Regeringens proposition 2025/26:250

En statlig e-legitimation

Prop. 2025/26:250

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 7 maj 2026

Ebba Busch

Erik Slottner
(Finansdepartementet)

Propositionens huvudsakliga innehåll

I propositionen föreslås en ny lag om statlig e-legitimation och elektronisk identifiering. En statlig e-legitimation ska kunna ges till personer med svenskt medborgarskap, utlänningar som är folkbokförda i Sverige och personer som har ett s.k. immunitetsnummer och som omfattas av lagen (1976:661) om immunitet och privilegier i vissa fall. För att få en statlig e-legitimation krävs det att sökanden har fyllt eller innevarande kalenderår ska fylla nio år. Förslaget syftar till att säkra samhällets tillgång till elektronisk identifiering och säkerställa att kraven i EU:s förordning om elektronisk identifiering uppfylls.

Den nya lagen föreslås träda i kraft den 1 december 2026.

Innehållsförteckning

1 Förslag till riksdagsbeslut

Regeringens förslag:

Riksdagen antar regeringens förslag till lag om statlig e-legitimation och elektronisk identifiering.

2 Förslag till lag om statlig e-legitimation och elektronisk identifiering

Härigenom föreskrivs[1] följande.

1 kap. Allmänna bestämmelser

Lagens innehåll och förhållande till annan reglering

1 § Denna lag innehåller bestämmelser om en statlig e-legitimation och krav på erkännande av vissa medel för elektronisk identifiering.

Bestämmelser om medel för elektronisk identifiering finns i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, här benämnd EU:s förordning om elektronisk identifiering, och i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

2 § Denna lag kompletterar, i den del den avser behandling av personuppgifter, 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 EU:s dataskyddsförordning.

Vid behandlingen 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 föreskrifter som regeringen har meddelat i anslutning till denna lag.

Ord och uttryck

3 § Med autentisering, elektronisk identifiering, medel för elektronisk identifiering och nättjänst avses i denna lag detsamma som i EU:s förordning om elektronisk identifiering.

4 § Med en offentlig aktör avses i denna lag

1. en statlig eller kommunal myndighet, eller en beslutande församling i en kommun eller region,
2. en sammanslutning som inrättats särskilt för att tillgodose behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär, och som består av en eller flera myndigheter eller församlingar som anges i 1,
3. en privat aktör som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad och som

[1] Se Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

a) aktören bedriver i egenskap av enskild huvudman inom skolväsendet eller huvudman för en sådan internationell skola som avses i 24 kap. skollagen (2010:800),

b) utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen (2017:30) eller tandvård enligt tandvårdslagen (1985:125),

c) bedrivs enligt socialtjänstlagen (2025:400), lagen (1988:870) om vård av missbrukare i vissa fall, lagen (1990:52) med särskilda bestämmelser om vård av unga eller lagen (1993:387) om stöd och service till vissa funktionshindrade, eller

d) utgör personlig assistans som utförs med assistansersättning enligt 51 kap. socialförsäkringsbalken, eller

4. en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina, och som till största delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller av utbildning på forskarnivå.

En statlig e-legitimation

5 § Den statliga e-legitimationen är ett medel för elektronisk identifiering.

Utfärdande myndighet

6 § Den statliga e-legitimationen utfärdas av utfärdande myndighet.

Polismyndigheten är utfärdande myndighet inom riket.

Utom riket fullgör beskickningar och karriärkonsulat uppgifter som utfärdande myndighet i den utsträckning som beslutas av regeringen eller den myndighet som regeringen bestämmer.

7 § Utfärdande myndighet ska fullgöra de uppgifter som anges i denna lag och i föreskrifter som har meddelats i anslutning till lagen.

Vem som kan få en statlig e-legitimation

8 § En statlig e-legitimation får utfärdas till en svensk medborgare som har fyllt eller som innevarande kalenderår ska fylla nio år.

9 § En statlig e-legitimation får utfärdas till en utlänning som har fyllt eller som innevarande kalenderår ska fylla nio år och som

1. är folkbokförd i Sverige enligt folkbokföringslagen (1991:481), eller

2. har tilldelats ett personnummer enligt 18 b § samma lag och som omfattas av lagen (1976:661) om immunitet och privilegier i vissa fall.

Giltighetstiden

10 § En e-legitimation ska utfärdas med en giltighetstid om fem år. Om sökanden inte har fyllt tolv år ska giltighetstiden vara tre år.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att den statliga e-legitimationen i särskilt angivna fall ska ha en kortare giltighetstid.

Villkor för användningen av den statliga e-legitimationen

11 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om villkor för användningen av den statliga e-legitimationen.

2 kap. Ansökan, utfärdande och återkallelse

En ansökan krävs

1 § Den statliga e-legitimationen utfärdas efter ansökan.

Om sökanden är under arton år krävs det vårdnadshavares medgivande, om det inte finns synnerliga skäl för utfärdandet.

Personlig inställelse

2 § Den som ansöker om en statlig e-legitimation ska lämna ansökan vid personlig inställelse.

Styrkande av identitet

3 § Sökanden ska vid ansökan styrka sin identitet och övriga personuppgifter som krävs för att en statlig e-legitimation ska utfärdas.

Ansiktsbild och fingeravtryck

4 § Sökanden ska låta den utfärdande myndigheten ta sökandens ansiktsbild och fingeravtryck i samband med ansökan om statlig e-legitimation.

Sökanden ska även låta den utfärdande myndigheten ta sökandens ansiktsbild och fingeravtryck vid utlämnande av den statliga e-legitimationen, om den utfärdande myndigheten begär det.

5 § Ansiktsbilden som tas i samband med ansökan enligt 4 § första stycket ska sparas i ett lagringsmedium i bäraren av den statliga e-legitimationen. Om fingeravtryck har tagits ska även dessa sparas i lagringsmediet.

6 § Om sökanden styrker sin identitet med en identitetshandling som är försedd med en ansiktsbild eller innehåller ett lagringsmedium där ansiktsbild eller fingeravtryck är sparade, får den utfärdande myndigheten kontrollera att dessa motsvarar den ansiktsbild och de fingeravtryck som tas enligt 4 §.

Den utfärdande myndigheten får även kontrollera att ansiktsbild och fingeravtryck som tas i samband med utlämnande enligt 4 § andra stycket motsvarar de som finns lagrade i den statliga e-legitimationen.

7 § De fingeravtryck som tas enligt 4 § första stycket och de biometriska uppgifter som tas fram ur dessa ska omedelbart förstöras när den statliga e-legitimationen har lämnats ut eller, om e-legitimationen inte har lämnats ut, när det har gått 90 dagar från den dag då den utfärdades. Om ett ansökningsärende har avslutats på något annat sätt ska uppgifterna också förstöras omedelbart.

Den ansiktsbild och de fingeravtryck som tas enligt 4 § andra stycket och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken ska omedelbart förstöras när kontrollen enligt 6 § andra stycket har genomförts.

Den ansiktsbild och de fingeravtryck som vid kontroll enligt 6 § tas fram ur ett lagringsmedium och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken ska omedelbart förstöras när kontrollen har genomförts.

Avslag av ansökan och utfärdande av statlig e-legitimation

8 § En ansökan om en statlig e-legitimation ska avslås om de krav som framgår av denna lag eller de föreskrifter som har meddelats i anslutning till lagen inte är uppfyllda och sökanden inte har följt en uppmaning att rätta till bristen. I annat fall ska den statliga e-legitimationen utfärdas och skyndsamt vara tillgänglig för utlämnande.

Återkallelse och spärr av statlig e-legitimation

9 § En statlig e-legitimation ska återkallas och spärras om

1. det fanns hinder mot att utfärda en e-legitimation vid tiden för utfärdandet och hindret fortfarande består,
2. någon väsentlig uppgift som en e-legitimation innehåller är felaktig,
3. det är nödvändigt av säkerhetsskäl,
4. den är utfärdad på en fysisk identitetshandling som därefter har upphört att gälla, eller
5. innehavaren har avlidit.

En statlig e-legitimation får även återkallas och spärras på begäran av innehavaren. Om begäran avser ett barn under arton år krävs det vårdnadshavares medgivande, om det inte finns synnerliga skäl för återkallelsen och spärren.

10 § En statlig e-legitimation ska, utöver i de fall som anges i 9 §, spärras

1. i samband med att en ny e-legitimation lämnas ut till sökanden, eller
2. när giltighetstiden har löpt ut.

Avgifter

11 § Utfärdande myndighet får ta ut avgifter för ansökan om statlig e-legitimation.

Rätt att meddela föreskrifter

12 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om förfarandet vid

1. ansökan,
2. utfärdande,
3. utlämnande, och
4. återkallelse och spärr.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen även meddela föreskrifter om den statliga e-legitimationens

1. innehåll, bärare och utformning i övrigt, och
2. aktivering.

Regeringen eller den myndighet som regeringen bestämmer får vidare meddela föreskrifter om

1. avgifter för ansökan om statlig e-legitimation, och
2. undantag från skyldigheten att lämna fingeravtryck enligt 4 §.

3 kap. Behandling av personuppgifter

Ändamålen med behandlingen

1 § Personuppgifter får behandlas av utfärdande myndighet om det är nödvändigt för att

1. handlägga ärenden om statlig e-legitimation,
2. föra ett register över ärenden om statlig e-legitimation, och
3. vidta åtgärder för en säker användning av statliga e-legitimationer.

2 § Personuppgifter som behandlas enligt 1 § får också behandlas av utfärdande myndighet

1. om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet, och
2. om det är nödvändigt för att lämna ut uppgifter i enlighet med lag eller förordning.

Personuppgifterna får även behandlas för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Begränsning av rätten att göra invändningar

3 § Artikel 21.1 i EU:s dataskyddsförordning om rätten att göra invändningar gäller inte vid sådan behandling som är tillåten enligt denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Säkerhetsåtgärder

4 § Tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter i verksamheten med den statliga e-legitimationen.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om

1. begränsningen av tillgången till personuppgifter enligt första stycket, och
2. säkerhetsåtgärder till skydd för personuppgifter.

Register över ärenden om statlig e-legitimation

5 § Polismyndigheten ska med hjälp av automatiserad behandling föra ett register över ärenden om statlig e-legitimation.

6 § Registret över ärenden om statlig e-legitimation får endast innehålla

1. namn, personnummer, samordningsnummer, medborgarskap, födelsedatum och kontaktuppgifter till sökanden,
2. ansiktsbilder som har tagits vid ansökan enligt 2 kap. 4 § första stycket och biometriska uppgifter som har tagits fram ur sådana bilder,
3. handlingar eller uppgifter från handlingar som har kommit in eller upprättats i ärenden om statlig e-legitimation,
4. uppgifter som rör handläggningen av ärenden om statlig e-legitimation, och
5. uppgifter om utfärdade statliga e-legitimationer.

Längsta tid som personuppgifter i registret får behandlas

7 § Personuppgifter i registret över ärenden om statlig e-legitimation får inte behandlas längre än tio år från utgången av det kalenderår som det ärende som uppgifterna hänför sig till avslutades.

Förbud mot vissa sökningar

8 § Det är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller sådana personuppgifter om lagöverträdelser som avses i artikel 10 i EU:s dataskyddsförordning.

9 § Det är förbjudet att som sökbegrepp använda

1. ansiktsbilder, biometriska uppgifter som har tagits fram ur ansiktsbilder och andra känsliga personuppgifter som avses i 10 §, och
2. uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden.

Trots förbuden i första stycket får den ansiktsbild som tas enligt 2 kap. 4 § första stycket och de biometriska uppgifter som tas fram ur ansiktsbilden användas vid sökning i registret över ärenden om statlig e-legitimation i ett ärende om statlig e-legitimation. Sökning är då tillåten endast för att kontrollera sökandens identitet och innehav av en e-legitimation i samband med ansökan.

Behandling av känsliga personuppgifter

10 § Personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) får behandlas endast om det är absolut nödvändigt för ändamålet med behandlingen.

Känsliga personuppgifter får dock behandlas

1. i registret när det är tillåtet enligt 6 § 2,
2. vid kontroller som är tillåtna enligt 2 kap. 6 §, och
3. vid sökningar som är tillåtna enligt 9 § andra stycket.

Personuppgiftsansvar

11 § Varje utfärdande myndighet är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten själv utför.

Polismyndigheten är personuppgiftsansvarig för behandling av personuppgifter i registret över ärenden om statlig e-legitimation.

Rätt att meddela föreskrifter

12 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter som avses i 7 § får fortsätta att behandlas under en viss tid för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, och
2. avskiljande och begränsningar av åtkomsten till personuppgifter som behandlas enligt 1.

4 kap. Erkännande av medel för elektronisk identifiering

Krav på erkännande av medel för elektronisk identifiering

1 § När medel för elektronisk identifiering krävs för att få tillgång till en nättjänst som tillhandahålls av en offentlig aktör, och tjänsten helt eller delvis riktar sig till enskilda, ska medel erkännas för autentisering för tjänsten om

1. medlet för elektronisk identifiering tillhandahålls inom ramen för ett auktorisationssystem i enlighet med lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post, och
2. tillitsnivån för medlet motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga aktören kräver för åtkomst till nättjänsten.

Bemyndiganden

2 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. undantag från kravet i 1 §, och
2. hur kravet i 1 § ska fullgöras.

5 kap. Överklagande och verkställighet

1 § Beslut enligt denna lag eller enligt föreskrifter som har meddelats i anslutning till lagen får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

2 § Beslut enligt denna lag gäller omedelbart, om inte annat anges i beslutet.

Denna lag träder i kraft den 1 december 2026.

3 Ärendet och dess beredning

Regeringen beslutade i december 2022 att ge en särskild utredare i uppdrag att utreda och lämna förslag på hur staten kan utfärda en e-legitimation på högsta tillitsnivå.

Utredningen, som antog namnet Utredningen om säker och tillgänglig digital identitet (I2022:04), överlämnade i oktober 2023 delbetänkandet En säker och tillgänglig statlig e-legitimation (SOU 2023:61). En sammanfattning av delbetänkandet finns i *bilaga 1*. Delbetänkandets lagförslag finns i *bilaga 2*. Delbetänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissyttrandena finns tillgängliga på regeringens webbplats (regeringen.se) och i Finansdepartementet (Fi2023/02704). I denna proposition behandlas förslagen i delbetänkandet.

Lagrådet

Regeringen beslutade den 22 januari 2026 att inhämta Lagrådets yttrande över de lagförslag som finns i *bilaga 4*. Lagrådet lämnar förslagen utan erinran. Lagrådets yttrande finns i *bilaga 5*. I förhållande till lagrådsremissens lagförslag görs vissa språkliga och redaktionella ändringar.

Lagrådsremissen innehöll, utöver de lagförslag som föreslås i propositionen, även ett förslag om ändring i 22 kap. 1 § offentlighets- och sekretesslagen (2009:400), förkortad OSL. Den 7 maj 2026 beslutade regeringen propositionen Utökade befogenheter för Skatteverket inom folkbokföringsverksamheten (prop. 2025/26:261). I propositionen föreslår regeringen en ändring i 22 kap. 1 § OSL som innefattar förslaget i lagrådsremissen En statlig e-legitimation. Ändringen föreslås träda i kraft den 1 december 2026. Mot denna bakgrund har regeringen inte tagit med förslaget i denna proposition (se avsnitt 9.4).

4 EU-lagstiftning om elektronisk identifiering

4.1 EU:s förordning om elektronisk identifiering

Inom EU finns bestämmelser om elektronisk identifiering i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, i fortsättningen EU:s förordning om elektronisk identifiering. Förordningen syftar bl.a. till att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att säkerställa att det tillhandahålls en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster som används i hela unionen (artikel 1 och skäl 2). Medel för elektronisk identifiering definieras i artikel 3.2 som en materiell och/eller immateriell enhet som innehåller uppgifter för personidentifiering och som används för autentisering för en nättjänst eller, i tillämpliga fall, för en offlinetjänst.

Betrodda tjänster är elektroniska tjänster som vanligen tillhandahålls mot ersättning och innehåller vissa utpekade funktioner kopplade till bl.a. elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar eller certifikat för autentisering av webbplatser (artikel 3.16). För att uppnå syftet med EU:s förordning om elektronisk identifiering ställs det ett krav på ömsesidigt erkännande av bl.a. medel för elektronisk identifiering som medlemsstater har anmält till Europeiska kommissionen för gränsöverskridande användning under vissa förutsättningar (artikel 6 och skäl 12 och 14). Det ställs dock inte något krav på att anmäla system för elektronisk identifiering till kommissionen och förordningen är inte tillämplig på system som inte har anmälts (artikel 2.1).

EU:s förordning om elektronisk identifiering kompletteras i svensk rätt genom lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

4.2 Revidering av EU:s förordning om elektronisk identifiering

EU:s förordning om elektronisk identifiering har reviderats i syfte att göra den mer effektiv, utvidga tillämpningsområdet till den privata sektorn och främja tillgången till digitala identiteter för alla européer. Ändringarna i förordningen, som beslutades genom 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, trädde i kraft den 20 maj 2024.

I den reviderade förordningen ställs nya krav på medlemsstaterna. En betydande förändring är skyldigheten att säkerställa att alla fysiska och juridiska personer i EU kan tillhandahållas en europeisk digital identitetsplånbok. En digital identitetsplånbok är ett medel för elektronisk identifiering som gör det möjligt för användaren att på ett säkert sätt lagra, hantera och validera personidentitetsuppgifter och elektroniska attributsintyg (artikel 3.42).

Den europeiska digitala identitetsplånboken syftar till att ge alla fysiska och juridiska personer i unionen tillgång till offentliga och privata tjänster genom att användaren bl.a. kan begära, dela och visa uppgifter för personidentifiering (artikel 5a). Utfärdandet, användningen och återkallandet av europeiska digitala identitetsplånböcker ska vara utan kostnad för alla fysiska personer (artikel 5a.13). Det ska vidare vara frivilligt att använda identitetsplånboken och avsaknaden av en sådan ska inte påverka tillgången till service eller möjligheten att bedriva verksamhet (skäl 15). Användaren kan förse identitetsplånboken med olika attributsintyg (artikel 3.42). Med attribut avses egenskaper, kvaliteter, rättigheter eller tillstånd hos en fysisk eller juridisk person eller hos ett föremål (artikel 3.43). Det kan t.ex. röra sig om studieintyg eller intyg om körkortsbehörighet.

4.3 Medel för elektronisk identifiering

E-legitimationer är medel för elektronisk identifiering. Elektronisk identifiering definieras i EU:s förordning om elektronisk identifiering som en process inom vilken uppgifter för personidentifiering i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en annan fysisk person eller en juridisk person, används (artikel 3.1). Med uppgifter för personidentifiering avses en uppsättning uppgifter som utfärdas i enlighet med unionsrätten eller nationell rätt, som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller på en fysisk person som företräder en annan fysisk person eller en juridisk person (artikel 3.3). De svenska identitetsbeteckningarna för att identifiera en fysisk person, personnummer och samordningsnummer, utgör uppgifter för personidentifiering (se avsnitt 6). Medel för elektronisk identifiering, dvs. bl.a. e-legitimationer, ska under vissa förutsättningar omfattas av ömsesidigt erkännande (artikel 6). Det gäller sådana e-legitimationer som är utfärdade inom ramen för ett system för elektronisk identifiering, som har anmälts av en medlemsstat och har förts upp på en särskild förteckning som offentliggörs av kommissionen (artikel 9). Det är endast medlemsstater som kan anmäla e-legitimationssystem, men det behöver inte vara medlemsstaten som utfärdar e-legitimationerna i systemet. De krav som måste vara uppfyllda för att anmäla ett e-legitimationssystem framgår av artikel 7.

I artikel 8 finns bestämmelser om tillitsnivåer för e-legitimationssystem. Tillitsnivåerna återger graden av tillit till en e-legitimation vid fastställande av en persons identitet och skapar visshet om att den person som gör anspråk på en viss identitet faktiskt är den person som har tilldelats denna identitet (skäl 16).

Det finns ingen skyldighet för medlemsstaterna att anmäla ett e-legitimationssystem på högsta tillitsnivå. Minst en europeisk digital identitetsplånbok ska däremot tillhandahållas av varje medlemsstat inom ramen för ett system för elektronisk identifiering och uppfylla de krav i artikel 8 vad gäller tillitsnivå hög (artikel 5a.1, 5a.5 d, 5a.5 f och 5a.24). Förordningen möjliggör att även få tillgång till en identitetsplånbok genom en e-legitimation på nivå väsentlig i kombination med ytterligare förfaranden för anslutning på distans, s.k. förstärkningsåtgärder. Förstärkningsåtgärderna regleras i kommissionens genomförandeförordning (EU) 2026/798 av den 7 april 2026 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller referensstandarder och specifikationer för anslutning på distans av användare till de europeiska digitala identitetsplånböckerna med hjälp av medel för elektronisk identifiering som motsvarar tillitsnivå väsentlig i kombination med ytterligare förfaranden för anslutning på distans där kombinationen uppfyller kraven på tillitsnivå hög.

I EU:s förordning om elektronisk identifiering ställs det vidare krav på tillhandahållandet av medel för elektronisk identifiering. Medel för elektronisk identifiering ska göras tillgängliga på ett klart och begripligt språk, i enlighet med Förenta nationernas konvention om rättigheter för personer med funktionsnedsättning och med tillgänglighetskraven i Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster. De ska

därmed även gynna personer med funktionsbegränsningar, såsom äldre personer, och personer med begränsad tillgång till digital teknik (artikel 15).

5 Tjänster för elektronisk identifiering i Sverige

5.1 Lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post

Lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post innehåller bestämmelser om auktorisationssystem i fråga om sådana tjänster. Anskaffning genom auktorisationssystem är ett alternativ till upphandling enligt lagen (2016:1145) om offentlig upphandling.

Med auktorisationssystem avses ett system där den myndighet som tillhandahåller systemet godkänner att leverantörer av tjänster för elektronisk identifiering av enskilda eller för digital post ingår ett avtal inom systemet om utförande av sådana tjänster. En enskild har rätt att välja den leverantör som ska utföra tjänsterna för den enskildes räkning och en offentlig aktör kan använda tjänsterna i sin verksamhet enligt avtal med den tillhandahållande myndigheten (2 § lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post). Med begreppet elektronisk identifiering avses detsamma som i EU:s förordning om elektronisk identifiering (3 § samma lag).

En statlig myndighet som kräver elektronisk identifiering av enskilda för åtkomst till myndighetens digitala tjänster ska använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystem enligt lagen, se 3 § förordningen (2023:709) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

Myndigheten för digital förvaltning är tillhandahållande myndighet enligt lagen. Myndigheten ska ta ut en avgift för användningen av tjänster inom ett auktorisationssystem och får meddela föreskrifter om avgifterna, se 22 § samma lag och 2 och 7 §§ förordningen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

5.2 Tillitsramverket för svensk e-legitimation

Myndigheten för digital förvaltning utvecklar och förvaltar tillitsramverket för svensk e-legitimation med stöd av 3 § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning, där det framgår att myndigheten ska främja användningen av elektronisk identifiering. Ramverket syftar till att etablera gemensamma krav för utfärdare av kvalitetsmärkta svenska e-legitimationer som granskas och godkänns av myndigheten. Kraven, som bl.a. vilar på internationella standarder, är för-

delade på olika skyddsklasser eller tillitsnivåer som svarar mot bl.a. olika grader av teknisk och operationell säkerhet hos utfärdaren (Myndigheten för digital förvaltning – Vägledning till uppfyllande av tillitsramverkets krav för Svensk e-legitimation, senast uppdaterad 2025-03-14).

5.3 Svenska e-legitimationer

I Sverige finns det flera privata utfärdare av e-legitimationer, bl.a. AB Svenska pass, Finansiell ID-Teknik BID AB och Freja eID Group AB.

Finansiell ID-Teknik BID AB äger och förvaltar e-legitimationen Bank-id. Bolagets kunder är de flesta av de stora svenska bankerna, som i sin tur säljer och förmedlar e-legitimationen. I dagsläget är det tio banker som utfärdar Bank-id. Det finns tre olika typer av Bank-id, mobilt bank-id, bank-id på fil och bank-id på kort. Vilka lösningar som de olika bankerna erbjuder sina kunder skiljer sig åt. Vissa banker tar betalt för bank-id på kort. Bank-id är godkänd på tillitsnivå 3 enligt Myndigheten för digital förvaltnings tillitsramverk. Bank-id är även anmäld för gränsöverskridande användning inom ramen för EU:s förordning om elektronisk identifiering på nivå väsentlig. För att kunna skaffa Bank-id måste en person ha ett svenskt personnummer och vara kund i någon av de banker som utfärdar Bank-id. Varje bank bestämmer själv vilken åldersgräns som krävs för att få Bank-id. Om sökanden är under arton år krävs det medgivande av vårdnadshavare.

AB Svenska pass e-legitimation finns på Skatteverkets identitetskort för folkbokförda i Sverige. För att kunna få identitetskortet, och därmed AB Svenska pass e-legitimation, måste sökanden vara folkbokförd i Sverige, ha fyllt tretton år och kunna styrka sin identitet, se 1 och 2 §§ lagen (2015:899) om identitetskort för folkbokförda i Sverige. Om sökanden är under arton år krävs det ett skriftligt medgivande från vårdnadshavare, se 5 § förordningen (2015:904) om identitetskort för folkbokförda i Sverige. AB Svenska pass e-legitimation är godkänd enligt Myndigheten för digital förvaltnings tillitsramverk på tillitsnivå 4. E-legitimationen är inte anmäld för gränsöverskridande användning inom ramen för EU:s förordning om elektronisk identifiering. AB Svenska pass e-legitimation används i praktiken endast för identifiering gentemot Skatteverket. För att kunna använda e-legitimationen krävs en dator och en kortläsare. Avgiften för identitetskortet för folkbokförda i Sverige är 400 kronor.

Freja eID Group AB utvecklar, äger och förvaltar Freja+, som är en mobil e-legitimation. Det är kostnadsfritt för användare att skaffa Freja+. För att skaffa Freja+ krävs det för närvarande bl.a. att sökanden är svensk medborgare och kan legitimera sig med en svensk identitetshandling. Även personer med styrkt samordningsnummer kan i vissa fall få Freja+. Lägsta ålder för att få Freja+ är fem år. Om sökanden är under arton år krävs det medgivande av vårdnadshavare. Freja+ är godkänd enligt Myndigheten för digital förvaltnings tillitsramverk på tillitsnivå 3 och anmäld för gränsöverskridande användning inom ramen för EU:s förordning om elektronisk identifiering på nivå väsentlig. Anmälan för gränsöverskridande användning gäller dock endast för Freja+ som skaffats genom besök med fysisk identitetskontroll hos ett ATG-ombud.

5.4 Användningen av e-legitimationer i Sverige

I en årlig rapport från Internetstiftelsen för 2025 redovisas att 5 procent av befolkningen saknar e-legitimation och att andelen användare har ökat med 2 procent sedan 2024 (Internetstiftelsen, Svenskarna och internet 2025 s. 16). Av 2025 års rapport, som utgår från användningen av mobilt bank-id, framgår också att så gott som alla i arbetsför ålder använder sig av mobilt bank-id och att endast 84 procent av de som är 65 år eller äldre använder mobilt bank-id. Bland de som är 76 år eller äldre är det drygt 70 procent som använder mobil bank-id. År 2021 var motsvarande siffra 50 procent, vilket visar på en tydlig ökning bland de äldsta sett över tid. Det är alltså de som är 65 år eller äldre som är den grupp i befolkningen som inte använder mobilt bank-id. Det är framför allt de äldsta, de som är 76 år eller äldre, som inte använder mobilt bank-id.

I undersökningen Svenskarna med funktionsnedsättning och internet (SMFOI) som avser 2025 svarar 60 procent att de känner sig delaktiga i det digitala samhället, 29 procent att de känner sig delaktiga till viss del, 8 procent att de inte känner sig delaktiga alls och 2 procent att de inte vet. I samma grupp uppger 83 procent att de använder mobilt bank-id och 15 procent att de använder en e-legitimation som inte är mobilt bank-id (Begripsam, Användning av internet SMFOI 2025, publicerad den 12 februari 2026).

6 Identitetsbeteckningar i Sverige

I Sverige finns det två identitetsbeteckningar för fysiska personer som används i folkbokföringen och samhället i övrigt. För den som folkbokförs fastställs ett personnummer som identitetsbeteckning enligt folkbokföringslagen (1991:481). Den som inte är eller har varit folkbokförd kan tilldelas ett samordningsnummer enligt lagen (2022:1697) om samordningsnummer.

Personnummer är avsett att vara en identitetsbeteckning för varje folkbokförd person (18 § folkbokföringslagen). Även om personen skulle avregistreras från folkbokföringen, exempelvis vid utflyttning, behåller personen sitt personnummer (prop. 2008/09:111 s. 14). För personer som är utländska medborgare krävs, utöver bosättning i landet, som huvudregel uppehållsrätt eller uppehållstillstånd för att få vistas i Sverige och därmed folkbokföras (3 och 4 §§ folkbokföringslagen). Barn som föds här i landet, ska också folkbokföras om bl.a. modern är folkbokförd eller fadern är folkbokförd och vårdnadshavare. Även barn som föds utomlands ska under vissa förutsättning folkbokföras (2 och 2 a §§ folkbokföringslagen).

Personnummer kan även tilldelas personer som enligt 5 § folkbokföringslagen inte ska folkbokföras i landet. Det avser personer som har rätt till immunitet och privilegier enligt lagen (1976:661) om immunitet och privilegier i vissa fall, t.ex. den som tjänstgör vid ett annat lands ambassad eller konsulat i Sverige (18 b § folkbokföringslagen). Ett sådant särskilt personnummer benämns av Skatteverket som immunitetsnummer (Skatteverkets rättsliga vägledning om personnummer, tilldelning och upp-

byggnad, publicerad den 30 januari 2025). Syftet med att ge dessa personer personnummer har varit att göra det lättare för dem att ta del av olika tjänster i samhället, t.ex. vid kontakter med vården (prop. 2008/09:111 s. 34). Skatteverket tilldelar sådana personnummer efter begäran av Regeringskansliet enligt 5 § första stycket folkbokföringsförordningen (1991:749).

