig i en utsatt situation, exempelvis i samband med ett omhändertagande av sociala myndigheter, eller i en vårdsituation. När det gäller känsliga personuppgifter ska sådana – enligt våra förslag – inte få sparas eller användas för andra ändamål än att kunna genomföra en biometrisk verifiering av identitet med stöd av den nya lagen.

Sammantaget bedömer vi att förslagen är förenliga med barnkonventionen och principen om barnets bästa.

30.4 Konsekvenser för arbetet med att förebygga och i övrigt motverka brottslighet

Enligt våra förslag i avsnitt 23.4 ska *brottsbekämpande* verksamhet som bedrivs av vissa myndigheter uttryckligen undantas från möjligheten att biometriskt verifiera identitet med stöd av den nya lagen. Som vi noterat i nyss nämnda avsnitt ingår det som ett övergripande uppdrag för många myndigheter att på olika sätt arbeta för att förebygga och motverka brottslighet. Sådant *brottsförebyggande* arbete kan bland annat innefatta att myndigheter arbetar med utökade kontroller för att upptäcka felaktigheter i ärendeslag som myndigheten handlägger. Som exempel kan nämnas Försäkringskassan, vars insatser som vidtas inom ramen för myndighetens brottsförebyggande arbete syftar till att minska viljan att begå bidragsbrott, genom att informera om de kontroller som genomförs och till att upptäcka de individer som faktiskt begår bidragsbrott, genom utökad kontrollverksamhet. Enligt myndigheten utgör en hög och tidig upptäcktsrisk en central komponent i det förebyggande arbetet, då den minskar incitamenten för felaktigheter.[9] En möjlighet att tillförlitligt kontrollera att den som

[9] Försäkringskassan, *Rapport – Uppdrag att bidra till att utveckla det brottsförebyggande arbetet*, dnr FK 2024/028157, den 25 augusti 2025, s. 7.

förekommer i ett ärende är den som han eller hon påstår sig vara utgör en viktig komponent i att tidigt upptäcka olika felaktigheter, även innan de hunnit uppstå i ett ärende. Av naturliga skäl kommer sådana effekter för det brottsförebyggande arbetet att variera utifrån olika myndigheters verksamhet och uppgifter. I likhet med vad vi anfört ovan i fråga om konsekvenser för enskilda är det också svårt att dra några säkra slutsatser i stort om konsekvenserna för arbetet med att förebygga och i övrigt motverka brottslighet. Detta med hänsyn till att våra förslag inte utgör en skyldighet för myndigheter att använda biometrisk verifiering av identitet utan en möjlighet, när förutsättningarna för det är uppfyllda.

En kraftigt utökad möjlighet för myndigheter att på ett säkert sätt kontrollera identitet hos personer de möter kan också ha en allmänt medvetandehöjande effekt hos myndigheterna, genom att säker kontroll av identitet får en mer framträdande roll i myndigheternas arbete jämfört med i dag. Myndigheterna kan också få större erfarenhet av att kontrollera identitetshandlingar av olika slag. Sådana omständigheter kan, om än på ett mer indirekt plan, förväntas bidra till en stärkt och mer tillförlitlig ärendehandläggning, inte bara i samband med att beslut fattas. Vi anser vidare att detta sammantaget kan bidra till en mer sammanhållen identitetsförvaltning i stort, eftersom våra förslag kan användas brett i förvaltningen, utifrån olika myndigheters behov.

Även om det alltså kan vara svårt att på förhand veta i vilken utsträckning våra förslag kommer att användas i praktiken bedömer vi att redan *möjligheten* för myndigheter att i stor omfattning använda biometrisk verifiering av identitet kan vara handlingsdirigerande och ha ett avskräckande och avhållande syfte. Redan den omständigheten att den enskilde kan behöva lämna en förklaring till myndigheten i ett ärende avseende varför han eller hon inte avser, eller har underlåtit, att följa en begäran om att biometriskt verifiera sin identitet, kan enligt vår bedömning antas få en tröskelhöjande effekt, som motverkar utnyttjande av identitet, genom id-kapning eller genom användning av e-legitimationer som tillhör så kallade ”målvakter”. Risken att vara tvungen att verifiera sin identitet med hjälp av biometriska uppgifter bedömer vi gör det mindre attraktivt att använda den form av upplägg som bygger på att personer tillfälligt hämtas till Sverige för att etablera en identitet som sedan – efter att personen återvänt till hemlandet – används av andra i olika ärenden; även med

en möjlighet att biometriskt verifiera identitet på distans behöver kontakt upprätthållas med den person vars identitet ska utnyttjas också efter den initiala fasen. Sådana brottsförebyggande effekter kan som vi ser det uppnås även utan att myndigheten i det enskilda fallet i ett andra steg förelägger den enskilde att medverka och kopplar en konkret konsekvens till utebliven medverkan. Utnyttjande av identiteter främjas av att kontakterna mellan personer och myndigheter i allt större utsträckning sker på digital väg. Det möjliggör att den som utnyttjar någons identitet kan vara ”anonym” på ett annat sätt än om han eller hon är tvungen att inställa sig personligen hos en myndighet. Även om biometrisk verifiering med stöd av våra förslag ska kunna genomföras på distans medför den koppling till en viss individ som uppnås genom användningen av biometriska uppgifter, att det blir svårare för personen att gömma sig bakom en form av digital anonymitet.

Våra förslag skulle kunna få betydelse bland annat i Försäkringskassans verksamhet. I betänkandet *Ett stärkt och samlat skydd av välfärdssystemen* lyftes bland annat fram att en viktig aspekt av en minskad brottslighet som riktas mot välfärdssystemen är att det kan ha betydelse för annan, ännu grövre brottslighet. Brott mot välfärdssystemen används ibland för att finansiera annan brottslig verksamhet.[10] Vi har inte någon annan uppfattning. En ökad möjlighet att med hjälp av biometriska uppgifter upptäcka identitetsmissbruk i ärendeslag som avser välfärdsförmåner av olika slag kan därmed också indirekt få betydelse för att förebygga och motverka även annan brottslighet än sådan som riktar sig direkt mot det allmänna.

I detta sammanhang kan vi även notera Riksrevisionens rapport från år 2026, *Infiltration i staten – tre myndigheters arbete för att motverka illojalt beteende*. I rapporten anförs att flera fall av infiltration har uppmärksammats i offentlig verksamhet under senare år. Mörkertalet kan vara betydande och konsekvenserna bli allvarliga: röjda uppgifter som gynnar grov kriminalitet, förvanskad eller förstörd information, ekonomiska oegentligheter och störningar i samhällsviktig verksamhet med höga kostnader som följd.[11] Försäkringskassan har, som ett led i sitt brottsförebyggande arbete, förbättrat rekryteringsprocessen för att motverka sådan infiltration. I en rekryteringsprocess ingår normalt en identitetskontroll. Våra förslag möjliggör att

[10] SOU 2023:52, s. 776.
[11] RiR 2026:3, s. 4.

biometrisk verifiering av identitet används i en sådan situation, under förutsättning att det är nödvändigt och görs i samband med att identitetskontroller genomförs. Vi bedömer att våra förslag kan ha en viss brottsförebyggande effekt i sådana situationer, genom att look-a-likes inte kan användas i syfte att infiltrera myndigheter.

Även med beaktande av de osäkerhetsfaktorer som vi pekat på ovan bedömer vi att våra förslag kan få positiva konsekvenser för myndigheters arbete med att förebygga och i övrigt motverka brottslighet, såväl direkt som indirekt.

Effekterna av våra förslag är i första hand hänförliga till utnyttjande av identiteter i olika sammanhang och bedöms ha liten betydelse i fråga om att förebygga brottslighet som kan hänföras till användning av multipla identiteter. Förslagen är dessutom begränsade genom att de inte gör det möjligt för privata aktörer att använda biometrisk verifiering mot handlingar (se avsnitt 21.3.2). Förslagen kan därför inte förväntas få någon effekt på identitetsmissbruk som riktar sig mot privata aktörer, exempelvis i samband med köp eller leverans av varor.

30.5 Konsekvenser för det allmänna

Vi anser att det bör understrykas att en *rättslig* möjlighet för myndigheter att verifiera identitet biometriskt mot handlingar genom det regelverk vi föreslår, inte i sig medför några direkta kostnader för det allmänna. Ett ikraftträdande av regelverket förutsätter inte heller att samtliga myndigheter som potentiellt sett kan komma att verifiera identitet med stöd av den nya lagen har faktiska möjligheter att göra det. Redan det faktum att den nya lagen ger myndigheter rättslig befogenhet att, under vissa förutsättningar verifiera identitet biometriskt, bör enligt vår mening kunna ha en avskräckande effekt för de personer som har för avsikt att vilseleda en myndighet om sin identitet (jfr avsnitt 30.4).

Det är, enligt vår bedömning, primärt utveckling och drift av tekniska system som möjliggör biometrisk verifiering som i praktiken kommer att driva kostnader. Myndigheter som redan i dag använder biometriska uppgifter i sin verksamhet – till exempel Skatteverket och Migrationsverket – och som därmed har tillgång till den teknik som krävs för detta bör därmed kunna tillämpa den nya lagen i viss

utsträckning utan att det medför andra kostnader än vissa handläggningskostnader. Förutsättningarna för en gemensam användning av teknik eller arbetssätt på Statens servicecenter, som har serviceavtal med Skatteverket och Migrationsverket, är enligt uppgift från förstnämnda myndighet dock begränsade utifrån avtalen, tekniken och särskilda behandlingsregler i varandras miljöer.

Vi har efterfrågat underlag från de experter i utredningen som företräder Skatteverket, Polismyndigheten, Försäkringskassan, Digg och Migrationsverket för att på ett adekvat sätt kunna analysera konsekvenserna av våra förslag och för att uppskatta kostnader som kan uppkomma med anledning av förslagen. Samtliga experter har påpekat att det varit mycket svårt att ta fram några kvalitetssäkrade kostnadsuppskattningar, som kan användas som underlag i utredningens konsekvensanalys. Detta med hänsyn bland annat till att det handlar om ett helt nytt förfarande, där det fortfarande finns oklarheter till exempel gällande den tekniska implementeringen och när i en myndighets process en verifiering kan aktualiseras. Vi vill därför poängtera att i de avseenden vi redogör för en beloppsmässig kostnad är det fråga om en grov uppskattning – utifrån nu kända omständigheter och tillgängliga uppgifter – som sannolikt kommer behöva justeras under den fortsatta beredningen av frågan.

30.5.1 Verifierande myndigheter

Med verifierande myndigheter avses här de myndigheter som vill genomföra en biometrisk verifiering av identitet med stöd av den nya lagen. De verifierande myndigheterna kan – i vart fall i teorin – komma att bli flera hundra till antalet och det handlar om såväl statliga som kommunala och regionala myndigheter av olika storlek och med varierande verksamheter. Det är därför givet att konsekvenserna inte blir samma för samtliga myndigheter. Utöver myndighetens storlek och verksamhet finns det flera andra omständigheter som har betydelse för vilka konsekvenserna blir för verifierande myndigheter vid ett genomförande av våra förslag. En av dessa omständigheter är hur förslagen implementeras i tekniskt hänseende, till exempel genom att varje myndighet själv ansvarar för sina system för biometrisk verifiering eller genom att en myndighetsgemensam lösning tas i bruk och görs tillgänglig. Av central betydelse för vilken

påverkan våra förslag får på de verifierande myndigheterna är också om biometrisk verifiering möjliggörs på distans eller om sådan verifiering förutsätter personlig inställelse. I detta avsnitt lyfter vi fram potentiella konsekvenser för de verifierande myndigheterna, i form av bland annat behov av att anpassa handläggningsrutiner och utbilda personal.

Tekniska system för biometrisk verifiering

En grundläggande fråga gällande tekniska system är om de myndigheter som vill använda möjligheten att verifiera identitet biometriskt med stöd av den nya lagen själva kan, och ska, utveckla de tekniska lösningar som behövs eller om en myndighetsgemensam lösning av det slag vi beskrivit i avsnitt 27.4 bör användas. En fördel med en myndighetsgemensam lösning är att kostnader för utveckling av snarlika lösningar inte uppstår hos flera myndigheter. Andra fördelar är att det skapar mer enhetliga säkerhets- och kvalitetsnormer, ger bättre förutsättningar för samordnad förvaltning och bidrar till en mer likvärdig hantering för enskilda. Vi återkommer i nästa avsnitt till konsekvenserna av att en myndighetsgemensam lösning utvecklas och förvaltas av en tekniskt ansvarig myndighet.

Om de verifierande myndigheterna själva ska ansvara för tillgång till de tekniska system som behövs för biometrisk verifiering av identitet mot handlingar kan det antas medföra att mindre myndigheter och myndigheter med ett begränsat behov av biometrisk verifiering väljer att inte nyttja den rättsliga möjlighet som den nya lagen kommer att ge. Genomslaget av våra förslag kan alltså antas bli betydligt mindre utan en myndighetsgemensam lösning. Myndigheter som redan i dag tar upp biometriska underlag och använder biometriska uppgifter i sin verksamhet – såsom Skatteverket, Polismyndigheten och Migrationsverket – får anses ha ett försteg genom att de i viss mån kan bygga vidare på befintliga lösningar och dra nytta av den kompetens och de erfarenheter myndigheten har. Vid användning av en teknisk lösning som inte tillåter biometrisk verifiering på distans blir förekomsten av eller möjligheten att ingå serviceavtal med Statens servicecenter också relevant. Här kan vi notera att enligt 3 § lagen (2019:212) om viss gemensam offentlig service får, som utgångspunkt, förvaltningsuppgifter som innefattar myndighetsutövning och

som en kommun eller en region ansvarar för inte omfattas av ett serviceavtal.

Det är, som vi ser det, inte möjligt att göra en beloppsmässig uppskattning av vad det skulle kosta för en verifierande myndighet att på egen hand få tillgång till sådana tekniska system som behövs. Potentiella myndigheters förutsättningar ser väldigt olika ut, beroende på bland annat storlek och egen teknisk kompetens; många myndigheter saknar egna it-resurser helt, medan vi kan notera att Försäkringskassans it-avdelning består av cirka 1 000 medarbetare.[12] Om en myndighetsgemensam lösning inte tas fram och görs tillgänglig kan man tänka sig att det i stället skulle behöva ske en myndighetsgemensam upphandling, i syfte att uppnå någon form av ramavtalshantering. Oavsett den verifierande myndighetens förutsättningar bedömer vi dock att det kommer att innebära en kostnad för myndigheten för att ta fram eller på annat sätt få tillgång till tekniska system som möjliggör biometrisk verifiering.

Dataanalyser, urval och ändrade arbetssätt

Biometrisk verifiering av identitet ska enligt våra förslag få genomföras när en sådan verifiering är nödvändig antingen vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde, eller, i annat fall, när myndigheten inom ramen för sin verksamhet genomför identitetskontroller. Rekvisitet *nödvändig* kräver som utgångspunkt att den verifierande myndigheten utvärderar behovet av biometrisk verifiering i verksamheten på ett generellt plan, för att kunna kartlägga i vilka ärendeslag och situationer sådan verifiering kan aktualiseras hos myndigheten. Omfattningen av ett sådant arbete beror framför allt på bredden på myndighetens verksamhet och variationen på och typen av ärenden myndigheten handlägger. För en större myndighet som till exempel Försäkringskassan, som handlägger ett stort antal olika socialförsäkringsförmåner, kan det antas vara en relativt omfattande process att ta ställning till hur urvalsprofileringen ska göras. Vidare kan det – framför allt för en myndighet med omfattande verksamhet – antas behövas interna riktlinjer, rutiner, vägledningar och instruktioner som tar sikte på hur möjligheten att

[12] https://www.sgit.se/uppdraget, senast besökt den 8 juli 2026.

verifiera identitet biometriskt med stöd av den nya lagen ska tillämpas i praktiken.

Berörda myndigheters arbetssätt kommer också att påverkas om biometrisk verifiering av identitet implementeras i verksamheten. Påverkan på handläggningen och ärendeprocesserna blir dock i hög grad beroende av hur den nya lagen tillämpas och hur den tekniska lösningen utformas. Om biometrisk verifiering begärs automatiskt – till exempel i samband med att en elektronisk ansökan görs efter inloggning med en e-legitimation – och genomförs direkt – till exempel genom användning av en myndighetsgemensam mobilapplikation – blir det sannolikt ingen eller endast mindre påverkan på handläggningen. Om en handläggare däremot behöver ta ställning till om en biometrisk verifiering ska genomföras, initiera kontrollen manuellt eller följa upp att den genomförs kommer handläggningstiden sannolikt att öka. Det bör dock påpekas att en möjlighet att verifiera identitet biometriskt i ett ärende där myndigheten bedömt att det finns en risk för identitetsmissbruk kan betraktas som en effektiviserande åtgärd; med den enskildes medverkan går det sannolikt snabbare att genomföra verifieringen än att utreda personens identitet på ett mer traditionellt sätt.

En möjlighet att biometriskt verifiera identitet medför, som vi ser det, att myndigheter som redan i dag arbetar riskbaserat vad gäller identitetsmissbruk får en mer effektiv metod för att komma till rätta med sådant missbruk, och i och med det en kvalitetshöjning i detta arbete och i ärendehandläggningen. Även myndigheter som i dag saknar verktyg eller rutiner för att motverka identitetsmissbruk får en möjlighet att göra detta på ett effektivt sätt vid genomförande av våra förslag. Det kan antas att vissa myndigheter även kommer att få i uppgift av regeringen att arbeta mer aktivt med frågor om identitetsmissbruk och på så sätt få kännedom om vilka åtgärder som kan och bör vidtas i verksamheten för att motverka sådant missbruk, och öka sin kompetens på det aktuella området; vi kan konstatera att frågor om att motverka identitetsmissbruk och stärka myndigheters identitetskontroller har fått mer fokus de senaste åren och det kan antas att förväntan om att myndigheter ska arbeta aktivt med detta inte kommer att avta.

Innan en myndighet har klarlagt i vilka fall biometrisk verifiering av identitet med stöd av den nya lagen ska användas, vem som ska avgöra detta och hur urvalsprofileringen ska utformas är det svårt

att uppskatta påverkan på den berörda myndighetens verksamhet och kostnaderna för anpassning av ärendehanteringen till att inkludera biometrisk verifiering. Om urvalsprofilering kan göras gemensamt för alla eller många ärenden hos en myndighet och it-lösningen automatiskt levererar svar till ärendet avseende en biometrisk verifiering i samband med att en digital framställan, till exempel en ansökan om en socialförsäkringsförmån, har gjorts kan effekterna för handläggningsprocessen antas bli mindre. Om det däremot krävs ett aktivt ställningstagande från en medarbetare under handläggningen av ett ärende behövs det rutiner för när biometrisk verifiering får eller ska begäras, hur ställningstagandet ska dokumenteras, hur resultatet ska hanteras och hur ärenden där en biometrisk verifiering trots begäran inte genomförs, eller där en verifiering har genomförts men jämförelsen misslyckats, ska följas upp.

Ny sekretessbestämmelse

Vi föreslår en ny bestämmelse i offentlighets- och sekretesslagen (2009:400) som innebär att sekretess ska gälla för uppgift i form av fingeravtryck eller ansiktsbild som tagits upp med stöd av den nya lagen, och biometriska uppgifter som har tagits fram ur fingeravtrycket eller ansiktsbilden. I praktiken reglerar bestämmelsen som utgångspunkt tystnadsplikt, eftersom biometriska underlag och biometriska uppgifter ska förstöras omedelbart efter att kontrollen har genomförts (se avsnitt 24.9). Vi bedömer att denna typ av uppgifter om den enskilde sannolikt inte kommer att begäras ut av allmänheten mer än i mycket begränsad omfattning samt att en prövning av om uppgifterna ska lämnas ut i sådant fall kommer att vara förhållandevis enkel, med hänsyn till att den föreslagna bestämmelsen inte förutsätter en skadebedömning. Som vi pekat på i avsnitt 25.2.2 talar mycket också för att sådana uppgifter inte utgör allmänna handlingar hos den verifierande myndigheten; en begäran kan då avslås redan på den grunden.

Alfanumeriska uppgifter om enskilda som behövs för att en biometrisk verifiering med stöd av den nya lagen ska kunna genomföras skyddas, enligt vår bedömning, av bestämmelser om sekretess som är tillämpliga i den aktuella verksamheten hos den verifierande myndigheten. För denna typ av uppgifter kommer alltså samma sekretess-

bestämmelser att bli tillämpliga som i dagsläget, vid handläggningen av det aktuella ärendet eller i den aktuella verksamheten. Vi bedömer att våra förslag om biometrisk verifiering av identitet inte kommer att få någon märkbar påverkan på de verifierande myndigheternas verksamhet i form av utlämnande av allmänna handlingar i detta avseende.

Utbildningsinsatser

För de myndigheter som väljer att använda möjligheten att verifiera identitet biometriskt med stöd av den nya lagen kommer det sannolikt att krävas vissa utbildningsinsatser för berörda medarbetare – till exempel ärendehandläggare och personal vid kundcenter – både initialt för befintlig personal och löpande för nyanställda. Relevanta utbildningsinsatser kan, enligt vår bedömning, antas ta en del resurser i anspråk framför allt i samband med ikraftträdande av den nya lagen alternativt när möjligheten att verifiera identitet börjar nyttjas av myndigheten i fråga, om detta sker vid ett senare tillfälle. Sett i ett längre perspektiv bör utbildningsinsatser i frågor om biometrisk verifiering av identitet i större utsträckning kunna integreras i andra utbildningar, till exempel för nyanställda eller avseende handläggningen av en viss förmån där biometrisk verifiering regelmässigt används med hänsyn till risken för identitetsmissbruk. De kan därför inte antas medföra annat än mindre kostnader för de verifierande myndigheterna.

Informationsinsatser

En generell möjligt för myndigheter att biometrisk verifiera identitet mot handlingar med stöd av den lag vi föreslår är något helt nytt som förutsätter externa informationsinsatser i förhållande till enskilda. Som vi återkommer till i nästa avsnitt kan det finnas skäl för myndighetsgemensamma informationsinsatser, som på ett generellt plan upplyser allmänheten om de möjligheter myndigheter har respektive de skyldigheter enskilda har med anledning av det nya regelverket. Myndigheter som väljer att nyttja möjligheteten att använda biometrisk verifiering i sin verksamhet kommer dock även att behöva tillhandahålla myndighets- eller verksamhetsspecifik information, till

exempel på sin webbplats, om hur den nya lagen tillämpas i verksamheten eller i vissa ärendeslag. Detta kan antas medföra vissa kostnader för de verifierande myndigheterna.

30.5.2 Tekniskt ansvarig myndighet

Införande av en rättslig möjlighet för myndigheter att verifiera identitet biometriskt mot handlingar förutsätter, som vi redogjort för i avsnitt 30.5.1, inte i sig att det finns tekniska lösningar för berörda myndigheter att också nyttja denna möjlighet. Ett brett genomslag av regelverket förutsätter däremot att de myndigheter som potentiellt sett har ett behov av att verifiera identitet i sin verksamhet har tillgång till tekniska system som möjliggör biometrisk verifiering mot handlingar. Enligt vår bedömning har en myndighetsgemensam teknisk lösning flera positiva effekter, framför allt om en sådan lösning möjliggör verifiering på distans.

Till att börja med framstår det som mer ändamålsenligt från ett användarperspektiv att den enskilde, vars identitet ska verifieras, möter en och samma tekniska användargränssnitt oberoende av vilken myndighet det är som vill verifiera identitet. Om varje myndighet utvecklar en egen teknisk lösning riskerar den enskilde att möta olika applikationer, flöden och instruktioner beroende på vilken myndighet som bestämt att verifieringen ska genomföras. En annan effekt av en myndighetsgemensam lösning är att även myndigheter med ett relativt begränsat behov av biometrisk verifiering mot handlingar får möjlighet att verifiera identitet på detta sätt, utan att behöva ta den sannolikt oproportionerliga kostnaden för att ta fram ett eget system. Den nya lagens genomslag kan därmed antas bli betydligt större med en myndighetsgemensam lösning.

Det finns också andra fördelar med en myndighetsgemensam lösning i form av bland annat minskad risk för dubbelutveckling och förutsättningar för mer enhetliga säkerhets- och kvalitetskrav. En ökad standardisering på området bidrar vidare till ökad enhetlighet och jämförbarhet av vad en biometrisk verifiering faktiskt ger för resultat och vad det innebär. En myndighetsgemensam lösning ger även bättre förutsättningar för att följa och styra utvecklingen på området och se till att det inte finns stora skillnader i olika myndig-

heters förmåga att verifiera identitet biometriskt med stöd av den nya lagen.

Sammanfattningsvis ser vi ett antal positiva konsekvenser av att en myndighet får i ansvar att utveckla och förvalta en myndighetsgemensam lösning, däribland förutsättningar för en mer kostnadseffektiv hantering och en mer enhetlig funktionalitet. För det fall regeringen ger en viss myndighet i uppgift att ta fram och förvalta en sådan teknisk lösning för verifiering av identitet med stöd av den nya lagen kommer denna myndighet att ha kostnader för detta (se avsnitt 30.5.4).

En myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet mot handlingar som kan nyttjas av de myndigheter som väljer att ansluta till systemet behöver bestå av flera olika delar för att vara funktionell. I avsnitt 27.4 har vi redogjort för en verifieringsprocess som bygger på myndighetsgemensamma komponenter och konstaterat att nödvändiga, grundläggande systemkomponenter är mobilapplikation, backend-system och gränssnitt mot verifierande myndigheters system.

Vi bedömer att en snabb, teknisk implementering i princip förutsätter att ansvarig myndighet upphandlar en helhetslösning i form av en tjänst för biometrisk verifiering av identitet mot handlingar som görs tillgänglig för andra myndigheter. En sådan upphandling skulle kunna göras med en kortare avtalstid på ett till två år, för att ansvarig myndighet under denna tid skulle kunna bygga upp en egen teknisk lösning, där enbart komponenter och inte en helhetslösning upphandlas. Såvitt vi har förstått innebär de prismodeller som finns för en helhetslösning generellt sett höga kostnader per slagning/verifiering; vid upphandling av en komplett tjänst för verifiering har det vid en grov uppskattning av en expert på Skatteverket antagits att kostnaden per verifiering kommer att uppgå till en krona. Med utgångspunkten att enskilda använder en e-legitimation för någon form av autentisering hos myndigheter närmare en halv miljard gånger per år[13] och utifrån antagandet att biometrisk verifiering mot handlingar med stöd av det regelverk vi föreslår skulle ske i en tiondel av dessa situationer handlar det om upp till 50 miljoner slagningar per år. Antagandet är givetvis mycket osäkert och situationerna inte helt jämförbara. Om biometrisk verifiering av identitet sker i en tjugondel av dessa situationer handlar det om 25 miljoner slagningar per år.

[13] Uppgift från Skatteverket den 23 april 2026.

Det är dock mycket svårt att på förhand uppskatta omfattningen av biometrisk verifiering med stöd av den nya lagen.

Förvaltning och drift

När en myndighetsgemensam teknisk lösning finns på plats och tagits i bruk behöver den förvaltas och fortsatt utvecklas för att säkerställa tillförlitlig drift och god funktionalitet. Förvaltning och drift kommer, enligt vår bedömning, att föra med sig kostnader, som sannolikt är större de första åren den tekniska lösningen används, för att därefter blir något lägre per år.

Support och kundportal

Det får antas finnas ett behov av en supportfunktion som kan ge stöd såväl till verifierande myndigheter som till enskilda som ska verifiera sin identitet biometriskt. För de verifierande myndigheternas del framstår det som givet att det behöver finnas kommunikationskanaler till den tekniskt ansvariga myndigheten samt personal hos denna som kan ge stöd i användningen av systemet och hantera eventuella tekniska problem. I detta avseende skulle man kunna tänka sig behov av någon form av kundportal med självbetjäning, support och stöd för anslutning, konfiguration och förvaltning hos anslutande, verifierande myndigheter. Vad gäller support till de enskilda användarna kan det diskuteras om de i första hand bör vända sig till den verifierande myndigheten eller till den tekniskt ansvariga myndigheten, till exempel vid problem med att ladda ner och använda en mobilapplikation för verifiering. I detta avseende går det sannolikt att påverka enskildas agerande, med tydlig information om vilken aktör som ska kontaktas i olika situationer. Det kan tänkas att den enskilde har frågor både om varför den biometriska verifieringen ska genomföras i det enskilda ärendet och om mobilapplikationens funktionalitet. Möjligen kan det upplevas som besvärligt att behöva ta kontakt med flera olika myndigheter i ett och samma ärende, vilket talar för att den verifierande myndigheten bör ansvara även för support i tekniskt hänseende i förhållande till enskilde. Det bör, som vi ser det, dock finnas en gemensam supportfunktion hos den tekniskt ansvarige aktören som ger stöd åt

verifierande myndigheter. Det kommer att medföra kostnader dels att bygga upp en sådan funktion, dels att tillhandahålla support över tid.

Informationsinsatser

För det fall en viss myndighet får ansvar för att ta fram en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet framstår det som rimligt att det också ingår att ta fram informationsmaterial som kan användas för att informera allmänheten om den nya lagen om biometrisk verifiering av identitet, men kanske framför allt om hur en sådan verifiering kan komma att genomföras i praktiken, till exempel genom användning av en mobilapplikation som den enskilde behöver ladda ner på en mobiltelefon eller en annan enhet. Vi bedömer att det kommer att uppstå en initial, större kostnad för att ta fram lämpligt informationsmaterial att sprida till allmänheten och en betydligt mindre kostnad för att löpande hålla materialet uppdaterat.

30.5.3 De allmänna förvaltningsdomstolarna

Våra förslag tar sikte på möjligheter för såväl statliga som kommunala och regionala myndigheter att, under vissa förutsättningar, verifiera identitet biometriskt vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde eller, i annat fall, när myndigheten, inom ramen för sin verksamhet genomför identitetskontroller. Vidare föreslår vi att en begäran om att verifiera identitet biometriskt vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde ska få överklagas endast i samband med talan mot beslut som innebär att ärendet avgörs. Det samma ska, enligt våra förslag, gälla för ett föreläggande om att medverka till en biometrisk verifiering (se kapitel 26). Förslagen innebär i dessa delar därmed, som utgångspunkt, ingen utökad måltillströmning till de allmänna förvaltningsdomstolarna. Den ytterligare prövning i ett överklagat ärende som domstolen kan behöva göra, med anledning av eventuella invändningar avseende biometrisk verifiering, bör enligt vår uppfattning inte bli särskilt tidskrävande.