Skatteverket får tilldela ett samordningsnummer bl.a. efter begäran av en myndighet eller efter ansökan av en enskild som har en sådan anknytning till Sverige att han eller hon kan antas behöva en identitetsbeteckning (2 kap. 1 § lagen om samordningsnummer). En anknytning till Sverige kan t.ex. bestå av att den enskilde eller någon annan i familjen äger fast egendom i landet. Anknytning kan även finnas för en EES-medborgare som med stöd av den fria rörligheten vistas i Sverige för t.ex. tillfälliga arbeten eller kortare studier. Möjligheten att tilldelas samordningsnummer efter egen ansökan gäller oavsett medborgarskap och behovet kan även finnas hos t.ex. en tredjelandsmedborgare som har ett tidsbegränsat uppehållstillstånd i Sverige. Den som har ett gällande avvisnings- eller utvisningsbeslut kan däremot i regel inte anses ha en sådan anknytning till Sverige att han eller hon kan antas ha ett behov av samordningsnummer (prop. 2020/21:160 s. 53, 54 och 98).

Samordningsnummer tilldelas i tre nivåer beroende på vilken identitetskontroll som har föregått tilldelningen. Uppgift om den enskildes identitet är styrkt, sannolik eller osäker registreras i folkbokföringsdatabasen. Huvudregeln är att samordningsnummer tilldelas den som vid personlig inställelse har styrkt sin identitet. Från huvudregeln finns vissa undantag där samordningsnummer får tilldelas även om personen endast har gjort sin identitet sannolik eller det råder osäkerhet om en persons identitet (2 kap. 1, 2, 5 och 6 §§ samma lag).

Uppgifter om en person som har tilldelats ett samordningsnummer registreras i folkbokföringsdatabasen och samordningsnumret är, på motsvarande sätt som ett personnummer, bestående och unikt genom att det är kopplat till en viss person oavsett om personen t.ex. har lämnat landet eller avlidit. En person som tilldelats ett samordningsnummer kan, till skillnad från någon som är folkbokförd, inte avregistreras. Det finns dock en möjlighet att förklara ett samordningsnummer vilande om det inte har förnyats inom utgången av det femte kalenderåret efter det år numret tilldelades, eller om det finns andra skäl för det. Ordningen med vilandeförklaring är en viktig del för att hålla uppgifterna i folkbokföringsdatabasen uppdaterade (prop. 2020/21:160 s. 65 och 66 och prop. 2021/22:276 s. 48).

7 En ny lag om statlig e-legitimation och elektronisk identifiering

7.1 Det ska införas en statlig e-legitimation

Regeringens förslag

Det ska införas en statlig e-legitimation.

Utredningens förslag

Förslaget från utredningen stämmer överens med regeringens.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *AB Svenska pass*, *Bolagsverket*, *Centrala studiestödsnämnden*, *Dals-Eds kommun*, *Domstolsverket*, *E-hälsomyndigheten*, *Ekobrottsmyndigheten*, *Finansinspektionen*, *Freja eID Group AB*, *Göteborgs kommun*, *Hovrätten över Skåne och Blekinge*, *Integritetsskyddsmyndigheten*, *Internetstiftelsen*, *Kriminalvården*, *Kronofogdemyndigheten*, *Länsstyrelsen i Blekinge län*, *Statens skolinspektion*, *Tierps kommun* och *Upphandlingsmyndigheten*, tillstyrker eller har inga synpunkter på förslaget. *Svenska kommunalpensionärernas förbund* anser att lagstiftningen på e-legitimationsområdet blir tydligare när den är samlad i en lag och att det stärker personuppgiftsskyddet. *Brottsförebyggande rådet* framför att en statlig e-legitimation kan medföra att säkerheten vid användning ökar, vilket är positivt ur ett brottsförebyggande perspektiv. *Sveriges riksbank* framhåller att en statlig e-legitimation kommer att göra det möjligt för fler att få tillgång till en e-legitimation, i synnerhet för de som saknar bankrelation. *Afasiförbundet i Sverige* framför att en statlig e-legitimation kommer att innebära att personer som i dag saknar möjlighet att få en e-legitimation kan få det.

IDnow Gmbh anser att en statlig e-legitimation inte bör införas förrän den europeiska digitala identitetsplånboken har utvärderats. Enligt bolaget finns det inte något krav i EU:s förordning om elektronisk identifiering på att införa ett system för identifiering på högsta tillitsnivå.

Skälen för regeringens förslag

En statlig e-legitimation kan göras tillgänglig för fler

Samhällsutvecklingen präglas i flera avseenden av digitalisering och det blir allt viktigare att kunna legitimera sig elektroniskt för att ta del av samhällets alla funktioner. Tillgång till e-legitimation erbjuder inte bara åtkomst till digitala tjänster hos exempelvis statliga myndigheter, kommuner och banker. En e-legitimation kan också skapa förutsättningar för att förenkla vardagen, eller till och med vara nödvändig, exempelvis vid köp av buss- eller tågbiljetter och vid inköp på fysiska eller digitala marknadsplatser.

En majoritet av befolkningen är delaktig i det digitala samhället. Det finns dock ett stort antal människor som ännu inte har tillgång till en e-

legitimation, vilket orsakar ett betydande utanförskap. Personer som är äldre eller som har en funktionsnedsättning har t.ex. inte tillgång till e-legitimation i samma utsträckning som den övriga befolkningen (se avsnitt 5.4). EU:s förordning om elektronisk identifiering ställer krav på tillgänglighet när det gäller tillhandahållandet av e-legitimationer (se avsnitt 4.3). En statlig e-legitimation kan, som också framhålls av *Sveriges riksbank* och *Afasiförbundet i Sverige*, på flera sätt göras mer tillgänglig jämfört med de e-legitimationer som i dag finns på den svenska marknaden.

En statlig e-legitimation kan stärka beredskapen och ge ökad redundans

Det försämrade omvärldsläget har ökat betydelsen av samhällets motståndskraft och ett fungerande totalförsvar. Flera utredningar och rapporter har pekat på bristen på konkurrens och den sårbarhet som finns inom e-legitimationsområdet genom att samhället i princip är beroende av en aktör (se t.ex. SOU 2023:16 s. 376 och Riksrevisionens rapport E-legitimation – en underutnyttjad resurs, RiR 2009:19).

Bristen på redundans, dvs. andra liknande tjänster som kan fungera som substitut, innebär en stor risk för samhället som helhet. Såväl användare som tillhandahållare av digitala tjänster riskerar att sakna alternativ om tjänsten inte är tillgänglig. Tillgängligheten till tjänsten kan t.ex. påverkas av en överbelastningsattack där någon angriper systemet genom att skicka så mycket trafik till en resurs att den blir otillgänglig.

Regeringen anser mot denna bakgrund att det finns ett stort behov av fler alternativ till dagens e-legitimationer. En statlig e-legitimation skulle skapa bättre motståndskraft och ett tillförlitligare system om en viss e-legitimation av någon anledning inte fungerar.

Nya krav till följd av EU:s förordning om elektronisk identifiering

EU:s förordning om elektronisk identifiering ställer krav på medlemsstaterna att tillhandahålla en digital identitetsplånbok. För att användare ska kunna få tillgång till en sådan plånbok krävs antingen en e-legitimation på tillitsnivå hög eller en e-legitimation på tillitsnivå väsentlig i kombination med s.k. förstärkningsåtgärder (se avsnitt 4.3). Sverige har anmält e-legitimationer på tillitsnivå väsentlig inom ramen för anmälningsförfarandet som regleras i EU:s förordning om elektronisk identifiering, men det finns ännu ingen svensk e-legitimation på tillitsnivå hög (se avsnitt 5.3). Regeringen bedömer, till skillnad från *IDnow Gmbh*, att det behövs en statlig e-legitimation som kan utformas på tillitsnivå hög för att säkerställa att förordningens krav på att tillhandahålla en digital identitetsplånbok uppfylls.

Det finns behov av en e-legitimation med en säker grundidentifiering

Med digitaliseringen har det skett en ökning av den identitetsrelaterade brottsligheten, en brottslighet som många gånger är sammankopplad med den grova organiserade brottsligheten. I en myndighetsgemensam rapport om organiserad brottslighet från 2023 beskrivs e-legitimation som en dörröppnare för kriminella aktörer. En kriminell aktör som förfogar över och kontrollerar ett större antal e-legitimationer med tillhörande konton kan enkelt och relativt riskfritt begå brott i den utnyttjade identitetens

namn och därefter förflytta brottsvinsterna mellan andra utnyttjade identiteter (Polismyndigheten, Nationella operativa avdelningen, Myndighetsgemensam lägesbild – Organiserad brottslighet 2023 s. 17).

En stor risk med elektronisk identifiering är kopplad till identifieringen i samband med att en e-legitimation utfärdas. En säker grundidentifiering, dvs. att identiteten styrks på ett tillförlitligt sätt i samband med ansökan av den statliga e-legitimationen, bedöms kunna motverka den identitetsrelaterade brottsligheten och ha en brottsförebyggande effekt.

I dagsläget finns det ingen anmäld svensk e-legitimationsutfärdare som genomför grundidentifiering som når upp till kravet för tillitsnivå hög enligt EU:s förordning om elektronisk identifiering eller motsvarande tillitsnivå 4 enligt det svenska tillitsramverket. Ett sådant högre krav innebär bl.a. att användarens identitet ska verifieras vid ett personligt besök. En statlig e-legitimation utfärdad på en sådan högre tillitsnivå skulle innebära en säkrare grundidentifiering med ökade möjligheter att säkerställa att en viss digital identitet representerar en viss fysisk person, som *Brottsförebyggande rådet* framför. Det finns mot den bakgrunden ett behov av en e-legitimation med en säker grundidentifiering.

En statlig e-legitimation bör regleras i en ny lag

Regeringen anser sammantaget att det bör införas en statlig e-legitimation. Det behövs för att så många som möjligt i samhället ska få tillgång till en e-legitimation och för att stärka samhällets säkerhet och motståndskraft vid t.ex. attacker på den digitala infrastrukturen. E-legitimationen bör kunna utformas på tillitsnivå hög. En e-legitimation på tillitsnivå hög behövs vidare för att säkerställa att svenska invånare inte utesluts från tillgång till digitala tjänster i andra EU-länder och att kraven i EU:s förordning om elektronisk identifiering uppfylls.

Den statliga e-legitimationen bör regleras i lag. I nationell lagstiftning finns det endast en lag som direkt berör e-legitimationer, lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. Lagen kompletterar och ska tillämpas med EU:s förordning om elektronisk identifiering. Regleringen av en statlig e-legitimation är däremot inte tänkt att komplettera EU-förordningen. De nya bestämmelserna bör därför samlas i en egen lag. Lagstiftningen blir på så sätt också mer överskådlig. Den nya lagen bör benämnas lagen om statlig e-legitimation och elektronisk identifiering.

Den statliga e-legitimationen bör ingå i ett auktorisationssystem för tjänster för elektronisk identifiering

Bristen på konkurrens på e-legitimationsområdet är ett skäl för förslaget att införa en statlig e-legitimation. Det finns i dag ett krav på att statliga myndigheter under regeringen ska använda de tjänster för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystem enligt lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post. Kravet gäller för myndigheter som kräver elektronisk identifiering av enskilda för åtkomst till myndighetens digitala tjänster, se 3 § förordningen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post (se avsnitt 5.1).

Om den statliga e-legitimationen anmäls till ett auktorisationssystem innebär det att den kommer att bli en av de tjänster som statliga myndigheter under regeringen måste använda om de kräver elektronisk identifiering för enskilda för inloggning i sina nättjänster. Det skulle leda till att fler e-legitimationer kan användas på marknaden, vilket skulle öka konkurrensen och därmed även samhällets motståndskraft. Det skulle vidare bidra till att öka tillgängligheten till digital offentlig service, eftersom den statliga e-legitimationen kommer att vara tillgänglig för en större personkrets än de e-legitimationer som för närvarande finns på marknaden (se avsnitt 8.1). I avsnitt 10 lämnar regeringen förslag om erkännande av medel för elektronisk identifiering som ingår i ett auktorisationssystem. Om den statliga e-legitimationen ansluts till ett auktorisationssystem kommer den att ingå i de tjänster som omfattas av det föreslagna kravet på erkännande.

Regeringen anser sammantaget att den statliga e-legitimationen bör anslutas till ett auktorisationssystem enligt lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

Myndigheten för digital förvaltning är tillhandahållande myndighet enligt lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post (se avsnitt 5.1). Myndigheten har meddelat föreskrifter om de krav som ska vara uppfyllda för att en ansökan om anslutning till ett auktorisationssystem ska godkännas (Föreskrifter om krav på leverantörers ansökan om anslutning till auktorisationssystem för tjänster för elektronisk identifiering och för digital post, MDFFS 2025:1). Regeringen anser att granskningen inför den statliga e-legitimationens anslutning till auktorisationssystem inte får medföra konsekvenser för Sveriges säkerhet.

7.2 Vissa ord och uttryck i lagen

Regeringens förslag

Med autentisering, elektronisk identifiering, medel för elektronisk identifiering och nättjänst ska i lagen avses detsamma som i EU:s förordning om elektronisk identifiering.

Det ska anges i lagen att en statlig e-legitimation är ett medel för elektronisk identifiering.

Det ska finnas en upplysning i lagen om att bestämmelser om medel för elektronisk identifiering finns i EU:s förordning om elektronisk identifiering och i lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att uttrycket statligt medel för elektronisk identifiering ska användas i stället för statlig e-legitimation. Utredningen föreslår följaktligen inte en bestämmelse som anger att en statlig e-legitimation är ett medel för elektronisk identifiering.

Remissinstanserna

Ingen remissinstans yttrar sig över förslaget.

Skälen för regeringens förslag

Ett av syftena med den statliga e-legitimationen är att den ska kunna anmälas för gränsöverskridande användning inom ramen för EU:s förordning om elektronisk identifiering (se avsnitt 7.1). Mot den bakgrunden anser regeringen att de ord och uttryck som används i den föreslagna lagen om statlig e-legitimation och elektronisk identifiering i relevanta delar bör motsvara de i förordningen. Dessa ord och uttryck är autentisering, elektronisk identifiering, medel för elektronisk identifiering och nättjänst. Av samma förordning följer att en e-legitimation är ett medel för elektronisk identifiering (artikel 3). Att den statliga e-legitimationen är ett medel för elektronisk identifiering bör även anges i den nya lagen.

Det bör även finnas en upplysning i lagen om att bestämmelser om medel för elektronisk identifiering finns i EU:s förordning om elektronisk identifiering och i lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

8 Förutsättningar för att få en statlig e-legitimation

8.1 En statlig e-legitimation ska kunna ges till personer med svenskt medborgarskap och till vissa utlänningar

Regeringens förslag

Den statliga e-legitimationen ska kunna utfärdas till personer som har svenskt medborgarskap, utlänningar som är folkbokförda i Sverige och personer som har ett s.k. immunitetsnummer och som omfattas av lagen om immunitet och privilegier i vissa fall. För att få den statliga e-legitimationen ska det även krävas att sökanden har fyllt eller innevarande kalenderår ska fylla nio år.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår inte att det uttryckligen ska anges att en statlig e-legitimation ska få utfärdas till personer med svenskt medborgarskap. Utredningen föreslår att en statlig e-legitimation ska få utfärdas till personer med ett svenskt personnummer och till personer med sådant samordningsnummer som tilldelas dem som har styrkt sin identitet.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *Centrala studiestödsnämnden*, *Göteborgs kommun*, *Huddinge kommun* och *Länsstyrelsen i Stockholms län*, tillstyrker eller har inga synpunkter på förslaget. *Föreningen svenskar i världen*, *Helsingborgs kommun* och *Kommerskollegium* ser positivt på att personer med styrkt samordningsnummer föreslås kunna få en statlig e-legitimation. *Myndigheten för digital förvaltning* och *Region Stockholm* ser behov av en e-legitimation även för personer med samordningsnummer som inte har styrkt sin identitet. *Ekobrottsmyndigheten* ser en risk för ökad ekonomisk och identitetsrelaterad brottslighet med en statlig e-legitimation som baseras på ett samordningsnummer. *Sveriges ambassad i Bangkok* menar att en sådan risk gör sig gällande vid utfärdanden för minderåriga med samordningsnummer som är bosatta utanför EU eller EES och anser att den gruppen endast bör få en statlig e-legitimation om det finns behov.

Finansiell ID-Teknik BID AB önskar ett förtydligande i fråga om personer med immunitetsnummer kan få en statlig e-legitimation. Flera remissinstanser, bl.a. *Arbetsförmedlingen*, *Funktionsrätt Sverige* och *Myndigheten för delaktighet*, menar att ställföreträdare också bör ges möjlighet att använda en statlig e-legitimation för sina huvudmän för att inte personer med t.ex. förvaltare och god man ska riskera att uteslutas från möjligheten att använda en statlig e-legitimation.

Freja eID Group AB anser att det inte bör finnas någon nedre åldersgräns för att kunna få en statlig e-legitimation. Enligt bolaget skulle möjligheten för barn att identifiera sig digitalt bl.a. motverka gromning, dvs. att vuxna tar kontakt med barn i sexuellt syfte. Enligt Region Stockholm är det angeläget att barn kan ges tillgång till en e-legitimation från tretton års ålder för att kunna ta del av digital information. *Försäkringskassan* anser däremot att en statlig e-legitimation på högsta tillitsnivå inte bör vara tillgänglig för barn på grund av risken för missbruk och oegentligheter. Enligt *Diskrimineringsombudsmannen* bör det kunna göras undantag från åldersgränsen, t.ex. för barn som har hoppat över en årskurs. *Tierps kommun* och *Statens skolverk* påpekar att det inte finns något behov av digital identifiering för elever i skolan.

Skälen för regeringens förslag

Personer med svenskt medborgarskap, utlänningar som är folkbokförda i Sverige och personer som har ett immunitetsnummer bör kunna få en statlig e-legitimation

I avsnitt 7.1 föreslås att det ska införas en statlig e-legitimation som kan utformas på tillitsnivå hög för att säkerställa att de krav på att tillhandahålla en digital identitetsplånbok som gäller enligt EU:s förordning om elektronisk identifiering uppfylls. Av förordningen följer också ett ansvar för medlemsstaterna att tillhandahålla sådana plånböcker för användning av fysiska och juridiska personer som är bosatta på deras territorium (artikel 5a och skäl 16). I skälen anges vidare att medlemsstaterna bör säkerställa lika tillgång till elektronisk identifiering för alla sina medborgare och invånare (skäl 5, 7 och 15).

Enligt regeringens mening bör en utgångspunkt vara att så många som möjligt ska få tillgång till en statlig e-legitimation för att kunna utöva sin

rättshandlingsförmåga och ta del av information digitalt (se avsnitt 7.1). Samtidigt är det viktigt att upprätthålla en hög säkerhet på e-legitimationen och att det ställs krav på en säker identifiering vid utfärdandet.

Den statliga e-legitimationen bör kunna utfärdas till personer som kvalificerar sig för någon av de statliga fysiska identitetshandlingarna. Det innefattar personer som är svenska medborgare och personer som är folkbokförda i Sverige, se 1 § lagen om identitetskort för folkbokförda i Sverige, 4 § passlagen (1978:302) och 1 § förordningen (2005:661) om nationellt identitetskort.

Till skillnad från utredningen anser regeringen att det saknas skäl att ge alla som har ett personnummer möjlighet att få en statlig e-legitimation. Personer som har folkbokförts i Sverige behåller sitt personnummer även om de avregistreras från folkbokföringen, exempelvis vid utflyttning från Sverige. Att en person har ett personnummer behöver alltså inte innebära att personen är folkbokförd eller bosatt i landet (jfr 3 § folkbokföringslagen). Regeringen anser att det inte finns behov av att kunna utfärda en statlig e-legitimation till en sådan person om den inte är svensk medborgare. Mot denna bakgrund bör den statliga e-legitimation utfärdas till personer som är svenska medborgare eller folkbokförda i Sverige.

Personer som enligt 5 § folkbokföringslagen inte ska folkbokföras på grund av att de omfattas av lagen om immunitet och privilegier i vissa fall får under vissa förutsättningar tilldelas ett personnummer, s.k. immunitetsnummer. Syftet med att tilldela dem personnummer har varit att göra det lättare för sådana personer att ta del av olika tjänster i samhället (se avsnitt 6). Regeringen anser att samma skäl gör sig gällande i fråga om möjligheten att få en statlig e-legitimation. Därför bör även personer som har fått ett personnummer tilldelat enligt 18 b § folkbokföringslagen ges möjlighet att få en statlig e-legitimation. Även för denna krets bör det krävas att personen befinner sig i Sverige och fortfarande omfattas av lagen om immunitet och privilegier i vissa fall. I annat fall skulle personer med obetydlig eller ingen anknytning till landet kunna få en statlig e-legitimation.

En avgränsning av personkretsen till de som är svenska medborgare, utlänningar som är folkbokförda i Sverige eller har ett immunitetsnummer utesluter dock fortfarande många som har anknytning till Sverige, t.ex. de som har ett tillfälligt arbete i landet, men som inte är bosatta här och därmed inte ska folkbokföras. Sådana personer har möjlighet att under vissa förutsättningar tilldelas ett samordningsnummer (se avsnitt 6).

Samordningsnummer kan tilldelas i tre nivåer beroende på vilken identitetskontroll som har föregått tilldelningen. Huvudregeln är att samordningsnummer ska tilldelas den som har styrkt sin identitet. En person som ska styrka sin identitet i samband med tilldelning ska som huvudregel inställa sig personligen för identitetskontroll, se 2 kap. 1 och 2 §§ lagen om samordningsnummer.

Utredningen har föreslagit att personer med sådant samordningsnummer som tilldelas personer som har styrkt sin identitet och som inte är vilande ska kunna få en statlig e-legitimation. Kravet för att tilldelas sådant samordningsnummer motsvarar det som gäller vid folkbokföring för personer som flyttar till Sverige från utlandet (prop. 2020/21:160 s. 56 och prop. 2021/22:276 s. 37). Med hänsyn till de strikta krav på en säker identifiering som ställs i samband med sådan tilldelning anser regeringen

att risken för ökad ekonomisk och identitetsrelaterad brottslighet om en e-legitimation utfärdas för dessa personer, som bl.a. *Ekobrottsmyndigheten* lyfter, inte bör överdrivas. Det finns dock vissa praktiska svårigheter som behöver hanteras för att utländska medborgare som tilldelas ett sådant samordningsnummer ska kunna ges möjlighet att få en statlig e-legitimation. Som flera remissinstanser framför, bl.a. *Föreningen svenskar i världen*, är det samtidigt angeläget att en statlig e-legitimation kan utfärdas så snart som möjligt till personer som är bosatta i landet. Regeringen bedömer mot denna bakgrund att personer med samordningsnummer och som inte är svenska medborgare för närvarande inte kan omfattas av den personkrets som bör ges möjlighet att få en statlig e-legitimation. Med hänsyn till det behov som finns för utländska medborgare med samordningsnummer, som har styrkt sin identitet, att få tillgång till en svensk e-legitimation, har regeringen för avsikt att återkomma i frågan.

Regeringen anser sammanfattningsvis att en statlig e-legitimation bör kunna utfärdas till personer som har svenskt medborgarskap, utlänningar som är folkbokförda i Sverige och personer som har ett s.k. immunitetsnummer och som omfattas av lagen om immunitet och privilegier i vissa fall.

Något förslag om att ställföreträdare ska ha tillgång till den statliga e-legitimationen för sina huvudmäns räkning, som efterfrågas av flera remissinstanser, har inte lämnats och bereds därmed inte vidare inom ramen för detta lagstiftningsarbete.

Möjligheten att få en e-legitimation bör vara begränsad till personer som har fyllt eller som innevarande kalenderår ska fylla nio år

Det uppställs inte någon åldersgräns för att få ett svenskt pass. Om den som ansöker om ett pass är under arton år måste dock, som huvudregel, vårdnadshavare lämna medgivande för att passet ska få utfärdas (7 § passlagen). Samma krav gäller för det nationella identitetskortet (3 § förordningen om nationellt identitetskort) och identitetskortet för folkbokförda i Sverige (5 § förordningen om identitetskort för folkbokförda i Sverige). För identitetskortet för folkbokförda finns det dock en åldersgräns om tretton år (1 § lagen om identitetskort för folkbokförda i Sverige).

Det är inte enbart myndiga som kommer att ha behov av en statlig e-legitimation. Många barn använder redan i lågstadiet internet dagligen (Internetstiftelsen, Svenskarna och internet 2025 s. 202). Underåriga har vidare en viss rättshandlingsförmåga. De har rätt att i vissa fall råda över egendom som de t.ex. har fått genom villkorad gåva eller genom eget arbete (se t.ex. 9 kap. 1 och 3 §§ föräldrabalken). I likhet med vad *Region Stockholm* påpekar kan det också finnas behov för de som har fyllt tretton år att använda en statlig e-legitimationen för att t.ex. boka vårdtider och förnya recept. Regeringen har dessutom när det gäller barns möjlighet till inflytande i hälso- och sjukvården bedömt att det inte bör införas särskilda åldersgränser. I stället ska barnets ålder och mognad beaktas vad gäller barns möjlighet till inflytande och information i olika medicinska frågor (prop. 2013/14:106). Dessa omständigheter talar till viss del för att inte införa någon åldersgräns för den statliga e-legitimationen, som *Freja eID Group AB* förordar.

Som *Försäkringskassan* lyfter finns det dock olika risker kopplade till ungas användning av en e-legitimation. En uppenbar risk är att barn kan bli målgrupp för den grova organiserade brottsligheten (se avsnitt 7.1). Det finns vidare inte något som tyder på att de allra yngsta är i behov av en e-legitimation. Detta talar för att möjligheten för underåriga att få en statlig e-legitimation bör begränsas till barn som har uppnått en viss ålder och mognad som vanligtvis följs av ett behov av att legitimera sig digitalt.

Fram till nyligen har det funnits föreskrifter meddelade av Statens skolverk om digitala nationella prov för elever i årskurs tre, dvs. för elever som innevarande kalenderår har fyllt eller ska fylla nio år. Utredningen föreslår att den statliga e-legitimationen ska utfärdas till den som är eller innevarande kalenderår ska fylla nio år, bl.a. för att de som går i årskurs tre självständigt ska kunna identifiera sig för att genomföra digitala nationella prov. Även om det inte längre genomförs digitala nationella prov i årskurs tre, som *Statens skolverk* påpekar, anser regeringen att den åldersgräns som föreslagits av utredningen framstår som väl avvägd. Det kan inte heller uteslutas att det i framtiden införs digitala tjänster som kräver elektronisk identifiering från den åldern.

I avsnitt 8.2 föreslår regeringen att det ska krävas vårdnadshavares medgivande vid ansökan om en statlig e-legitimation. Ett sådant krav innebär att det ytterst är vårdnadshavaren som avgör om barnet kan anses ha uppnått tillräcklig mognad för att ha en e-legitimation. En reglering som i stället skulle innebära att en utfärdande myndighet ska göra en individuell mognadsbedömning av sökanden bedöms inte vara aktuellt att införa med hänsyn till ändamålet med lagstiftningen. Regeringen anser mot denna bakgrund att den statliga e-legitimationen bör kunna utfärdas till personer som har fyllt eller som innevarande kalenderår ska fylla nio år.

Eftersom det inte ställs några krav på unga att legitimera sig digitalt finns det inte något behov av ett sådant undantag från åldersgränsen som *Diskrimineringsombudsmannen* efterfrågar.

8.2 För att få en statlig e-legitimation ska det krävas en ansökan

Regeringens förslag

Den statliga e-legitimationen ska utfärdas efter ansökan. Den som ansöker om en statlig e-legitimation ska lämna ansökan vid personlig inställelse. Sökanden ska styrka sin identitet och de övriga personuppgifter som krävs för att en statlig e-legitimation ska kunna utfärdas. För den som är under arton år ska det krävas vårdnadshavares medgivande om det inte finns synnerliga skäl.

Lagen ska innehålla en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om förfarandet vid ansökan, utfärdande och utlämnande.

Utredningens förslag

Förslagen från utredningen stämmer i sak överens med regeringens. Utredningen föreslår att kravet på personlig inställelse ska regleras i förordning. Det föreslås också en upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter för verkställigheten av kontrollen av att sökanden har styrkt sin identitet. Utredningen föreslår slutligen att undantaget från kravet på vårdnadshavares medgivande ska regleras i förordning.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *Boverket*, *Centrala studiestödsnämnden*, *E-hälsomyndigheten*, *Huddinge kommun*, *Internetstiftelsen* och *Länsstyrelsen i Skåne län*, tillstyrker eller har inga synpunkter på förslaget.

Länsstyrelsen i Västra Götalands län framför att ett ansökningsförfarande innebär en begränsning för flera grupper i samhället. *Länsstyrelsen i Blekinge län* anser att det bör framgå av lagen att en sökande ska inställa sig personligen och att ansökan ska avges på heder och samvete i likhet med regleringen i passlagen. *Funktionsrätt Sverige*, *Myndigheten för delaktighet* och *Synskadades riksförbund* anser att det bör göras undantag från kravet på personlig inställelse för personer som inte kan ta sig till en utfärdande myndighets lokaler och att andra lösningar bör utredas vidare. *Sorsele kommun* konstaterar att det i många kommuner saknas tillgång till myndigheter och att det kommer att innebära långa resor för att ansöka om och hämta ut en e-legitimation för de som bor i glesbygdsområden. *Skatteverket* önskar ett förtydligande av huruvida ansökan, grundidentifiering, utlämnande och, i förekommande fall, aktivering av e-legitimationen kan ske vid ett och samma tillfälle. *Sveriges ambassad i Berlin* påpekar att ambassaden kan ha svårt att bedöma äktheten av utländska identitetshandlingar som är utfärdade i tredje land.