De verifierande myndigheterna kan komma att fatta fler avvisnings- eller avslagsbeslut, eftersom myndigheterna får bättre förut-

sättningar för att upptäcka identitetsmissbruk genom möjligheten att verifiera identitet biometriskt. Det kan, enligt vår mening, dock antas att andelen sådana beslut som överklagas inte kommer att vara särskilt stor i de fall en biometrisk verifiering visat att personen i fråga inte är den som han eller hon påstått. I de fall den enskilde inte medverkat till att en sådan verifiering kunnat genomföras kan man möjligen tänka sig en högre andel överklaganden. Huruvida den enskilde överklagar eller inte i en sådan situation torde, enligt vår bedömning, bero på anledningen till att verifieringen inte har genomförts. Om förutsättningar för att verifiera identitet biometriskt på distans saknas är det sannolikt att fler personer kommer att motsätta sig en begäran om biometrisk verifiering, till exempel för att de inte vill behöva ta sig till myndighetens kontor eller Statens servicecenter, med de eventuella kostnader som det kan medföra (se avsnitt 30.3).

Vad gäller biometrisk verifiering av identitet, i annat fall än vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde, när en myndighet genomför identitetskontroller, föreslår vi inga särskilda överklagandebestämmelser i den nya lagen, vilket innebär att förvaltningslagens bestämmelser blir tillämpliga i detta avseende. I dessa situationer kan den enskilde tänkas vilja överklaga myndighetens begäran om biometrisk verifiering och/eller ett beslut som kan ha fattats med anledning av resultatet av verifieringen alternativt med anledning av en utebliven verifiering. Det skulle, såvitt vi kan bedöma, i dessa fall eventuellt kunna bli fråga om en ny typ av mål i de allmänna förvaltningsdomstolarna. En första fråga för domstolarna att ta ställning till skulle i sådant fall bli om det – med beaktande av den aktuella situationen – alls är fråga om ett överklagbart beslut som har gått den enskilde emot. Hur stor påverkan blir för de allmänna förvaltningsdomstolarna i denna del är svår att förutse och beror dels på i vilken utsträckning myndigheterna använder möjligheten att verifiera identitet biometriskt i aktuella situationer, dels på hur praxis på området utvecklas. Allmänhetens acceptans för biometrisk verifiering av identitet med stöd av den nya lagen är också relevant i sammanhanget.

Sammantaget bedömer vi att konsekvenserna för de allmänna förvaltningsdomstolarna bör bli relativt begränsade. Därmed bedömer vi att eventuella tillkommande kostnader ryms inom domstolarnas befintliga ekonomiska ramar.

30.5.4 Kostnadsuppskattningar

Som vi tidigare har påpekat är det mycket svårt – för att inte säga omöjligt – att utifrån aktuella omständigheter göra kvalitetssäkrade kostnadsuppskattningar. Vi bedömer att det finns en klar risk för att beloppsbestämda kostnadsuppskattningar blir missvisande, innebärande att felaktiga siffror riskerar att ligga till grund för bedömningar av kostnader vid den fortsatta beredningen av frågan om biometrisk verifiering av identitet. Vi avstår därför, som utgångspunkt, från att försöka beloppsmässigt specificera de kostnader som kan antas uppkomma för det allmänna vid ett genomförande av våra förslag.

Vi vill dock även här erinra om att kostnader för att genomföra förslagen framför allt är hänförliga till de tekniska lösningar som kan behöva tas fram, och då i första hand ett myndighetsgemensamt system. Vid behov av kostnadsuppskattningar för en myndighetsgemensam lösning i den fortsatta beredningen av frågan om biometrisk verifiering kan det finnas anledning att inhämta information om andra tekniska system – om möjligt av liknande karaktär – och projekt om införande av dessa. Här kan Diggs utveckling av covidbevis[14] samt Polismyndighetens arbete med den statliga e-legitimationen *Sverige-id* och tillhörande mobilapplikation nämnas som exempel.

I det här avsnittet redogör vi översiktligt för de kostnadsposter vi bedömer kommer att uppstå för verifierande myndigheter respektive en eventuell tekniskt ansvarig myndighet och om dessa kan antas rymmas inom befintliga ekonomiska ramar.

Verifierande myndigheter

Konsekvenserna för de verifierande myndigheterna kommer, som vi redogjort för i avsnitt 30.5.1, att variera, beroende på bland annat den enskilda myndighetens storlek och behov av biometrisk verifiering av identitet. Översiktligt kan det handla om potentiella kostnader för tekniska system, dataanalyser och urval, ändrat arbetssätt, interna utbildningsinsatser och externa informationsinsatser.

För samtliga myndigheter som väljer att använda sig av den rättsliga möjligheten att verifiera identitet biometriskt med stöd av den nya lagen kommer det att uppstå ökade kostnader under en över-

[14] Se bland annat *Covidbevis – en biljett till samhället*, dnr 2021-0227, 2023-12-15.

gångsperiod, dels för teknisk implementation, dels för urvalsanalyser, ändrade arbetssätt med mera. Sådana kostnader kan som vi ser det antas uppkomma oavsett om myndigheten använder egna system för biometrisk verifiering eller en myndighetsgemensam lösning. För myndigheter med omfattande verksamhet och ett stort behov av biometrisk verifiering kan det antas att dessa initiala kostnader behöver finansieras genom omprioriteringar i myndigheternas verksamhet eller att myndigheternas ekonomiska ramar tillfälligt ökas. Detsamma gäller om egna tekniska system behöver utvecklas, då kostnader för detta kan antas vara betydligt större för den enskilda myndigheten än om en myndighetsgemensam teknisk lösning används. Även på sikt kan vissa myndigheter komma att ha ökade kostnader med anledning av arbetet med biometrisk verifiering av identitet. Det kan bland annat röra sig om kostnader för dataanalyser och urval, som kan behöva utföras och justeras löpande. Även interna utbildningsinsatser kan behöva vidtas löpande. Samtidigt kan det antas att kvaliteten i myndigheternas handläggning förbättras med möjligheten till att verifiera identitet biometriskt.

För mindre myndigheter, som får möjlighet att ansluta till en myndighetsgemensam teknisk lösning, bör såväl de initiala kostnaderna som de löpande kunna täckas av befintliga ekonomiska ramar.

Tekniskt ansvarig myndighet

Det står, såvitt vi kan bedöma, klart att en myndighet som får ansvar för en myndighetsgemensam lösning för biometrisk verifiering av identitet med stöd av den nya lagen kommer att behöva ökade anslag både initialt och löpande. Översiktligt kan det handla om kostnader för tekniska system i form av en mobilapplikation, ett backend-system och gränssnitt mot verifierande myndigheters system, förvaltning och drift, kundportal och support samt informationsinsatser.

Med reservation för att det är en grov uppskattning, utifrån nu kända faktorer, kan vi i sammanhanget redogöra för att en initial bedömning som gjorts under arbetets gång är att kostnaderna för att ta fram och implementera en myndighetsgemensam teknisk lösning för biometrisk verifiering skulle uppgå till cirka 25–30 miljoner kronor och den årliga förvaltningen och driften av en sådan lösning schablonmässigt 10 procent, det vill säga cirka 2,5–3 miljoner kronor.

Beloppet kan visa sig vara så väl högre som lägre vid närmre utredning. Som vi nämnt i avsnitt 30.5.2 kan sådana kostnader förväntas bli större de första åren för att därefter blir något lägre per år. Kostnader för kundportal och support samt informationsinsatser har inte varit möjliga att uppskatta med någon rimlig säkerhet.

30.5.5 Finansiering

En särskild fråga är hur en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet ska finansieras. Oavsett vilken myndighet som får uppdraget att utveckla och ta fram en lösning kommer det initialt att vara fråga om betydande kostnader som inte kan rymmas inom en myndighets befintliga ekonomiska ramar utan att det påverkar myndighetens befintliga verksamhet. Förvaltning och fortsatt utveckling av en myndighetsgemensam lösning kommer, enligt vår bedömning, också att föra med sig märkbara kostnader. Det kommer alltså att behövas utökade anslag för den myndighet som får ansvar för att ta fram och förvalta en myndighetsgemensam teknisk lösning.

De verifierande myndigheterna kan i varierande utsträckning antas ha kostnader för att inkludera biometrisk verifiering av identitet i sin verksamhet och sina rutiner, även för det fall en myndighetsgemensam teknisk lösning tillhandahålls. Det kan till exempel handla om ändrat arbetssätt samt interna och externa utbildnings- och informationsinsatser. Storleken på dessa kostnader kommer, enligt vår bedömning, att variera mycket stort för olika myndigheter. För vissa myndigheter kan det antas vara fråga om ett relativt omfattande arbete, som kan kräva omprioriteringar i verksamheten om de ska finansieras inom befintliga ekonomiska ramar. En tillfällig ökning av anslagen kan behövas för att sådana myndigheter ska kunna genomföra implementeringen på ett ändamålsenligt och snabbt sätt. Försäkringskassan, som handlägger ett stort antal socialförsäkringsförmåner där ansökningar regelmässigt görs med e-legitimation, kan antas vara en sådan myndighet. För andra myndigheter handlar det om ett mer begränsat arbete, som kan antas rymmas inom befintliga ekonomiska ramar.

Det bör i sammanhanget också beaktas att en rättslig och faktisk möjlighet för myndigheter att verifiera identitet biometriskt mot

handlingar dels kan ha en avskräckande effekt, dels kan bidra till att identitetsmissbruk upptäcks. Det kan i sin tur leda bland annat till att brott mot välfärdssystemen upptäcks, vilket innebär minskade kostnader för det allmänna. De kostnader en myndighetsgemensam lösning kommer att föra med sig för staten kommer, enligt vår bedömning, i vart fall att motsvaras av minskade kostnader för det allmänna. Beroende på omfattningen och effektiviteten av verifieringen av identiteter kan det bli fråga om en påtaglig kostnadsminskning för det allmänna på totalen.

30.5.6 En myndighetsgemensam teknisk lösning bör vara avgiftsfri

Vår bedömning

Anslutning till och användning av en myndighetsgemensam teknisk lösning för biometrisk verifiering av identitet med stöd av den nya lagen bör vara avgiftsfri för myndigheter.

En relevant fråga i sammanhanget är om verifierande myndigheter bör betala en avgift för att få ansluta till och nyttja en myndighetsgemensam teknisk lösning. Olika prismodeller kan då övervägas och vald modell kan påverka vilka myndigheter som väljer att ansluta till den gemensamma tjänsten, men även hur frekvent de då väljer att verifiera identitet biometriskt med hjälp av den. Skatteverkets system för distribution av folkbokföringsuppgifter till offentliga aktörer – Navet – är till exempel avgiftsfritt för statliga myndigheter. Kommunala och regionala myndigheter betalar däremot en avgift enligt Skatteverkets prislista och avgiften beror på vilken tjänst som används och består av en fast del och en rörlig del.[15] Det går också att söka ledning i den avgifts- och ersättningsmodell som tillämpas av Digg inom ramen för auktorisationssystem för elektronisk identifiering och digital post.[16]

[15] https://www.skatteverket.se/offentligaaktorer/informationsutbyte/navethamtauppgifteromfolkbokforing.4.18e1b10334ebe8bc80001754.html, senast besökt den 15 juni 2026.
[16] Se 7 § förordningen (2023:709) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post samt Diggs föreskrifter om uttag av avgifter för användning av sådana tjänster, MDFFS 2025:2.

Ingen eller en relativt låg avgift – för såväl anslutning som faktisk användning – bidrar enligt vår bedömning till en lägre tröskel för myndigheter att ansluta, och därmed sannolikt till att fler biometriska verifieringar mot handlingar genomförs, vilket generellt sett får anses gynna både det allmänna och enskilda genom att det ökar chanserna att upptäcka och motverka identitetsmissbruk. I de fall det finns ett behov av biometrisk verifiering av identitet för en myndighet – och förutsättningarna för sådan verifiering enligt den nya lagen är uppfyllda – bör myndighetens möjligheter att faktiskt genomföra verifieringen, enligt vår bedömning, som utgångspunkt inte begränsas av myndighetens ekonomiska förutsättningar. Det talar som vi ser det starkt för att anslutning till och användning av en myndighetsgemensam teknisk lösning för biometrisk verifiering bör vara avgiftsfri inte bara för statliga myndigheter, som är fallet med Navet, utan även för kommunala och regionala myndigheter.

30.6 Konsekvenser för företag

Våra förslag medför enligt vår bedömning inte några direkta kostnader för företag. Företag kan däremot indirekt komma att påverkas, genom att bolagsföreträdare kan omfattas av en begäran om att biometriskt verifiera sin identitet med stöd av den nya lagen. Ett sådant behov av verifiering kan till exempel finnas om myndigheten har misstankar om att företrädaren är en så kallad målvakt, det vill säga en person som anmäls som företrädare för ett företag i syfte att dölja för allmänheten och myndigheter vem som egentligen styr företaget, eller att de identitetsuppgifter som lämnats är oriktiga.[17] En begäran om att biometriskt verifiera identitet med stöd av den nya lagen kan därmed, på samma sätt som för enskilda, medföra en kostnad för företrädaren – och därmed indirekt företaget – för att resa, om verifieringen inte kan genomföras på distans; sådana kostnader är alltså beroende av vilken teknisk lösning som kan användas. Vår bedömning är att antalet situationer där det i ett bolag som är avsett att användas för seriös verksamhet finns sådana oklarheter att exempelvis Skatteverket anser det nödvändigt att begära att en företrädares identitet ska verifieras biometriskt kan antas vara relativt få. Kostnaden

[17] Jfr *Åtgärder mot mervärdesskattebedrägerier*, SOU 2024:32, s. 274.

för att inställa sig för biometrisk verifiering bör också vara begränsad, i de fall det skulle förekomma.

Biometrisk verifiering av identitet med stöd av den nya lagen är en utredningsåtgärd som kompletterar användning av e-legitimation för att få tillgång till nättjänster och kommer därför inte att vara en konkurrent till eller ersätta de e-legitimationer som utfärdas av privata aktörer. Vi bedömer i övrigt att våra förslag inte kommer att ha några konsekvenser för företag.

30.7 Övriga konsekvenser

Vi bedömer att våra förslag i betänkandet inte får några konsekvenser för regionerna eller det kommunala självstyret; våra förslag innebär en möjlighet – inte en skyldighet – att använda biometrisk verifiering av identitet. Vidare bedöms förslagen inte få några konsekvenser för jämställdheten mellan män och kvinnor. Förslagen bedöms inte heller, trots potentiellt ökad datatrafik, inverka negativt på klimat eller miljö i någon beaktansvärd omfattning.

31 Förslagens genomförande och ikraftträdande

31.1 Ikraftträdande

Vårt förslag

Författningsförslagen ska träda i kraft den 1 januari 2028.

Våra författningsförslag syftar till att motverka identitetsmissbruk som riktar sig mot det allmänna, däribland välfärdssystemen (se kapitel 9). Det är enligt vår mening därför viktigt att de bestämmelser om utökade möjligheter till säkrare verifiering av identitet som vi föreslår kan träda i kraft så snart som möjligt.

Viss tid behövs för remittering av förslagen och fortsatt beredning inom Regeringskansliet samt remittering till Lagrådet och efterföljande riksdagsbehandling. För att den utökade möjlighet att biometriskt verifiera identitet mot handlingar som vi föreslår ska kunna användas i praktiken krävs även att nödvändiga tekniska system är på plats. Vi har i kapitel 27 beskrivit de två huvudsakliga tekniska modeller som vi anser är aktuella. För det fall en verifieringsprocess som bygger på myndighetsgemensamma komponenter i form av en mobilapplikation och ett backend-system ska implementeras behövs tid för att ta fram, driftsätta och testa systemet och integrera det med befintliga myndighetsspecifika system. Detta kan behöva omfatta att vissa systemkomponenter upphandlas, och kan uppskattas ta i vart fall 12 till 24 månader. Det kan även finnas behov av att utbilda personal vid myndigheterna i hur ett sådant system ska användas. Vi anser emellertid att ikraftträdandet av våra förslag inte bör knytas till när sådana tekniska lösningar som behövs för biometrisk veri-

fiering av identitet kan finnas på plats. Vi kan dessutom konstatera att för det alternativ som innebär att biometrisk verifiering med stöd av den nya lagen genomförs med hjälp av tekniska system som den verifierande myndigheten ansvarar för – på det sätt vi beskrivit i avsnitt 27.3 – krävs sannolikt en betydligt kortare startsträcka, särskilt om befintliga tekniska system som används för sådana kontroller redan i dag kan användas. Oaktat detta kan det antas att berörda myndigheter behöver viss tid för att förbereda personal och egna system för att använda biometrisk verifiering i fler situationer än i dag. Med hänsyn till att våra författningsförslag kommer att påverka enskilda på ett direkt sätt kan det också vara nödvändigt att informera allmänheten innan biometrisk verifiering börjar användas generellt på det sätt vi föreslår.

Våra förslag innehåller inte några skyldigheter för myndigheter som ger anledning att vänta med ett ikraftträdande, utan det är som vi anfört ovan viktigt att den rättsliga möjlighet till säkrare verifiering av identitet som vi föreslår kan tillämpas så snart som möjligt. Vi lämnar inte heller några författningsförslag som innebär att någon viss myndighet får ett särskilt ansvar, som skulle kunna förutsätta en senare ikraftträdandetidpunkt.

Vid ställningstagande till tidpunkt för ikraftträdande kan de parallella processer som pågår avseende bland annat ett statligt identitetskort, som ska kunna innehålla en e-legitimation, och en separat statlig e-legitimation beaktas. Genomslaget av våra förslag kan antas påverkas bland annat av förslaget om ett statligt identitetskort. Det kan som vi ser det eventuellt finnas ett värde i att samordna ett ikraftträdande av våra författningsförslag med dessa lagstiftningsprojekt. Vi ser emellertid inte att det är en förutsättning med samordning i detta avseende. Det nuvarande nationella identitetskortet, som ska ersättas av det föreslagna statliga identitetskortet, kan till exempel användas för biometrisk verifiering av identitet med stöd av den nya lagen.

Mot bakgrund av det ovan anförda föreslår vi att författningsförslagen om en ny lag om biometrisk verifiering av identitet ska träda i kraft den 1 januari 2028. Några omständigheter som talar för att våra förslag som avser ändringar i offentlighets- och sekretesslagen (2009:400) ska träda i kraft vid någon annan tidpunkt har inte kommit fram. Vi föreslår därför att även dessa förslag ska träda i kraft detta datum.

31.2 Övergångsbestämmelser

Vår bedömning

Det saknas behov av övergångsbestämmelser.

Huvudregeln inom förvaltningsrätten är att rättstillämparen ska tillämpa den lag som gäller vid tidpunkten för prövningen om inget annat föreskrivs. Det innebär att nya processuella och materiella regler tillämpas från ikraftträdandetidpunkten även i ärenden som vid denna tidpunkt är öppna, om annat inte anges i övergångsbestämmelser.

De begränsade möjligheter att på ett säkert sätt verifiera identitet som finns i dag för många myndigheter medför en stor risk för identitetsmissbruk, vilket vi redogjort för i kapitel 9. Det är därför angeläget att den nya lagen om biometrisk verifiering av identitet får ett fullt genomslag så snart som möjligt. Vidare ska våra författningsförslag inte ersätta befintliga möjligheter att biometriskt verifiera identitet mot handlingar, utan det är fråga om en ny möjlig utredningsåtgärd. Inte heller ska befintliga bestämmelser om personuppgiftsbehandling i nationell rätt ersättas.

Att det under handläggningen av ett ärende träder i kraft ny lagstiftning som kan påverka utfallet av prövningen innebär inte i sig att krav på rättssäkerhet, förutsebarhet och likabehandling frångås.[1] Våra förslag om en ny lag om biometrisk verifiering av identitet ska ge myndigheter möjlighet att i befintlig verksamhet verifiera en persons identitet biometriskt under vissa förutsättningar. Den påverkan på enskilda som kommer i kontakt med myndigheter i olika sammanhang som detta kan få ger, enligt vår bedömning, inte anledning att tillåta att biometrisk verifiering genomförs endast i ärenden som har inletts efter ikraftträdandet av regelverket.

Dessa omständigheter talar för att lagen bör tillämpas direkt från och med den dag den träder i kraft, även i fråga om sådana ärenden som inletts före den tidpunkten. Inte heller i övrigt har vi identifierat ett behov av övergångsbestämmelser, varken avseende den nya lag som vi föreslår eller förslagna tillägg och ändringar i offentlighets- och sekretesslagen. Våra författningsförslag bör därför kunna tillämpas från ikraftträdandetidpunkten, i enlighet med huvudregeln, i

[1] *Preskription av avlägsnandebeslut och vissa frågor om återreseförbud,* prop. 2024/25:92, s. 39.

samtliga situationer som kan bli aktuella. Några särskilda övergångsbestämmelser behövs enligt vår bedömning därmed inte.

32 Författningskommentar

32.1 Förslaget till lag om biometrisk verifiering av identitet

1 kap. Allmänna bestämmelser

Lagens syfte

1 § Syftet med denna lag är att motverka identitetsmissbruk genom att ge myndigheter möjlighet att med hjälp av biometriska uppgifter som kan tas fram ur en handling kontrollera om en påstådd identitet är riktig och att skydda den som kontrolleras mot att hans eller hennes personliga integritet kränks vid en sådan kontroll.

I paragrafen anges det övergripande syftet med lagen. Övervägandena finns i avsnitt 23.2.2.

Bestämmelsen tydliggör lagens dubbla syften, det vill säga att dels ge myndigheter möjlighet att biometrisk verifiera identitet mot en handling, dels skydda den som kontrolleras mot att hans eller hennes personliga integritet kränks vid en sådan kontroll. Lagen innehåller både bestämmelser som reglerar när biometrisk verifiering får användas och bestämmelser som reglerar den behandling av personuppgifter som då behöver utföras.

Förhållandet till annan reglering

2 § Denna lag kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), här benämnd dataskyddsförordningen.

Vid behandling av personuppgifter enligt denna lag gäller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen, om inte annat

följer av denna lag eller av föreskrifter som har meddelats i anslutning till lagen.

I paragrafen klargörs att lagen kompletterar den allmänna dataskyddslagstiftningen. Övervägandena finns i avsnitt 24.3.

Första stycket är en upplysningsbestämmelse som tydliggör att lagen innehåller kompletterande bestämmelser till dataskyddsförordningen, som är direkt tillämplig i svensk rätt och gäller oavsett om det i lagen finns en bestämmelse som hänvisar till den. Hänvisningen är dynamisk, vilket innebär att den avser förordningen i dess vid varje tidpunkt gällande lydelse.

I *andra stycket* tydliggörs hur dataskyddslagen förhåller sig till lagen. Att dataskyddslagen är subsidiär i förhållande till annan nationell dataskyddsreglering och att eventuella specialbestämmelser om behandling av personuppgifter i andra författningar ska tillämpas framför de allmänna bestämmelserna i dataskyddslagen, följer direkt av 1 kap. 6 § dataskyddslagen. Detta tydliggörs genom upplysningsbestämmelsen i andra stycket.

3 § Om en annan lag eller förordning innehåller en bestämmelse som ger en myndighet uttrycklig rätt att kontrollera om en persons fingeravtryck eller ansiktsbild motsvarar dem som finns i en handling ska den bestämmelsen tillämpas.

I paragrafen regleras förhållandet till bestämmelser om biometrisk verifiering av identitet mot handlingar i annan lag eller i förordning. Övervägandena finns i avsnitt 23.3.

Paragrafen innebär att lagen utgör ett komplement till befintliga bestämmelser om möjligheter för myndigheter att biometriskt verifiera identitet mot handlingar och att lagen inte ersätter befintliga sådana möjligheter. Om en annan lag eller en förordning innehåller en bestämmelse som ger en myndighet uttrycklig rätt att i en viss situation kontrollera om en persons ansiktsbild eller fingeravtryck motsvarar dem som finns i eller på en handling, kan myndigheten inte välja att i stället genomföra en sådan kontroll i den i annan författning reglerade situationen med stöd av lagen om biometrisk verifiering av identitet. Det innebär att om förutsättningarna för biometrisk verifiering mot en handling i en bestämmelse i en annan lag eller i förordning inte är uppfyllda i den reglerade situationen, kan myndigheten inte i stället tillämpa lagen om biometrisk verifiering av identitet för att ändå genomföra en sådan verifiering. Inte heller

kan lagen tillämpas i en situation då förutsättningarna för biometrisk verifiering i och för sig är uppfyllda, för att till exempel kontrollera uppgifter i en annan handling än sådana som omfattas av den andra bestämmelsen.

Lagen kan, med andra ord, inte användas för att kringgå de rekvisit som gäller för biometrisk verifiering av identitet i en specifik situation som reglerats i en bestämmelse i en annan lag eller i förordning. Om det däremot är fråga om en situation som inte regleras i den andra bestämmelsen kan lagen om biometrisk verifiering av identitet tillämpas som grund för genomförandet av en sådan verifiering, till exempel i ett annat skede av handläggningen av ett ärende än vad som regleras i den andra bestämmelsen. Det kan bland annat vara fråga om att en myndighet, med stöd av lagen, biometriskt verifierar identiteten i ett inledande skede för att kontrollera att en ansökan har getts in av rätt eller behörig person.

Att det ska vara fråga om en *uttrycklig* rätt i en annan bestämmelse i lag eller förordning utesluter inte att lagen om biometrisk verifiering av identitet kan tillämpas av en myndighet även om myndigheten skulle bedöma att det finns stöd för att genomföra en biometrisk verifiering av identitet mot en handling med tillämpning av till exempel 3 kap. 3 § dataskyddslagen, om behandling av känsliga personuppgifter med hänsyn till ett viktigt allmänt intresse.

Undantag för brottsbekämpande verksamhet

4 § En biometrisk verifiering får inte genomföras med stöd av lagen i verksamhet som en sådan behörig myndighet som avses i brottsdatalagen (2018:1177) utför i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Paragrafen anger att biometrisk verifiering av identitet med stöd av lagen inte får genomföras i brottsbekämpande verksamhet som utförs av sådana behöriga myndigheter som avses i brottsdatalagen. Övervägandena finns i avsnitt 21.4 och 23.4.

För att undantaget ska vara tillämpligt krävs inte att brottsdatalagen är tillämplig vid handläggningen av det aktuella ärendet eller vid genomförandet av de aktuella identitetskontrollerna. Det räcker att det är fråga om verksamhet som en sådan behörig myndighet som avses i brottsdatalagen utför i syfte att bekämpa brott för att lagen

inte ska få tillämpas som grund för biometrisk verifiering av identitet. Det innebär att även Säkerhetspolisens brottsbekämpande verksamhet omfattas av undantaget, trots att det framgår av 1 kap. 4 § brottsdatalagen att den lagen inte gäller vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet.

Undantaget omfattar verksamhet som utförs i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder och upprätthålla allmän ordning och säkerhet. I detta avseende är det fråga om sådan verksamhet som avses i 1 kap. 2 § brottsdatalagen.

Definitioner

5 § I denna lag avses med

1. *identitet*: uppgifter om namn, födelsetid och medborgarskap,
2. *biometriska uppgifter*: personuppgifter som genom en särskild teknisk behandling har tagits fram ur fingeravtryck eller ansiktsbild, i syfte att verifiera en persons identitet,
3. *biometrisk verifiering av identitet*: en-till-en-jämförelse av en grupp av uppgifter, däribland biometriska uppgifter, med en annan för att fastställa om en påstådd identitet är riktig,
4. *myndighet*: statliga och kommunala organ, med undantag för beslutande politiska församlingar.

Paragrafen innehåller definitioner av fyra begrepp som är centrala för tillämpningen av lagen. Övervägandena finns i avsnitt 23.5.

Av *första punkten* följer att med *identitet* avses uppgifter om namn, födelsetid och medborgarskap. Definitionen syftar till att tydliggöra vad som avses med identitet vid tillämpning av lagen och ska inte ses som en mer generellt tillämplig legaldefinition av begreppet. Vad som avses med identitet är avgörande för innebörden av biometrisk verifiering av identitet i tredje punkten.

I *andra punkten* definieras *biometriska uppgifter* som personuppgifter som genom en särskild teknisk behandling har tagits fram ur fingeravtryck eller ansiktsbild, i syfte att verifiera en persons identitet. Definitionen av biometriska uppgifter i lagen skiljer sig från den i artikel 4.14 i dataskyddsförordningen. Till att börja med har en avgränsning gjorts till fysiska kännetecken i form av fingeravtryck och ansiktsbild. Vidare ska uppgifterna ha tagits fram i syfte att *verifiera* en persons identitet, och inte för att möjliggöra eller bekräfta identifieringen av en fysisk person. Dessa preciseringar syftar till att tyd-

liggöra dels att inga andra fysiska kännetecken än fingeravtryck och ansiktsbild får användas vid biometrisk verifiering av identitet med stöd av lagen, dels att lagen ger rättsligt stöd endast för att verifiera en persons identitet (genom en-till-en-jämförelse) och inte för att identifiera en okänd person (genom en-till-många-jämförelse).

Tredje punkten definierar vad som avses med *biometrisk verifiering av identitet*, nämligen en-till-en-jämförelse av en grupp av uppgifter, däribland biometriska uppgifter, med en annan för att fastställa om en påstådd identitet är riktig. Den påstådda identiteten utgörs av de uppgifter om namn, födelsedatum och medborgarskap som en person har uppgett för en myndighet, exempelvis i en ansökan eller genom uppvisande av en identitetshandling. Sådana uppgifter kan också uppges indirekt, till exempel genom att personen anger ett personnummer som är kopplat till identitetsuppgifter i folkbokföringen. I praktiken genomförs en biometrisk verifiering av identitet i två steg: dels en jämförelse mellan den påstådda identiteten och de identitetsuppgifter som finns i den handling som används vid verifieringen, dels en jämförelse mellan den ansiktsbild och/eller de fingeravtryck som tas upp vid verifieringstillfället och de som finns i eller på handlingen. Den senare jämförelsen syftar till att på ett tillförlitligt sätt koppla ihop identitetsuppgifterna i handlingen – vilka utgör jämförelseunderlag – med individen.