Barnombudsmannen anser att kravet på vårdnadshavares medgivande behöver utvecklas och efterfrågar en fördjupad analys av vad kravet innebär för barn. Enligt *Föreningen Sveriges överförmyndare* och *Lessebo kommun* bör det rätteligen vara förmyndare och inte vårdnadshavare som ska lämna medgivande till ansökan om e-legitimation för barn. Även *Sveriges Kommuner och Regioner* (*SKR*) framför att förmyndare bör kunna ansöka om e-legitimation för sina barn, t.ex. i fall där vårdnadshavare fråntagits sitt förmyndarskap. SKR föreslår vidare att det ska föreskrivas att kommuner ska yttra sig i ärenden om utfärdande av e-legitimation för barn, på samma sätt som i passärenden. *Stockholms kommun* framför att det är oklart vad den kommunala likställighetsprincipen innebär i fall där vårdnadshavare avstår från att skaffa en e-legitimation till sitt barn.

Skälen för regeringens förslag

För att få en e-legitimation bör det krävas en ansökan

Att en e-legitimation på tillitsnivå hög måste utfärdas efter ansökan följer av EU:s förordning om elektronisk identifiering och av kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och förfaranden för tillits-

nivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. Dessutom utfärdas även de nationella identitets- och resehandlingarna efter ansökan. Regeringen anser därför, till skillnad från *Länsstyrelsen i Västra Götalands län*, att det bör krävas en ansökan för att en statlig e-legitimation ska utfärdas.

Ytterligare föreskrifter om förfarandet vid ansökan, utfärdande och utlämnande kan meddelas av regeringen eller den myndighet som regeringen bestämmer. Den nya lagen bör innehålla en upplysningsbestämmelse om detta.

En ansökan bör göras personligen

Syftet med en identitetshandling är att den ska vara ett tillförlitligt bevis för innehavarens identitet. Den som granskar handlingen ska kunna vara säker på att uppgifterna om innehavaren är korrekta. För att säkerställa detta är det av stor vikt att den som vill ha en identitetshandling inställer sig personligen.

Den personliga inställelsen fyller flera funktioner. Den möjliggör att bilderna av sökandens ansikte och, i förekommande fall, fingeravtryck kan tas på plats av en utfärdande myndighet. Förutom att bilderna då får rätt format och tekniska egenskaper innebär det att den utfärdande myndighetens personal enkelt kan säkerställa att det som tas in i handlingen är en ansiktsbild av sökanden. Det personliga mötet innebär dessutom att personalen kan göra en bedömning av om sökandens uppgifter i fråga om t.ex. födelsedatum är korrekta. Vid behov kan personalen även enkelt ställa kontroll- eller följdfrågor.

Ett krav på personlig inställelse vid en ansökan om e-legitimation ger alltså goda förutsättningar för ett korrekt utfärdande. Det finns därför starka skäl för att uppställa ett krav på personlig inställelse trots att det kan innebära längre resor för de som bor i glesbygdsområden, som *Sorsele kommun* påpekar.

Krav på personlig inställelse gäller även vid ansökan om pass, nationellt identitetskort och identitetskort för folkbokförda i Sverige. I fråga om pass regleras det i 6 § passlagen. Eftersom kravet på personlig inställelse är centralt för säkerheten i förfarandet bör kravet, i likhet med vad *Länsstyrelsen i Blekinge län* anser, regleras i lag. Flera remissinstanser, bl.a. *Myndigheten för delaktighet* och *Synskadades riksförbund*, anser att det bör göras undantag från kravet på personlig inställelse för personer som inte kan ta sig till en utfärdande myndighets lokaler. Något sådant förslag lämnas emellertid inte av utredningen och regeringen anser att det i nuläget inte bör införas något undantag från kravet. Regeringen anser således att det bör uppställas ett krav på personlig inställelse vid ansökan om statlig e-legitimation. Det kan dock noteras att det i betänkandet Ett säkert statligt id-kort – med e-legitimation (SOU 2019:14) ansågs vara möjligt att i vissa undantagsfall ansöka om en statlig e-legitimation genom bud. Betänkandet bereds i Regeringskansliet. Det kan därför finnas skäl att återkomma till frågan i framtiden.

Det finns inte inom ramen för detta lagstiftningsärende beredningsunderlag för att, som Länsstyrelsen i Blekinge län efterfrågar, införa ett krav på att en ansökan om e-legitimation ska avges på heder och samvete.

Hur det praktiskt ska gå till med ansökan, utfärdande, utlämnande och aktivering av e-legitimationen, som *Skatteverket* efterfrågar ett förtydligande om, bör regleras i förordning eller genom myndighetsföreskrifter. Det bör då också beaktas en utfärdande myndighets möjligheter att kontrollera biometriska uppgifter (se avsnitt 8.3).

Sökandens identitet bör vara styrkt

Vid ansökan om pass, nationellt identitetskort, identitetskort för folkbokförda i Sverige och svenskt medborgarskap krävs det att sökanden har styrkt sin identitet. För att få ett pass måste sökanden även styrka sitt svenska medborgarskap och övriga personuppgifter (6 § passlagen). Identiteten kan styrkas på de sätt som anges i 3 kap. 2 och 3 §§ Polismyndighetens föreskrifter och allmänna råd om pass och nationellt identitetskort (PMFS 2021:3, FAP 530-1). Enligt dessa ska sökanden i första hand styrka sin identitet genom att visa upp en godtagbar identitetshandling, t.ex. ett svenskt vanligt eller extra pass eller körkort. Identiteten kan även styrkas genom en skriftlig försäkran där en intygsgivare, t.ex. en vårdnadshavare, intygar att sökandens uppgifter är riktiga.

Den statliga e-legitimationen ska vara säker. Ett av syftena med den statliga e-legitimationen är vidare att den ska kunna anmälas för gränsöverskridande användning inom ramen för EU:s förordning om elektronisk identifiering (se avsnitt 7.1). För att kunna göra det måste det uppställas ett krav på att sökanden har styrkt sin identitet (punkt 2.1.1 i bilagan till kommissionens genomförandeförordning 2015/1502). Det bör därför krävas att sökanden har styrkt sin identitet och de övriga personuppgifter som krävs för utfärdande av den statliga e-legitimationen. Kravet bör motsvara det som gäller för pass och nationellt identitetskort. Det är dock tillräckligt att närmare bestämmelser om kravet på styrkt identitet meddelas i förordning eller genom myndighetsföreskrifter.

Som *Sveriges ambassad i Berlin* påpekar kan identitetskontrollen i vissa fall behöva innefatta en kontroll av utländska identitetshandlingar. Regeringen konstaterar att vissa myndigheter redan i dag måste göra sådana kontroller, t.ex. i utlännings- och viseringsärenden. Det bör därför finnas en upparbetad kunskap om hur utländska identitetshandlingar ska granskas. Föreskrifter om förfarandet vid ansökan kan exempelvis reglera hur kontrollen av sådana handlingar ska gå till.

Det bör krävas vårdnadshavares medgivande om sökanden är under arton år

För pass, nationellt identitetskort och identitetskort för folkbokförda i Sverige gäller i dag som huvudregel att den som är under arton år behöver ett medgivande från sin eller sina vårdnadshavare för att kunna få identitetshandlingen. Som *Barnombudsmannen* lyfter innebär kravet på vårdnadshavares medgivande att barn inte självständigt kan bestämma över sin ansökan om en statlig e-legitimation. Motsvarande krav på medgivande gäller såväl för andra e-legitimationer (se avsnitt 5.3) som för de fysiska identitetshandlingarna. I avsnitt 8.1 konstaterar regeringen att

det finns olika risker kopplade till ungas användning av en e-legitimation. Riskerna bör till viss del kunna motverkas av att en aktör som tillhandahåller en nättjänst som kräver e-legitimation kan begränsa tillgången till tjänsten för vissa ålderskategorier. Samtidigt bedöms det viktigt att ett barn som har uppnått åldersgränsen för att få e-legitimationen också har uppnått tillräcklig mognad för att kunna hantera och använda den på ett säkert sätt. Som utgångspunkt bör barnet kunna ges större möjlighet att bestämma själv över användningen i takt med stigande ålder och utveckling (jfr bl.a. prop. 1981/82:168 s. 22 och 23 samt prop. 2013/14:106 s. 120). Den typen av bedömningar bör göras av barnets vårdnadshavare. Regeringen anser därför att det bör krävas vårdnadshavares medgivande om sökanden är under arton år. Till skillnad från utredningen anser regeringen att kravet på medgivande är så grundläggande att det bör framgå av lag.

Regeringen anser vidare att den som är under arton år bör kunna få en e-legitimation utan vårdnadshavarnas medgivande om det finns synnerliga skäl. Det bör bl.a. anses finnas synnerliga skäl om en av föräldrarna är tillfälligt förhindrad att lämna sitt medgivande, t.ex. på grund av sjukdom, och det är uppenbart att dennes medgivande annars skulle ha lämnats (jfr prop. 1977/78:156 s. 44). Eftersom ett barn kommer att kunna få en e-legitimation i situationer där vårdnadshavare är förhindrade att lämna sitt medgivande finns det, till skillnad från vad bl.a. *Föreningen Sveriges överförmyndare* anser, inte anledning att föreskriva att det är förmyndare som ska lämna medgivande till ansökan. Lagstiftningen bör i stället, i relevanta delar, utformas med passlagen som förebild.

Det finns dock inte något behov av att, som *SKR* efterfrågar, på motsvarande sätt som i passärenden föreskriva att en kommunal nämnd som fullgör uppgifter inom socialtjänsten ska yttra sig i ett ärende om utfärdande av e-legitimation för barn under arton år utan vårdnadshavares medgivande. Till skillnad från pass är den statliga e-legitimationen inte en resehandling. De behov som kan finnas för att utfärda ett pass utan vårdnadshavares medgivande, t.ex. att få hem ett barn som mot sin vilja förts ur landet, aktualiseras därför inte i ett ärende om statlig e-legitimation (jfr prop. 2005/06:144 s. 10–16). Det bör därför inte krävas något yttrande från kommunens socialtjänst i ett sådant ärende.

Stockholms kommun anför att det är oklart vad likställighetsprincipen enligt 2 kap. 3 § kommunallagen (2017:725) innebär i de fall där vårdnadshavare avstår från att skaffa en e-legitimation till sitt barn. Likställighetsprincipen innebär att kommuner och regioner ska behandla sina medlemmar lika. Att ansöka om en statlig e-legitimation kommer att vara en möjlighet och inte en skyldighet för de som kan få en sådan e-legitimation utfärdad. Det finns för närvarande inte heller något krav på att ha någon e-legitimation, vare sig för barn eller vuxna. Likställighetsprincipen aktualiseras därmed inte i den här situationen.

8.3 Ansiktsbild och fingeravtryck ska lämnas

Regeringens förslag

Sökanden ska i samband med ansökan om statlig e-legitimation låta utfärdande myndighet ta hans eller hennes ansiktsbild och fingeravtryck. Ansiktsbild och fingeravtryck ska sparas i ett lagringsmedium i bäraren av e-legitimationen. Sökanden ska vidare låta utfärdande myndighet ta sökandens ansiktsbild och fingeravtryck vid utlämnande av den statliga e-legitimationen, om myndigheten begär det.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om undantag från skyldigheten att låta utfärdande myndighet ta sökandens fingeravtryck.

Lagen ska innehålla en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om den statliga e-legitimationens innehåll, bärare, utformning i övrigt och aktivering.

Utredningens förslag

Förslagen från utredningen stämmer i huvudsak överens med regeringens. Utredningen föreslår inte att sökanden ska låta den utfärdande myndigheten ta hans eller hennes ansiktsbild och fingeravtryck vid utlämnande av den statliga e-legitimationen, om myndigheten begär det. Utredningen föreslår inte en upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om den statliga e-legitimationens bärare, innehåll och aktivering.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *AB Svenska pass*, *Barnombudsmannen*, *Bolagsverket*, *Brottsförebyggande rådet*, *Brottsoffermyndigheten*, *Diskrimineringsombudsmannen*, *Försvarets radioanstalt*, *Göteborgs kommun*, *Säkerhetspolisen* och *Åklagarmyndigheten*, tillstyrker eller har inga synpunkter på förslaget. *Försäkringskassan* anser att biometriska uppgifter bör användas vid legitimering med den statliga e-legitimationen i syfte att säkerställa en korrekt autentisering.

Synskadades riksförbund framför att personer med ögonskador eller ögonproteser måste kunna använda biometrisk ansiktsigenkänning som identifieringsmetod vid användning av den statliga e-legitimationen. *Totalförsvarets forskningsinstitut* är positivt till att e-legitimationen ska innehålla biometriska uppgifter och att det därmed finns beredskap för framtida teknisk utveckling. *Svenska kommunalpensionärernas förbund* anser att det finns fördelar med att använda biometriska uppgifter men påpekar att det också finns en risk för att uppgifterna inte alltid är tillförlitliga, särskilt i fall där användarens fysiska egenskaper har förändrats över tid.

Några remissinstanser, bl.a. *Myndigheten för digital förvaltning*, anser att det inte bör lagras biometriska uppgifter på e-legitimationen eftersom det för närvarande saknas teknik som möjliggör användning av sådana uppgifter vid autentisering på distans. *Sveriges ambassad i Washington*

anser att en utfärdande myndighet även ska få ta sökandens signatur digitalt.

Skälen för regeringens förslag

Starka skäl talar för att den statliga e-legitimationen bör innehålla innehavarens ansiktsbild och fingeravtryck

En lagring av innehavarens ansiktsbild och fingeravtryck i den statliga e-legitimationen skulle fylla flera viktiga funktioner ur säkerhetssynpunkt. Lagringen i den fysiska bäraren av e-legitimationen innebär t.ex. att informationen i bäraren går att kontrollera med hjälp av biometri. Uppgifterna i den fysiska bäraren skulle t.ex. kunna användas av en utfärdande myndighet vid grundidentifieringen i samband med utlämnandet. En utfärdande myndighet skulle då kunna ta sökandens ansiktsbild och fingeravtryck och göra en jämförelse av dessa uppgifter med de som finns sparade i bäraren. Om sökanden styrker sin identitet med hjälp av en handling som innehåller ansiktsbild eller fingeravtryck skulle en utfärdande myndighet vidare kunna kontrollera att de uppgifterna stämmer överens med uppgifterna i bäraren på den statliga e-legitimationen. Uppgifterna i den fysiska bäraren skulle även kunna användas i jämförande syfte vid ansökan om förnyelse av en statlig e-legitimation (se avsnitt 9.4).

De biometriska uppgifter som skulle komma i fråga är sådana kännetecken som är bestående över tid och därmed opåverkade av åldrande. Det finns därför inte någon risk för att uppgifterna inte skulle vara tillförlitliga på det sätt som *Svenska kommunalpensionärernas förbund* befarar.

Vissa utfärdare av e-legitimationer möjliggör redan användning av ansiktsigenkänning vid e-legitimering. Att kunna använda sig av den typen av teknik för autentisering på distans höjer säkerheten betydligt. Det skulle kunna motverka identitetsrelaterad brottslighet och missbruk av den statliga e-legitimationen. Möjligheten att använda sig av ansiktsigenkänning innebär också, som *Synskadades riksförbund* lyfter, att fler kan använda sig av den statliga e-legitimationen. Trots att det, som bl.a. *Myndigheten för digital förvaltning* påpekar, för närvarande inte fullt ut går att använda sig av biometriska uppgifter för autentisering på distans anser regeringen, i likhet med bl.a. *Försäkringskassan*, att användningen av biometriska uppgifter är befogad av säkerhetsskäl och därför bör möjliggöras.

Regeringen anser mot denna bakgrund att starka skäl talar för att den statliga e-legitimationen bör innehålla innehavarens ansiktsbild och fingeravtryck.

Grundläggande fri- och rättigheter måste beaktas

Enligt 2 kap. 6 § första stycket regeringsformen är var och en skyddad mot påtvingade kroppsliga ingrepp från det allmännas sida. Fotografering räknas inte som ett kroppsligt ingrepp. Det gör däremot fingeravtryckstagning (se t.ex. prop. 2017/18:35 s. 12 och prop. 2020/21:120 s. 16). Var och en är alltså skyddad mot att behöva lämna fingeravtryck till en myndighet.

Skyddet mot påtvingade kroppsliga ingrepp är dock inte absolut utan får i vissa fall begränsas genom lag (2 kap. 20 § regeringsformen). Begränsningen får göras endast för att tillgodose ändamål som är godtagbara i ett

demokratiskt samhälle och får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett dem. Begränsningen får vidare inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 21 § regeringsformen). För den som inte är svensk medborgare får skyddet mot påtvingade kroppsliga ingrepp begränsas genom lag utan att de förutsättningar som anges i 2 kap. 21 § regeringsformen är uppfyllda (2 kap. 25 § regeringsformen).

Ett skydd mot integritetsintrång av olika slag följer även av den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Enligt artikel 8 i Europakonventionen har var och en rätt till respekt för sitt privat- och familjeliv. Det inbegriper i vissa fall en rätt till skydd mot att bli fotograferad. Likaså får det antas att rätt till skydd mot fingeravtryckstagning omfattas av skyddet (prop. 2014/15:32 s. 26 och prop. 2020/21:120 s. 17). Inskränkningar i skyddet godtas bara om de har stöd i lag och i ett demokratiskt samhälle är nödvändiga med hänsyn till vissa ändamål, däribland statens säkerhet, den allmänna säkerheten eller förebyggande av oordning eller brott. En motsvarande rätt till respekt för privatlivet och familjelivet gäller enligt artikel 7 i EU:s stadga om de grundläggande rättigheterna och artikel 16 i FN:s konvention om barnets rättigheter (barnkonventionen). Av barnkonventionen följer bl.a. att en bedömning av barnets bästa är det som i första hand ska beaktas vid alla åtgärder som rör barn och att barn ska skyddas från godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv (artiklarna 3 och 16).

Det finns redan i dag en skyldighet för en sökande att låta myndigheten ta ansiktsbild och fingeravtryck i samband med ansökan om pass och nationellt identitetskort (6 § passlagen och 3 § förordningen om nationellt identitetskort). Att använda två typer av biometriska underlag ökar säkerheten betydligt. Syftet med en lagring av biometriskt underlag i den statliga e-legitimationen är att motverka missbruk av e-legitimationen och säkerställa att den utfärdas till rätt person. Regeringen bedömer mot den bakgrunden att ändamålet med skyldigheten att lämna fingeravtryck får anses utgöra ett viktigt allmänt intresse som kan motivera en begränsning av skyddet mot kroppsliga ingrepp i 2 kap. 6 § regeringsformen. När dessa intressen vägs mot det integritetsintrång som förslagen innebär för den enskilde måste det beaktas att den enskilde själv får välja att ansöka om en statlig e-legitimation. Det ligger vidare i den enskildes intresse att förhindra missbruk av e-legitimationen (se avsnitt 9.4). Enligt regeringens bedömning finns det inte några mindre ingripande sätt att uppnå syftet att motverka missbruk av e-legitimationen och säkerställa att den utfärdas till rätt person. Det allmänna intresset av att förebygga missbruk och brottslighet väger alltså i detta sammanhang tyngre än integritetsaspekten.

Enligt regeringens bedömning bör det införas en skyldighet för sökanden av en statlig e-legitimation att låta utfärdande myndighet ta hans eller hennes ansiktsbild och fingeravtryck. Ansiktsbilden och fingeravtrycken bör sparas i ett lagringsmedium i bäraren av e-legitimationen.

Ansiktsbild och fingeravtryck bör få tas i samband med ansökan och utlämnande av den statliga e-legitimationen

Utredningen har föreslagit att sökanden ska låta den utfärdande myndigheten ta hans eller hennes fingeravtryck i samband med ansökan. Syftet är enligt utredningen att det, på samma sätt som för pass och nationellt identitetskort, ska gå att kontrollera sökandens identitet för att göra e-legitimationen säker och för att motverka identitetsrelaterad brottslighet. I linje med det föreslår utredningen också att det ska vara möjligt att behandla biometriska uppgifter för att kontrollera sökandens identitet och innehav av statlig e-legitimation i samband med ansökan. Syftet är att dessa uppgifter ska kunna tas i samband med ansökan och behandlas under hela handläggningen av ärendet om statlig e-legitimation. Enligt regeringens mening bör sökanden låta utfärdande myndighet ta ansiktsbild och fingeravtryck även vid utlämnande av den statliga e-legitimationen för att möjliggöra en jämförelse med uppgifterna som är lagrade i den statliga e-legitimationen. Det bör dock lämnas åt utfärdande myndigheten att avgöra om ansiktsbild och fingeravtryck ska lämnas då. Regeringen anser därför att det bör införas en skyldighet för sökanden att i samband med ansökan om statlig e-legitimation låta utfärdande myndighet ta hans eller hennes ansiktsbild och fingeravtryck. Sökanden bör vidare låta utfärdande myndighet ta ansiktsbild och fingeravtryck vid utlämnande av den statliga e-legitimationen, om myndigheten begär det.

Regeringen ser inte något behov av att i lagen reglera att en utfärdande myndighet bör få ta sökandens signatur digitalt, som *Sveriges ambassad i Washington* efterfrågar.

I avsnitt 9.4 lämnar regeringen förslag på i vilka situationer personuppgifter i form av ansiktsbild och fingeravtryck bör få behandlas i en utfärdande myndighets verksamhet.

Grundläggande krav bör finnas i lag och undantag i förordning

Det bör vara möjligt att göra undantag från skyldigheten att låta utfärdande myndighet ta sökandens fingeravtryck. Undantag kan t.ex. avse barn som är i en viss ålder och personer som har skador på fingrarna (se t.ex. prop. 2008/09:132 s. 10 och 11). Det bedöms dock vara tillräckligt att sådana undantag meddelas i förordning eller genom myndighetsföreskrifter. I lagen bör det därför införas en bestämmelse om att regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om undantag från skyldigheten att låta utfärdande myndighet ta fingeravtryck.

Vidare bör lagen innehålla en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om e-legitimationens innehåll, bärare, utformning i övrigt och aktivering. Sådana föreskrifter kan t.ex. avse vilken tillitsnivå e-legitimationen ska ha och den närmare utformningen av e-legitimationen, exempelvis vilken fysisk handling som e-legitimationen ska finnas på. Det kan t.ex. avse föreskrifter om att den statliga e-legitimationen kan placeras på ett identitetskort som utfärdas av en passmyndighet för medborgare eller, för övriga personkategorier, på ett kort som i fråga om utformning och innehåll motsvarar ett sådant kort. Att en e-legitimation aktiveras innebär att den

rent praktiskt blir tillgänglig för innehavaren att använda, t.ex. genom en mobilapplikation.

8.4 Avslag av ansökan och utfärdande av statlig e-legitimation

Regeringens förslag

En ansökan om en statlig e-legitimation ska avslås om de krav som framgår av den nya lagen eller föreskrifter som har meddelats i anslutning till lagen inte är uppfyllda och sökanden inte har följt en uppmaning att rätta till bristen. I annat fall ska den statliga e-legitimationen utfärdas och skyndsamt vara tillgänglig för utlämnande till sökanden.

Utredningens förslag

Förslaget från utredningen stämmer i sak överens med regeringens. Utredningen föreslår att bestämmelser om att den statliga e-legitimationen skyndsamt ska lämnas ut till sökanden ska regleras i förordning.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *AB Svenska pass*, *Bolagsverket*, *Socialstyrelsen*, *Statens servicecenter* och *Växjö kommun*, tillstyrker eller har inga synpunkter på förslaget. *Patent- och registreringsverket* anser att det bör övervägas om utfärdandet av en e-legitimation bör föregås av en registerkontroll. Myndigheten förespråkar att tidigare brottslighet, t.ex. missbruk av e-legitimation, bedrägeriförsök och liknande, ska hindra att en statlig e-legitimation utfärdas. *Skatteverket* anser att en ansökan ska kunna avslås om förutsättningarna för återkallelse på grund av säkerhetsskäl är uppfyllda.

Skälen för regeringens förslag

En ansökan om pass eller nationellt identitetskort ska avslås om de bestämmelser som gäller för ansökan inte har iakttagits och sökanden inte har följt uppmaningen att avhjälpa bristen (7 § 1 passlagen och 8 § förordningen om nationellt identitetskort). En ansökan om identitetskort för folkbokförda i Sverige ska vidare avslås om sökanden inte hör till den personkrets som kan få identitetskortet. Den ska också avslås om det som anges i lagen eller som har föreskrivits av regeringen i fråga om ansökan inte har iakttagits och sökanden inte har följt en uppmaning att avhjälpa bristen (4 § lagen om identitetskort för folkbokförda i Sverige).

En motsvarande reglering om när en ansökan ska avslås bör införas för den statliga e-legitimationen. En ansökan om en statlig e-legitimation bör därför avslås om de krav som framgår av den nya lagen eller föreskrifter som har meddelats i anslutning till lagen inte är uppfyllda och sökanden inte har följt en uppmaning att rätta till bristen. Om samtliga krav däremot

är uppfyllda bör en statlig e-legitimation utfärdas och skyndsamt vara tillgänglig för att lämnas ut till sökanden.

Något förslag om att tidigare brottslighet ska utgöra hinder för utfärdande av en statlig e-legitimation, som *Patent- och registreringsverket* efterfrågar, har inte remitterats. Regeringen anser att det saknas beredningsunderlag för att införa ett sådant hinder mot utfärdande av en statlig e-legitimation inom ramen för detta lagstiftningsarbete. *Skatteverket* föreslår att en ansökan ska kunna avslås om förutsättningarna för återkallelse på grund av säkerhetsskäl är uppfyllda redan vid ansökan. En sådan grund för avslag av en ansökan finns inte för de fysiska identitetshandlingarna. Enligt regeringens uppfattning finns det för närvarande inte anledning att införa en sådan grund för avslag vid ansökan av en statlig e-legitimation.

8.5 En statlig e-legitimation ska ha en begränsad giltighetstid

Regeringens förslag

Den statliga e-legitimationen ska ha en giltighetstid om fem år. Om sökanden inte har fyllt tolv år ska giltighetstiden vara tre år.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om att den statliga e-legitimationen i särskilt angivna fall ska ha en kortare giltighetstid.

Utredningens förslag

Förslaget från utredningen stämmer i sak överens med regeringens. Utredningen föreslår att giltighetstiden ska regleras i förordning.

Remissinstanserna

Samtliga remissinstanser tillstyrker eller har inga synpunkter på förslaget.

Skälen för regeringens förslag

Ett identitetskort för folkbokförda i Sverige är giltigt i högst fem år. Även pass och nationellt identitetskort är som huvudregel giltiga i fem år. För sökande under tolv år begränsas giltighetstiden dock till högst tre år. Giltighetstiden har ansetts vara av stor betydelse ur ett säkerhetsperspektiv, eftersom innehavarens utseende förändras över tid. Barns utseende genomgår vidare väsentliga förändringar under uppväxtåren, vilket kan göra det svårt att avgöra om ansiktsbilden verkligen föreställer innehavaren efter en tid. Eftersom detta ökar risken för att barns identitetshandlingar missbrukas har det ansetts motiverat med en kortare giltighetstid för barn, trots att det kan medföra vissa praktiska svårigheter och ökade kostnader för barnfamiljer (prop. 2015/16:81 s. 20–22).

Det saknas skäl att ha en annan giltighetstid för den statliga e-legitimationen än den som gäller för andra identitetshandlingar. Giltighetstiden för den statliga e-legitimationen bör därför vara högst fem år. För

barn under tolv år bör giltighetstiden dock vara högst tre år. Regeringen anser att huvudregeln om giltighetstiden för den statliga e-legitimationen är av sådan central betydelse att den bör anges direkt i lagen (jfr prop. 1977/78:156 s. 42 och 43). Regeringen eller den myndighet som regeringen bestämmer bör dock få meddela föreskrifter om att den statliga e-legitimationen i särskilt angivna fall ska ha en kortare giltighetstid. Det kan t.ex. behövas om den statliga e-legitimationen placeras på en statlig identitetshandling med en kortare giltighetstid. Om e-legitimationen placeras på det nationella identitetskortet kan giltighetstiden behöva begränsas till den tidpunkt när en person kan antas förlora sitt svenska medborgarskap, se 5 § förordningen om nationella identitetskort.

8.6 En statlig e-legitimation ska i vissa fall kunna återkallas och spärras

Regeringens förslag

En statlig e-legitimationen ska återkallas och spärras om
- det fanns hinder mot att utfärda e-legitimationen vid tiden för utfärdandet och hindret fortfarande består,
- någon väsentlig uppgift som e-legitimationen innehåller är felaktig,
- det är nödvändigt av säkerhetsskäl,
- den är utfärdad på en fysisk identitetshandling som därefter har upphört att gälla, eller
- innehavaren har avlidit.

En statlig e-legitimation ska vidare kunna återkallas och spärras på begäran av innehavaren. Om begäran avser ett barn under arton år ska vårdnadshavares medgivande krävas, om det inte finns synnerliga skäl för återkallelsen och spärren.

En statlig e-legitimation ska också spärras i samband med att en ny lämnas ut till sökanden eller när giltighetstiden har löpt ut.

Lagen ska innehålla en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om förfarandet vid återkallelse och spärr av statlig e-legitimation.

Utredningens förslag

Förslagen från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att vissa utpekade situationer ska föranleda återkallelse och spärr på grund av säkerhetsskäl. Utredningen föreslår vidare att återkallelse och spärr ska ske om e-legitimationen inte har aktiverats inom sex månader från att ansökan gjordes. Utredningen föreslår inte att den statliga e-legitimationen ska återkallas och spärras om den är utfärdad på en fysisk identitetshandling som därefter har upphört att gälla. Utredningen föreslår inte heller någon bestämmelse om vårdnadshavares medgivande för återkallelse och spärr. Utredningen föreslår slutligen att en statlig e-legitimation ska spärras senast i samband med att en ny utfärdas.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen*, *Falköpings kommun*, *Försäkringskassan*, *Länsstyrelsen i Blekinge län*, *Statens tjänstepensionsverk* och *Totalförsvarets forskningsinstitut*, tillstyrker eller har inga synpunkter på förslaget.

Riksförbundet för barn, unga och vuxna med intellektuell funktionsnedsättning anser att spärren av en e-legitimation bör kunna hävas när en bedrägerisituation inte längre är aktuell eller att innehavaren annars ska erbjudas en ny kostnadsfri e-legitimation. *Finansiell ID-Teknik BID AB* anser att även brottsutredande myndigheter bör kunna återkalla och spärra e-legitimationer från samtliga utfärdare vid misstanke om att de används vid brott. *Svenska bankföreningen* anser att det bör övervägas en begränsning i antal utfärdade e-legitimationer som en person kan få. Vid upprepade förlustanmälningar bör det inte gå att beställa en ny statlig e-legitimation utan någon trovärdig förklaring till att den tidigare kommit bort, menar föreningen. *E-hälsomyndigheten* ser en risk för missbruk av möjligheten att spärra en e-legitimation på innehavarens begäran och framhåller vikten av att det säkerställs att begäran görs av rätt person. *Skatteverket* anser att det finns andra säkerhetsskäl än de uppräknade som bör aktualisera en återkallelse, t.ex. när någon använder sin egen e-legitimation som ett led i ett brottsligt förfarande.

Myndigheten för digital förvaltning avstyrker utredningens förslag om att den statliga e-legitimationen ska spärras när giltighetstiden har löpt ut, eftersom giltighetstiden kontrolleras vid autentisering med e-legitimationen. Vidare önskar myndigheten ett förtydligande av vad som avses med återkallelse av e-legitimation eftersom den fysiska bäraren inte ska lämnas tillbaka om e-legitimationen har spärrats eller blivit ogiltig.

Skälen för regeringens förslag

En statlig e-legitimation bör kunna återkallas och spärras

Den statliga e-legitimationen ska vara ett tillförlitligt bevis för innehavarens identitet. Den som erbjuder möjlighet till elektronisk identifiering med en statlig e-legitimation ska kunna vara säker på att den har utfärdats på rätt sätt och att uppgifterna om innehavaren är korrekta. En statlig e-legitimation bör därför kunna återkallas i vissa fall.

En statlig e-legitimation som har återkallats eller upphört att gälla bör göras obrukbar genom att den spärras elektroniskt. Med spärr avses den tekniska åtgärd som gör att e-legitimationen blir permanent obrukbar på grund av ett beslut om återkallelse eller att e-legitimationen av andra skäl har upphört att gälla.

Regeringen anser, till skillnad från *Finansiell ID-Teknik BID AB*, att det är tillräckligt att utfärdande myndighet beslutar om återkallelse och spärr av den statliga e-legitimationen.

Det finns inget behov av att e-legitimationen ska återlämnas efter att den har återkallats och spärrats, oavsett om den tillhandahålls på en egen fysisk bärare eller en nationell identitetshandling, eftersom den kommer att bli obrukbar efter sådana åtgärder. I det senare fallet skulle identitetshandlingen dessutom fortsatt kunna vara giltig även om e-legitimationen återkallats och spärrats.

Regeringen anser vidare, till skillnad från *Riksförbundet för barn, unga och vuxna med intellektuell funktionsnedsättning*, att det inte bör införas någon möjlighet att häva en spärr om det exempelvis skulle visa sig att grunden för återkallelse har upphört. Syftet med det skulle främst vara att bespara den enskilde en ny ansökningsprocess och att undvika administration för utfärdande myndighet i samband med en ny ansökan. En sådan lösning framstår dock inte som lämplig av säkerhetsskäl. Förslaget om att den statliga e-legitimationen ska spärras i vissa fall hindrar dock inte att det meddelas föreskrifter om tillfällig begränsning av innehavarens användning av den statliga e-legitimationen, t.ex. vid upprepade felslagningar av inloggningsuppgifter (se avsnitt 8.7).

Det ligger utanför detta lagstiftningsärende att, som Finansiell ID-Teknik BID AB efterfrågar, föreslå åtgärder för spärr av andra e-legitimationer än den statliga e-legitimationen. *Svenska bankföreningen* framför att det bör övervägas en begränsning i antal utfärdade e-legitimationer som en person kan få. Enligt regeringens bedömning finns det för närvarande inte anledning att införa en sådan begränsning.

Den nya lagen bör innehålla en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om förfarandet vid återkallelse och spärr av statlig e-legitimation. Sådana föreskrifter kan t.ex. avse hur en begäran om återkallelse från innehavaren ska vara utformad.

I det följande redogörs för de återkallelsegrunder som regeringen anser bör införas och andra fall som bör leda till att en statlig e-legitimation spärras.

Återkallelse om det fanns hinder mot att utfärda e-legitimationen

En statlig e-legitimation bör kunna återkallas om det efter utfärdandet visar sig att det fanns hinder mot det vid tidpunkten för utfärdandet och hindret fortfarande består. En liknande bestämmelse finns för pass, det nationella identitetskortet och identitetskortet för folkbokförda (jfr 12 § 8 passlagen, 9 § förordningen om nationellt identitetskort och 6 § lagen om identitetskort för folkbokförda i Sverige). Det skulle t.ex. finnas grund för återkallelse om innehavaren har fått en e-legitimation i en annan persons namn (jfr prop. 2015/16:28 s. 55) eller om något annat av de krav som ställs i samband med ansökan inte var uppfyllt vid tiden för utfärdandet och det inte har blivit uppfyllt i efterhand (jfr prop. 1977/78:156 s. 48).

Återkallelse om väsentliga uppgifter i den statliga e-legitimationen är felaktiga

Det bör finnas skäl att återkalla en statlig e-legitimation om den innehåller väsentliga uppgifter som är felaktiga. En liknande återkallelsegrund finns för identitetskort för folkbokförda i Sverige (6 § lagen om identitetskort för folkbokförda i Sverige). Förändrade uppgifter kan medföra att nya säkerhetsöverväganden måste göras eller att förutsättningarna för utfärdande inte längre kan anses vara uppfyllda, även om de var det när e-legitimationen utfärdades. Så kan exempelvis vara fallet vid namnbyte eller byte av personnummer.

Återkallelse om det är nödvändigt av säkerhetsskäl

En statlig e-legitimation bör kunna återkallas om säkerhetsbrister upptäcks eller om det finns misstanke om att den används i brottslig verksamhet. Grund för återkallelse kan t.ex. finnas när någon annan än den som e-legitimationen är utställd till kan misstänkas obehörigen förfoga över e-legitimationen eller om den som e-legitimationen är utställd till själv använder den för brottslig verksamhet, exempelvis i en bulvansituation. Regeringen anser, i likhet med *Skatteverket*, att möjligheten att återkalla en statlig e-legitimation av säkerhetsskäl inte bör vara begränsad till vissa i lagen angivna situationer.

Återkallelse om den statliga e-legitimationen är utfärdad på en fysisk identitetshandling som därefter har upphört att gälla

Den statliga e-legitimationen ska kunna utfärdas på en fysisk identitetshandling, t.ex. det nationella identitetskortet (se avsnitt 8.3). Om den statliga e-legitimationen har utfärdats på en fysisk identitetshandling som därefter har upphört att gälla, t.ex. om giltighetstiden har gått ut eller den har återkallats, bör den statliga e-legitimationen återkallas och spärras.

Återkallelse efter begäran från innehavaren eller när innehavaren avlidit

Den statliga e-legitimationen bör kunna återkallas efter begäran av innehavaren, t.ex. om bäraren av e-legitimationen kommit bort, jfr 5 kap. 1 § Polismyndighetens föreskrifter och allmänna råd om pass och nationellt identitetskort (PMFS 2021:3, FAP 530-1). Som *E-hälsomyndigheten* påpekar är det givetvis av stor vikt att det säkerställs att en sådan begäran görs av den som e-legitimationen är utställd till. Den närmare reglering som behövs för förfarandet vid en sådan begäran bör dock regleras i förordning eller myndighetsföreskrifter.

På samma sätt som för ansökan av en statlig e-legitimation bör det krävas vårdnadshavares medgivande för återkallelse och spärr av en statlig e-legitimation som är utfärdad till ett barn, om det inte finns synnerliga skäl för att ändå återkalla och spärra e-legitimationen. Det bör bl.a. anses finnas synnerliga skäl om en av föräldrarna är tillfälligt förhindrad att lämna sitt medgivande, t.ex. på grund av sjukdom, och det är uppenbart att dennes medgivande annars skulle ha lämnats (jfr avsnitt 8.2). Det kan också finnas situationer där återkallelse och spärr bör ske utan vårdnadshavares medgivande, t.ex. om e-legitimationen används i brottslig verksamhet och den enskilde skulle lida skada om återkallelsen och spärren skulle dröja.

Regeringen anser slutligen att en e-legitimation även bör kunna återkallas om innehavaren avlidit.

En statlig e-legitimation bör spärras i samband med att en ny lämnas ut och när giltighetstiden löpt ut

Utredningen har föreslagit att en statlig e-legitimation ska spärras senast i samband med att en ny e-legitimation utfärdas, exempelvis i ett fall då den enskilde ansöker om en ny e-legitimation innan giltighetshetstiden har löpt ut. Regeringen anser att det bör finnas en sådan möjlighet till spärr av säkerhetsskäl och för att det inte ska vara möjligt att inneha fler än en statlig e-legitimation samtidigt. Av samma skäl bör en statlig e-legitimation

alltid spärras när giltighetstiden löpt ut, till skillnad från vad *Myndigheten för digital förvaltning* anser. Regeringen anser dock att spärr i samband med utfärdande av en ny e-legitimation bör ske vid utlämnande av den nya e-legitimationen. På så sätt riskerar inte den enskilde att vara utan e-legitimation under tiden mellan utfärdandet och utlämnandet av den nya e-legitimationen.

Det saknas skäl att återkalla en statlig e-legitimation på grund av att den inte har tagits i bruk inom en viss tid

Regeringen anser, till skillnad från utredningen, att det inte finns behov av att återkalla en e-legitimation på grund av att den inte har aktiverats inom sex månader från tiden för ansökan.

8.7 Användningen av den statliga e-legitimationen

Regeringens förslag

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om villkor för användningen av den statliga e-legitimationen.

Utredningens förslag

Förslaget från utredningen stämmer i sak överens med regeringens. Utredningens förslag har en annan redaktionell utformning.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *Arbetsförmedlingen*, *Finansinspektionen*, *Helsingborgs kommun* och *Säkerhetspolisen*, tillstyrker eller har inga synpunkter på förslaget. *Myndigheten för digital förvaltning* anser att det är oklart om bemyndigandet innefattar en rätt att föreskriva om användning av biometriska uppgifter. *Konkurrensverket* anser att det behövs ett förtydligande av hur utfärdande myndighet får agera gentemot privata aktörer som vill erbjuda sina användare möjlighet att legitimera sig med den statliga e-legitimationen. Sådana aktörer har inte möjlighet att anskaffa tjänsten genom auktorisationssystem, påpekar myndigheten.

Skälen för regeringens förslag

Regeringen bedömer att den statliga e-legitimationen bör anslutas till ett auktorisationssystem enligt lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post. Den kommer då att bli en av de tjänster för elektronisk identifiering som statliga myndigheter under regeringen i vissa fall måste använda i sina nättjänster (se avsnitt 7.1). Utöver den användning som kommer att följa av auktorisationssystemet kan den statliga e-legitimationen även komma att användas i privata aktörers nättjänster.

Syftet med en statlig e-legitimation är främst att den ska kunna användas för identifiering. Mot bakgrund av de risker som finns med användningen,

bl.a. risken för obehörig användning, kan det finnas anledning att meddela föreskrifter om villkor i fråga om vilka situationer den statliga e-legitimationen ska kunna användas. Det kan t.ex. behöva regleras vilka krav som ska ställas för att en aktör, offentlig eller privat, ska få använda identifiering med den statliga e-legitimationen i sin nättjänst, men även meddelas villkor för enskildas användning. Sådana villkor kan behöva ställas för att säkerställa att den statliga e-legitimationen inte används i oseriösa sammanhang. Ett annat villkor för ökad säkerhet kan exempelvis vara kontroll av biometriska uppgifter i samband med identifiering eller vid betalningstransaktioner. Det bör även ges möjlighet att meddela föreskrifter om att tillfälligt begränsa innehavarens användning av den statliga e-legitimationen, t.ex. vid upprepade felslagningar av inloggningsuppgifter (se avsnitt 8.6). Regeringen eller den myndighet som regeringen bestämmer bör därför få meddela föreskrifter om användningen av den statliga e-legitimationen.

Under vilka förutsättningar privata aktörer kommer att få använda den statliga e-legitimationen för identifiering i sina nättjänster, som *Konkurrensverket* efterfrågar ett förtydligande av, är en sådan fråga som kan regleras i förordning eller myndighetsföreskrifter.

8.8 Utfärdande myndighet

Regeringens förslag

Den statliga e-legitimationen ska utfärdas av utfärdande myndighet. Utfärdande myndighet ska fullgöra de uppgifter som anges i den nya lagen och föreskrifter som har meddelats i anslutning till lagen.

Polismyndigheten ska vara utfärdande myndighet inom riket.

Utom riket ska beskickningar och karriärkonsulat fullgöra uppgifter som utfärdande myndighet i den utsträckning som beslutas av regeringen eller den myndighet som regeringen bestämmer.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att det ska utses identitetskontrollerande myndighet och utfärdande myndighet på förordningsnivå.

Remissinstanserna

Ingen remissinstans yttrar sig särskilt över förslaget om att regeringen ska få utse utfärdande myndighet. Flera remissinstanser, bl.a. *Afasiförbundet i Sverige*, *Diskrimineringsombudsmannen*, *Försvarsmakten*, *Försäkringskassan*, *Polismyndigheten*, *Svensk Handel*, *Sveriges advokatsamfund* och *Säkerhetspolisen* anser att samma myndighet bör ansvara för grundidentifiering och utfärdande av e-legitimationen. Några myndigheter, bl.a. *Svensk handel*, förordar att Polismyndigheten ska utses till utfärdande myndighet.

Skälen för regeringens förslag

I avsnitt 8.2 föreslår regeringen att det ska göras en kontroll av sökandens identitet i samband med en ansökan om statlig e-legitimation. Det finns en upparbetad kunskap hos flera befintliga myndigheter som bör utnyttjas vid valet av utfärdande myndighet. Det finns t.ex. myndigheter som har kunskap om hur identitetskontroller ska göras och som arbetar med att motverka identitetsrelaterad brottslighet. Det finns även erfarenhet av bl.a. den hantering av ansiktsbild och fingeravtryck som regeringen föreslår i avsnitt 9.4, och som kräver särskild säkerhet i processen.

Polismyndigheten ansvarar i dag för utfärdandet av pass och nationellt identitetskort inom riket. Utom riket ansvarar bl.a. beskickningar och karriärkonsulat för utfärdandet av dessa identitetshandlingar (2 § passlagen och 1 § förordningen om nationellt identitetskort). Polismyndigheten, beskickningarna och karriärkonsulaten har därigenom en upparbetad kunskap och tillgång till utrustning för att hantera utfärdandet av nationella identitetshandlingar. Regeringen bedömer mot denna bakgrund, i likhet med *Svensk handel*, att det är lämpligt att dessa myndigheter även ansvarar för utfärdandet av den statliga e-legitimationen. Den statliga e-legitimationen ska dessutom kunna utfärdas på en nationell identitetshandling, vilket också talar för att uppgiften ges till dessa myndigheter. Polismyndigheten bör alltså vara utfärdande myndighet inom riket. Utom riket bör beskickningar och karriärkonsulat fullgöra uppgifter som utfärdande myndighet i den utsträckning som beslutas av regeringen eller den myndighet som regeringen bestämmer.

Genom den valda lösningen kommer en myndighet att ansvara för såväl grundidentifieringen som utfärdandet av e-legitimationen, vilket förordas av många remissinstanser, bl.a. *Försvarsmakten* och *Sveriges advokatsamfund*. Förslaget utgör dock inte något hinder för att den utfärdande myndigheten kan ingå serviceavtal med en annan myndighet om att för dennes räkning lämna upplysningar, vägledning, råd och i övrigt handlägga förvaltningsärenden enligt lagen (2019:212) om viss gemensam offentlig service.

De myndigheter som kommer att ansvara för utfärdandet av den statliga e-legitimationen bör i lagen kallas för utfärdande myndighet.

8.9 Ansökan om en statlig e-legitimation ska avgiftsbeläggas

Regeringens förslag

Utfärdande myndighet ska få ta ut avgifter för ansökan om en statlig e-legitimation.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om avgifterna.

Utredningens förslag

Förslagen från utredningen stämmer i huvudsak överens med regeringens. Utredningen föreslår inte något bemyndigande avseende föreskrifter om avgifterna.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *Diskrimineringsombudsmannen*, *Ekonomistyrningsverket*, *Kommerskollegium*, *Polismyndigheten* och *Upphandlingsmyndigheten*, tillstyrker eller har inga synpunkter på förslaget. Några remissinstanser, bl.a. *Afasiförbundet i Sverige* och *Funktionsrätt Sverige*, anser att det inte bör tas ut någon avgift eftersom det riskerar att leda till att vissa grupper som saknar ekonomiska förutsättningar inte kommer att ansöka om en statlig e-legitimation.

Skälen för regeringens förslag

Uppgiften att utfärda den statliga e-legitimationen ska enligt förslaget läggas på statliga myndigheter (se avsnitt 8.8). Regeringen bedömer, till skillnad från bl.a. *Funktionsrätt Sverige*, att verksamheten med den statliga e-legitimationen bör avgiftsfinansieras. Regeringen eller den myndighet som regeringen bestämmer bör få meddela föreskrifter om avgifterna för ansökan om statlig e-legitimation. Det kan t.ex. röra sig om storleken på avgifterna. Det skulle också kunna vara aktuellt med olika avgifter om e-legitimationen placeras på olika bärare. Avgifterna kan även behöva anpassas och samordnas med befintliga avgifter om e-legitimationen placeras på en nationell identitetshandling.

Huvudregeln enligt avgiftsförordningen (1992:191) är att avgifter ska beräknas så att de helt täcker verksamhetens kostnader (full kostnadstäckning). Till skillnad från utredningen anser regeringen att huvudregeln om full kostnadstäckning bör följas. Regeringen bedömer vidare att avgifternas nivå inte kommer att bli så hög att det kommer att påverka viljan eller möjligheten för majoriteten av befolkningen att ansöka om en statlig e-legitimation. Som bl.a. *Afasiförbundet i Sverige* påpekar kan vissa grupper dock komma att se avgiften som ett hinder för att skaffa en statlig e-legitimation. De som saknar ekonomiska förutsättningar bör dock ha möjlighet att ansöka om ekonomiskt bistånd till en statlig e-legitimation.

9 Personuppgiftsbehandling i verksamheten med den statliga e-legitimationen

9.1 Bestämmelser om personuppgiftsbehandling i den nya lagen om statlig e-legitimation och elektronisk identifiering

Regeringens förslag

Bestämmelserna om personuppgiftsbehandling i den nya lagen ska komplettera EU:s dataskyddsförordning.

Vid behandling av personuppgifter enligt lagen ska dataskyddslagen och föreskrifter som har meddelats i anslutning till dataskyddslagen gälla, om inte annat följer av den nya lagen eller föreskrifter som har meddelats i anslutning till den.

Varje utfärdande myndighet ska vara personuppgiftsansvarig för den behandling av personuppgifter som myndigheten själv utför. Polismyndigheten ska vara personuppgiftsansvarig för behandling av personuppgifter i registret över ärenden om statlig e-legitimation.

Utredningens förslag

Förslagen från utredningen stämmer i sak överens med regeringens. Utredningen föreslår att personuppgiftsansvariga myndigheter ska pekas ut i förordning.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *Kammarkollegiet*, *Svenska bankföreningen*, *Säkerhetspolisen* och *Åklagarmyndigheten*, tillstyrker eller har inga synpunkter på förslaget. Flera remissinstanser, bl.a. *Länsstyrelsen i Gävleborgs län*, framför att något personuppgiftsbiträdesförhållande inte borde aktualiseras. *Länsstyrelsen i Stockholms län* framför att det borde vara tillräckligt att precisera ändamålen för respektive myndighets behandling av personuppgifter för att ansvarsfördelningen ska vara tydlig. *Sveriges advokatsamfund* anser att bestämmelserna om personuppgiftsansvar behöver vara tydligare och precisera vad berörda myndigheter ansvarar för. *Myndigheten för digital förvaltning* anser att utfärdande myndighet bör ges rätt att meddela föreskrifter om personuppgiftsbiträdesavtal.

Integritetsskyddsmyndigheten framför att det behövs en redogörelse för om de parter som kommer att erbjuda nättjänster där den statliga e-legitimationen används kommer att behandla personuppgifter och i så fall om det finns grund för sådan behandling. *Patent- och registreringsverket* framför en liknande synpunkt. Myndigheten menar att de som erbjuder nättjänster behöver spara åtminstone personnummer för att e-legitimationen över tid ska fungera.

Utfärdande myndigheter får behandla personuppgifter

Utfärdande myndigheter kommer att behandla personuppgifter i verksamheten med den statliga e-legitimationen. Bestämmelser om behandling av personuppgifter finns i 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 upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i fortsättningen EU:s dataskyddsförordning, och i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, i fortsättningen dataskyddslagen.

En förutsättning för att EU:s dataskyddsförordning ska vara tillämplig är att personuppgifter behandlas. Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person som är i livet. Det avgörande är om den personuppgiftsansvarige eller någon annan kan knyta den aktuella uppgiften, ensamt eller i kombination med andra uppgifter, till en individ (artikel 4.1 och skäl 26 och 27 i EU:s dataskyddsförordning). Behandling är ett brett begrepp och omfattar exempelvis insamling, registrering, lagring, bearbetning, framtagning, läsning, utlämnande genom överföring, spridning, radering eller förstöring (artikel 4.2). Av artikel 6 i EU:s dataskyddsförordning framgår att all behandling av personuppgifter ska vila på en rättslig grund. Utan rättslig grund är behandlingen inte tillåten. Rättslig grund finns bl.a. om behandlingen är nödvändig för att fullgöra en rättslig förpliktelse (artikel 6.1 c), för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1 e). Den grund för behandlingen som avses i artikel 6.1 c och e ska enligt artikel 6.3 fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av.

Enligt artikel 6.3 i EU:s dataskyddsförordning ska syftet med behandlingen, i fråga om behandling enligt artikel 6.1 e, vara nödvändig för att utföra en uppgift av allmänt intresse. Ändamålet med varje enskild behandling måste vara nödvändig för att utföra den fastställda uppgiften. Detta krav på samband framgår även av artikel 5.1 b, där det anges att de särskilda ändamålen ska vara berättigade.

Biometriska uppgifter för att entydigt identifiera en fysisk person får som huvudregel inte behandlas (artikel 9.1) och är att betrakta som känsliga uppgifter, se 3 kap. 2 § dataskyddslagen. Undantag gäller bl.a. om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse (artikel 9.2 g). Personnummer och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl (3 kap. 10 § dataskyddslagen).

Artikel 10 i EU:s dataskyddsförordning innehåller särskilda bestämmelser om behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder (personuppgifter som rör lagöverträdelser). Utöver de villkor som gäller vid all behandling av personuppgifter gäller att personuppgifter som rör lagöverträdelser endast får behandlas under kontroll av en myndighet eller om behandlingen är tillåten enligt unionsrätten eller medlemsstaternas

nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.

En utfärdande myndighets behandling av personuppgifter kommer bl.a. att avse sökandens namn, person- eller samordningsnummer, medborgarskap och ansiktsbild. För underåriga kommer det även att avse uppgifter om vårdnadshavare. Myndigheten kan även komma att behandla personuppgifter som rör lagöverträdelser i samband med återkallelse och spärr av en statlig e-legitimation. Behandlingen är nödvändig för att en utfärdande myndighet ska kunna fullgöra den nya lagens krav avseende handläggning av ärenden om statlig e-legitimation. Det gäller både den behandling som utförs inom ramen för enskilda ärenden och den som sker i myndighetens register. Behandlingen av personuppgifter kommer alltså att grundas på en rättslig förpliktelse som följer av lag. Behandlingen av personnummer och samordningsnummer är bl.a. nödvändig för att tillgodose behovet av en säker identifiering (jfr 3 kap. 10 § dataskyddslagen). Handläggningen av ärenden om statlig e-legitimation kommer vidare att innefatta myndighetsutövning och behandlingen är därför även nödvändig som ett led i myndighetsutövning. Att uppgiften följer av lag innebär att den också ska anses vara av allmänt intresse (prop. 2017/18:105 s. 56 och 57). Behandlingen av personuppgifter är även nödvändig för att säkerställa att den statliga e-legitimationen är tillförlitlig och korrekt utfärdad. Regeringen gör mot denna bakgrund bedömningen att den behandling av personuppgifter som behövs i verksamheten med den statliga e-legitimationen är proportionerlig i förhållande till de angivna syftena, bl.a. att säkerställa en säker grundidentifiering och ett korrekt utfärdande (se vidare avsnitt 8.2 och 9.4). Behandlingen av personuppgifter är därmed tillåten enligt EU:s dataskyddsförordning, dataskyddslagen och de föreskrifter som har meddelats med stöd av lagen. Detta gäller även behandlingen av biometriska uppgifter (se avsnitt 9.4).

Personuppgiftsansvaret bör framgå av lagen

EU:s dataskyddsförordning tillåter nationella bestämmelser som anger vilken eller vilka myndigheter som ska ha personuppgiftsansvaret för en viss behandling av personuppgifter (artikel 4.7). Eftersom flera myndigheter kommer att vara involverade i verksamheten med den statliga e-legitimationen bör det, till skillnad från vad *Länsstyrelsen i Stockholms län* anser, framgå tydligt i lagen vilka myndigheter som är personuppgiftsansvariga för behandlingen av personuppgifter.

I verksamheten med den statliga e-legitimationen kommer personuppgifter att behandlas vid handläggningen av enskilda ärenden och i registret över ärenden om statlig e-legitimation. Som huvudregel bör den myndighet som bestämmer över personuppgiftsbehandlingen också ansvara för behandlingen, om det inte finns skäl för något annat (jfr t.ex. prop. 2014/15:148 s. 32–34 och prop. 2015/16:65 s. 55).

I avsnitt 8.8 föreslår regeringen att Polismyndigheten ska vara utfärdande myndighet inom riket och att beskickningar och karriärkonsulat, i den utsträckning som regeringen bestämmer, ska fullgöra uppgifter som utfärdande myndighet utom riket. Såväl Polismyndigheten som beskickningarna och karriärkonsulaten är självständiga myndigheter. En utfär-

dande myndighet kommer att sköta de uppgifter och utföra den personuppgiftsbehandling som följer av lagen. Detta talar för att varje myndighet också ska ansvara för den personuppgiftsbehandling som myndigheten utför. Till skillnad från *Sveriges advokatsamfund* anser regeringen att personuppgiftsansvaret kopplat till varje specifik uppgift inte behöver preciseras i lagen. Regeringen anser mot denna bakgrund att det i lagen bör anges att varje utfärdande myndighet ska vara personuppgiftsansvarig för den behandling av personuppgifter som myndigheten själv utför. Eftersom Polismyndigheten ska ansvara för registret över ärenden om statlig e-legitimation bör det i lagen även anges att myndigheten ansvarar för personuppgiftsbehandlingen i registret (se avsnitt 9.3).

Flera remissinstanser, bl.a. *Länsstyrelsen i Gävleborgs län*, framför att något personbiträdesförhållande inte borde aktualiseras. Vem som är att betrakta som personuppgiftsbiträde följer av EU:s dataskyddsförordning (se t.ex. artikel 28). Regeringen anser därför, till skillnad från *Myndigheten för digital förvaltning*, att frågan inte behöver regleras särskilt. Det måste vara upp till den personuppgiftsansvarige att bedöma vem som är att betrakta som personuppgiftsbiträde och se till att nödvändiga avtal finns.

Offentliga aktörer som erbjuder nättjänster kommer också att behandla personuppgifter

Som bl.a. *Integritetsskyddsmyndigheten* framför kommer offentliga aktörer som erbjuder nättjänster med möjlighet till legitimering med e-legitimation sannolikt att behandla personuppgifter. Sådan personuppgiftsbehandling sker dock redan i dessa aktörers verksamhet. De förslag som regeringen lämnar i denna proposition innebär inte någon tillkommande personuppgiftsbehandling för offentliga aktörer. Det finns därför inte anledning att redogöra för offentliga aktörers personuppgiftsbehandling inom ramen för sina respektive verksamheter.

Grundläggande bestämmelser om personuppgiftsbehandling bör införas i lag

Skydd för den personliga integriteten vid behandling av personuppgifter regleras även i regeringsformen. Enligt 2 kap. 6 § andra stycket regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Begreppet personliga förhållanden har samma innebörd som i sekretesslagstiftningen och omfattar bl.a. namn och andra identifikationsuppgifter (prop. 2009/10:80 s. 177).

Avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning är inte dess huvudsakliga syfte utan vilken effekt åtgärden har. Vid bedömningen av vilka åtgärder som kan anses utgöra betydande intrång ska bl.a. åtgärdens omfattning och arten av det intrång åtgärden innebär beaktas (prop. 2009/10:80 s. 181 och 184). Grundlagsskyddet får enligt 2 kap. 20 § första stycket regeringsformen endast begränsas genom lag. Det ställs också krav på att begränsningar endast får göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle, se 2 kap. 21 § regeringsformen. Konstitutionsutskottet har i flera lagstiftningsärenden som rört myndigheters personuppgiftsbehandling framhållit att

målsättningen bör vara att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras särskilt i lag (se t.ex. bet. 1990/91:KU11 s. 11 och bet. 1997/98:KU18 s. 43). Regeringen har vid åtskilliga tillfällen instämt i den bedömningen (se t.ex. prop. 1999/2000:39 s. 78).