I *fjärde punkten* definieras *myndighet* som statliga och kommunala organ, med undantag för beslutande politiska församlingar. Eftersom samtliga myndigheter får verifiera identitet biometriskt med stöd av lagen, om förutsättningarna för verifiering är uppfyllda, klargörs innebörden av begreppet. Definitionen innebär att varken de organ som anges i bilagan till offentlighets- och sekretesslagen (2009:400) eller bolag, föreningar och stiftelser där kommuner eller regioner utövar ett rättsligt bestämmande inflytande, är att betrakta som myndigheter i lagens mening.

2 kap. Biometrisk verifiering av identitet mot handlingar

Typer av handlingar som får användas

1 § Hemlandspass och identitetskort som har utfärdats av behörig myndighet och som har ett lagringsmedium där fingeravtryck eller ansiktsbild är sparade får användas för att biometriskt verifiera innehavarens identitet

med stöd av 2 §. Även uppehållstillståndskort som har utfärdats av svenska myndigheter får användas för sådan verifiering.

Paragrafen anger vilka typer av handlingar som får användas för biometrisk verifiering av identitet med stöd av lagen. Övervägandena finns i avsnitt 19.3, 19.4 och 23.6.2.

Hemlandspass som har ett lagringsmedium där fingeravtryck eller ansiktsbild är sparade får användas för att biometriskt verifiera innehavarens identitet med stöd av lagen. Begreppet *hemlandspass* utgör i svenskt hänseende en avgränsning mot främlingspass och resedokument och omfattar sådana pass som avses i 3 § passlagen (1978:302), det vill säga vanligt pass och särskilt pass. Med hemlandspass avses dock även pass utfärdade av myndigheter i andra länder för medborgare i det aktuella landet. Även utländska pass får alltså användas för biometrisk verifiering av identitet med stöd av lagen, om passet har ett lagringsmedium där fingeravtryck eller ansiktsbild är sparade. Hemlandspass är per definition utfärdade av behörig myndighet – annars är det inte fråga om ett hemlandspass.

För att ett identitetskort ska få användas för biometrisk verifiering av identitet enligt lagen ska kortet dels ha utfärdats av behörig myndighet, dels ha ett lagringsmedium där fingeravtryck eller ansiktsbild är sparade. Identitetskort som utfärdats av någon annan aktör får alltså inte användas, trots att sådana kort också kan innehålla ett lagringsmedium med biometriska underlag. Identitetskort som *endast* har en synlig ansiktsbild får inte heller användas. Ett nationellt identitetskort som utfärdas enligt förordningen (2005:661) om nationellt identitetskort och ett sådant statligt identitetskort som enligt förslag ska utfärdas enligt en ny lag om statligt identitetskort utgör sådana identitetskort som avses i paragrafen.

Uppehållstillståndskort som utfärdats av svenska myndigheter har ett lagringsmedium där fingeravtryck och ansiktsbild är sparade, vilket följer av 4 kap. 22 § utlänningsförordningen (2006:97) och rådets förordning (EG) nr 1030/2002 av den 13 juni 2002 om en enhetlig utformning av uppehållstillstånd för medborgare i tredje land. Det behöver därför inte framgå av paragrafen att uppehållstillståndskort ska ha ett sådant lagringsmedium för att kortet ska få användas för biometrisk verifiering av identitet med stöd av lagen. Uppehållstillståndskort utfärdade av andra EU-medlemsstater får inte användas för biometrisk verifiering av identitet med stöd av lagen.

Lagringsmediet på de handlingar som avses i paragrafen innehåller, som utgångspunkt, också identitetsuppgifter, det vill säga uppgifter om namn, födelsetid och medborgarskap. Det är en förutsättning att lagringsmediet innehåller även dessa uppgifter för att en biometrisk verifiering av identitet ska kunna genomföras på distans och gör verifiering vid personlig inställelse säkrare, eftersom identitetsuppgifterna i lagringsmediet är svårare att manipulera än de som är synliga på handlingen. Att en handling inte innehåller *samtliga* identitetsuppgifter, till exempel medborgarskap, synligt på handlingen eller i ett lagringsmedium, utgör inget hinder mot att använda handlingen för biometrisk verifiering av identitet med stöd av lagen om det är en sådan handling som anges i paragrafen.

När biometrisk verifiering av identitet får användas

2 § Den som har fyllt sex år och innehar en sådan handling som anges i 1 § ska på begäran av en myndighet göra handlingen tillgänglig samt låta myndigheten ta fingeravtryck och ansiktsbild för kontroll av att de motsvarar dem som finns i eller på handlingen, om en biometrisk verifiering av innehavarens identitet är nödvändig

1. vid handläggningen av ett ärende som omfattas av förvaltningslagens (2017:900) tillämpningsområde, eller
2. i annat fall, när myndigheten, inom ramen för sin verksamhet, genomför identitetskontroller.

När en kontroll enligt första stycket har genomförts ska fingeravtryck och ansiktsbilder samt de biometriska uppgifter som har tagits fram omedelbart förstöras.

I paragrafen anges vem som är skyldig att på begäran av en myndighet medverka till en biometrisk verifiering av identitet och under vilka förutsättningar en myndighet har rätt att begära detta. Paragrafen reglerar också längsta tid för behandling av fingeravtryck, ansiktsbilder och de biometriska uppgifter som tagits fram ur dessa. Övervägandena finns i avsnitt 20.6, 21.3–21.5, 23.6 och 24.9.

Av *första stycket* framgår att den som har fyllt sex år och innehar en sådan handling som anges i 1 § på begäran av en myndighet ska göra handlingen tillgänglig samt låta myndigheten ta fingeravtryck och ansiktsbild för kontroll av att de motsvarar dem som finns i eller på handlingen, om biometrisk verifiering är nödvändig i enlighet med första eller andra punkten. Att endast den som *innehar* en sådan handling som omfattas av 1 § är skyldig att göra handlingen tillgänglig

innebär att det inte finns någon skyldighet att skaffa en sådan handling i syfte att en biometrisk verifiering av identitet med stöd av lagen ska kunna genomföras.

Att göra en handling *tillgänglig* innefattar både att handlingen överlämnas fysiskt till myndigheten vid personlig inställelse och att myndigheten får tillgång till uppgifter i handlingen på distans. Beroende på vilken teknisk lösning myndigheten använder vid verifieringen i det enskilda fallet kan en skyldighet att göra en handling tillgänglig alltså i praktiken innefatta en skyldighet att inställa sig personligen. Bestämmelsen kräver inte att det anges särskilt i begäran från myndigheten att personlig inställelse förutsätts, men det kan naturligtvis vara lämpligt i upplysningssyfte.

Skyldigheten att *låta myndigheten ta* fingeravtryck och ansiktsbild för kontroll av att de motsvarar dem som finns i eller på handlingen kan fullgöras antingen vid personlig inställelse eller på distans, om det finns tekniska förutsättningar för myndigheten att ta upp relevanta biometriska underlag på detta sätt. Det är, som utgångspunkt, den myndighet som begär att verifieringen ska genomföras som bestämmer hur det praktiskt och tekniskt ska gå till. Med ordalydelsen *i eller på handlingen* avses att såväl biometriska underlag som finns sparade i ett digitalt lagringsmedium som en ansiktsbild som finns synlig på handlingen kan användas. Användning av en synlig ansiktsbild för den biometriska jämförelsen bör dock ses som en reservmetod. Det överlåts till den myndighet som vill verifiera identitet att ta ställning till vilken metod som är lämplig. Användning av en synlig ansiktsbild bör emellertid, med utgångspunkt i nuvarande teknik, tillämpas endast vid personlig inställelse och inte på distans. Detta med hänsyn till att det med nuvarande teknik inte går att på distans säkerställa att ansiktsbilden härrör från handlingen.

För att en biometrisk verifiering av identitet ska få genomföras med stöd av paragrafen ska verifieringen vara nödvändig antingen vid handläggningen av ett ärende som omfattas av förvaltningslagens (2017:900) tillämpningsområde, eller, i annat fall, när myndigheten inom ramen för sin verksamhet genomför identitetskontroller. Syftet med den nya lagen är inte att ge myndigheter en generell möjlighet att kontrollera vissa typer av handlingar som ett led i att den enskilde ska styrka sin identitet, utan den nya lagen ska möjliggöra en säkrare verifiering av identitet mot handlingar med hjälp av biometriska uppgifter. Detta tydliggörs genom att det anges i bestämmelsen att det

är den biometriska verifieringen av identiteten som ska vara nödvändig. Enskilda är alltså inte enligt lagen skyldiga att göra en handling tillgänglig för en myndighet av andra skäl än att möjliggöra en kontroll av de biometriska underlag som är lagrade i eller synliga på handlingen, och därmed möjliggöra en säker verifiering av innehavarens identitet. Rekvisitet *nödvändig* har samma betydelse som det dataskyddsrättsliga begreppet nödvändig. Att den biometriska verifieringen ska vara nödvändig innebär därmed inte ett krav på att den ska vara oundgänglig; det räcker att den behövs för att uppnå ändamålet med den, nämligen säker verifiering av identitet i den aktuella situationen. Genom att den materiella bestämmelsen om verifiering av identitet knyts till det dataskyddsrättsliga rekvisitet nödvändig, säkerställs att biometrisk verifiering av identitet får användas endast när det behövs vid myndighetens handläggning av det aktuella ärendet eller annars vid en myndighets genomförande av identitetskontroller.

För det fall myndigheten bedömer att det finns ett behov av biometrisk verifiering av identitet får det som utgångspunkt anses vara nödvändigt med en sådan verifiering. Myndigheten behöver dock kunna peka på någon konkret omständighet som innebär att användning av biometriska uppgifter är nödvändig för att uppnå ändamålet med kontrollen. Sådana omständigheter kan finnas både på en mer övergripande nivå och hänföra sig till omständigheter i det enskilda fallet. Exempel på omständigheter på övergripande nivå är att det finns indikationer på att det förekommer identitetsmissbruk i det aktuella ärendeslaget eller att ärendet inletts av den enskilde på distans genom användning av en e-legitimation. Även om initiering av ett ärende på distans med hjälp av en e-legitimation självständigt kan utgöra en konkret omständighet för biometrisk verifiering är avsikten inte att bestämmelsen ska tillämpas generellt i samtliga ärenden som inleds på detta sätt, utan att en bedömning har gjorts av behovet av biometrisk verifiering i aktuellt ärendeslag, eller i ett enskilt fall.

I det enskilda fallet kan det till exempel handla om att det kommit fram omständigheter som ger anledning att misstänka att en person inte är den han eller hon utger sig för att vara eller att en okulär kontroll av en identitetshandling av något slag inte är tillräcklig, eller möjlig att genomföra. I de fall en myndighet har personlig kännedom om personen i fråga kan det normalt sett inte anses vara nödvändigt att biometriskt verifiera personens identitet. Som exempel kan nämnas en person som regelbundet får ekonomiskt bistånd från socialtjänsten

och som träffat handläggaren av ärendet vid upprepade tillfällen och vars identitet inte är ifrågasatt.

Vilka ärenden som *omfattas av tillämpningsområdet för förvaltningslagen*, enligt *första punkten*, framgår av 1 § förvaltningslagen. Med hänsyn till att förvaltningslagen är subsidiär kan det finnas avvikande bestämmelser i annan lag som ska tillämpas i stället. Även i de fall det finns verksamhetsspecifika bestämmelser i annat regelverk som reglerar handläggningen av det aktuella ärendet – till exempel skatteförfarandelagen (2011:1244), socialtjänstlagen (2025:400) och socialförsäkringsbalken – är det emellertid fråga om ett ärende som omfattas av förvaltningslagens tillämpningsområde, och därmed av denna lag.

Handläggningen av ett ärende omfattar i princip alla åtgärder som vidtas av en myndighet från det att ärendet inleds tills att det avslutas. En biometrisk verifiering av identitet enligt lagen kan alltså genomföras i olika situationer under handläggningen av det aktuella ärendet.

En myndighet kan genomföra identitetskontroller, inom ramen för sin verksamhet, i annat fall än vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde. Om en biometrisk verifiering är nödvändig i en sådan situation finns det stöd i bestämmelsens *andra punkt* för att genomföra den. Denna punkt blir i stor utsträckning tillämplig i en myndighets faktiska verksamhet, och det skulle exempelvis kunna vara fråga om identitetskontroller som genomförs för personer som söker vård, i skolverksamhet, i samband med genomförande av högskoleprov eller vid röstning till val. Biometrisk verifiering av identitet skulle även kunna förekomma i samband med identitetskontroller vid besök i en myndighets lokaler, under förutsättning att verifieringen inte görs inom ramen för myndighetens brottsbekämpande verksamhet. Biometrisk verifiering av identitet enligt andra punkten skulle också kunna aktualiseras om det är nödvändigt för att på ett korrekt sätt kunna genomföra en sekretessprövning i samband med en begäran om utlämnande av en allmän handling, under förutsättning att prövningen är beroende av vem personen som begärt ut handlingen är.

I *andra stycket* regleras längsta tillåtna tid för behandling av de fingeravtryck och ansiktsbilder som tagits upp för att den biometriska verifieringen ska kunna genomföras samt de biometriska uppgifter som har tagits fram ur dessa. Dessa ska förstöras omedelbart när en kontroll enligt första stycket har genomförts. Uppgifterna får alltså inte lagras. Bestämmelsen utgör inte en sådan avvikande bestämmelse

som avses i 10 § tredje stycket arkivlagen (1990:782) och reglerar alltså inte gallring av allmänna handlingar. Den personuppgiftsansvariga myndigheten ska säkerställa att bestämmelsen efterlevs, även om uppgifterna hanteras av en annan myndighet som ett led i teknisk bearbetning.

Föreläggande om att medverka

3 § Om det inte har kommit fram omständigheter som talar mot det får en myndighet förelägga den som inte har följt en begäran enligt 2 § första stycket 1, och som har inlett ärendet, att göra en handling tillgänglig och låta myndigheten ta fingeravtryck och ansiktsbild, för att en biometrisk verifiering av identitet ska kunna genomföras.

I föreläggandet ska det anges vad följden av att det inte följs kan bli.

I paragrafen regleras förutsättningarna för att en myndighet ska få meddela ett föreläggande om att medverka till en biometrisk verifiering av identitet enligt lagen, samt att det i föreläggandet ska anges vad följden av det inte följs kan bli. Övervägandena finns i avsnitt 23.8.

I *första stycket* anges att ett föreläggande inte får meddelas om det har kommit fram *omständigheter som talar mot det*. Det innebär att en myndighet inte per automatik ska förelägga den som inte har följt en begäran om biometrisk verifiering av identitet med stöd av lagen. I stället ska en bedömning göras av om de omständigheter som kommit till myndighetens kännedom talar mot att ett föreläggande meddelas. Det ska inte krävas att den enskilde gör gällande en viss omständighet för att den ska kunna beaktas. Att ett föreläggande kan upplevas som betungande för den enskilde bör inte ensamt leda till att ett föreläggande inte meddelas. Detsamma gäller ett påstående från den enskilde om att han eller hon inte innehar en sådan handling som kan användas för biometrisk verifiering av identitet med stöd av lagen; i dessa fall får trovärdigheten i en sådan invändning med hänsyn till omständigheterna i stället beaktas.