Utfärdande myndighets behandling av personuppgifter i verksamheten med den statliga e-legitimationen kommer sannolikt att avse många personer och därmed omfatta dels ett stort antal uppgifter, dels flera personliga identifikationsuppgifter, t.ex. namn, person- eller samordningsnummer och medborgarskap. Utfärdande myndighet kommer också att behandla integritetskänsliga uppgifter, såsom ansiktsbild och fingeravtryck med tillhörande biometriska uppgifter. Behandlingen kommer bl.a. att ske vid handläggningen av enskilda ärenden och i register. Mot denna bakgrund får behandlingen anses innebära en sådan kartläggning av enskildas personliga förhållanden som avses i 2 kap. 6 § andra stycket regeringsformen, även om syftet med behandlingen är ett annat.

Bestämmelsen i 2 kap. 6 § andra stycket regeringsformen omfattar endast sådant intrång i den personliga integriteten som är betydande. Vid bedömningen av hur ingripande intrånget anses vara i samband med insamling, lagring och bearbetning eller utlämnande av uppgifter om enskildas personliga förhållanden är det naturligt att stor vikt läggs vid uppgifternas karaktär och ändamålet med behandlingen. Därutöver kan mängden uppgifter vara en betydelsefull faktor i sammanhanget (jfr prop. 2009/10:80 s. 183).

Ändamålen med behandlingen av personuppgifter i verksamheten med den statliga e-legitimationen är bl.a. att möjliggöra handläggningen av ärenden om statlig e-legitimation, säkerställa att utfärdandet sker till rätt person och därigenom motverka missbruk av e-legitimationen (se vidare avsnitt 9.2 om ändamålen med personuppgiftsbehandlingen). Som anges ovan kommer personuppgiftsbehandlingen att avse vissa personliga identifikationsuppgifter och ansiktsbild och fingeravtryck med tillhörande biometriska uppgifter. Merparten av de uppgifter som kommer att behandlas är dock inte av känslig karaktär. Vidare väljer den enskilde själv om den vill ansöka om en statlig e-legitimation och kommer då att ha kännedom om vilka personuppgifter som en utfärdande myndighet kommer att behandla med anledning av ansökan. Mot denna bakgrund anser regeringen att det inte rör sig om ett sådant betydande intrång i den personliga integriteten att grundlagsskyddet i 2 kap. 6 § andra stycket regeringsformen blir tillämpligt. Eftersom utfärdande myndigheter kommer att behandla en stor mängd uppgifter om enskilda i verksamheten med den statliga e-legitimationen anser regeringen dock att ramarna för behandlingen bör regleras i lag.

Förhållandet till EU:s dataskyddsförordning och dataskyddslagen bör anges i lagen

Lagen om statlig e-legitimation och elektronisk identifiering föreslås innehålla bestämmelser som kompletterar EU:s dataskyddsförordning. Att lagen kompletterar förordningen bör anges i en särskild bestämmelse i lagen. Lagens hänvisningar till EU:s dataskyddsförordning bör vara utformade på så sätt att de avser förordningen i den vid varje tidpunkt

gällande lydelsen, s.k. dynamisk hänvisning. Genom dynamiska hänvisningar säkerställs att eventuella ändringar i förordningen får omedelbart genomslag. Det kan dock inte uteslutas att den nya lagen ändå kan behöva ändras i samband med ändringar i EU:s dataskyddsförordning (prop. 2017/18:105 s. 24). Det bör också anges att vid behandling av personuppgifter som omfattas av EU:s dataskyddsförordning gäller även dataskyddslagen och föreskrifter som har meddelats i anslutning till den lagen, om inte annat följer av lagen om statlig e-legitimation och elektronisk identifiering eller föreskrifter som regeringen har meddelat i anslutning till den lagen (jfr 1 kap. 6 § dataskyddslagen).

9.2 Ändamålen med personuppgiftsbehandlingen

Regeringens förslag

Personuppgifter ska få behandlas av utfärdande myndighet om det är nödvändigt för att
- handlägga ärenden om statlig e-legitimation,
- föra ett register över ärenden om statlig e-legitimation, och
- vidta åtgärder för en säker användning av statliga e-legitimationer.

Personuppgifter som behandlas för dessa ändamål ska även få behandlas
- om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet,
- om det är nödvändigt för att lämna ut uppgifter i enlighet med lag eller förordning, och
- för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Känsliga personuppgifter ska endast få behandlas i verksamheten med den statliga e-legitimationen om det är absolut nödvändigt för ändamålet med behandlingen.

Utredningens förslag

Förslaget från utredningen stämmer i sak överens med regeringens. Utredningen föreslår en särskild bestämmelse om att utfärdande myndighet ska få behandla personuppgifter om det är nödvändigt för att kontrollera en sökandes identitet i samband med ansökan. Utredningen föreslår vidare att ordet databas ska användas i stället för register.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *AB Svenska pass*, *Diskrimineringsombudsmannen*, *Internetstiftelsen* och *Växjö kommun*, tillstyrker eller har inga synpunkter på förslaget. *Integritetsskyddsmyndigheten* framför att

integritetsanalysen även bör omfatta en redogörelse för vilka skyddsåtgärder som krävs för att behandlingen ska anses vara proportionerlig, t.ex. om det går att begränsa möjligheten att lämna uppgifter för brottslighet av viss allvarlighetsgrad. *Myndigheten för digital förvaltning* anser att ändamålen med personuppgiftsbehandlingen inte bör anges uttryckligen, eftersom det följer av de materiella bestämmelserna. Vidare anser myndigheten att begreppet register bör användas i stället för databas. *Chalmers tekniska högskola AB* framför att det är av vikt att det säkerställs att informationen i registret bara används för nödvändiga ändamål. *Pensionsmyndigheten* framför att det bör införas bestämmelser, likt de i 1 kap. 6 § 2 lagen (2023:457) om behandling av personuppgifter vid Utbetalningsmyndigheten, för att undvika fel och missbruk i samband med såväl registrering som efter att e-legitimationen utfärdats. *Polismyndigheten* anser att brottsbekämpande myndigheter behöver få ta del av uppgifter hos utfärdande myndighet.

Skälen för regeringens förslag

Vad är ändamålsbestämmelser?

Förslagen i denna proposition innebär att utfärdande myndigheter kommer att behöva behandla personuppgifter. En grundläggande princip i EU:s dataskyddsförordning är att personuppgifter endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål och att de inte senare får behandlas på ett sätt som är oförenligt med dessa ändamål (artikel 5.1 b). Denna princip kallas i förordningen för principen om ändamålsbegränsning. Kravet på att senare behandling inte får ske för ändamål som är oförenliga med insamlingsändamålet brukar kallas för finalitetsprincipen.

Principen om ändamålsbegränsning är central i det dataskyddsrättsliga regelverket. Den innebär att den personuppgiftsansvarige måste göra klart för sig i vilket syfte personuppgifter samlas in. Möjligheten att senare behandla dessa personuppgifter för ett annat ändamål än det ursprungliga är begränsad (artikel 5.1 b). Den registrerade skyddas på det sättet mot oväntad och integritetskränkande behandling av de personuppgifter som har samlats in.

EU:s dataskyddsförordning ger medlemsstaterna utrymme att införa ändamålsbestämmelser i nationell rätt (artiklarna 6.2, 6.3, 6.4 och 23.2 a). Om det inte finns sådana bestämmelser ska den personuppgiftsansvarige själv bestämma ändamålet med insamlingen av uppgifter. Prövningen av om en ny behandling av uppgifterna är förenlig med detta ändamål ska därefter göras direkt enligt förordningen. Enligt artikel 6.4 ska den personuppgiftsansvarige då beakta flera faktorer, bl.a. kopplingar mellan ändamålet för insamlingen och det nya ändamålet, förhållandet mellan den registrerade och den personuppgiftsansvarige, uppgifternas art, konsekvenser för den registrerade och förekomsten av lämpliga skyddsåtgärder.

Ytterligare behandling av personuppgifter för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller vissa statistiska ändamål ska inte anses vara oförenlig med de ursprungliga ändamålen (artikel 5.1 b).

Det finns olika typer av ändamålsbestämmelser, primära och sekundära

De allra flesta registerförfattningar, dvs. författningar som innehåller särskild reglering om framför allt myndigheters personuppgiftsbehandling, innehåller en reglering av tillåtna ändamål för behandlingen av personuppgifter. Ändamålsbestämmelserna brukar delas in i primära och sekundära ändamål. Bestämmelserna om primära ändamål avser behovet av att behandla personuppgifter i en myndighets egen verksamhet och anger för vilka ändamål inom lagens tillämpningsområde myndigheten får samla in personuppgifter. Bestämmelser om sekundära ändamål reglerar hur personuppgifter som redan har samlats in och behandlas i verksamheten för de primära ändamålen får vidarebehandlas. I de sekundära ändamålsbestämmelserna anges ofta att uppgifter får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Det brukar också anges att uppgifter även får behandlas för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in (finalitetsprincipen).

Den nya lagen bör innehålla ändamålsbestämmelser

Regeringen anser, till skillnad från *Myndigheten för digital förvaltning*, att lagen om statlig e-legitimation och elektronisk identifiering bör innehålla ändamålsbestämmelser. Det kommer att innebära att utfärdande myndigheter inte får bestämma för vilka ändamål personuppgifter behandlas i verksamheten med den statliga e-legitimationen. Genom sådana bestämmelser blir det tydligt för de registrerade vilken behandling av personuppgifter som är tillåten. På så sätt säkerställs också att personuppgiftsbehandlingen i verksamheten med den statliga e-legitimationen endast används för nödvändiga ändamål, som *Chalmers tekniska högskola AB* efterfrågar. Ändamålsbestämmelserna i lagen bör utgå från en uppdelning mellan primära och sekundära ändamål.

Ärendehandläggning, registrering av ärenden om statlig e-legitimation och säker användning av e-legitimationen som primära ändamål

Utfärdande myndighet kommer att behöva behandla personuppgifter för att handlägga ärenden om statlig e-legitimation. Som Myndigheten för digital förvaltning påpekar kommer det även att framgå av de materiella bestämmelserna i lagen om statlig e-legitimation och elektronisk identifiering vilka personuppgifter som behöver samlas in och hur de behöver hanteras vid handläggningen. Det finns därför inte något behov av att i ändamålsbestämmelserna i detalj gå in på vilken typ av handläggningsåtgärder som kommer att innebära behandling av personuppgifter, t.ex. för att kunna kontrollera sökandens identitet. Det är därmed tillräckligt att fastställa att ett primärt ändamål för behandling av personuppgifter är att handlägga ärenden om statlig e-legitimation. En sådan bestämmelse omfattar all personuppgiftsbehandling som behövs för att ärenden ska kunna handläggas, t.ex. prövning av en ansökan eller återkallelse och spärr av en e-legitimation. Dessutom omfattas alla åtgärder som är nödvändiga att vidta i ett ärende. Exempel på sådana åtgärder är mottagande av uppgifter, diarieföring, kommunicering och utlämnande i samband med expediering. Det kan vidare avse behandling av uppgifter i brottmålsdomar

i samband med ett beslut om återkallelse och spärr av en statlig e-legitimation.

Vidare bör en utfärdande myndighet få behandla personuppgifter för att föra ett register över ärenden om statlig e-legitimation. Myndigheten behöver t.ex. kontrollera om sökanden redan har en giltig statlig e-legitimation. Det kommer därför att vara nödvändigt att spara personuppgifter som hänför sig till ärenden om statliga e-legitimation i ett register. Att en utfärdande myndighet, närmare bestämt Polismyndigheten, ska föra ett register över ärenden om statliga e-legitimation kommer också att framgå av en uttrycklig bestämmelse i lagen (se avsnitt 9.3). Det bör för tydlighets skull även framgå av ändamålsbestämmelserna att utfärdande myndighet får behandla personuppgifter för att föra ett register över ärenden om statlig e-legitimation. Regeringen anser, i likhet med Myndigheten för digital förvaltning, att ordet register bör användas i stället för databas (jfr prop. 2022/23:34 s. 138 och artikel 4.6 i EU:s dataskyddsförordning).

En utfärdande myndighet bör vidare få behandla personuppgifter i syfte att möjliggöra en säker användning av den statliga e-legitimationen. Myndigheten kan t.ex. behöva behandla personuppgifter för att motverka identitetsrelaterad brottslighet kopplad till användningen av e-legitimationen. För dessa syften föreslås att vissa biometriska uppgifter ska få sparas i ett register och lagras i bäraren till e-legitimationen (se avsnitt 8.3 och 9.3). En säker användning av e-legitimationen kan också handla om att vidta åtgärder för att den ska kunna användas på ett säkert sätt i offentliga och privata aktörers nättjänster för elektronisk identifiering, t.ex. genom villkor för användningen av den statliga e-legitimationen (se avsnitt 8.7). I samband med sådana åtgärder kan det uppstå ett behov att behandla personuppgifter, t.ex. om innehavare av e-legitimationen eller en kontaktperson hos en offentlig eller privat aktör.

Enligt regeringens uppfattning saknas det skäl att tillåta insamling av personuppgifter för andra ändamål än handläggning av ärenden om statlig e-legitimation, att föra ett register över ärenden om statlig e-legitimation och för att möjliggöra en säker användning av e-legitimationen. De primära ändamålsbestämmelserna som föreslås innebär en uttömmande reglering av de ändamål som utfärdande myndighet får samla in personuppgifter för.

Brottsbekämpning som sekundärt ändamål

Till Polismyndighetens huvuduppgifter hör att förebygga, förhindra och upptäcka brottslig verksamhet, utreda och lagföra brott och upprätthålla allmän ordning och säkerhet. I den verksamheten används inte sällan personuppgifter som har samlats in i passverksamheten (Ds 2019:5 s. 114).

Brottsbekämpning, lagföring och upprätthållande av allmän och nationell säkerhet är viktiga samhällsintressen som erkänns i EU:s dataskyddsförordning (artikel 23.1). Det är uppenbart att Polismyndigheten skulle få avsevärt bättre möjligheter att bekämpa och lagföra brott och upprätthålla allmän ordning och säkerhet om personuppgifter från verksamheten med den statliga e-legitimationen kan användas för sådana ändamål. På samma sätt som Polismyndigheten i dag har möjlighet att använda sig av uppgifter i passregistret för brottsbekämpande ändamål bör de personuppgifter som

har samlats in i verksamheten med den statliga e-legitimationen kunna användas av myndigheten för brottsbekämpande ändamål, så som *Polismyndigheten* efterfrågar. Det gäller framför allt de ansiktsbilder som är sparade i registret över ärenden om statlig e-legitimation, men också andra personuppgifter som har samlats in.

När det kommer till risken för den personliga integriteten kan det konstateras att brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område (polisens brottsdatalag) kommer att gälla om personuppgifter från verksamheten med den statliga e-legitimationen behandlas för brottsbekämpande ändamål. Ett uttryckligt syfte med dessa lagar är att skydda fysiska personers grundläggande rättigheter och friheter (se t.ex. 1 kap. 1 § brottsdatalagen). Behandlingen kommer att omfattas av lagarnas bestämmelser om bl.a. rättslig grund, ändamål, lagringstider och överföring till tredjeland. Personuppgiftsbehandlingen kommer också att stå under tillsyn av Integritetsskyddsmyndigheten och Säkerhets- och integritetsskyddsnämnden vid Myndigheten för säkerhet och integritetsskydd. En behandling för brottsbekämpande ändamål kommer alltså att omfattas av ett väl utvecklat regelverk till skydd för den enskildes personliga integritet. Enligt regeringens mening finns det därför inte anledning att, som *Integritetsskyddsmyndigheten* framför, begränsa behandlingen för vissa typer av brott.

Regeringen bedömer sammanfattningsvis att Polismyndigheten bör få använda de personuppgifter som har samlats in i verksamheten med den statliga e-legitimationen även i brottsbekämpande syfte. Utfärdande myndighet bör därför även få behandla de personuppgifter som samlats in i verksamheten med den statliga e-legitimationen om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet. De angivna ändamålen motsvarar de i polisens brottsdatalag (2 kap. 1 §). En sådan bestämmelse, tillsammans med den primära ändamålsbestämmelsen om att möjliggöra en säker användning av e-legitimationen, är enligt regeringens bedömning tillräcklig för att stävja missbruk av den statliga e-legitimationen. Det finns därför inte något behov av att införa en särskild ändamålsbestämmelse om att en utfärdande myndighet ska få behandla personuppgifter för att kunna förebygga, förhindra och upptäcka felaktigt utfärdade e-legitimationer, som *Pensionsmyndigheten* efterfrågar.

Uppgiftslämnande som sekundärt ändamål

Det finns situationer där utfärdande myndighet kommer att behöva behandla personuppgifter, som t.ex. har samlats in för handläggningen av ärenden om statlig e-legitimation, för att lämna ut dessa till andra myndigheter eller till enskilda. En bestämmelse som uttryckligen tillåter behandling för sådana ändamål bör därför införas.

En allmän förutsättning för att behandling av detta slag ska vara tillåten bör vara att uppgiftslämnandet sker i överensstämmelse med lag eller förordning. När bestämmelser som kräver eller tillåter utlämnande har införts får det förutsättas att det har gjorts en avvägning mellan intresset av att uppgifterna lämnas ut och intresset av att skydda enskilda personers

integritet, och att den avvägningen har resulterat i att uppgifterna ska eller får lämnas ut (prop. 2007/08:126 s. 60 och prop. 2014/15:148 s. 41).

Utfärdande myndighet kan vara skyldig att lämna ut uppgifter enligt flera olika bestämmelser. När det gäller uppgifter som inte omfattas av sekretess finns det exempelvis en allmän skyldighet för en myndighet att på begäran av en annan myndighet lämna ut uppgifter, om det inte skulle hindra arbetets behöriga gång, se 6 kap. 5 § OSL. De flesta uppgifter i verksamheten med den statliga e-legitimationen är offentliga och ska därmed lämnas ut enligt dessa regler, på begäran av en annan myndighet. På begäran av en enskild ska en myndighet dessutom lämna uppgift ur en allmän handling som förvaras hos myndigheten, om den inte är sekretessbelagd eller det skulle hindra arbetets behöriga gång (6 kap. 4 § OSL).

Det finns vidare fall när det inte finns någon uttrycklig skyldighet att lämna uppgifter men där det ändå kan anses föreskrivet eller önskvärt att göra detta. Det kan exempelvis vara fråga om åtgärder som vidtas för att fullgöra den allmänna serviceskyldigheten gentemot enskilda. Det kan ifrågasättas om det behövs en bestämmelse som tillåter behandling av personuppgifter i dessa situationer eller om det räcker att uppgiftsskyldigheten i sig är reglerad. Av tydlighetsskäl finns det dock anledning att införa en sekundär ändamålsbestämmelse som anger att uppgifter som har samlats in för de primära ändamålen även får behandlas för uppgiftslämnande som sker i enlighet med gällande lagar och förordningar. Liknande bestämmelser finns i t.ex. 12 § lagen om identitetskort för folkbokförda i Sverige, 7 § domstolsdatalagen (2015:728) och 4 § kriminalvårdsdatalagen (2018:1235).

Behandling för andra sekundära ändamål

Personuppgifter som har samlats in för t.ex. handläggning av ärenden om statlig e-legitimation bör även kunna behandlas för vissa andra sekundära ändamål. Uppgifterna bör bl.a. få behandlas om det behövs för arkivändamål. För att tydliggöra detta bör det införas en bestämmelse som anger att personuppgifter som behandlas för de primära ändamålen, även får behandlas för andra ändamål under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med de primära ändamålen. Det bör alltså införas en bestämmelse som motsvarar finalitetsprincipen i artikel 5.1 b i EU:s dataskyddsförordning (jfr 12 § lagen om identitetskort för folkbokförda i Sverige, 7 § domstolsdatalagen och 4 § kriminalvårdsdatalagen).

Behandling av känsliga personuppgifter

Med känsliga personuppgifter avses personuppgifter som t.ex. avslöjar ras eller etniskt ursprung, politiska åsikter och biometriska uppgifter för att entydigt identifiera en fysisk person, se 3 kap. 1 § dataskyddslagen och artikel 9.1 i EU:s dataskyddsförordning. Känsliga personuppgifter får enligt EU:s dataskyddsförordning t.ex. behandlas om det är nödvändigt av hänsyn till ett viktigt allmänt intresse. Enligt Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra

brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977, i fortsättningen brottsdatadirektivet, gäller i stället en högre tröskel för behandling av sådana uppgifter. Det ska nämligen vara absolut nödvändigt för ändamålet med behandlingen, se t.ex. 2 kap. 4 § polisens brottsdatalag och prop. 2017/18:269 s. 296. För att känsliga personuppgifter ska få behandlas räcker det då inte att behandlingen är nödvändig, dvs. att den t.ex. effektiviserar handläggningen (prop. 2017/18:105 s. 45–48).

För att motverka risken för integritetsintrång bör det vara tydligt att det ställs särskilda krav för den behandling av känsliga personuppgifter som kommer att ske med stöd av lagen om statlig e-legitimation och elektronisk identifiering. Även om brottsdatadirektivet inte är tillämpligt på den personuppgiftsbehandling som sker i verksamheten med den statliga e-legitimationen finns det inga hinder mot att tillämpa direktivets högre tröskel även på andra områden, se t.ex. 9 § andra stycket lagen (2021:319) om Transportstyrelsens olycksdatabas. Det bör därför, i likhet med utredningens förslag, införas en bestämmelse som anger att känsliga personuppgifter får behandlas i verksamheten endast om det är absolut nödvändigt för ändamålet med behandlingen. I avsnitt 9.4 redogörs för i vilka särskilda fall det bör anses vara tillåtet för en utfärdande myndighet att behandla känsliga personuppgifter.

9.3 Register över ärenden om statlig e-legitimation

Regeringens förslag

Polismyndigheten ska föra ett register över ärenden om statlig e-legitimation. Registret ska föras med hjälp av automatiserad behandling.

Registret ska endast få innehålla

- namn, personnummer, samordningsnummer, medborgarskap, födelsedatum och kontaktuppgifter till sökanden,
- ansiktsbilder som har tagits vid ansökan om statlig e-legitimation och biometriska uppgifter som har tagits fram ur sådana ansiktsbilder,
- handlingar eller uppgifter i handlingar som har kommit in eller upprättats i ärenden om statlig e-legitimation,
- uppgifter som rör handläggningen av ärenden om statlig e-legitimation, och
- uppgifter om utfärdade statliga e-legitimationer.

Utredningens förslag

Förslaget från utredningen stämmer i huvudsak överens med regeringens. Utredningen föreslår att de uppgifter som registret får innehålla ska regleras i förordning. Utredningen föreslår inte att uppgift om medborgarskap ska få registreras som en särskild kategori av uppgift.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *AB Svenska pass*, *Diskrimineringsombudsmannen*, *Internetstiftelsen* och *Vännäs kommun*, tillstyrker eller har inga synpunkter på förslaget. *Myndigheten för civilt försvar* anser att registret bör innehålla uppgift om vilken identitetshandling som har legat till grund för grundidentifieringen och en kopia av handlingen. Enligt *Totalförsvarets forskningsinstitut* bör utfärdande myndighet även få spara fingeravtryck med tillhörande biometriska uppgifter i registret för att kontrollera identiteten i samband med utfärdande av nya identitetshandlingar. *Ekobrottsmyndigheten* menar att brottsförebyggande skäl talar för att utfärdande myndighet bör få möjlighet att bevara biometriska uppgifter. *Försäkringskassan* framför att det bör förtydligas om det, vid sidan av det föreslagna registret, kommer att finnas ett ärendehanteringssystem och personuppgiftsbehandlingen för det. I annat fall bör det enligt myndigheten förtydligas att registret över statliga e-legitimationer inte ska användas för handläggningsändamål. *Göteborgs kommun* anser att det bör förklaras vad som avses med automatiserad behandling.

Skälen för regeringens förslag

Polismyndigheten bör föra ett register över ärenden om statlig e-legitimation

Ett register över ärenden om statlig e-legitimation är nödvändigt för att t.ex. kontrollera giltigheten av utfärdade e-legitimationer och för att återkalla och spärra sådana e-legitimationer som inte uppfyller föreskrivna krav. Ett register minskar också risken för att det utfärdas flera statliga e-legitimationer till samma person.

I avsnitt 8.8 föreslås att samma ansvarsfördelning ska gälla mellan Polismyndigheten, beskickningar och karriärkonsulat för utfärdandet av den statliga e-legitimationen som för utfärdandet av pass och nationellt identitetskort. Eftersom samma myndigheter ska utfärda den statliga e-legitimationen framstår det som ändamålsenligt att även ansvaret för registret fördelas på samma sätt som för registren över pass och nationellt identitetskort. Regeringen anser mot denna bakgrund att Polismyndigheten bör föra ett register över ärenden om statlig e-legitimation med hjälp av automatiserad behandling. En bestämmelse om detta bör införas i lagen.

Automatiserad behandling avser behandling med tekniska hjälpmedel, t.ex. med hjälp av datorer, till skillnad från manuell behandling som avser t.ex. renodlad pappershantering (jfr prop. 2017/18:105 s. 47). De ändamålsbestämmelser som föreslås i avsnitt 9.2 kommer även att gälla för personuppgiftsbehandlingen i registret, med undantag för bestämmelserna om att möjliggöra en säker användning av den statliga e-legitimationen. Att utfärdande myndighet får behandla personuppgifter i registret för att kunna handlägga ärenden om statlig e-legitimation, som *Försäkringskassan* efterfrågar ett förtydligande av, följer av den primära ändamålsbestämmelsen om ärendehandläggning (se avsnitt 9.2).

Det bör införas en bestämmelse om vad registret får innehålla

De ändamålsbestämmelser som föreslås i avsnitt 9.2 sätter gränser för vilka uppgifter som kan behandlas i registret över ärenden om statlig e-

legitimation. Ur ett integritetsskyddsperspektiv är det ändå lämpligt att närmare reglera vilka uppgifter som får behandlas i registret över ärenden om statlig e-legitimation. Enligt regeringens uppfattning bör det alltså framgå av lagen vad registret får innehålla. En sådan reglering kan underlätta både för utfärdande myndighet och för tillsynsmyndigheten. Det blir också tydligt för enskilda vilka uppgifter registret får innehålla. Bestämmelserna bör säkerställa att de uppgifter som krävs för en ändamålsenlig och säker verksamhet får finnas i registret. Bestämmelserna bör inte vara så detaljerade att de hindrar vissa anpassningar över tid, men bör ge en tydlig bild av vilka kategorier av uppgifter som får behandlas i registret. Regeringen bedömer att följande uppgifter behöver framgå av registret:

- namn, personnummer, samordningsnummer, medborgarskap, födelsedatum och kontaktuppgifter till sökanden,
- ansiktsbilder som har tagits vid ansökan om statlig e-legitimation och biometriska uppgifter som har tagits fram ur sådana ansiktsbilder,
- handlingar eller uppgifter i handlingar som har kommit in eller upprättats i ärenden om statlig e-legitimation,
- uppgifter som rör handläggningen av ärenden om statlig e-legitimation, och
- uppgifter om utfärdade statliga e-legitimationer.

Registret över ärenden om statlig e-legitimation bör alltså innehålla namn, person- och samordningsnummer, medborgarskap, födelsedatum och kontaktuppgifter till sökanden. Registret bör också få innehålla ansiktsbilder som tas vid ansökan om statlig e-legitimation och biometriska uppgifter som tagits fram ur ansiktsbilderna, som *Ekobrottsmyndigheten* påpekar. Detta är av stor vikt för identifieringen av sökanden och för att motverka missbruk av den statliga e-legitimationen (se avsnitt 8.3). Vidare bör registret även innehålla handlingar eller uppgifter i handlingar som har kommit in eller upprättats i ärenden om statlig e-legitimation. Det gör det möjligt att registrera skriftliga medgivanden från vårdnadshavare och andra handlingar som ges in eller upprättas i ett ärende, t.ex. identitetshandlingar som ligger till grund för en ansökan, som *Myndigheten för civilt försvar* efterfrågar. Att uppgifter i upprättade handlingar får sparas medför att t.ex. beslut i ärenden kan registreras. Det kan avse såväl beslut om beviljade och nekade ansökningar som återkallelse och spärr av statliga e-legitimationer. I registret bör också uppgifter som rör handläggningen av ärenden få behandlas. Detta krävs för att det ska gå att registrera bl.a. uppgifter om när en ansökan gjordes, vilken handläggare som tog emot ansökan och vilka åtgärder som har vidtagits i ärendet. Slutligen bör registret också få innehålla uppgifter om utfärdade statliga e-legitimationer. Sådana uppgifter kan t.ex. avse unik identifierare och serienummer, aktiveringskod, utfärdandedatum och giltighetstid. Uppgifterna i registret bör alltså avse ärenden om statlig e-legitimation, dvs. även ärenden som inte har lett till att en e-legitimation har utfärdats. Registret bör inte få innehålla några andra uppgifter än de uppräknade.

Utredningen har inte lämnat något förslag om att fingeravtryck ska kunna sparas i registret, som *Totalförsvarets forskningsinstitut* efterfrågar.

Regeringen anser därför att det inte finns ett tillräckligt underlag för att gå fram med ett sådant förslag i det här lagstiftningsärendet.

9.4 Behandling av biometriska uppgifter

Regeringens förslag

Den ansiktsbild som tas vid ansökan om statlig e-legitimation och de biometriska uppgifter som har tagits fram ur sådana bilder ska få användas för sökning i registret över ärenden om statlig e-legitimation. Sökning är endast tillåten för att kontrollera sökandens identitet och innehav av statlig e-legitimation i samband med ansökan om statlig e-legitimation.

Biometriska uppgifter ska också få behandlas om den handling som sökanden styrker sin identitet med är försedd med en ansiktsbild eller innehåller ett lagringsmedium med ansiktsbild och fingeravtryck. Utfärdande myndighet ska då få kontrollera att ansiktsbilden och fingeravtrycken motsvarar de som tas i det aktuella ärendet om statlig e-legitimation.