Möjligheten att meddela ett föreläggande med stöd av paragrafen är begränsad till biometrisk verifiering av identitet vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde, och kan riktas endast till den som har inlett det aktuella ärendet. Det innebär att ett föreläggande inte kan meddelas med stöd av bestämmelsen vid så kallade initiativärenden som inletts av myndigheten själv. Ett föreläggande kan inte heller meddelas med stöd av bestäm-

melsen när det är fråga om biometrisk verifiering av identitet vid genomförande av identitetskontroller i annat fall än vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde. Inte heller kan eventuella andra parter i ärendet än den som har inlett det, eller andra personer, föreläggas med stöd av bestämmelsen, även om en begäran enligt bestämmelsen i 2 § första stycket 1 kan riktas också till dessa personkategorier.

Den enskilde kan endast föreläggas att *göra en handling tillgänglig* och att *låta myndigheten ta fingeravtryck och ansiktsbild*. Ett föreläggande om att göra en handling tillgänglig innefattar inte en skyldighet att ansöka om att få en sådan handling utfärdad som omfattas av lagen. Att göra en handling tillgänglig kan dock innefatta ett krav på personlig inställelse, om den biometriska verifieringen inte går att genomföra på distans, till exempel på grund av att myndigheten inte har tillgång till den teknik som krävs för detta eller på grund av att lagringsmediet i den aktuella handlingen är skadat. Den enskilde kan, som en följd av detta, alltså föreläggas att låta myndigheten ta fingeravtryck och ansiktsbild antingen vid personlig inställelse, eller på distans med användning av en teknisk lösning som möjliggör verifiering på distans.

I *andra stycket* klargörs att ett föreläggande enligt lagen ska innehålla en upplysning om vad följden av att det inte följs kan bli. Det är upp till den myndighet som meddelar föreläggandet att ta ställning till vilken konsekvens som kan bli aktuell i det enskilda fallet. För att den enskildes bristande medverkan att följa föreläggandet ensamt ska kunna medföra en viss konsekvens förutsätts det alltså att konsekvensen anges redan i föreläggandet. De konsekvenser som framför allt kan vara aktuella är att en framställan inte prövas i sak, det vill säga avvisas, eller att den avslås.

Överklagande

4 § En begäran enligt 2 § första stycket 1 och ett föreläggande enligt 3 § får överklagas endast i samband med talan mot beslut som innebär att ärendet avgörs.

Av paragrafen framgår vissa begränsningar av rätten att överklaga. Övervägandena finns i avsnitt 26.3.1.

En begäran om biometrisk verifiering av identitet vid handläggningen av ett ärende som omfattas av förvaltningslagens tillämpningsområde får överklagas endast i samband med talan mot beslut som innebär att ärendet avgörs. Detsamma gäller för ett föreläggande om att göra en handling tillgänglig samt lämna fingeravtryck och ansiktsbild för att en biometrisk verifiering ska kunna genomföras. Paragrafen innebär att en begäran enligt 2 § första stycket 1 och ett föreläggande enligt 3 § inte får överklagas särskilt även om det skulle vara fråga om ett överklagbart beslut enligt förvaltningslagen som kan anses ha gått den enskilde emot. Vid överklagande av ett beslut som innebär att ärendet avgörs kan den enskilde framföra invändningar avseende en begäran eller ett föreläggande om biometrisk verifiering med stöd av lagen. Paragrafen syftar till att det slutliga avgörandet av det aktuella ärendet inte ska fördröjas av en domstolsprocess.

Vid ställningstagande till om en begäran om biometrisk verifiering av identitet med stöd av 2 § första stycket 2, när en myndighet inom ramen för sin verksamhet genomför identitetskontroller, får överklagas i det enskilda fallet, blir bestämmelserna om överklagande i förvaltningslagen tillämpliga.

Rätt att meddela föreskrifter

5 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om tillämpningen av denna lag.

I paragrafen finns en upplysningsbestämmelse som anger att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om tillämpningen av lagen med stöd 8 kap. 7 § regeringsformen. Övervägandena finns i avsnitt 23.9.

Bestämmelsen tydliggör att det kan finnas kompletterande bestämmelser i förordning eller – efter bemyndigande av regeringen – i myndighetsföreskrifter. Det kan vara fråga dels om verkställighetsföreskrifter, dels om föreskrifter som meddelats med stöd av regeringens så kallade restkompetens. I sak skulle det till exempel kunna handla om begränsningar av vilka handlingar som får användas för biometrisk verifiering av identitet med stöd av lagen eller av i vilka situationer sådan verifiering får användas. Exempelvis kan det bli känt att en specifik handling – exempelvis ett hemlandspass från ett visst land

– utfärdas på ett sätt som inte är tillförlitligt ur identitetshänseende och därför inte bör kunna användas för biometrisk verifiering enligt lagen. Ett annat exempel är föreskrifter avseende de tekniska system som används för biometrisk verifiering, till exempel avseende en myndighetsgemensam teknisk lösning för verifiering.

3 kap. Personuppgiftsbehandling

Tillämpningsområde

1 § Detta kapitel tillämpas vid behandling av personuppgifter som utförs i syfte att biometriskt verifiera identitet med stöd av lagen.

I paragrafen anges tillämpningsområdet för bestämmelserna om personuppgiftsbehandling i kapitlet. Övervägandena finns i avsnitt 24.4.

Bestämmelserna ska tillämpas när en myndighet behandlar personuppgifter i syfte att biometriskt verifiera identitet med stöd av lagen. De är alltså inte tillämpliga vid behandling av personuppgifter i viss verksamhet eller vid handläggning av vissa ärendeslag. I stället är det syftet med behandlingen som avgör. Det innebär att vid handläggningen av ärenden som omfattas av förvaltningslagens tillämpningsområde och vid genomförandet av identitetskontroller ska myndigheten som utgångspunkt tillämpa myndighets- eller verksamhetsspecifika bestämmelser om personuppgiftsbehandling eller, i avsaknad av sådana, allmänna dataskyddsbestämmelser. Det är endast den behandling av personuppgifter som utförs i syfte att biometriskt verifiera identitet med stöd av lagen som omfattas av bestämmelserna i detta kapitel.

Ändamål och tillgång till personuppgifter

2 § Personuppgifter får behandlas endast för att en biometrisk verifiering av identitet med stöd av lagen ska kunna genomföras. Detta gäller även sådana personuppgifter som avses i artikel 9.1 i dataskyddsförordningen (känsliga personuppgifter).

I paragrafen anges för vilket ändamål en myndighet får behandla personuppgifter enligt lagen. Övervägandena finns i avsnitt 24.8.

Av bestämmelsen i 2 kap. 2 §, som anger under vilka förutsättningar en myndighet får använda biometrisk verifiering, följer att

den biometriska verifieringen ska vara *nödvändig* i den aktuella situationen för att få genomföras. Med hänsyn till att rekvisitet nödvändig framgår redan av 2 kap. 2 § behöver det inte anges i den nu aktuella paragrafen. Om den biometriska verifieringen är nödvändig enligt 2 kap. 2 § är det också nödvändigt att behandla de personuppgifter som behövs för att verifieringen ska kunna genomföras.

Att personuppgifter får behandlas *endast* för att en biometrisk verifiering av identitet med stöd av lagen ska kunna genomföras innebär att den så kallade finalitetsprincipen i artikel 5.1 b i dataskyddsförordningen inte är tillämplig. Personuppgifter får alltså inte behandlas för något annat ändamål än det som anges i paragrafen, även om behandlingen kan anses vara förenlig med ändamålet biometrisk verifiering av identitet med stöd av lagen.

Ändamålet gör det möjligt för myndigheter att behandla personuppgifter i den omfattning det behövs för att en biometrisk verifiering av identitet mot en handling ska kunna genomföras, samtidigt som det inte ger rättsligt stöd för behandling av personuppgifter för andra syften eller för behandling av andra personuppgifter än sådana som behövs för en verifiering enligt lagen. Att känsliga personuppgifter får behandlas endast för att en biometrisk verifiering av identitet med stöd av lagen ska kunna genomföras, innebär att inga andra känsliga personuppgifter än biometriska uppgifter som tagits fram ur fingeravtryck och ansiktsbild får behandlas med stöd av lagen.

3 § Tillgången till personuppgifter ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Paragrafen tydliggör att de myndigheter som behandlar personuppgifter i syfte att biometriskt verifiera identitet med stöd av lagen har ett ansvar att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att personuppgifter inte sprids utanför den krets av personer som behöver ha tillgång till dessa för att kunna utföra sina arbetsuppgifter. Övervägandena finns i avsnitt 24.10.

Personuppgiftsansvar

4 § Den myndighet som bestämmer att en biometrisk verifiering av identitet ska genomföras med stöd av 2 kap. 2 § är personuppgiftsansvarig för den behandling av personuppgifter som utförs med anledning av det.

Paragrafen innehåller en bestämmelse om personuppgiftsansvar. Övervägandena finns i avsnitt 24.6 och 24.7.

En definition av begreppet personuppgiftsansvarig finns i artikel 4.7 i dataskyddsförordningen. Personuppgiftsansvaret innebär ett ansvar för att behandlingen stämmer överens med dataskyddsförordningen och de kompletterande bestämmelser till denna som finns i nationell rätt, det vill säga i den generella regleringen i dataskyddslagen, i denna lag och i föreskrifter som meddelats med stöd av dessa lagar.

Paragrafen fastställer att den myndighet som bestämmer att en biometrisk verifiering av identitet ska genomföras med stöd av lagen ansvarar för den behandling av personuppgifter som utförs med anledning av det. I de fall myndigheten själv genomför en biometrisk verifiering, i tekniska system som myndigheten ansvarar för, innebär detta att huvudregeln att den som utför själva behandlingen också är personuppgiftsansvarig gäller. Om myndigheten i stället väljer att anlita en annan aktör för tillhandahållande av de tekniska system som behövs för att genomföra en biometrisk verifiering bearbetas personuppgifterna i praktiken i system som en annan aktör ansvarar för. Även i detta fall är det dock den myndighet som bestämmer att en biometrisk verifiering av identitet ska genomföras med stöd av lagen som ansvarar för den behandling av personuppgifter som utförs med anledning av det. Vem som ansvarar för de tekniska system där personuppgifter faktiskt behandlas i samband med biometrisk verifiering med stöd av den nya lagen påverkar alltså inte vem som är personuppgiftsansvarig. Det ankommer därmed på den myndighet som bestämmer att en biometrisk verifiering av identitet ska genomföras att på lämpligt sätt säkerställa bland annat att biometriska underlag och biometriska uppgifter som används vid biometrisk verifiering av identitet med stöd av lagen omedelbart förstörs när en kontroll har genomförts.

Vad gäller myndigheters möjligheter att anlita personuppgiftsbiträde för genomförande av biometrisk verifiering av identitet med stöd av lagen blir den generella dataskyddsregleringen tillämplig.

Rätt att göra invändningar

5 § Artikel 21.1 i dataskyddsförordningen om rätten att göra invändningar gäller inte vid sådan behandling av personuppgifter som är tillåten enligt denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Paragrafen innehåller ett undantag från den registrerades rätt att göra invändningar enligt artikel 21.1. i dataskyddsförordningen. Undantaget säkerställer förutsättningarna för myndigheter att behandla relevanta personuppgifter vid biometrisk verifiering av identitet med stöd av lagen. Övervägandena finns i avsnitt 24.11.3.

32.2 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

40 kap.

Biometrisk verifiering

5 a §

Sekretess gäller för uppgift i form av fingeravtryck eller ansiktsbild som tagits upp med stöd av lagen (202X:000) om biometrisk verifiering av identitet, och biometrisk uppgift som har tagits fram ur fingeravtrycket eller ansiktsbilden.

Paragrafen, som är ny, reglerar sekretess för biometriska underlag som tagits upp med stöd av lagen om biometrisk verifiering av identitet och biometriska uppgifter som tagits fram ur dessa underlag. Övervägandena finns i avsnitt 25.2.2.

Sekretessen gäller oavsett i vilken situation en biometrisk verifiering med stöd av lagen genomförs och är inte begränsad till vissa verksamheter eller vissa typer av ärenden. Oberoende av om uppgifterna – det vill säga såväl de biometriska underlagen som de biometriska uppgifterna – förekommer hos den myndighet som har bestämt att en verifiering ska genomföras eller hos en annan myndighet, till exempel en myndighet som tillhandahåller tekniska system för verifiering, gäller alltså sekretessen.

Med fingeravtryck eller ansiktsbild som *tagits upp med stöd av lagen* avses såväl de biometriska underlag som tagits upp från den person vars identitet ska verifieras som de biometriska underlag som lästs in från ett lagringsmedium i eller en synlig ansiktsbild på den hand-

ling som används för verifieringen. Vidare saknar det betydelse för bestämmelsens tillämpning om de biometriska underlagen tagits upp vid personlig inställelse eller på distans, till exempel genom att den enskilde använder en mobilapplikation.

Paragrafen är inte försedd med något skaderekvisit. Sekretess gäller därför oberoende av om ett röjande av uppgifterna kan medföra skada eller men för den enskilde. De uppgifter som omfattas av paragrafen ska därmed hemlighållas utan någon skadeprövning; sekretessen är absolut.

Biometriska underlag som tagits upp med stöd av lagen om biometrisk verifiering av identitet och biometriska uppgifter som tagits fram ur dessa underlag ska enligt bestämmelser i den lagen omedelbart förstöras när en kontroll av om fingeravtryck och ansiktsbild som tagits upp motsvarar dem som finns i eller på en handling har genomförts. Som utgångspunkt kommer dessa uppgifter därmed inte att ingå i en allmän handling. Med denna utgångpunkt innebär paragrafen i praktiken endast att tystnadsplikt gäller för fingeravtryck och ansiktsbild som tagits upp med stöd av lagen samt för de biometriska uppgifter som tagits fram ur dessa, om personal hos en myndighet får del av en sådan uppgift.

8 §

Den tystnadsplikt som följer av 1, 2, 4, 5, 5 a, 7 d och 7 g §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Paragrafen ändras genom att den nya 5 a § läggs till. Övervägandena finns i avsnitt 25.2.2.

Ändringen innebär att den tystnadsplikt som följer av 5 a § inskränker rätten att meddela och offentliggöra uppgifter enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

Kommittédirektiv 2025:22

Säkrare verifiering av identitet

Beslut vid regeringssammanträde den 6 mars 2025.

Sammanfattning

En särskild utredare ska analysera och lämna förslag som stärker kopplingen mellan fastställd grundidentitet och verifiering av identitet. Syftet är att skapa en effektivare och säkrare process vid verifiering av identitet som utgår från biometriska uppgifter. Förslagen ska bidra till en effektiv, tillförlitlig och ändamålsenlig identitetsförvaltning i Sverige.

Utredaren ska bl.a.

- lämna förslag som stärker kopplingen mellan fastställd grundidentitet och verifiering av identitet med grund i biometriska uppgifter och i det sammanhanget undersöka lämpligheten med ett system med en unik identitetsnyckel,
- undersöka vilket eller vilka tekniska stöd som behövs för att stärka kopplingen mellan grundidentitet och verifiering av identitet,
- analysera vilka risker som behandlingen av personuppgifter kan innebära och göra nödvändiga säkerhetsanalyser,
- lämna förslag om vilken eller vilka myndigheter som ska ansvara för de uppgifter som behöver utföras, och
- vid behov omhänderta förslag som identifierats i pågående myndighetsuppdrag.

Uppdraget ska redovisas senast den 31 augusti 2026.