Biometriska uppgifter ska dessutom få behandlas genom att den ansiktsbild och de fingeravtryck som får tas innan en statlig e-legitimation lämnas ut jämförs med de som finns lagrade i den statliga e-legitimationen.

Fingeravtryck som tas i samband med ansökan om statlig e-legitimation och de biometriska uppgifter som tas fram ur dessa ska omedelbart förstöras när e-legitimationen har lämnats ut eller, om e-legitimationen inte har lämnats ut, när det har gått 90 dagar från den dag då den utfärdades. Om ett ansökningsärende har avslutats på något annat sätt ska uppgifterna också förstöras omedelbart.

Ansiktsbilden och fingeravtrycken som får tas i samband med utlämnande av en statlig e-legitimation och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken ska omedelbart förstöras efter att en kontroll av uppgifterna har genomförts. Ansiktsbilden och fingeravtrycken som vid kontroll tas fram ur ett lagringsmedium och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken ska också omedelbart förstöras när en sådan kontroll har genomförts.

Utredningens förslag

Förslaget från utredningen stämmer i delvis överens med regeringens. Utredningen föreslår att jämförelsen av biometriska uppgifter i den handling som sökanden uppvisar för att styrka sin identitet och de i den statliga e-legitimationen ska regleras i förordning. Utredningen föreslår inte en bestämmelse om att biometriska uppgifter får behandlas i samband med att en statlig e-legitimation lämnas ut. Utredningen föreslår inte heller att fingeravtryck som har tagits i ett ärende om statlig e-legitimation och de biometriska uppgifter som tas fram ur dessa ska förstöras 90 dagar efter utfärdandet om e-legitimationen inte har lämnats ut. Utredningen föreslår

inte att ansiktsbilden och fingeravtrycken som får tas i samband med utlämnande av en statlig e-legitimation och de biometriska uppgifter som tas fram ur ansiktsbilden ska förstöras omedelbart efter att en kontroll av uppgifterna har genomförts. Inte heller att ansiktsbilden och fingeravtrycken som vid kontroll tas fram ur ett lagringsmedium och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken omedelbart ska förstöras när en sådan kontroll har genomförts.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *Brottsförebyggande rådet*, *Gislaveds kommun*, *Polismyndigheten* och *Sveriges advokatsamfund*, tillstyrker eller har inga synpunkter på förslaget. *Föreningen för digitala fri- och rättigheter* menar att det är problematiskt ur integritetssynpunkt att samla in biometriska uppgifter för att spara dem i bäraren. *Försäkringskassan* anser att det behöver förtydligas om känsliga personuppgifter även kommer att hanteras i utfärdande myndighets ärendehanteringssystem. *Integritetsskyddsmyndigheten* ifrågasätter om behandlingen av biometriska uppgifter är nödvändig mot bakgrund av att verifiering på distans för närvarande inte är fullt tekniskt eller praktiskt möjligt. Myndigheten anser vidare att det bör framgå av lagen vilket undantag i artikel 9.2. i EU:s dataskyddsförordning som är tillämpligt. Slutligen framför myndigheten att integritetsanalysen även bör omfatta en redogörelse för vilka skyddsåtgärder som krävs för att behandlingen ska anses vara proportionerlig.

Skatteverket anser att det finns behov av en sekretessbrytande bestämmelse för att möjliggöra tillhandahållande av uppgifter från utfärdande myndighet till brottsbekämpande myndigheter.

Skälen för regeringens förslag

Vad är biometri och biometriska uppgifter?

En definition av begreppet biometriska uppgifter finns i artikel 4.14 i EU:s dataskyddsförordning. Där definieras biometriska uppgifter som 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 fingeravtrycksuppgifter. Av skäl 51 framgår att behandling av fotografier inte systematiskt anses utgöra behandling av känsliga personuppgifter, eftersom fotografier endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person.

Begreppet biometriska uppgifter definieras på samma sätt i artikel 3.13 i brottsdatadirektivet. Brottsdatadirektivet har genomförts i svensk rätt i brottsdatalagen. I förarbetena till den lagen anges att biometri är ett samlingsnamn för automatiserad teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är riktig. Tekniken baseras på mätning av fysiska karaktärsdrag hos den som ska identifieras. När det gäller pass är det framför allt mönster av fingeravtryck, ansiktsgeometri och ögats iris som brukar användas. Gemensamt för teknikerna är att kroppen mäts elektroniskt. Biometriska uppgifter är den information som kan tas fram ur ett biometriskt underlag. Dessa uppgifter kan användas för att skapa en

referensmall eller för att jämföra tidigare lagrade referensmallar i syfte att kontrollera en persons identitet. I dataskyddsdirektivets definition av biometriska uppgifter anges ansiktsbilder som ett exempel på sådana uppgifter. Det kan leda tanken till att vanliga fotografier och filmer skulle omfattas av definitionen. Om de inte bearbetas tekniskt genom en särskild metod som syftar till identifiering faller de utanför definitionen. Om de däremot bearbetas i exempelvis ett ansiktsigenkänningsprogram så att det går att identifiera personer på bilden eller filmen omfattas de av definitionen (prop. 2017/18:232 s. 86, 150, 151 och 435).

Möjligheten att behandla biometriska uppgifter

Biometriska uppgifter för att entydigt identifiera en fysisk person utgör s.k. särskilda kategorier av personuppgifter enligt EU:s dataskyddsförordning (artikel 9.1). I nationell rätt betecknas de som känsliga personuppgifter (3 kap. 1 § dataskyddslagen).

Behandling av känsliga personuppgifter är som huvudregel förbjuden enligt EU:s dataskyddsförordning, om inte något av undantagen i artikel 9.2 a–j är tillämpligt. Enligt artikel 9.2 g får känsliga personuppgifter behandlas om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt. Behandlingen ska vidare stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

I EU:s dataskyddsförordning förtydligas inte vad som avses med viktigt allmänt intresse. Regeringen har tidigare bedömt att verksamhet som innefattar myndighetsutövning borde betraktas som ett viktigt allmänt intresse (prop. 2017/18:105 s. 83). Bestämmelserna i artikel 9.2 g kompletteras av 3 kap. 3 § dataskyddslagen. Där framgår att känsliga personuppgifter får behandlas av en myndighet med stöd av artikel 9.2 g i EU:s dataskyddsförordning om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, om behandlingen är nödvändig för handläggningen av ett ärende eller i annat fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades integritet.

Behandling av biometriska uppgifter bör vara tillåten för att kontrollera sökandens identitet och innehav av statlig e-legitimation

För att den statliga e-legitimationen ska vara tillförlitlig föreslår regeringen att det ska ställas krav på att sökanden i samband med ansökan styrker sin identitet genom personlig inställelse (se avsnitt 8.2). Ett sådant krav bör åtföljas av kontroll av ett biometriskt underlag i form av ansiktsbild och fingeravtryck. Regeringen föreslår därför att ansiktsbild och fingeravtryck ska lagras i den statliga e-legitimationen och att ansiktsbilden och tillhörande biometriska uppgifter ska få behandlas i myndighetens register för att möjliggöra jämförande kontroller (se avsnitt 8.3 och 9.3). Till skillnad från *Integritetsskyddsmyndigheten* och *Föreningen för digitala fri- och rättigheter* anser alltså regeringen att det finns skäl för lagring av biometriska uppgifter i bäraren av den statliga e-legitimationen. En sådan lagring möjliggör bl.a. en tillförlitlig grundiden-

tifiering i samband med ansökan och vid utlämnande av en statlig e-legitimation (se även avsnitt 8.3). Integritetsskyddsmyndigheten efterfrågar också en redogörelse för vilka skyddsåtgärder som krävs för att personuppgiftsbehandlingen ska vara proportionerlig. I det följande redogörs bl.a. för de överväganden som görs i fråga om den enskildes integritetsintressen vid utfärdande myndighets behandling av känsliga personuppgifter och för föreslagna skyddsåtgärder.

Som konstateras i avsnitt 7.1 har det skett en ökning av identitetsrelaterad brottslighet med tydliga kopplingar till den organiserade brottsligheten. Brottsligheten får inte bara konsekvenser för enskilda personer och företag, utan också omfattande ekonomiska konsekvenser för brottsbekämpande myndigheter och staten i övrigt. Många transaktioner och avtalsslut sker i dag digitalt. Felaktigt utfärdade statliga e-legitimationer, som t.ex. kan användas för att skaffa andra e-legitimationer, kan därför snabbt få allvarliga konsekvenser genom ökad identitetsrelaterad brottslighet.

En möjlighet att använda biometriska uppgifter för jämförande sökningar i ärenden om statlig e-legitimation skulle väsentligt minska de risker som finns för felaktigt utfärdade e-legitimationer. Det finns alltså starka skäl för att en utfärdande myndighet ska få använda den ansiktsbild och de biometriska uppgifter som sökanden lämnar i samband med ansökan av en e-legitimation för sökningar. Syftet med en sådan sökning bör endast få vara att i samband med en ansökan om statlig e-legitimation kontrollera sökandens identitet och innehav av statlig e-legitimation för att myndigheten t.ex. ska kunna säkerställa att samma person inte innehar flera e-legitimationer. Av samma skäl bör en utfärdande myndighet få behandla biometriska uppgifter om sökanden i ett ärende om statlig e-legitimation styrker sin identitet med hjälp av en handling som är försedd med en ansiktsbild eller innehåller ansiktsbild eller fingeravtryck i ett lagringsmedium. Ett pass, som en sökande kan använda för att styrka sin identitet, innehåller vanligtvis såväl en ansiktsbild på passet som ansiktsbild och fingeravtryck i ett lagringsmedium i passet. Myndigheten bör då få kontrollera att ansiktsbilden och fingeravtrycken motsvarar de som tas i det aktuella ärendet om statlig e-legitimation. Det kan t.ex. vara en biometrisk jämförelse av ansiktsbilden på identitetshandlingen eller en ansiktsbild som finns i ett lagringsmedium på identitetshandlingen med den ansiktsbild som tas i ärendet om statlig e-legitimation. Det kan också vara en okulär jämförelse av ansiktsbilderna.

Regeringen anser, till skillnad från Föreningen för digitala fri- och rättigheter, att integritetsriskerna med den föreslagna behandlingen av biometriska uppgifter är begränsade. Det är endast ansiktsbilden som tas i samband med ansökan med tillhörande biometriska uppgifter som kommer att få sparas i registret över ärenden om statlig e-legitimation (se avsnitt 9.3). Det bör också uttryckligen anges i den föreslagna lagen om statlig e-legitimation och elektronisk identifiering att de känsliga uppgifter som inte får sparas ska förstöras. Det gäller t.ex. de fingeravtryck som tas vid ansökan av den statliga e-legitimationen, och de biometriska uppgifter som tas fram ur fingeravtrycken. Dessa bör omedelbart förstöras när e-legitimationen har lämnats ut eller, om e-legitimationen inte har lämnats ut, 90 dagar från den dag då den utfärdades. Om ett ansökningsärende har avslutats på något annat sätt ska uppgifterna också omedelbart förstöras.

Det kan nämligen efter denna tidpunkt inte längre anses finnas skäl för behandlingen av uppgifterna. Ett ärende kan avslutas t.ex. genom att ansökan återkallas, avslås eller skrivs av från vidare handläggning. Förslaget innebär att fingeravtrycken och de biometriska uppgifter som tas fram ur dessa får behandlas under handläggningen av en ansökan om statlig e-legitimation.

Identitetskontrollen och jämförelsen av biometriska uppgifter som en utfärdande myndighet föreslås få göra i samband med ansökan om och utlämnande av en statlig e-legitimation kan innefatta en jämförelse av ansiktsbild, fingeravtryck och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken. Den ansiktsbild och de fingeravtryck som vid en kontroll tas fram ur ett lagringsmedium och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken bör också förstöras omedelbart när kontrollen har genomförts. Även ansiktsbilden och fingeravtrycken, med tillhörande biometriska uppgifter, som myndigheten får ta i samband med utlämnandet av en statlig e-legitimation, bör omedelbart förstöras efter att en jämförande kontroll har gjorts av uppgifterna med de som finns lagrade i den statliga e-legitimationen. Det bör vägas in att de föreslagna kontrollmöjligheterna skyddar enskilda mot att någon annan använder deras identitet. Risken för sådant missbruk måste för de flesta människor framstå som ett större hot mot den personliga integriteten än att vissa myndigheter får jämföra biometriska uppgifter under reglerade former. I avsnitt 9.6 och 9.7 lämnar regeringen ytterligare förslag i syfte att minimera de risker för den personliga integriteten som behandling av biometriska uppgifter kan medföra. Även de föreslagna bestämmelserna om ändamål tillgodoser den registrerades grundläggande intressen och rättigheter (se avsnitt 9.2).

Samtliga förslag om behandling av biometriska uppgifter syftar till att motverka missbruk av den statliga e-legitimationen och att säkerställa att e-legitimationen utfärdas till rätt person. Syftet måste anses utgöra ett sådant viktigt allmänt intresse som avses i artikel 9.2 g i EU:s dataskyddsförordning. Behandlingen får vidare anses stå i proportion till det angivna syftet. Enligt regeringens bedömning finns det inte något mindre ingripande sätt som lika effektivt kan uppnå syftet med de föreslagna åtgärderna. Behandlingen är därför nödvändig och därmed förenlig med såväl EU:s dataskyddsförordning som dataskyddslagen.

Till skillnad från *Integritetsskyddsmyndigheten* anser regeringen att det inte bör göras någon hänvisning till artikel 9.2 g i EU:s dataskyddsförordning för att klargöra med vilket stöd behandlingen av känsliga personuppgifter sker. Regeringen föreslår att behandlingen av känsliga personuppgifter ska vara absolut nödvändig för ändamålet med behandlingen (se avsnitt 9.2), vilket är ett mer omfattande skydd än det som föreskrivs i EU:s dataskyddsförordning. En hänvisning till artikel 9.2 g i EU:s dataskyddsförordning riskerar därför att vara missvisande.

Försäkringskassan efterfrågar ett förtydligande av om känsliga personuppgifter kommer att behandlas i utfärdande myndighets ärendehanteringssystem. Utfärdande myndighet kommer även att behöva hantera känsliga personuppgifter i myndighetens ärendehandläggning, vid t.ex. diarieföring av handlingar. Sådan behandling som sker inom ramen för ett elektroniskt ärendehanteringssystem får enligt regeringens bedömning betraktas som nödvändig och därmed tillåten vid handläggningen av ett

ärende oavsett om uppgifterna förekommer i löpande text eller inte (jfr prop. 2017:18:105 s. 87 och 88).

Det finns inte något behov av bestämmelser om sekretess

För att utfärdande myndighet ska kunna utföra de uppgifter som föreslås i den nya lagen om statlig e-legitimation och elektronisk identifiering kommer myndigheten att behöva få tillgång till och behandla ett stort antal personuppgifter. Registret över ärenden om statlig e-legitimation kommer t.ex. att innehålla namn, person- och samordningsnummer och ansiktsbild.

För uppgifter om enskilds personliga förhållanden gäller sekretess enligt 22 kap. 1 § OSL om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs och uppgiften förekommer i verksamhet som avser folkbokföringen eller annan liknande registrering av befolkningen och, i den utsträckning regeringen meddelar föreskrifter om det, i annan verksamhet som avser registrering av en betydande del av befolkningen. Sekretess gäller också i sådan verksamhet för uppgift i form av fotografisk bild av den enskilde om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. Regeringen har med stöd av 22 kap. 1 § OSL meddelat föreskrifter som innebär att bestämmelserna bl.a. omfattar Polismyndighetens passregister, registret över nationella identitetskort och Skatteverkets databas över identitetskort för folkbokförda i Sverige, se 6 § offentlighets- och sekretessförordningen (2009:641).

Registret över ärenden om statlig e-legitimation kommer sannolikt att omfatta en stor del av befolkningen. Regeringen bedömer därför att det finns förutsättningar för att registret ska kunna omfattas av samma sekretesskydd som de register som omfattas av 6 § offentlighets- och sekretessförordningen. För ansiktsbilder i sådana register gäller i dag ett omvänt skaderekvisit, dvs. en presumtion för sekretess. Regeringen har motiverat presumtionen bl.a. utifrån de enskildas intresse av att fotografierna inte kommer till användning i ett sammanhang som de upplever som hotfullt (prop. 2003/04:93 s. 34–41).

I propositionen Utökade befogenheter för Skatteverket inom folkbokföringsverksamhet (prop. 2025/26:261) föreslår regeringen att sekretess bl.a. ska gälla för uppgift i form av biometrisk uppgift som har tagits fram ur fotografisk bild, om det inte står klart att uppgifterna kan röjas utan att den enskilde eller någon närstående till honom eller henne lider men. De biometriska uppgifter som tas fram ur ansiktsbilder föreslås alltså, liksom ansiktsbilder, omfattas av en presumtion för sekretess enligt 22 kap. 1 § OSL. Sekretess kommer därmed även att kunna gälla för sådana biometriska uppgifter som har tagits fram ur ansiktsbilder och som får behandlas i registret över ärenden om statlig e-legitimation (se avsnitt 9.3). Regeringen bedömer att det inte finns något behov av ytterligare sekretessbestämmelser till skydd för uppgifter som kommer att behandlas i verksamheten med den statliga e-legitimationen.

Till skillnad från *Skatteverket* anser regeringen att det inte behövs någon sekretessbrytande bestämmelse för att möjliggöra tillhandahållande av uppgifter från registret över ärenden om statlig e-legitimation till brottsbekämpande myndigheter. Enligt den föreslagna lagen får nämligen personuppgifter behandlas om uppgiftslämnandet sker i överensstämmelse

med lag eller förordning. Sedan den 1 december 2025 gäller också att sekretess till skydd för enskilda inte hindrar att en uppgift lämnas till en annan myndighet, om det behövs för att bl.a. förebygga, förhindra eller upptäcka brottslig verksamhet, utreda brott, eller förebygga eller förhindra att en ekonomisk förmån, ett ekonomiskt stöd, en skatt eller en avgift beslutas, betalas ut eller tillgodoräknas felaktigt eller med ett för högt eller ett för lågt belopp (10 kap. 15 a § OSL). Det finns alltså rättslig grund för att lämna vidare uppgifter som behandlas i registret till andra myndigheter i syfte att bekämpa brott.

9.5 Vissa integritetskänsliga sökningar ska vara förbjudna

Regeringens förslag

Det ska vara förbjudet att använda ansiktsbilder och biometriska uppgifter som har tagits fram ur sådana bilder som sökbegrepp i andra fall än vid kontroll av sökandens identitet och innehav av statlig e-legitimation i samband med en ansökan om statlig e-legitimation.

Det ska också vara förbjudet att använda andra känsliga personuppgifter och uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden som sökbegrepp.

Det ska inte heller vara tillåtet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller personuppgifter som rör lagöverträdelser som innefattar brott.

Utredningens förslag

Förslagen från utredningen stämmer delvis överens med regeringens. Utredningen föreslår inte någon bestämmelse som förbjuder sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller personuppgifter som rör lagöverträdelser som innefattar brott.

Remissinstanserna

Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens förslag

Enligt passlagen och förordningen om nationellt identitetskort gäller för närvarande ett absolut förbud mot sökningar med hjälp av ansiktsbilder, fingeravtryck och biometriska uppgifter som kan tas fram ur ansiktsbilder och fingeravtryck (6 b § passlagen och 18 § förordningen om nationellt identitetskort). Syftet med bestämmelserna är att värna den registrerades personliga integritet (prop. 2008/09:132 s. 13). Ett motsvarande sökförbud finns i 3 kap. 3 § dataskyddslagen men det gäller bara när känsliga personuppgifter behandlas med stöd av den paragrafen (prop. 2017/18:105 s. 195). I verksamheten med den statliga e-legitimationen ska känsliga

personuppgifter i form av vissa biometriska uppgifter få behandlas med stöd av de bestämmelser som föreslås i avsnitt 9.4.

För att stärka den registrerades personliga integritet bör motsvarande förbud mot att använda känsliga personuppgifter i pass och identitetskortsverksamheten gälla i verksamheten med den statliga e-legitimationen. Ansiktsbilder, fingeravtryck och biometriska uppgifter som har tagits fram ur sådana underlag bör därför inte få användas som sökbegrepp när personuppgifter behandlas i verksamheten med den statliga e-legitimationen. Som ett undantag från detta förbud bör den kontroll av ansiktsbilder, och de biometriska uppgifter som har tagits fram ur sådana bilder, som beskrivs i avsnitt 9.4 dock vara tillåten. Förbudet mot användningen av sökbegrepp bör också gälla andra känsliga personuppgifter.

Uppgifter i t.ex. brottmålsdomar kan komma att behöva behandlas i ärenden om återkallelse och spärr av statlig e-legitimation på grund av säkerhetsskäl. Den typen av uppgifter kommer i så fall även att finnas i registret över ärenden om statlig e-legitimation. Sådana uppgifter är integritetskänsliga även om de inte är känsliga personuppgifter i rättslig mening. De bör därför inte få användas som sökbegrepp i den utfärdande myndighetens verksamhet med den statliga e-legitimationen. Flera registerförfattningar innehåller bestämmelser om sökbegränsningar för uppgifter om lagöverträdelser till skydd för den personliga integriteten. Sökbegränsningarna avser då lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden (se t.ex. 17 § lagen om identitetskort för folkbokförda i Sverige och prop. 2017/18:95 s. 64–67 och 122). Regeringen anser att motsvarande sökbegränsning bör finnas i den föreslagna lagen om statlig e-legitimation och elektronisk identifiering.

Till skillnad från utredningen anser regeringen att det bör införas ett förbud mot att göra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning, dvs. som rör fällande domar i brottmål och lagöverträdelser som innefattar brott. Även om renodlade uppgifter om etniskt ursprung inte kommer att behandlas i verksamheten med den statliga e-legitimationen kan en kombination av andra uppgifter, exempelvis ansiktsbild och uppgifter om medborgarskap och födelseort, avslöja en persons etniska ursprung. Genom ett förbud mot att göra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter klargörs att det exempelvis inte får göras sökningar för att få fram ett urval personer utifrån ett visst etniskt ursprung. Förbudet hindrar inte sökningar som görs i ett annat syfte än att identifiera ett urval av individer, t.ex. för att få fram viss statistik eller för registervård.

De föreslagna sökförbuden bör gälla när personuppgifter behandlas för såväl de i lagen angivna primära som sekundära ändamålen.

9.6 Längsta tid för behandling av personuppgifter i registret

Regeringens förslag

Personuppgifter i registret över ärenden om statlig e-legitimation ska inte få behandlas under längre tid än tio år räknat från utgången av det kalenderår som det ärende som uppgifterna hänför sig till avslutades.

Lagen ska innehålla en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om

- att personuppgifter i registret får behandlas under längre tid för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål, och
- avskiljande och begränsningar av åtkomsten till personuppgifter som behandlas för sådana ändamål.

Utredningens förslag

Förslagen från utredningen stämmer i huvudsak överens med regeringens. Utredningen föreslår att bestämmelser om den längsta tid som uppgifter och handlingar får lagras i registret ska regleras i förordning. Utredningen föreslår inte någon upplysningsbestämmelse om möjligheten att meddela föreskrifter om att personuppgifter i vissa fall får behandlas under längre tid och om avskiljande och begränsningar av åtkomsten till personuppgifter. Utredningen föreslår att begreppet gallring ska användas i stället för längsta tid för behandling.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *Dals-Eds kommun*, *Integritetsskyddsmyndigheten*, *Region Stockholm*, *Svenska bankföreningen* och *Sveriges advokatsamfund*, tillstyrker eller har inga synpunkter på förslaget. *Riksarkivet* avstyrker förslaget om en gallringsbestämmelse och föreslår att bestämmelsen i stället ska utformas som en reglering av längsta tid för behandling av uppgifter i registret. Vidare framhåller myndigheten att det med en sådan utformning inte finns skäl att bemyndiga myndigheten att meddela föreskrifter om bevarande.

Skälen för regeringens förslag

En längsta tid för personuppgiftsbehandling i registret bör införas

Enligt artikel 5.1 e i EU:s dataskyddsförordning får personuppgifter inte förvaras i en form som möjliggör identifiering av den registrerade under längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får dock lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Huvudprincipen enligt arkivlagen (1990:782) är att allmänna handlingar ska bevaras (3 §). Statliga myndigheter får enligt 14 § arkivförordningen (1991:446) gallra allmänna

handlingar endast i enlighet med föreskrifter eller beslut av Riksarkivet, om inte särskilda gallringsföreskrifter finns i lag eller förordning.

Register som innehåller ett stort antal personuppgifter innebär integritetsrisker för den enskilde. Det är anledningen till att registerförfattningar vanligtvis innehåller bestämmelser som, i motsats till arkivlagens huvudprincip om bevarande, anger att gallring ska ske på visst sätt eller anger en längsta tid för behandling av uppgifterna (se t.ex. 17 § förordningen om nationellt identitetskort och 13 § förordningen om identitetskort för folkbokförda i Sverige). Regeringen har tidigare konstaterat att orden bevarande och gallring enbart bör användas i den betydelse de har i arkivlagstiftningen, för att så långt som möjligt skilja mellan arkivrättsliga regler och regler om dataskydd. När syftet med bestämmelser är att skydda den personliga integriteten bör regleringen i stället ange den yttersta gränsen för hur länge personuppgifterna får behandlas (prop. 2017/18:269 s. 120 och 121). I likhet med vad *Riksarkivet* framför anser regeringen att det inte finns skäl att nu göra en annan bedömning.

För att skydda den registrerades personliga integritet anser regeringen att det bör införas särskilda bestämmelser om den längsta tiden som personuppgifter får behandlas i registret över ärenden om statlig e-legitimation. Att personuppgifter upphör att behandlas innebär inte nödvändigtvis att handlingarna gallras, dvs. förstörs. Det innebär enbart att de inte längre behandlas för de ändamål som anges i den föreslagna lagen. Allmänna handlingar som inte ska gallras med stöd av gällande regelverk ska bevaras i enlighet med arkivlagstiftningens krav (jfr prop. 2022/23:34 s. 150).

Vid bestämmandet av den längsta tillåtna tiden för behandling av personuppgifter bör en avvägning göras mellan å ena sidan intresset av skyddet för den personliga integriteten och å andra sidan verksamhetens behov. Det är av stor vikt för utfärdandeprocessen att en utfärdande myndighet kan kontrollera uppgifterna i registret i samband med att en person ansöker om en statlig e-legitimation. Uppgifterna behövs för att kunna kontrollera att samma person inte har flera e-legitimationer med olika identiteter eller ansöker om att få en e-legitimation i någon annan persons identitet. Många uppgifter kan av det skälet behöva sparas under lång tid. I likhet med utredningen anser regeringen att en tidsfrist på tio år tillgodoser dessa behov. Personuppgifter i registret över ärenden om statlig e-legitimation bör alltså få behandlas som längst tio år från utgången av det år som det ärende som uppgifterna hänför sig till avslutades. Detta hindrar inte att Polismyndigheten gallrar uppgifter från registret tidigare i enlighet med 14 § arkivförordningen. Polismyndigheten måste som personuppgiftsansvarig göra en bedömning av behovet av olika typer av uppgifter och utifrån det behovet ta fram rutiner för hur länge olika uppgifter ska behandlas (se avsnitt 9.1).

Undantag från bestämmelserna om längsta tid för behandling

Som framgår ovan kan personuppgifter bevaras under längre tid än tio år för exempelvis vetenskapliga, statistiska eller historiska ändamål. Riksarkivet framför att det därför saknas skäl att bemyndiga myndigheten att meddela föreskrifter om bevarande. Regeringen anser dock att en upplysningsbestämmelse bör tas in i lagen om att regeringen eller den

myndighet som regeringen bestämmer kan meddela föreskrifter om att personuppgifter i registret över ärenden om statlig e-legitimation får fortsätta att behandlas under viss tid för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål. För att fristen ska få genomslag kan det vidare behöva införas föreskrifter om att sådana personuppgifter som bevaras under längre tid, för t.ex. arkivändamål, ska avskiljas från annan information i registret och att åtkomsten till dessa uppgifter ska begränsas. Dessa föreskrifter bedöms också kunna meddelas med stöd av regeringens restkompetens. Upplysningsbestämmelsen bör därför även omfatta möjligheten att meddela sådana föreskrifter.

9.7 Tillgång till personuppgifter

Regeringens förslag

Tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter i verksamheten med den statliga e-legitimationen.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om begränsningen av tillgången till personuppgifter och om säkerhetsåtgärder till skydd för personuppgifter.

Utredningens förslag

Förslagen från utredningen stämmer i sak överens med regeringens. Utredningen föreslår inte något bemyndigande om möjligheten att meddela föreskrifter om på vilket sätt tillgången till personuppgifter kan begränsas och om säkerhetsåtgärder till skydd för personuppgifter.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *AB Svenska pass*, *Diskrimineringsombudsmannen*, *Hovrätten över Skåne och Blekinge* och *Integritetsskyddsmyndigheten*, tillstyrker eller har inga synpunkter på förslaget. *Försäkringskassan* framför att det bör övervägas att i lag reglera att åtkomsten till personuppgifter ska följas upp regelbundet eller genom ett bemyndigande för sådana föreskrifter.

Skälen för regeringens förslag

Tillgången till personuppgifter bör begränsas

Enligt artikel 24.1 i EU:s dataskyddsförordning ska den personuppgiftsansvarige, med beaktande av bl.a. behandlingens art, omfattning och ändamål, genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter utförs i enlighet med förordningen. Enligt artikel 25.2 ska den personuppgiftsansvarige också genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för

dess lagring och deras tillgänglighet. Enligt artikel 32 har den personuppgiftsansvarige vidare en skyldighet att se till att en lämplig säkerhetsnivå för behandlingen av personuppgifter upprätthålls. Detta ska ske bl.a. genom lämpliga tekniska och organisatoriska åtgärder. Den personuppgiftsansvariges skyldigheter i denna del finns även i de allmänna principer för personuppgiftsbehandling som framgår av artikel 5.1 f i samma förordning.

Även om skyldigheten för personuppgiftsansvariga att på olika sätt begränsa tillgången till personuppgifter följer direkt av EU:s dataskyddsförordning har regeringen bedömt att tillgången till personuppgifter kan regleras särskilt i nationell rätt (se t.ex. prop. 2017/18:254 s. 36 och prop. 2017/18:248 s. 28). Sådana bestämmelser finns därför i flertalet registerförfattningar, t.ex. 7 § kriminalvårdsdatalagen och 16 § utlänningsdatalagen (2016:27).

Mot bakgrund av att verksamheten med den statliga e-legitimationen kommer att innebära behandling av en stor mängd personuppgifter, bl.a. känsliga personuppgifter, bedömer regeringen att tillgången så långt som möjligt bör begränsas med hänsyn till den registrerades integritet. Det bör därför införas en bestämmelse i den nya lagen om att tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter i verksamheten med den statliga e-legitimationen. Den som inte arbetar med uppgifter kopplade till verksamheten med den statliga e-legitimationen ska alltså inte ha rätt att befatta sig med uppgifterna i den verksamheten.

Regeringen eller den myndighet som regeringen bestämmer bör få meddela vissa föreskrifter till skydd för personuppgifter

Det bör i den nya lagen införas en rätt för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om begränsningen av tillgången till personuppgifterna. På så sätt kan regleringen av tillgången till personuppgifter enklare justeras vid behov. Det innebär att regleringen kan följas upp regelbundet, som *Försäkringskassan* efterfrågar. Den nya lagen bör också innehålla ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om säkerhetsåtgärder till skydd för personuppgifter. Sådana föreskrifter kan meddelas för att ytterligare tillvarata den enskildes integritetsintresse, t.ex. om nya säkerhetsåtgärder blir tillgängliga på grund av den tekniska utvecklingen.

9.8 Undantag från rätten att invända mot personuppgiftsbehandling

Regeringens förslag

Den rätt att invända mot personuppgiftsbehandling som följer av artikel 21.1 i EU:s dataskyddsförordning ska inte gälla vid behandling som är tillåten enligt den nya lagen om statlig e-legitimation och elektronisk identifiering eller föreskrifter som har meddelats i anslutning till lagen.

Utredningens förslag

Förslaget från utredningen stämmer överens med regeringens.

Remissinstanserna

Ingen remissinstans yttrar sig särskilt över förslaget.

Skälen för regeringens förslag

Av artikel 21.1 i EU:s dataskyddsförordning framgår att den registrerade har rätt att när som helst göra invändningar mot personuppgiftsbehandling som bl.a. sker för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning (artikel 6.1 e). Om en sådan invändning har gjorts får den personuppgiftsansvarige inte längre behandla personuppgifterna, såvida denne inte 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.

Rätten att göra invändningar kan sannolikt bli aktuell i flera av de situationer där utfärdande myndighet behandlar personuppgifter i verksamheten med den statliga e-legitimationen. En rätt för den registrerade att invända mot behandlingen av personuppgifter kan tänkas påverka effektiviteten i myndighetens verksamhet. Begränsningar i rätten att göra invändningar får enligt artikel 23.1 göras i syfte att säkerställa bl.a. ett viktigt mål av generellt allmänt intresse för medlemsstaten. Det krävs också att begränsningen uppfyller krav på nödvändighet och proportionalitet.

Den behandling av personuppgifter som följer av den föreslagna lagen om statlig e-legitimation och elektronisk identifiering är en förutsättning för att utfärdande myndighet ska kunna utföra sina uppgifter på ett korrekt, rättssäkert och effektivt sätt. Den personuppgiftsansvariga myndigheten får närmast undantagslöst anses kunna visa skäl för fortsatt behandling som väger tyngre än den registrerades intressen i det enskilda fallet. Under sådana förhållanden och för att fullt ut säkerställa förutsättningarna för utfärdande myndighet att behandla relevanta personuppgifter bör den registrerade inte ha någon rätt att motsätta sig sådan personuppgiftsbehandling som är tillåten enligt lagen. En sådan begränsning måste anses utgöra en nödvändig och proportionell åtgärd i syfte att säkerställa ett viktigt mål av generellt allmänt intresse (jfr prop. 2017/18:95 s. 85 och 86 och prop. 2017/18. 105 s. 106). Den föreslagna lagen innehåller dessutom ett flertal integritetsskyddande bestämmelser, bl.a. om ändamålen och längsta tid för behandling av personuppgifter. Regeringen anser därför att det i den nya lagen om statlig e-legitimation och elektronisk identifiering bör införas en bestämmelse om att rätten att enligt artikel 21.1 i EU:s dataskyddsförordning göra invändningar inte gäller vid sådan personuppgiftsbehandling som är tillåten enligt lagen och föreskrifter som har meddelats i anslutning till lagen.

10 Krav på erkännande av vissa medel för elektronisk identifiering i offentliga aktörers nättjänster

Regeringens förslag

Offentliga aktörer ska, för autentisering i sina nättjänster, erkänna medel för elektronisk identifiering som tillhandahålls inom ramen för ett auktorisationssystem enligt lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post. Kravet ska gälla när en e-legitimation krävs för att få tillgång till en nättjänst och tjänsten helt eller delvis riktar sig till enskilda.

Kravet ska endast gälla om tillitsnivån för medlet motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga aktören kräver för åtkomst till nättjänsten.

Med offentlig aktör ska det avses detsamma som i lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post. Offentligt styrda organ och sådana juridiska personer som tillgodoser behov i det allmännas intresse ska dock inte omfattas.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om hur kravet att erkänna medel för elektronisk identifiering i auktorisationssystem ska fullgöras och om undantag från kravet.

Utredningens förslag

Förslagen från utredningen stämmer i sak överens med regeringens. Utredningens förslag har dock en annan redaktionell utformning.

Remissinstanserna

Majoriteten av remissinstanserna, bl.a. *Bolagsverket*, *Finansinspektionen*, *Göteborgs kommun*, *Integritetsskyddsmyndigheten*, *Kammarkollegiet*, *Kronofogdemyndigheten*, *Lantmäteriet*, *Länsstyrelsen i Skåne län*, *Sveriges advokatsamfund* och *Upphandlingsmyndigheten*, tillstyrker eller har inga synpunkter på förslaget.

Sveriges Kommuner och Regioner (*SKR*) anser att kravet endast innebär förenklingar för kommuner om det säkerställs att en hög andel leverantörer av medel för elektronisk identifiering ansluter sig till auktorisationssystemet. Flera remissinstanser, bl.a. *Freja eID Group AB* och *Försvarsmakten*, framför att kravet även bör omfatta privata aktörer, alternativt att frågan bör utredas vidare. Freja eID Group AB anser vidare att det bör göras obligatoriskt för de som tillhandahåller nättjänster att hantera samordningsnummer, eftersom det i dagsläget är få aktörer som har möjlighet att hantera sådana i sina system. *Konkurrensverket* påpekar att få kommer att vilja ha en statlig e-legitimation om privat sektor inte omfattas av kravet. Myndigheten anser vidare att det krävs ytterligare överväganden av om verksamheten hänförlig till den statliga e-legitimationen kan påverka konkurrensen och handeln mellan EU:s medlemsstater enligt statsstödsreglerna. *TechSverige* anser att det är problematiskt ur ett kon-

kurrensrättsligt perspektiv om tillgången till elektronisk identifiering i en nättjänst måste anskaffas genom ett auktorisationssystem och det inte finns möjlighet för offentliga aktörer att fortsatt upphandla sådana tjänster.

Region Stockholm framhåller att kravet riskerar att medföra att befintlig marknad för elektronisk identifiering försvinner och att det, åtminstone tillfälligt, kan bromsa digitaliseringstakten. Några myndigheter, bl.a. *Försvarets materielverk*, anser att det bör finnas möjlighet till undantag från kravet att erkänna medel för elektronisk identifiering som tillhandahålls av leverantörer i auktorisationssystemet och att myndigheter som tillhör Försvarsdepartementet bör omfattas av ett sådant undantag.

Skälen för regeringens förslag

Det bör införas ett krav på att vissa medel för elektronisk identifiering ska godtas vid identifiering i nättjänster

I avsnitt 7.1 föreslår regeringen att det ska införas en statlig e-legitimation. Syftet är bl.a. att säkra samhällets tillgång till elektronisk identifiering och stärka samhällets motståndskraft genom att öka konkurrensen på området.

Att en statlig e-legitimation införs innebär dock inte i sig att den kommer att kunna användas i olika nättjänster eftersom det som utgångspunkt är upp till förlitande part, dvs. tillhandahållaren av den nättjänsten som kräver elektronisk identifiering, att avgöra vilka medel som godtas för autentisering i tjänsten. I avsnitt 7.1 bedömer regeringen att den statliga e-legitimationen bör anslutas till ett auktorisationssystem enligt lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post. Ett krav på att medel för elektronisk identifiering som tillhandahålls inom ramen för ett auktorisationssystem ska erkännas för autentisering kommer sannolikt att leda till att urvalet av e-legitimationer som kan användas i nättjänsterna blir större. Det skulle i sin tur bidra till ökad konkurrens på marknaden för elektronisk identifiering och tillgänglighet till digital offentlig service, till skillnad från vad *Region Stockholm* framför. En enskild som ska skaffa en e-legitimation skulle på så sätt få möjlighet att välja bland fler leverantörer av medel för elektronisk identifiering.

Som *SKR* påpekar är anslutningsgraden till auktorisationssystemet en avgörande faktor för att systemet ska vara effektivt och göra nytta (se prop. 2023/24:6 s. 32). Ett krav på att ett medel för elektronisk identifiering som ingår i ett sådant system ska godtas i vissa aktörers nättjänster innebär dock inte att de aktörer som berörs av kravet måste anskaffa tjänsten genom att ansluta till auktorisationssystemet. Det är upp till varje aktör som berörs av kravet att ta ställning till om de medel för elektronisk identifiering som ingår i systemet i stället ska anskaffas genom exempelvis upphandling enligt lagen om offentlig upphandling eller på något annat sätt. Det finns inte heller något som hindrar en sådan aktör från att upphandla andra tjänster, utöver de som ingår i auktorisationssystemet. En sådan ordning begränsar inte konkurrensen på marknaden, som *Tech-Sverige* befarar.

Utredningen har föreslagit att ett medel för elektronisk identifiering ska erkännas för autentisering i en nättjänst bl.a. om medlet tillhandahålls av en leverantör som är godkänd i enlighet med lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

Eftersom en leverantör kan tillhandahålla flera medel för elektronisk identifiering, och vissa medel kanske inte ingår i ett auktorisationssystem, bör kravet på erkännande i stället avse de medel som ingår i ett sådant system. Regeringen anser mot denna bakgrund att det bör införas en skyldighet att erkänna medel för elektronisk identifiering som tillhandahålls inom ramen för ett auktorisationssystem enligt lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post. Skyldigheten att erkänna medel för elektronisk identifiering innebär inte en skyldighet att ge enskilda åtkomst till nättjänsten.

Kravet bör omfatta nättjänster som tillhandahålls av offentliga aktörer och som riktar sig till enskilda

Enligt lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post får offentliga aktörer använda de medel för elektronisk identifiering som ingår i ett auktorisationssystem, bl.a. för identifiering av enskilda för åtkomst till sina digitala tjänster.

Det föreslagna kravet på att medel för elektronisk identifiering som ingår i ett auktorisationssystem under vissa förutsättningar ska erkännas syftar till att öka konkurrensen och redundansen inom e-legitimationsområdet och till att öka tillgängligheten till digitala tjänster. För att det ska kunna uppnås är det motiverat att en stor del av den offentliga sektorn omfattas av kravet. Detta skulle också vara ett effektivt sätt att öka incitamenten för anslutning till auktorisationssystem för elektronisk identifiering. Kravet bör därför omfatta statliga myndigheter, kommuner och regioner och sammanslutningar av dessa aktörer som inrättats särskilt för att tillgodose behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär.

För att inte utesluta en stor del av den kommunala verksamheten som utförs i privat regi bör även vissa privata aktörer som bedriver offentligt finansierad verksamhet omfattas. När det gäller vilka privata aktörer som bör omfattas kan ledning hämtas från lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post och lagen (2018:1937) om tillgänglighet till digital offentlig service. Med offentlig aktör i dessa lagar avses bl.a. en privat aktör som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad inom olika verksamhetsområden. Ett utpekat område är verksamhet som bedrivs av en enskild huvudman inom skolväsendet eller av enskild huvudman för en sådan internationell skola som avses i 24 kap. skollagen (2010:800). Även verksamhet som utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen (2017:30) eller tandvård enligt tandvårdslagen (1985:125) omfattas. Vidare omfattas verksamhet som bedrivs enligt socialtjänstlagen (2025:400), lagen (1988:870) om vård av missbrukare i vissa fall, lagen (1990:52) med särskilda bestämmelser om vård av unga och lagen (1993:387) med stöd och service till vissa funktionshindrade. Även personlig assistans som utförs med assistansersättning enligt socialförsäkringsbalken omfattas. Med offentlig finansiering avses ett direkt stöd eller betalning för att driva verksamheten inom de aktuella verksamhetsområdena (prop. 2023:24:6 s. 51 och prop. 2017/18:299 s. 87).

När lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post infördes övervägdes om en bredare krets

skulle få använda sig av tjänsterna i auktorisationssystemet. I förarbetena konstateras att tillämpningen av auktorisationssystem är ett annat sätt för offentliga aktörer att anskaffa tjänster än genom offentlig upphandling. Privata aktörer som inte omfattas av upphandlingsregelverket har inte samma begränsningar i fråga om möjligheten att ingå avtal med flera leverantörer som tillhandahåller tjänster för elektronisk identifiering. Mot bakgrund av bl.a. detta ansågs det inte finnas skäl att utvidga kretsen användare av auktorisationssystemet till fler privata aktörer än de som bedriver verksamhet som till någon del är offentligt finansierad (prop. 2023/24:6 s. 32–34). Regeringen anser, till skillnad från bl.a. *Försvarsmakten* och *Konkurrensverket*, att det inte skulle vara ändamålsenligt att en större krets skulle omfattas av kravet. Det framstår också som olämpligt att ett sådant krav skulle gälla aktörer som inte har möjlighet att använda sig av auktorisationssystemet.

Sammanfattningsvis bör det alltså införas ett krav på att statliga myndigheter, kommuner och regioner och privata aktörer som yrkesmässigt bedriver offentligt finansierad verksamhet inom de uppräknade områdena ska erkänna de medel för elektronisk identifiering som tillhandahålls inom ramen för ett auktorisationssystem enligt lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

Kravet bör gälla när en sådan aktör kräver e-legitimation för att få tillgång till en nättjänst som aktören tillhandahåller och som helt eller delvis riktar sig till enskilda. En förutsättning bör vidare vara att tillitsnivån för medlet för elektronisk identifiering motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga aktören kräver för åtkomst till nättjänsten.

Regeringen eller den myndighet som regeringen bestämmer bör ges rätt att föreskriva om hur kravet på att erkänna medel för elektronisk identifiering i auktorisationssystemet ska fullgöras. Det kan t.ex. avse inom vilken tid ett medel för elektronisk identifiering som har tillkommit i auktorisationssystem ska erkännas.

Regeringen ser, till skillnad från *Freja eID Group AB*, inte något behov av att ställa särskilda krav på att offentliga aktörer ska kunna hantera vissa typer av uppgifter i sina nättjänster.

Undantag från kravet

Det kan i vissa fall finnas ett behov av att göra undantag från kravet för offentliga aktörer att erkänna medel för elektronisk identifiering i auktorisationssystemet. Som *Försvarets materielverk* framför bör t.ex. hänsyn till rikets säkerhet kunna utgöra skäl för att undanta vissa myndigheter från kravet (jfr 3 § förordningen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post). Det kan också avse undantag från kravet i förhållande till vissa medel för elektronisk identifiering om det t.ex. finns flera överlappande auktorisationssystem med delvis likartade tjänster.

Regeringen bedömer att det bör vara tillräckligt att sådana undantag meddelas i förordning eller genom myndighetsföreskrifter. Regeringen eller den myndighet som regeringen bestämmer bör därför bemyndigas att meddela föreskrifter om undantag från kravet att erkänna medel för elektronisk identifiering.

Statsstöd är finansiering med offentliga medel som ger ett eller flera företag en fördel i förhållande till övriga konkurrenter. Huvudregeln är att det är förbjudet att ge sådant stöd. Bestämmelser om statsstöd finns i artiklarna 107–109 i fördraget om Europeiska unionens funktionssätt.

För att en åtgärd ska utgöra statligt stöd krävs bl.a. att stödet ges av en medlemsstat eller med hjälp av statliga medel och att det gynnar vissa företag eller viss produktion. När det gäller frågan om en åtgärd innebär en ekonomisk fördel har EU-domstolen slagit fast att det, för att det ska kunna bedömas om en statlig åtgärd utgör stöd, måste avgöras om det mottagande företaget får ekonomiska fördelar som det inte skulle ha fått under normala marknadsvillkor (EU-domstolens dom den 11 juli 1996 i målet SFEI m.fl. mot La Poste m.fl., C-39/94, EU:C:1196:285 och den 2 september 2010 i målet kommissionen mot Deutsche Post, C-399/08 P, EU:C:2010:481, punkt 40). Regeringens förslag är att den statliga e-legitimationen ska finansieras genom ansökningsavgifter utifrån principen om full kostnadstäckning (se avsnitt 8.9). Det är därmed inte fråga om statligt stöd, eftersom finansieringen endast ska täcka kostnaderna och verksamheten därmed inte får några ekonomiska fördelar. Reglerna om statsstöd aktualiseras därför inte.

11 Överklagande av beslut

Regeringens förslag

Beslut enligt lagen om statlig e-legitimation och elektronisk identifiering eller enligt föreskrifter som har meddelats i anslutning till lagen ska få överklagas till allmän förvaltningsdomstol. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Beslut enligt lagen ska gälla omedelbart, om inte annat anges i beslutet.

Utredningens förslag

Förslagen från utredningen stämmer i huvudsak överens med regeringens. Utredningen föreslår inte en bestämmelse om att beslut som har fattats med stöd av föreskrifter som har meddelats i anslutning till lagen ska få överklagas till allmän förvaltningsdomstol.

Remissinstanserna

Ingen remissinstans yttrar sig över förslaget.

Skälen för regeringens förslag

Överklagande av beslut

Beslut enligt den nya lagen eller enligt föreskrifter som har meddelats i anslutning till lagen bör kunna överklagas. Ytterligare bestämmelser om

överklagande, bl.a. vem som får överklaga ett beslut, hur man överklagar ett beslut och tiden för överklagande finns i förvaltningslagen (2017:900).

Vid överklagande av förvaltningsrättens avgöranden bör prövningstillstånd krävas i kammarrätten.

Besluten bör som huvudregel gälla omedelbart

Det är viktigt att utfärdande myndighets beslut om exempelvis återkallelse av en statlig e-legitimation kan verkställas så fort som möjligt. Beslut enligt lagen om statlig e-legitimation och elektronisk identifiering bör därför, på samma sätt som beslut enligt passlagen, gälla omedelbart om inte något annat anges i beslutet. Det innebär t.ex. att en e-legitimation fortsätter att vara spärrad om ett beslut om återkallelse och spärr, som gäller omedelbart, överklagas. En spärr bör vidare inte kunna hävas (se avsnitt 8.6). Det innebär att utfärdande myndighet får utfärda en ny e-legitimation om innehavaren överklagar ett beslut om återkallelse och spärr och får rätt i domstol.

12 Ikraftträdande

Regeringens förslag

Lagen om statlig e-legitimation och elektronisk identifiering ska träda i kraft den 1 december 2026.

Utredningens förslag

Förslaget från utredningen stämmer inte överens med regeringens. Utredningen föreslår att lagen om statlig e-legitimation och elektronisk identifiering ska träda i kraft den 1 mars 2026.

Remissinstanserna

Ingen av remissinstanserna yttrar sig särskilt över förslaget.

Skälen för regeringens förslag

Den tidpunkt för ikraftträdande som föreslås av utredningen har passerat och ikraftträdandet behöver därför senareläggas. Lagen om statlig e-legitimation och elektronisk identifiering bör träda i kraft så snart som möjligt, vilket bedöms vara den 1 december 2026.

Det bedöms inte finnas något behov av övergångsbestämmelser.

13 Konsekvenser

13.1 Allmänt om förslagen

Regeringen föreslår att det ska införas en statlig e-legitimation. Syftet med förslaget är bl.a. att säkra samhällets tillgång till elektronisk identifiering. En statlig e-legitimation behövs också för att Sverige ska kunna säkerställa att kraven i EU:s förordning om elektronisk identifiering uppfylls.

Regeringen föreslår vidare att vissa offentliga aktörer som kräver medel för elektronisk identifiering i sina nättjänster ska erkänna de medel för elektronisk identifiering som tillhandahålls inom ramen för ett auktorisationssystem i enlighet med lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post. Syftet med förslaget är att främja ett större urval av e-legitimationer i auktorisationssystemet bl.a. för att öka konkurrensen och redundansen inom e-legitimationsområdet. Enligt regeringens bedömning bör även den statliga e-legitimationen anslutas till ett sådant system.

13.2 Ekonomiska konsekvenser för utfärdande myndigheter

Polismyndigheten föreslås utses till utfärdande myndighet inom riket. Utom riket föreslås beskickningar och karriärkonsulat fullgöra uppgifter som utfärdande myndighet i den utsträckning som beslutas av regeringen eller den myndighet som regeringen bestämmer (se avsnitt 8.8). En utfärdande myndighet ska bl.a. hantera ansökningar och utfärda den statliga e-legitimationen. För att kunna utfärda en statlig e-legitimation behöver det göras en identitetskontroll av sökanden. De myndigheter som ska ansvara för utfärdandet av den statliga e-legitimationen kommer att ha erfarenhet av att utföra identitetskontroller och ha en upparbetad kunskap om hantering av känsliga uppgifter. Utfärdande myndigheter behöver därmed inte etablera verksamheten med den statliga e-legitimationen från grunden utan kan i stor utsträckning dra nytta av befintlig verksamhet.

Utfärdande myndigheter kommer att ha kostnader för att hantera ansökningsförfarandet, utfärdandet av den statliga e-legitimationen och drift och support av e-legitimationen samt nödvändiga it-system. De kommer också att ha förvaltningskostnader, dvs. utgifter för bl.a. löner, lokaler och övriga driftskostnader.

Verksamheten med den statliga e-legitimationen kommer i stor utsträckning att motsvara den för pass och nationellt identitetskort, bl.a. i fråga om ansökningsprocess och utfärdande. Samtliga kostnader för verksamheten med den statliga e-legitimationen kommer att finansieras genom den ansökningsavgift som sökanden ska betala. Polismyndigheten kommer även att få vissa intäkter genom ersättningen som ska betalas inom auktorisationssystemet (se avsnitt 13.3.1 om ersättning till leverantörer inom ett auktorisationssystem). Till skillnad från *Totalförsvarets forskningsinstitut* och *Sveriges ambassad i Berlin* anser regeringen att det för närvarande inte krävs någon ytterligare finansiering.

13.3 Ekonomiska konsekvenser för offentlig sektor i övrigt

13.3.1 Kravet på erkännande av medel för elektronisk identifiering

Regeringen föreslår att det ska införas ett krav för vissa offentliga aktörer att erkänna medel för elektronisk identifiering som tillhandahålls inom ramen för ett auktorisationssystem enligt lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post (se avsnitt 10). Kravet kan komma att innebära kostnader för teknisk anpassning och för användning av tjänsterna. Det är dock svårt att närmare bedöma omfattningen av kostnaderna, bl.a. mot bakgrund av osäkerheten kring hur många fler e-legitimationer som aktörerna kommer att behöva godta i sina tjänster jämfört med om kravet inte hade ställts. Kravet kommer i vart fall att innebära ett behov av att godta ytterligare en e-legitimation, förutsatt att den statliga e-legitimationen ansluts till ett auktorisationssystem (se avsnitt 7.1). Det får också antas att offentliga aktörer redan godkänner de medel för elektronisk identifiering som finns i Sverige. Det bedöms därför att kostnaderna kommer att vara begränsade för de allra flesta offentliga aktörer som träffas av kravet.

De offentliga aktörer som omfattas av det nu föreslagna kravet på erkännande kan behöva anpassa sina tjänster till de e-legitimationer som för närvarande finns i auktorisationssystemet. Det beror bl.a. på om aktören redan godtar sådana e-legitimationer för användning i sin nättjänst. För en offentlig aktör som redan godtar en e-legitimation som använder samma anslutningsmetod medför kravet inte ett behov av tekniska anpassningar. Offentliga aktörer som inte redan använder samma anslutningsmetod kommer däremot att behöva göra sådana anpassningar.

Ett krav på användning av tjänster som ingår i ett auktorisationssystem uppställs redan i dag för statliga myndigheter. I promemorian Auktorisationssystem för elektronisk identifiering och för digital post (I2020/03268) som låg till grund för det kravet bedömdes att de statliga myndigheterna skulle behöva möjliggöra inloggning med fler e-legitimationer. Någon uppskattning av hur många e-legitimationer det skulle röra sig om angavs dock inte. Kostnaderna för teknisk anpassning bedömdes vara marginella med hänsyn till att myndigheterna ändå skulle behöva anpassa sig till att ta emot fler e-legitimationer, bl.a. till följd av skyldigheten att godta utländska e-legitimationer som följer av EU:s förordning om elektronisk identifiering (samma promemoria s. 51 och 52).

Anpassningskostnaden, dvs. kostnaden för att anpassa de tekniska systemen för användning av en e-legitimation, bedöms för närvarande uppgå till cirka 31 000 kronor för den första e-legitimationen och därefter 12 000 kronor per e-legitimation. Därutöver behöver aktörerna betala en ersättning för användningen av tjänsterna, antingen genom ett auktorisationssystem eller direkt till leverantören. Myndigheten för digital förvaltning har beslutat om en modell för ersättning för auktorisationssystem där avgiften för offentliga aktörer uppgår till 0,12 kronor per genomförd elektronisk identifiering.

Flera kommuner har anfört att ersättningsmodellen för auktorisationssystemet riskerar att leda till oförutsebara kostnader för kommuner. För de aktörer som väljer att uppfylla kravet genom att ansluta till auktorisationssystemet blir den ersättningsmodell som Myndigheten för digital förvaltning har beslutat tillämplig. Det innebär att kostnaden för användningen av tjänsterna i ett auktorisationssystem utgår från den faktiska användningen av e-legitimationer i kommunens nättjänster. En sådan modell bedöms som mer fördelaktig för kommunerna än om ersättningen hade bestämts till ett fast belopp. Det innebär t.ex. att kommuner med färre invånare kommer att ha en lägre kostnad än kommuner med ett större antal invånare, eftersom användningen sannolikt också kommer att vara mindre.

Det går inte att närmare förutse hur omfattande användningen av medel för elektronisk identifiering som tillhandahålls inom ramen för ett auktorisationssystem kommer att vara. Användningen av sådana medel i tidigare valfrihetssystem enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering kan ligga till grund för en uppskattning. Användningen har varierat mellan olika offentliga aktörer. Under 2024 uppgick antal legitimeringar för en mellanstor kommun med 46 600 invånare till 98 580, och för en större statlig myndighet till 54 513 534. Vid ett antagande om en användning på mellan 100 000 och 55 000 000 antal digitala legitimeringar per år kommer kostnaden för en offentlig aktör att uppgå till mellan 12 000 och 6 600 000 kronor. Detta bedöms dock vara kostnader som aktörerna som omfattas av förslaget sannolikt skulle ha haft även ett utan ett krav på att erkänna medel för elektronisk identifiering som tillhandahålls i ett auktorisationssystem. Förslaget att införa en statlig e-legitimation möjliggör att fler ska få tillgång till en e-legitimation, vilket kan leda till att antalet digitala legitimeringar i offentliga aktörers nättjänster ökar och därmed även kostnaderna för användningen av medel för elektronisk identifiering.

Europaparlamentets och rådets direktiv (EU) 2016/2102 av den 26 oktober 2016 om tillgänglighet avseende offentliga myndigheters webbplatser och mobila applikationer (webbtillgänglighetsdirektivet) syftar bl.a. till att göra myndigheters webbplatser och mobila applikationer mer tillgängliga för användarna. Direktivet har genomförts genom lagen om tillgänglighet till digital offentlig service och föreskrifter som meddelats i anslutning till lagen. I föreskrifterna ställs det krav på tillgänglighet på digitala tjänster som tillhandahålls av en offentlig aktör. Kraven avser bl.a. e-tjänster för autentisering, identifiering och betalning. Det ställs alltså redan krav på tillgänglighet på den här typen av tjänster i webbplatser och mobila applikationer som tillhandahålls av offentliga aktörer. Syftet med kravet på erkännande av vissa medel för elektronisk identifiering är, i linje med detta, bl.a. att öka tillgängligheten till digital offentlig service. Regeringen bedömer mot denna bakgrund att kostnaderna till följd av kravet på erkännande av medel för elektronisk identifiering när det gäller statliga myndigheter bör finansieras inom ramen för den ordinarie verksamheten.

Den kommunala finansieringsprincipen innebär bl.a. att kommuner och regioner inte ska åläggas nya uppgifter utan att de samtidigt får möjlighet att finansiera dessa på annat sätt än genom höjda skatter (prop. 1991/92:150, bet. 1991/92:FiU29, rskr. 1991/92:345). De krav på tillgänglighet som ställs på statliga myndigheter gäller även kommuner.

Regeringen anser därför, till skillnad från *Malmö kommun* och *Tanum kommun*, att den kommunala finansieringsprincipen inte är tillämplig.