Svensk identitetsförvaltning

Ansvaret för identitetsförvaltningen i Sverige är delat mellan olika aktörer som var och en har begränsade ansvarsområden. Att fastställa identitet kan beskrivas med följande fyra delmoment: fastställande av grundidentitet, registrering av identitet, utfärdande av identitetshandling och verifiering av identitet.

Fastställande av grundidentitet

Fastställande av grundidentitet sker i samband med födelsen för barn som föds och ska folkbokföras i Sverige. Skatteverket fastställer också identiteten i samband med folkbokföring, när en person anmäler inflyttning till Sverige, och i samband med tilldelning eller förnyelse av samordningsnummer. Vid inflyttning och tilldelning av samordningsnummer med uppgift om styrkt identitet, utförs identitetskontroll vid personlig inställelse där den enskilde på begäran är skyldig att överlämna en identitetshandling och låta Skatteverket ta fingeravtryck och ansiktsbild i digitalt format för att kontrollera att dessa motsvarar dem som finns i handlingen. Identitetskontrollen genomförs i de flesta fall vid något av de servicekontor som drivs av Statens servicecenter. När det gäller tredjelandsmedborgare som ansöker om uppehållstillstånd i Sverige, fastställer Migrationsverket identiteten. Vid prövningen krävs en kontroll av om personen redan förekommer under en befintlig identitet i Sverige.

Registrering av identitet

Även registreringen av identitetsuppgifter utförs av olika myndigheter. Skatteverket ansvarar för att registerföra identitetsuppgifter i folkbokföringsdatabasen. Informationen från folkbokföringsdatabasen förmedlas till offentliga aktörer via Skatteverkets system för distribution av folkbokföringsuppgifter (Navet) och till privata aktörer via det statliga personadressregistret (SPAR). Migrationsverket registrerar identitetsuppgifter i den centrala utlänningsdatabasen. Det finns också andra databaser och register på myndighetsspecifik, nationell och internationell nivå där identitetsuppgifter registreras och utbyts

mellan myndigheter i olika situationer och syften, t.ex. Schengen Information System (SIS), Visa Information System (VIS) och Eurodac.

Utfärdande av identitetshandling

För att en person som fått sin identitet fastställd och registrerad ska kunna verifiera sig hos olika myndigheter behövs någon form av fysisk eller elektronisk id-handling som kan styrka kopplingen mellan personen och den registrerade grundidentiteten. Det finns i dag flera statliga och privata aktörer som utfärdar fysiska legitimationer och e-legitimationer. Polismyndigheten är passmyndighet och utfärdar även nationella id-kort. Vissa utlandsmyndigheter är passmyndighet utom riket. Skatteverket utfärdar id-kort till folkbokförda och Transportstyrelsen utfärdar körkort. I fråga om e-legitimationer utfärdas dessa i dagsläget endast av privata aktörer. Myndigheten för digital förvaltning (Digg) granskar och godkänner e-legitimationer som används i digitala tjänster inom offentlig sektor. Digg ansvarar också för eIDAS-noden som möjliggör e-legitimering över landsgränserna. I Regeringskansliet bereds för närvarande flera förslag om nya id-handlingar, bl.a. ett nytt statligt identitetskort (SOU 2019:14), en statlig e-legitimation (SOU 2023:61) och en digital identitetsplånbok (SOU 2024:45).

Verifiering av identitet

Slutligen kopplar svenska myndigheter ihop identitetsuppgifterna från en befintlig grundidentitet med personen som myndigheten möter i en process för verifiering. Det sker genom att personen identifierar sig med en fysisk eller elektronisk id-handling som har utfärdats.

Brister och problembild

Dagens ordning i identitetsförvaltningen försvårar överblick och kontroll. Brister i samordning, styrning och utveckling av svensk identitetsförvaltning har öppnat upp för fusk, identitetsmissbruk och annan brottslighet, vilket bedöms generera stora kostnader för staten och samhället.

Bristerna i identitetsförvaltningen innebär att det är svårt att i praktiken säkert veta vem individen bakom en identitetshandling och e-legitimation faktiskt är, vilket har bidragit till att problemen med organiserad brottslighet, utanförskap och bidragsbrottslighet är omfattande. Olika former av identitetsmissbruk förekommer bl.a. vid bedrägerier, arbetslivskriminalitet och brott mot välfärdssystemen. Redan vid fastställande av grundidentitet kan det finnas behov av att stärka myndigheternas arbete i syfte att uppnå en mer enhetlig hantering. Andra brister är att förekomsten av multipla identiteter i folkbokföringsdatabasen kan få stora konsekvenser genom de spridningseffekter som uppgifter ur folkbokföringsdatabasen har i samhället. I dag bedöms risken för utnyttjade och kapade identiteter vara mer omfattande än renodlat falska identiteter.

Bristerna har påtalats, bl.a. av Samverkansrådet mot terrorism 2021, Utredningen om folkbokföring, samordningsnummer och identitetsnummer (SOU 2021:57) och samverkansinitiativet MUR (Motståndskraft hos utbetalande och rättsvårdande myndigheter mot missbruk och brott i välfärdssystemen). I delbetänkandet En säker och tillgänglig statlig e-legitimation (SOU 2023:61) framhåller representanter för Skatteverket och Försäkringskassan i särskilda yttranden behovet av att ta ett samlat grepp om identitetsförvaltningskedjan. Riksrevisionen lämnade i juni 2024 en rapport om fastställande av identitet vid statliga myndigheter (RiR 2024:12) där Riksrevisionens övergripande bedömning är att myndigheternas insatser inte är tillräckligt effektiva för att säkerställa att en korrekt och unik identitet fastställs.

En sammanhållen identitetsförvaltning med ökad användning av biometri

Svensk identitetsförvaltning ska vara tillförlitlig och solid, och inte kunna utnyttjas för olika former av missbruk och brottslighet (skr. 2023/24:67). Ett gediget arbete behöver bedrivas för att skapa ett system för identiteter som är ändamålsenligt, sammanhängande, säkert och hållbart över tid. I detta ingår att säkerhetsnivån på fysiska och digitala handlingar som används i identifieringssyfte behöver vara anpassad efter de behov av säkrare kontrollfunktioner som den ökande digitaliseringen i samhället medför. Ett sätt att förstärka identitetsförvaltningen och motverka missbruk av personuppgifter är att

använda biometriska uppgifter i större utsträckning än i dag för identifiering, registrering och verifiering av individer som uppehåller sig i Sverige.

I dag agerar myndigheterna primärt baserat på den information som finns tillgänglig i deras egna system i stället för utifrån en helhetsbild. Till viss del har det motiverats av integritetshänsyn. Samtidigt har såväl samhället i stort som hotet från organiserad brottslighet utvecklats på ett sätt som gör att synen på vad som utgör hot mot den personliga integriteten och hur människors integritet bäst skyddas behöver omprövas. Behovet av att skyddas från brott och otrygghet, liksom att värna Sveriges funktionssätt och välfärd, har blivit allt starkare. För att öka myndigheternas förmåga att förebygga och bekämpa brott behövs ett perspektivskifte i synen på information.

Information som finns hos de olika myndigheterna, åtminstone inom staten, bör ses som en samlad strategisk resurs som i större utsträckning ska kunna tillgängliggöras och användas av den myndighet som behöver den.

Redan initierade åtgärder

Flera initiativ pågår för att stärka möjligheterna till identifiering, verifiering och kontroll i verksamheter som utfärdar id-handlingar samt bedömer och förlitar sig på identitetsuppgifter. Exempelvis bereds förslaget från 2017 års ID-kortsutredning om ett nytt regelverk för statliga identitetshandlingar (SOU 2019:14) i Regeringskansliet. Förslaget innebär att staten framöver ska utfärda två allmängiltiga och säkra identitetshandlingar: pass och ett statligt identitetskort. Handlingarna ska benämnas statliga identitetshandlingar.

Utredningen för säker och tillgänglig digital identitet har lämnat förslag på hur en kostnadseffektiv statlig e-legitimation på högsta tillitsnivå kan utformas och tillhandahållas av en statlig myndighet (SOU 2023:61). Utredningen föreslog att den statliga e-legitimationen ska tillhandahållas på ett kontaktlöst aktivt kort men så snart som möjligt bör tillhandahållas på ett statligt utfärdat identitetskort. Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet (den reviderade eIDAS-förordningen) innebär i praktiken en skyldighet för

medlemsstaterna att tillhandahålla en e-legitimation på högsta tillitsnivå senast fjärde kvartalet 2026. Förordningen innehåller också en skyldighet att acceptera utländska och anmälda e-legitimationer i nationella digitala tjänster samt att tillhandahålla en digital identitetsplånbok. I budgetpropositionen för 2025 aviserades att Polismyndigheten får uppdraget att utfärda en statlig e-legitimation på högsta tillitsnivå och Myndigheten för digital förvaltning får i uppdrag att utfärda en digital identitetsplånbok.

Utredningen om stärkt återvändandeverksamhet har bl.a. lämnat förslag om att Migrationsverket ska få ta upp och lagra fingeravtryck och fotografier i större utsträckning än i dag. Enligt förslagen ska fingeravtryck och fotografier få tas upp och lagras från alla som söker uppehållstillstånd i Sverige – oavsett grund – samt i ärenden om avvisning eller utvisning (SOU 2024:80). Utredningen föreslår också att fingeravtryck och fotografier ska få tas upp – och i vissa fall få lagras – i ärenden om medborgarskap. En förutsättning för att ta upp och lagra fingeravtryck ska vara att utlänningen har fyllt sex år. Utredningen föreslår vidare att de fingeravtryck och fotografier som lagras i Migrationsverkets register ska få användas för fler ändamål än i dag, bl.a. i alla ärenden om uppehållstillstånd, i ärenden om medborgarskap, för att verifiera en utlännings identitet vid vissa kontroller och vid utfärdande av uppehållstillståndskort. De lagrade uppgifterna ska även få användas för kontroller mot Polismyndighetens fingeravtrycks- och signalementsregister, t.ex. i medborgarskapsärenden.

En utredning om utökade befogenheter för Skatteverket inom brottsbekämpning och folkbokföring har fått i uppdrag att bl.a. se över om Skatteverkets möjligheter att använda biometriska uppgifter inom folkbokföringsverksamheten kan förstärkas (dir. 2023:134). Utredaren ska också analysera och ta ställning till om det finns ett behov av utbyte av ansiktsbilder och fingeravtryck mellan Migrationsverket och Skatteverket samt analysera och ta ställning till om Polismyndigheten ska få göra biometriska jämförelser med de uppgifter som behandlas hos Skatteverket. Uppdraget ska redovisas senast den 28 maj 2025.

Regeringen har beslutat om uppdrag till flera myndigheter att samarbeta mer och att dela och använda mer information och kompetens i arbetet med identitetskontroller. Skatteverket, Migrationsverket och Polismyndigheten har fått i uppdrag att utveckla det operativa samarbetet för att motverka identitetsmissbruk (Fi2024/02215). Myndig-

heternas arbete ska bl.a. inriktas mot de utmaningar som finns vad gäller en enhetlig hantering vid fastställande av grundidentitet samt att upprätthålla och stärka kompetensen om identitetsfrågor. En delredovisning om hur ett nationellt kompetenscentrum för identitetsfrågor kan inrättas ska lämnas den 31 mars 2025. Vidare har Skatteverket, Migrationsverket, Polismyndigheten och Statens servicecenter fått i uppdrag att stärka samarbetet för att upprätthålla och sprida kompetens om identitetsfrågor (Fi2024/02214). Det innebär bl.a. att om myndigheterna identifierar hinder i regelverket för ett effektivt samarbete ska de lämna en tydlig problembild och konsekvensanalys. Uppdraget ska redovisas senast den 13 juni 2025.

Uppdraget att stärka kopplingen mellan fastställd grundidentitet och verifiering av identitet

Förutsättningarna för identitetsförvaltningen i Sverige behöver stärkas. En tillförlitlig identitetsförvaltning syftar både till att skapa trygghet och säkerhet för medborgarna och till att motverka missbruk och bedrägerier som drabbar alla delar av samhället. Den ökade internationella rörligheten och digitaliseringen medför behov av en översyn av hur verifieringen av identiteten på en person som vistas i Sverige kan kopplas till grundidentiteten.

Ett system för säkrare verifiering av identitet

Biometriska uppgifter är personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtryck.

Regeringens arbete med att stärka identitetsförvaltningen innefattar bl.a. utökad användning av biometriska uppgifter i Polismyndighetens, Migrationsverkets och Skatteverkets respektive verksamheter. De förslag som lämnats och den utredning som pågår innebär att biometriska uppgifter ska kunna lagras och användas av myndigheterna i högre utsträckning än i dag.

Biometriska uppgifter kan användas för att identifiera en person som myndigheterna möter. Biometriska uppgifter kan jämföras med

lagrade biometriska uppgifter från andra registrerade identiteter i myndigheternas register. Behandlingen av biometriska uppgifter syftar då till att upptäcka om den person som lämnat det biometriska underlaget också uppträtt under andra identiteter i andra ärenden. Biometriska uppgifter som finns lagrade i en identitetshandling kan också jämföras mot personen som inställer sig för identitetskontroll, i syfte att stärka kontrollen av att personen myndigheten möter också är den person för vilken handlingen har utfärdats. Det rättsliga och tekniska stödet för sådan kontroll och lagring finns hos ett begränsat antal myndigheter men fler aktörer har behov av att få ta del av information från grundidentifieringen för att förstärka sin kontroll i verifieringssteget.

Kopplingen till den fastställda grundidentiteten behöver stärkas vid verifiering av identitet med hjälp av biometriska uppgifter. Det bör därför övervägas hur ett sådant system kan utformas och införas på ett kostnadseffektivt sätt i syfte att bidra till en säkrare process vid verifiering av identitet. De förslag som lämnats i tidigare och pågående utredningar om utökade möjligheter till insamling och lagring av biometriska uppgifter ska vara utgångspunkt för analysen. Det kan finnas behov av att ta ställning till och utreda om gällande rätt och föreslagna ändringar är tillräckliga för ändamålet verifiering av identitet. Det kan även finnas behov av att ta ställning till förslag eller problembilder som myndigheterna identifierat inom ramen för de pågående uppdragen om att samarbeta mer i arbetet med identitetskontroller (Fi2024/02214 och Fi2024/02215).

Det behöver vidare övervägas vilken personkrets som bör komma i fråga. Målsättningen bör vara att så många som möjligt som vistas i Sverige på sikt ska kunna ingå i ett nytt system för en säkrare verifiering av identitet.

Ett alternativ kan vara den lösningshypotes som utforskats av samverkansinitiativet MUR med ett gemensamt identitetsindex. Identitetsindexet bygger på biometri men sprids som en unik identitetsnyckel som kan kopplas till t.ex. personnummer, samordningsnummer, beslut och inloggningar med e-legitimation. Enligt hypotesen ska den unika identitetsnyckeln kunna skapas för en person som flyttar till Sverige, tilldelas ett samordningsnummer eller beviljas ett pass eller statligt id-kort. Identitetsnyckeln skulle kunna lagras och spridas tillsammans med personens identitetsbeteckning och även lagras i

individens identitetshandlingar, såväl fysiska som digitala. Avsikten är att identitetsnyckeln ska kunna användas vid verifiering av identitet.

Ett system med en unik identitetsnyckel behöver analyseras närmare. Det behöver bl.a. belysas om ett sådant system är tekniskt och rättsligt möjligt att införa och vilka fördelar och nackdelar en sådan lösning kan innebära. Vidare behöver det analyseras om en identitetsnyckel bestående av en numerär kod baserad på biometriska uppgifter är att betrakta som biometriska uppgifter i sig och således en känslig personuppgift. Det behöver också analyseras om och i så fall hur identitetsnyckeln på ett säkert och effektivt sätt skulle kunna spridas till andra aktörer för att användas i verifieringsprocessen samt om identitetsnyckeln bör lagras i en identitetshandling. Ett system med en unik identitetsnyckel behöver jämföras med andra alternativa lösningar.

Utredaren ska därför

- utgå från de förslag som lämnats i tidigare och pågående utredningar om utökade möjligheter till insamling och lagring av biometriska uppgifter,
- ta ställning till hur kopplingen mellan fastställd grundidentitet och verifiering av identitet kan stärkas och i det sammanhanget undersöka lämpligheten med ett system med en unik identitetsnyckel baserad på biometriska uppgifter,
- föreslå hur ett system på ett kostnadseffektivt sätt kan utformas, införas och användas,
- vid behov föreslå att information om en fastställd grundidentitet ska kunna delas med statliga myndigheter, andra offentliga aktörer respektive privata aktörer,
- vid behov omhänderta förslag som har identifierats i pågående myndighetsuppdrag i syfte att säkerställa en enhetlighet vid fastställande av grundidentitet, och
- lämna fullständiga författningsförslag.

Dataskydd och sekretess

Behandlingen av biometriska uppgifter innebär särskilda risker för intrång i skyddet för den personliga integriteten enligt regeringsformen, Europakonventionen för mänskliga rättigheter och EU:s rättighetsstadga. Behovet av den föreslagna regleringen måste vägas mot skyddet för grundläggande fri- och rättigheter. Om de förslag som utredaren lämnar begränsar grundläggande fri- och rättigheter måste förslagen uppfylla förutsättningarna för att sådana begränsningar ska få göras.

Frågor om såväl sekretess som dataskydd behöver övervägas när det gäller förslagens utformning. För att kunna bedöma om förslagen är förenliga med dataskyddsregleringen samt behovet av kompletterande nationell reglering finns bl.a. behov av att närmare analysera och kartlägga vilken personuppgiftsbehandling som aktualiseras, vilka integritetsrisker den medför samt redovisa vilka bedömningar som görs när det gäller skyddsåtgärder, bl.a. i fråga om sekretess och uppgifternas bevarande.

Förslagen ska vara förenliga med EU-rätten och grundläggande fri- och rättigheter.

Utredaren ska därför

- bedöma vilka risker som behandlingen av personuppgifter i ett system med stärkt koppling mellan fastställd grundidentitet och verifiering av identitet kan innebära, ta hänsyn till skyddet för den personliga integriteten och göra en integritetsanalys,
- analysera om förslagen är ändamålsenliga och proportionerliga i förhållande till skyddet för grundläggande fri- och rättigheter,
- bedöma om den behandling av personuppgifter som förslagen ger upphov till är förenlig med det EU-rättsliga dataskyddsregelverket och vid behov föreslå åtgärder och lämna författningsförslag som säkerställer att kraven i EU:s dataskyddslagstiftning för behandlingen av personuppgifter uppfylls,
- bedöma eventuella behov av skyddsåtgärder, och
- lämna nödvändiga författningsförslag.

Säkerhetsfrågor och andra förutsättningar för tekniska lösningar

Möjligheter och begränsningar när det gäller tekniska lösningar är av betydelse för vilket system som är lämpligt, proportionerligt och ändamålsenligt att införa. Utredaren ska därför inhämta uppgifter om vilket tekniskt stöd som kan behövas för att stärka kopplingen mellan fastställd grundidentitet och verifiering av identitet. Det är av vikt att processer utformas på ett sådant sätt att myndigheternas verksamhet skyddas, att uppgifter inte kan manipuleras och att enskildas personuppgifter behandlas på ett säkert sätt. Detta ställer höga krav på tillförlitliga, säkra och robusta lösningar för it-system. Den eller de myndigheter som får ansvaret för systemet kan komma att behöva utveckla nya tekniska lösningar alternativt anpassa befintlig teknik.

För att information om den fastställda grundidentiteten ska kunna distribueras och användas behövs en bakomliggande digital infrastruktur, t.ex. mot vilken en identitetsnyckel kan verifieras. Utredaren behöver därför även ta ställning till vilka tekniska lösningar som kan komma att behövas för dessa ändamål.

Utredaren ska därför

- kartlägga vilket tekniskt stöd som kan behövas för att stärka kopplingen mellan fastställd grundidentitet och verifiering av identitet,
- identifiera och analysera risker kopplade till informations- och cybersäkerhet samt lämna förslag för att hantera riskerna,
- identifiera och analysera risker kopplade till införandet av ett stärkt system vid verifiering av identitet utifrån kapacitetsbehov och krav på robusthet och lämna förslag till åtgärder för att hantera dessa risker,
- redogöra för behovet av tekniska lösningar för att kunna distribuera information till statliga och andra aktörer, och
- beräkna kostnaderna för utveckling och förvaltning av de tekniska lösningarna.

Ansvar och rollfördelning

En central fråga för ett system och andra förslag för att stärka kopplingen mellan fastställd grundidentitet och verifiering av identitet är vilken eller vilka myndigheter som ska ansvara för de uppgifter som behöver utföras. Ansvaret för identitetsförvaltningen är i dag uppdelat mellan flera olika aktörer och regeringen har konstaterat att ett sätt att förstärka identitetsförvaltningen är att begränsa antalet aktörer (skr. 2023/24:67). Det behöver bl.a. belysas vilka synergieffekter som kan finnas med andra uppgifter som myndigheterna ansvarar för i dag eller kan komma att få ansvar för i takt med genomförandet av förslag som bereds. Även frågor om kostnadseffektivitet, tillgänglighet och myndigheternas möjlighet att tillhandahålla service måste beaktas. Samtidigt är myndigheternas kapacitet att tillgodose krav på säkerhet och andra tekniska förutsättningar en viktig fråga vid övervägandena om hur ansvarsfördelningen ska se ut. I det sammanhanget måste det beaktas att uppgifter om identiteter kan vara mycket skyddsvärda. Såväl totalförsvarsplaneringen som säkerhetsskydd och informationssäkerhetsfrågor behöver belysas i övervägandena om ansvarsfördelningen. Exempelvis kan det med hänsyn till att det rör sig om skyddsvärd information finnas skäl att begränsa antalet ansvariga myndigheter.

Utredaren ska därför

- lämna förslag på vilken eller vilka myndigheter som ska ansvara för systemet och distributionen av information till andra aktörer, och
- lämna nödvändiga författningsförslag.

Konsekvensbeskrivningar

Utredaren ska redovisa konsekvenserna av de förslag som läggs fram i enlighet med kommittéförordningen (1998:1474) och förordningen (2024:183) om konsekvensutredningar. Utredaren ska också redovisa förslagens betydelse för arbetet med att förebygga och i övrigt motverka brottslighet. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras.

Kontakter och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som bedrivs inom Regeringskansliet, inom EU och inom andra utredningar och kommittéer. Utredaren ska särskilt följa beredningen av förslaget till ett nytt statligt identitetskort samt följa och beakta resultatet från myndigheternas arbete i uppdragen att stärka samarbetet för att upprätthålla och sprida kompetens om identitetsfrågor (Fi2024/02215) och att utveckla det operativa samarbetet för att motverka identitetsmissbruk (Fi2024/02214).

Under genomförandet av uppdraget ska utredaren i den utsträckning det behövs samråda med och inhämta upplysningar från de myndigheter och andra aktörer som kan vara berörda.

Uppdraget ska redovisas senast den 31 augusti 2026.

(Finansdepartementet)

Statens offentliga utredningar 2026

Kronologisk förteckning

1. Skatteincitament för forskning och utveckling – ett nytt incitament baserat på utgifter för FoU-personal. Fi.
2. 710 miljoner skäl till reformer. Ju.
3. Genomförande av plattformsdirektivet. A.
4. Rektor i fokus – förutsättningar för ett pedagogiskt ledarskap. U.
5. Utvidgad avdragsrätt för sponsring m.m. Fi.
6. En nationell digital infrastruktur i hälso- och sjukvården. Styrning med tydliga roller och ansvar för aktörerna. S.
7. Förstärkt uppföljning och utvärdering av folkhälsopolitiken.
   Del I: Effektivare folkhälsoinsatser genom hälsoekonomiska analyser.
   Del II: Utvärdering av alkoholpolitikens styrmedel. S.
8. Rättssäker samhällsvård för barn och unga. S.
9. Registrering av EES-medborgare. Ju.
10. Ökade möjligheter till tillgångsinriktad brottsbekämpning. Del 1 och 2. Ju.
11. Om överföring av Första AP-fondens verksamhet och tillgångar till Tredje och Fjärde AP-fonderna. Fi.
12. Om överföring av Sjätte AP-fondens verksamhet och tillgångar till Andra AP-fonden. Fi.
13. Straffansvar för deltagande i och samröre med kriminella sammanslutningar. Ju.
14. Ädelmetallutredningen – en moderniserad reglering av handel med ädelmetallarbeten. KN.
15. Marken, vattnet, tankarna. Konsekvenser för samer av svensk politik. Volym 1 och 2. Ku.
16. Försvarsexportinitiativ. För gemensam säkerhet. Fö.
17. Öresundsförbindelser 2050 – behov av kapacitet, redundans och svenskt-danskt samarbete. LI.
18. Odlingstorv och klimatet. Fi.
19. Stärkt tillsyn och uppföljning – förslag för att motverka oegentlig läkemedelsförskrivning. S.
20. Belägg för broms? Åtgärder för starkare incitament till lägre kommunalskattesatser. Fi.
21. Återkallelse av svenskt medborgarskap. Ju.
22. Stärkt läkemedelsförsörjning i samverkan. Nationella åtgärder för fördelning, omfördelning och inköp vid brist. S.
23. Tolkavgift och förbud mot barntolkning. A.
24. Mervärdesskatt vid uthyrning och överlåtelse av fastighet. Fi.
25. Ett smittskydd för framtiden. S.
26. Digitala verktyg inom bolagsrätten. Genomförande av EU:s direktiv om ytterligare digitalisering inom bolagsrätten. Ju.
27. Lättnader i kraven på hållbarhetsrapportering. Ju.
28. Tillgång till passageraruppgifter i brottsbekämpningen. Ju.
29. Förbud mot uppfödning av djur för pälsproduktion. LI.
30. Mer flexibla regler om verkställighet av häktning och fängelsestraff. Ju.
31. Ett investeringsprogram för kultur. Ku.
32. Att säga ja! Kommunernas förutsättningar att ta emot stora företagsetableringar och företagsexpansioner. KN.
33. Vägen mot utfasning. Styrmedel för ett fossilfritt samhälle. KN.

34. Nya nätbrott och andra åtgärder för genomförandet av direktivet om bekämpning av våld mot kvinnor och våld i nära relationer. Volym 1 & 2. Ju.
35. En åldersgräns för barns tillgång till sociala medier. S.
36. Bättre förutsättningar att inkludera personer med nedsatt beslutsförmåga i medicinsk forskning. S.
37. Förutsättningar för en likvärdig och språkutvecklande förskola. U.
38. Behovsstyrd vård. S.
39. Ett nytt system för återkrav inom socialförsäkringen. S.
40. Ny kärnkraft i Sverige – moderna regler för beredskap och skadeståndsansvar. KN.
41. Jämställdhet i en föränderlig tid – nuläge och vägar framåt. Volym 1 & 2. A.
42. Ett nytt regelverk för granskning av utländsk finansiering av trossamfund och andra verksamheter. Volym 1 och 2. Ju.
43. Åtgärder mot överskuldsättning. Fi.
44. En stärkt förmåga till modern datadelning – integritetsfrämjande teknik i offentlig förvaltning. Fi.
45. Effektiva ingripanden mot brott i cybermiljö. Ju.
46. Ett sammanhållet, robust och konkurrenskraftigt Sverige – framtidens politik för utveckling i landsbygder och regioner. LI.
47. Rätt till ersättning vid avveckling av kärnkraft på grund av politiska beslut – reaktorer som inte tagits i drift. KN.
48. Tillträdesförbud. Ju.
49. Traditionell eller rationell. En premiepension som kan nå målen. S.
50. En ny speciallärarutbildning. U.
51. Fri att lära och leva. Insatser mot hedersrelaterat våld och förtryck i förskolan, skolan och fritidshemmet. U.
52. En reform av den statliga barn- och ungdomsvården. Volym 1, 2 och 3. S.
53. Parallella samhällsstrukturer – ett kunskapsunderlag för förbättrad integration och minskat utanförskap. A.
54. Stärkt egendomsskydd i regeringsformen. Ju.
55. Säkrare verifiering av identitet. Volym 1 och 2. Fi.

Statens offentliga utredningar 2026

Systematisk förteckning

Att säga ja! Kommunernas förutsättningar att ta emot stora företagsetableringar och företagsexpansioner. [32]

Vägen mot utfasning. Styrmedel för ett fossilfritt samhälle. [33]

Ny kärnkraft i Sverige – moderna regler för beredskap och skadeståndsansvar. [40]

Rätt till ersättning vid avveckling av kärnkraft på grund av politiska beslut – reaktorer som inte tagits i drift. [47]

Kulturdepartementet

Marken, vattnet, tankarna. Konsekvenser för samer av svensk politik. Volym 1 och 2. [15]

Ett investeringsprogram för kultur. [31]

Landsbygds- och infrastrukturdepartementet

Öresundsförbindelser 2050 – behov av kapacitet, redundans och svenskt-danskt samarbete. [17]

Förbud mot uppfödning av djur för pälsproduktion. [29]

Ett sammanhållet, robust och konkurrenskraftigt Sverige – framtidens politik för utveckling i landsbygder och regioner. [46]

Socialdepartementet

En nationell digital infrastruktur i hälso- och sjukvården. Styrning med tydliga roller och ansvar för aktörerna. [6]

Förstärkt uppföljning och utvärdering av folkhälsopolitiken. Del I: Effektivare folkhälsoinsatser genom hälsoekonomiska analyser. Del II: Utvärdering av alkoholpolitikens styrmedel. [7]

Rättssäker samhällsvård för barn och unga. [8]

Stärkt tillsyn och uppföljning – förslag för att motverka oegentlig läkemedelsförskrivning. [19]

Stärkt läkemedelsförsörjning i samverkan. Nationella åtgärder för fördelning, omfördelning och inköp vid brist. [22]

Ett smittskydd för framtiden. [25]

En åldersgräns för barns tillgång till sociala medier. [35]

Bättre förutsättningar att inkludera personer med nedsatt beslutsförmåga i medicinsk forskning. [36]

Behovsstyrd vård. [38]

Ett nytt system för återkrav inom socialförsäkringen. [39]

Traditionell eller rationell. En premiepension som kan nå målen. [49]

En reform av den statliga barn- och ungdomsvården. Volym 1, 2 och 3. [52]

Utbildningsdepartementet

Rektor i fokus – förutsättningar för ett pedagogiskt ledarskap. [4]

Förutsättningar för en likvärdig och språkutvecklande förskola. [37]

En ny speciallärarutbildning. [50]

Fri att lära och leva. Insatser mot hedersrelaterat våld och förtryck i förskolan, skolan och fritidshemmet. [51]