13.3.2 Konsekvenser för Skatteverket och Statens servicecenter

Den statliga e-legitimationen kommer för folkbokförda utlänningar att placeras på en fysisk bärare som kan komma att innehålla samma uppgifter om innehavaren som finns på det identitetskort som Skatteverket utfärdar, nämligen identitetskortet för folkbokförda i Sverige. Vidare kan bäraren av den statliga e-legitimationen för denna persongrupp komma att utformas på ett sätt som motsvarar det nationella identitetskortet. Genom förslaget införs ytterligare en möjlighet för utländska medborgare i landet att få en identitetshandling. Det kan därför inte uteslutas att den lösning som Polismyndigheten kommer att erbjuda folkbokförda utlänningar kan medföra att enskilda väljer att ansöka om en statlig e-legitimation hos Polismyndigheten i stället för en identitetshandling hos Skatteverket. Förslaget bedöms därför successivt kunna medföra ett minskat behov av identitetskortet för folkbokförda som Skatteverket utfärdar.

Inledningsvis väntas antalet ärenden gällande nyansökningar eller förnyelser av identitetshandlingar hos Skatteverket minska något från dagens nivåer som uppgår till ca 170 000 identitetskort årligen. Med en avgift på 400 kronor per kort motsvarar detta intäkter på omkring 68 miljoner kronor årligen, vilket inte ger full kostnadstäckning. I takt med att den statliga e-legitimationen etableras kan antalet ansökningar komma att minska ytterligare och ge ett visst intäktsbortfall. Det kommer att innebära att en större del av Skatteverkets identitetskortsverksamhet kommer att behöva finansieras från förvaltningsanslaget jämfört med i dag eftersom fasta kostnader för verksamheten inte påverkas av minskat antal ärenden.

Behovet av personal vid servicekontor för handläggning, fotografering och utlämning av identitetshandlingar kan minska över tid till följd av lägre antal ärenden. Några av dessa uppgifter sköts i dag av Statens servicecenter genom avtal. De nämnda konsekvenserna, bl.a. minskat personalbehov, kan därför även påverka Statens servicecenter. De merkostnader som eventuellt kan uppstå till följd av förslagen bedöms rymmas inom ramen för Skatteverkets och Statens servicecenters befintliga ekonomiska ramar.

Konsekvenserna av att förslaget innebär ytterligare en möjlighet för utländska medborgare i landet att få en identitetshandling behöver analyseras ytterligare. Som en följd av förslaget avser regeringen överväga om lagen om identitetskort för folkbokförda i Sverige bör upphävas.

13.3.3 Konsekvenser för domstolarna

Beslut som rör den statliga e-legitimationen föreslås få överklagas till allmän förvaltningsdomstol. Som utgångspunkt för bedömning av konsekvenserna för förvaltningsdomstolarna kan en jämförelse göras med antalet mål enligt passlagen och förordningen om nationellt identitetskort. Överklaganden i ärenden enligt passlagen hanteras tillsammans med

ärenden om nationellt identitetskort. Enligt uppgifter från Domstolsverket registrerades det 148–300 mål under 2020–2024. Det kan antas att antalet mål som rör den statliga e-legitimationen kommer att uppgå till ungefär hälften av detta. Förslaget bedöms därmed innebära en marginell ökning av antalet mål för förvaltningsdomstolarna. De merkostnader som eventuellt kan uppstå bedöms rymmas inom ramen för Sveriges Domstolars befintliga anslag.

13.4 Påverkan på den kommunala självstyrelsen

Förslaget om att kommuner och regioner ska erkänna vissa medel för elektronisk identifiering innebär en ny skyldighet för kommuner och regioner och utgör därmed en inskränkning i den kommunala självstyrelsen. I 14 kap. 3 § regeringsformen anges att en inskränkning i den kommunala självstyrelsen inte bör gå utöver vad som är nödvändigt med hänsyn till de ändamål som föranlett den.

Ett syfte med kravet är att öka tillgängligheten till digital offentlig service. Vidare är syftet med kravet att skapa ökad konkurrens på marknaden för tjänster för elektronisk identifiering och i förlängningen stärka samhällets motståndskraft. Regeringen bedömer att detta inte kan uppnås med mindre ingripande åtgärder. Mot denna bakgrund anser regeringen att den inskränkning i den kommunala självstyrelsen som förslaget innebär är proportionerlig.

13.5 Ekonomiska konsekvenser för företag

Förslaget att införa en statlig e-legitimation bedöms leda till ökad konkurrens på marknaden för tjänster för elektronisk identifiering.

Regeringen föreslår också att offentliga aktörer ska erkänna de tjänster som finns i auktorisationssystemet, där den statliga e-legitimationen är avsedd att ingå. En sådan lösning bedöms inte vara konkurrensbegränsande, eftersom alla leverantörer som uppfyller villkoren för att ansluta till ett auktorisationssystem får göra det.

De företag som träffas av kravet på att erkänna vissa utpekade medel för elektronisk identifiering är sådana som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad inom förskola, skola, hälso- och sjukvård och omsorg. Uppgifter från Statistiska centralbyrån för 2023 visar att 18 procent av verksamheten inom välfärdssektorn utfördes av privata utförare. Högst andel privata utförare finns inom omsorg, följt av hälso- och sjukvård och därefter utbildning (statistiknyhet från den 16 september 2025).

Inom hälso- och sjukvård och omsorgsverksamhet utgörs de privata utförarna av ca 15 000 vård- och omsorgsföretag. Av denna sektor utgörs 93 procent av företag som har färre än 20 anställda (Vårdföretagarnas webbplats, Privat vårdfakta, information hämtad den 15 maj 2025). Det bedöms inte som sannolikt att företag av denna storlek kommer att erbjuda nättjänster med möjlighet till identifiering med medel för elektronisk

identifiering. Det får därför antas att majoriteten av privata företag inom vård och omsorg inte kommer att påverkas av det aktuella förslaget.

Vidare finns det drygt 4 200 fristående skolenheter i Sverige, varav drygt 2 800 är förskolor. Fristående skolor är ofta små. Majoriteten av de fristående huvudmännen driver få, och inte sällan relativt sett små, enheter. Det innebär dock inte nödvändigtvis att det är fråga om mindre företag. Ett bolag kan äga flera huvudmän med både en, två eller fler enheter. Friskolornas Riksförbunds lista över de största friskoleägarna i februari 2024 visar att de 24 största ägarna svarar för ca 600 skolenheter på grundskole- och gymnasienivå, motsvarande drygt 40 procent av alla fristående skolor på grundskole- och gymnasienivå.

Kravet omfattar även enskilda utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina, och som till största delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller för utbildning på forskarnivå. Det finns arton sådana företag enligt Universitetskanslersämbetets årsrapport för 2024 (s. 127).

Av den typ av företag som kravet riktas mot erbjuder inte samtliga digitala tjänster där inloggning med ett medel för elektronisk identifiering krävs. De flesta mindre företag kommer sannolikt inte att erbjuda sådana tjänster. Kostnaderna för de företag som berörs bedöms främst bestå av utvecklings- och anpassningskostnader för att hantera de medel för elektronisk identifiering som måste godtas för legitimering. De kommer också att ha kostnader för användningen av medel för elektronisk identifiering. Dessa kostnader bedöms vara i nivå med de uppskattade kostnaderna för de statliga och kommunala aktörerna (se avsnitt 13.3.1).

13.6 Konsekvenser för privatpersoner

Regeringen föreslår att det ska införas en statlig e-legitimation för personer med svenskt medborgarskap. En statlig e-legitimation ska även kunna utfärdas till utlänningar som är folkbokförda i Sverige och personer som har ett s.k. immunitetsnummer och som omfattas av lagen om immunitet och privilegier i vissa fall (se avsnitt 8.1). Vidare föreslås att en ansökningsavgift ska få tas ut enligt principen om full kostnadstäckning.

Som bl.a. *Helsingborgs kommun* framför kan en avgift minska möjligheterna för vissa grupper att ansöka om en statlig e-legitimation. Den statliga e-legitimationen kommer att vara en av flera e-legitimationer på marknaden. Enskilda kommer därför inte att behöva en statlig e-legitimation för att legitimera sig digitalt. De som väljer att ansöka om en statlig e-legitimation kommer dock att behöva betala en ansökningsavgift. Avgiften kommer sannolikt att uppgå till ca 400–500 kronor, vilket är i nivå med avgiften för pass. Om den statliga e-legitimationen tillhandahålls på en fysisk identitetshandling bör det kunna leda till samordningsvinster och en lägre total kostnad för både identitetshandlingen och e-legitimationen och därmed en lägre avgift för privatpersoner.

Regeringen bedömer att förslagen gör det möjligt för fler personer att skaffa en e-legitimation, vilket i sin tur kommer att minska det digitala utanförskapet (se avsnitt 7.1). Kraven på grundidentifiering innebär att det

kommer att vara svårare att få en e-legitimation i en annan persons identitet. Det bedöms leda till minskade risker för enskilda att utsättas för identitetsrelaterad brottslighet. Kravet på personlig inställelse kan innebära besvär för vissa grupper, men det är nödvändigt för att e-legitimationen ska utfärdas på ett säkert sätt (se avsnitt 8.2). Genom de föreslagna ändamålsbestämmelserna för personuppgiftsbehandling kommer det vidare att vara tydligt för enskilda och utfärdande myndigheter när och hur personuppgifter får behandlas. På så sätt tillvaratas den enskildes rättigheter och skydd för den personliga integriteten (se avsnitt 9.2).

Sammanfattningsvis bedöms förslagen kunna medföra vissa kostnader för de privatpersoner som väljer att ansöka om en statlig e-legitimation. Förslagen bedöms inte medföra några andra negativa konsekvenser för privatpersoner.

13.7 Konsekvenser för brottsligheten och det brottsförebyggande arbetet

Den statliga e-legitimationen bör utformas på tillitsnivå hög (se avsnitt 7.1). Regeringen föreslår ett krav på personlig inställelse i samband med ansökan och att sökanden ska styrka sin identitet för att en statlig e-legitimation ska kunna utfärdas (se avsnitt 8.2 och 8.4). Kravet på personlig inställelse är en grundläggande förutsättning för att motverka den identitetsrelaterade brottsligheten. Vidare föreslås att utfärdande myndighet ska få lagra vissa biometriska uppgifter och göra jämförande sökningar för att kontrollera sökandens identitet och innehav av statlig e-legitimation (se avsnitt 9.3 och 9.4). Även detta kan förväntas bidra till att motverka den identitetsrelaterade brottsligheten. För att motverka obehörig användning av den statliga e-legitimationen föreslås också att regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om användningen av den statliga e-legitimationen (se avsnitt 8.7). Regeringen föreslår vidare att Polismyndigheten, som har erfarenhet av brottsförebyggande arbete, ska vara utfärdande myndighet inom riket. Mot bakgrund av detta bedömer regeringen, till skillnad från *Försäkringskassan*, att förslagen inte förväntas leda till ökad brottslighet.

13.8 Förslagens konsekvenser i övrigt

Regeringen bedömer att den statliga e-legitimationen bör anmälas för gränsöverskridande användning inom ramen för EU:s förordning om elektronisk identifiering (se avsnitt 7.1). Förslagen påverkar dock inte tillämpningen av EU:s förordning om elektronisk identifiering och bedöms i övrigt vara förenliga med EU-rätten.

Förslagen bedöms inte medföra några andra konsekvenser. Förslagen bedöms exempelvis inte ha någon betydelse för sysselsättningen eller för offentlig service i olika delar av landet. Förslaget bedöms inte heller påverka små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags. Förslagen träffar vidare kvinnor

 och män på samma sätt och bedöms inte medföra några ekonomiska eller andra effekter för jämställdheten mellan kvinnor och män.

14 Författningskommentar

Förslaget till lag om statlig e-legitimation och elektronisk identifiering

1 kap. Allmänna bestämmelser

Lagens innehåll och förhållande till annan reglering

1 § Denna lag innehåller bestämmelser om en statlig e-legitimation och krav på erkännande av vissa medel för elektronisk identifiering.

Bestämmelser om medel för elektronisk identifiering finns i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, här benämnd EU:s förordning om elektronisk identifiering, och i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Paragrafen innehåller en upplysning om lagens innehåll och annan reglering om medel för elektronisk identifiering. Övervägandena finns i avsnitt 7.2.

I *första stycket* anges att lagen innehåller bestämmelser om en statlig e-legitimation och krav på erkännande av vissa medel för elektronisk identifiering.

I *andra stycket* finns en upplysningsbestämmelse om att ytterligare bestämmelser om elektronisk identifiering finns i EU:s förordning om elektronisk identifiering och lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. Hänvisningen till EU:s förordning om elektronisk identifiering är dynamisk och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen.

2 § Denna lag kompletterar, i den del den avser behandling av personuppgifter, 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 EU:s dataskyddsförordning.

Vid behandlingen 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 föreskrifter som regeringen har meddelat i anslutning till denna lag.

Paragrafen innehåller bestämmelser om lagens förhållande till EU:s dataskyddsförordning och lagen med kompletterande bestämmelser till EU:s dataskyddsförordning. Övervägandena finns i avsnitt 9.1.

I *första stycket* finns en upplysning om att lagen innehåller bestämmelser som kompletterar EU:s dataskyddsförordning. Förordningen är direkt tillämplig i svensk rätt. De kompletterande bestämmelserna finns i 3 kap. i denna lag.

Av *andra stycket* framgår att lagen med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen gäller för behandling av personuppgifter i verksamheten med den statliga e-legitimationen, om inte annat följer av denna lag eller av föreskrifter som har meddelats i anslutning till denna lag.

Ord och uttryck

3 § Med autentisering, elektronisk identifiering, medel för elektronisk identifiering och nättjänst avses i denna lag detsamma som i EU:s förordning om elektronisk identifiering.

Paragrafen innehåller bestämmelser om ord och uttryck i lagen. Övervägandena finns i avsnitt 7.2.

Av paragrafen framgår att uttrycken autentisering, elektronisk identifiering, medel för elektronisk identifiering och nättjänst ska förstås på samma sätt som i EU:s förordning om elektronisk identifiering. Definitionerna finns i artikel 3 i EU:s förordning om elektronisk identifiering. Med autentisering avses en elektronisk process som gör det möjligt att bekräfta en fysisk eller juridisk persons elektroniska identifiering eller att bekräfta ursprunget för och integriteten hos uppgifter i elektronisk form. Med elektronisk identifiering avses en process inom vilken uppgifter för personidentifiering i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person, används. Med medel för elektronisk identifiering avses en materiell och immateriell enhet som innehåller uppgifter för personidentifiering och som används för autentisering för en nättjänst eller, i tillämpliga fall, för en offlinetjänst. Nättjänst definieras inte i förordningen. Begreppet ska vid tillämpningen av denna lag ges samma innebörd som vid tillämpningen av EU:s förordning om elektronisk identifiering.

4 § Med en offentlig aktör avses i denna lag

1. en statlig eller kommunal myndighet, eller en beslutande församling i en kommun eller region,

2. en sammanslutning som inrättats särskilt för att tillgodose behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär, och som består av en eller flera myndigheter eller församlingar som anges i 1,

3. en privat aktör som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad och som

a) aktören bedriver i egenskap av enskild huvudman inom skolväsendet eller huvudman för en sådan internationell skola som avses i 24 kap. skollagen (2010:800),

b) utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen (2017:30) eller tandvård enligt tandvårdslagen (1985:125),

c) bedrivs enligt socialtjänstlagen (2025:400), lagen (1988:870) om vård av missbrukare i vissa fall, lagen (1990:52) med särskilda bestämmelser om vård av unga eller lagen (1993:387) om stöd och service till vissa funktionshindrade, eller

d) utgör personlig assistans som utförs med assistansersättning enligt 51 kap. socialförsäkringsbalken, eller

4. en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina, och som till största delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller av utbildning på forskarnivå.

I paragrafen anges vad som avses med en offentlig aktör. Övervägandena finns i avsnitt 10.

Paragrafen utformas med 4 § lagen (2018:1937) om tillgänglighet till digital offentlig service och 4 § lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post som förebilder. Viss vägledning för hur paragrafen ska tillämpas kan därför hämtas från förarbetena till de lagarna (prop. 2017/18:299 s. 30, 31 och 86–89 och prop. 2023/24:6 s. 51).

Av *första punkten* framgår att det med offentlig aktör avses en statlig eller kommunal myndighet eller en beslutande församling i en kommun eller en region. Detta innebär att statliga myndigheter, som t.ex. Skatteverket, Försäkringskassan och domstolarna omfattas av lagens tillämpningsområde. En kommunal myndighet utgörs av exempelvis en kommunal nämnd. Med beslutande församling i en kommun eller region avses kommun- eller regionfullmäktige.

Enligt *andra punkten* avses vidare med offentlig aktör en sammanslutning som inrättats särskilt för att tillgodose behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär, och som består av en eller flera myndigheter eller församlingar som avses i första punkten. Bedömningen av om det finns ett allmännyttigt behov som inte är av industriell eller kommersiell karaktär ska enligt EU-domstolen göras med hänsyn till samtliga relevanta faktiska och rättsliga omständigheter (se t.ex. SIEPSA, C-283/00, EU:C:2003:544, p. 81 och prop. 2017/18:299 s. 89).

I *tredje punkten* anges att det med offentlig aktör även avses privata aktörer som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad och som omfattas av de områden som räknas upp i punkten. Med privat bedriven verksamhet avses enskilda personer eller sammanslutningar av personer som bedriver ett medvetet arbete för att uppnå ett eller flera mål. Det kan röra sig om allt från enskilda näringsidkare, ideella organisationer och kooperativa driftsformer till stiftelser och koncerner. Att verksamheten bedrivs yrkesmässigt innebär att den bedrivs kontinuerligt och i förvärvssyfte. Kravet på att verksamheten ska vara yrkesmässig innebär att t.ex. familjehem och personlig assistans som inte bedrivs i företagsform, utan i egenskap av privatperson, faller utanför bestämmelsens tillämpningsområde.

Bestämmelsen omfattar även sådan verksamhet som bedrivs som en verksamhetsgren i en större organisation. Ett exempel på detta är när ett och samma företag både bedriver verksamhet inom skolväsendet och producerar läromedel. Kravet på erkännande av medel för elektronisk identifiering i 4 kap. 1 § kommer då att gälla endast i skolverksamheten eftersom läromedelsverksamheten inte bedrivs i egenskap av enskild huvudman inom skolväsendet och därmed inte omfattas av tillämpningsområdet.

Med offentlig finansiering avses ett direkt stöd eller betalning för att driva verksamheten inom de aktuella verksamhetsområdena. Det kan t.ex. vara fråga om bidrag till enskilda huvudmän inom skolväsendet som ges med stöd av skollagen, ersättning som utgår med stöd av lagen (1993:1651) om läkarvårdsersättning eller verksamhet som upphandlas av det allmänna. Det är tillräckligt att en enskild verksamhet till någon del

uppbär offentlig finansiering för att betraktas som offentligt finansierad. Stödet måste dock ha getts för att den aktuella verksamheten ska bedrivas. När en verksamhet finansieras av allmänna medel endast under en begränsad period omfattas verksamheten av definitionen endast under den perioden som den är offentligt finansierad.

De aktuella verksamhetsområdena i *punkterna 3 a–d* och *4* motsvarar de i 4 § 3 a–c och 4 lagen om tillgänglighet till digital offentlig service (se prop. 2017/18:299 s. 88).

En statlig e-legitimation

5 § Den statliga e-legitimationen är ett medel för elektronisk identifiering.

I paragrafen anges vad en statlig e-legitimation är för typ av identifieringsmedel. Övervägandena finns i avsnitt 7.2.

I paragrafen anges att den statliga e-legitimationen är ett medel för elektronisk identifiering. Vad som avses med ett medel för elektronisk identifiering framgår av 3 §, se författningskommentaren till den paragrafen.

Utfärdande myndighet

6 § Den statliga e-legitimationen utfärdas av utfärdande myndighet.

Polismyndigheten är utfärdande myndighet inom riket.

Utom riket fullgör beskickningar och karriärkonsulat uppgifter som utfärdande myndighet i den utsträckning som beslutas av regeringen eller den myndighet som regeringen bestämmer.

I paragrafen finns en bestämmelse om utfärdande myndighet. Övervägandena finns i avsnitt 8.8.

Av *första stycket* framgår att den statliga e-legitimationen utfärdas av utfärdande myndighet.

I *andra stycket* anges att Polismyndigheten är utfärdande myndighet inom riket.

Av *tredje stycket* framgår att beskickningar och karriärkonsulat fullgör uppgifter som utfärdande myndighet utom riket i den utsträckning som beslutas av regeringen eller den myndighet som regeringen bestämmer.

7 § Utfärdande myndighet ska fullgöra de uppgifter som anges i denna lag och i föreskrifter som har meddelats i anslutning till lagen.

Paragrafen reglerar utfärdande myndighets uppgifter. Övervägandena finns i avsnitt 8.8.

Av paragrafen följer att utfärdande myndighet ska fullgöra de uppgifter som anges i lagen och i föreskrifter som har meddelats i anslutning till lagen. De uppgifter som avses är exempelvis utfärdande av den statliga e-legitimationen enligt 2 kap. 1 § och återkallelse och spärr av statlig e-legitimation enligt 2 kap. 9 §.

Vem som kan få en statlig e-legitimation

8 § En statlig e-legitimation får utfärdas till en svensk medborgare som har fyllt eller som innevarande kalenderår ska fylla nio år.

Paragrafen innehåller bestämmelser om personkretsen för utfärdande av en statlig e-legitimation. Övervägandena finns i avsnitt 8.1.

Av paragrafen framgår att en statlig e-legitimation får utfärdas till svenska medborgare. En förutsättning för att kunna få en statlig e-legitimation är vidare att sökanden har fyllt eller ska fylla nio år under innevarande kalenderår. Var personen är bosatt, i Sverige eller utomlands, saknar betydelse, så länge han eller hon är svensk medborgare. Det saknar också betydelse om personen har ett personnummer eller har tilldelats ett samordningsnummer som identitetsbeteckning. Regeringen eller den myndighet som regeringen bestämmer får med stöd av bemyndigandet i 2 kap. 12 § andra stycket meddela föreskrifter om att den statliga e-legitimationen ska lagras exempelvis på ett nationellt identitetskort. Svenska medborgare skulle i så fall kunna få ett nationellt identitetskort och en statlig e-legitimation i samma fysiska identitetshandling.

9 § En statlig e-legitimation får utfärdas till en utlänning som har fyllt eller som innevarande kalenderår ska fylla nio år och som

1. är folkbokförd i Sverige enligt folkbokföringslagen (1991:481), eller
2. har tilldelats ett personnummer enligt 18 b § samma lag och som omfattas av lagen (1976:661) om immunitet och privilegier i vissa fall.

Paragrafen innehåller bestämmelser om personkretsen för utfärdande av en statlig e-legitimation. Övervägandena finns i avsnitt 8.1.

Av paragrafen framgår att en statlig e-legitimation under vissa förutsättningar får utfärdas till en utlänning som har fyllt eller som innevarande kalenderår ska fylla nio år.

I *första punkten* anges att en statlig e-legitimation får utfärdas till utlänningar som är folkbokförda i Sverige enligt folkbokföringslagen. Personer som har tilldelats samordningsnummer är inte folkbokförda och omfattas därför inte av den aktuella bestämmelsen.

Av *andra punkten* framgår att en statlig e-legitimation får utfärdas till en utlänning som har tilldelats ett personnummer enligt 18 b § folkbokföringslagen och som omfattas av lagen om immunitet och privilegier i vissa fall. Av 18 b § folkbokföringslagen följer att personnummer i vissa fall kan tilldelas personer som enligt 5 § folkbokföringslagen inte ska folkbokföras. Det gäller personer som har rätt till immunitet och privilegier enligt lagen om immunitet och privilegier i vissa fall. Det gäller bl.a. den som tjänstgör vid ett annat lands ambassad eller konsulat i Sverige, om förutsättningarna i övrigt i 18 b § folkbokföringslagen är uppfyllda. Det är dock inte tillräckligt att personen en gång har tilldelats ett sådant personnummer. Vid tidpunkten för ansökan om statlig e-legitimation måste personen fortfarande omfattas av lagen om immunitet och privilegier i vissa fall. Detta innebär att personen måste befinna sig i Sverige och i övrigt uppfylla förutsättningarna i 2, 3 eller 4 § lagen om immunitet och privilegier i vissa fall.

Giltighetstiden

10 § En e-legitimation ska utfärdas med en giltighetstid om fem år. Om sökanden inte har fyllt tolv år ska giltighetstiden vara tre år.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att den statliga e-legitimationen i särskilt angivna fall ska ha en kortare giltighetstid.

Paragrafen reglerar den statliga e-legitimationens giltighetstid. Övervägandena finns i avsnitt 8.5.

Enligt *första stycket* ska en statlig e-legitimation utfärdas med en giltighetstid om fem år eller, om sökanden inte har fyllt tolv år, tre år.

Av *andra stycket* framgår att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att den statliga e-legitimationen i särskilt angivna fall ska ha en kortare giltighetstid än det som föreskrivs i första stycket. Att föreskrifterna ska avse särskilt angivna fall innebär att giltighetstiden inte kan förkortas generellt för alla som ansöker om en e-legitimation. En kortare giltighetstid skulle t.ex. kunna föreskrivas för personer som av fysiska skäl är tillfälligt förhindrade att lämna fingeravtryck, jfr 5 § förordningen (2005:661) om nationellt identitetskort. Om e-legitimationen placeras på ett nationellt identitetskort kan giltighetstiden exempelvis begränsas till den tidpunkt då en person kan antas förlora sitt svenska medborgarskap, se 5 § andra stycket 3 samma förordning.

Villkor för användningen av den statliga e-legitimationen

11 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om villkor för användningen av den statliga e-legitimationen.

I paragrafen ges regeringen eller den myndighet som regeringen bestämmer rätt att meddela föreskrifter om villkor för användningen av den statliga e-legitimationen. Övervägandena finns i avsnitt 8.7.

Föreskrifter enligt paragrafen kan exempelvis avse villkor för offentliga eller privata aktörers användning av den statliga e-legitimationen i sina nättjänster, t.ex. om kontrollen av biometriska uppgifter i samband med identifiering. Det kan vidare avse föreskrifter om att tillfälligt begränsa en innehavare från att använda den statliga e-legitimationen. Det kan också avse villkor om användning för innehavaren av e-legitimationen, t.ex. aktsamhetskrav.

2 kap. Ansökan, utfärdande och återkallelse

En ansökan krävs

1 § Den statliga e-legitimationen utfärdas efter ansökan.

Om sökanden är under arton år krävs det vårdnadshavares medgivande, om det inte finns synnerliga skäl för utfärdandet.

Paragrafen innehåller bestämmelser om krav på ansökan och medgivande av vårdnadshavare. Övervägandena finns i avsnitt 8.2.

Enligt *första stycket* utfärdas den statliga e-legitimationen efter ansökan. I 12 § finns bestämmelser om att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om förfarandet vid ansökan och föreskrifter om avgifter.

Av *andra stycket* framgår att det krävs vårdnadshavares medgivande om sökanden under arton år, om det inte finns synnerliga skäl för att ändå utfärda e-legitimationen. Om föräldrarna har gemensam vårdnad om barnet, krävs medgivande från båda. Det kan exempelvis finnas synnerliga skäl för att göra undantag från huvudregeln om en av vårdnadshavarna är tillfälligt förhindrad att lämna sitt medgivande, t.ex. på grund av sjukdom, och det är uppenbart att dennes medgivande annars skulle ha lämnats (jfr prop. 1977/78:156 s. 44).

Personlig inställelse

2 § Den som ansöker om en statlig e-legitimation ska lämna ansökan vid personlig inställelse.

Paragrafen innehåller bestämmelser om personlig inställelse vid ansökan om statlig e-legitimation. Övervägandena finns i avsnitt 8.2.

Kravet på personlig inställelse innebär att den som vill ha en statlig e-legitimation som utgångspunkt ska komma till utfärdande myndighets lokaler och göra sin ansökan där. Bestämmelsen hindrar inte att myndigheten tar upp en ansökan utanför myndighetens lokaler, om de tekniska, ekonomiska och personalmässiga förutsättningarna för detta skulle finnas. Någon skyldighet för myndigheten att göra detta finns dock inte. I samband med den personliga inställelsen kan myndigheten ta sökandens ansiktsbild och fingeravtryck enligt 4 §.

Av 12 § första stycket 1 framgår att regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om förfarandet vid ansökan. Det kan t.ex. avse föreskrifter om var sökanden ska inställa sig vid ansökan om statlig e-legitimation.

Styrkande av identitet

3 § Sökanden ska vid ansökan styrka sin identitet och övriga personuppgifter som krävs för att en statlig e-legitimation ska utfärdas.

Paragrafen innehåller bestämmelser om styrkande av identitet och övriga personuppgifter vid ansökan om statlig e-legitimation. Övervägandena finns i avsnitt 8.2.

Den som ansöker om en statlig e-legitimation ska enligt paragrafen styrka sin identitet och de övriga personuppgifter som krävs för att e-legitimationen ska kunna utfärdas. Om sökanden inte styrker sin identitet och övriga personuppgifter, trots en uppmaning att göra det, ska ansökan avslås. Detta framgår av 8 §, se författningskommentaren till den paragrafen.

Av 12 § första stycket 1 framgår att regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om förfarandet vid ansökan. Det kan t.ex. vara föreskrifter om hur sökanden ska styrka sin identitet och övriga personuppgifter.

I 6 § första stycket finns bestämmelser om kontroll av ansiktsbild och fingeravtryck i den identitetshandling som en sökande visar upp för att styrka sin identitet, se författningskommentaren till den bestämmelsen.

4 § Sökanden ska låta den utfärdande myndigheten ta sökandens ansiktsbild och fingeravtryck i samband med ansökan om statlig e-legitimation.

Sökanden ska även låta den utfärdande myndigheten ta sökandens ansiktsbild och fingeravtryck vid utlämnande av den statliga e-legitimationen, om den utfärdande myndigheten begär det.

Paragrafen innehåller bestämmelser om sökandens ansiktsbild och fingeravtryck. Övervägandena finns i avsnitt 8.3 och 9.4.

Av paragrafen framgår att sökanden är skyldig att låta den utfärdande myndigheten ta sökandens ansiktsbild och fingeravtryck vid särskilt angivna tillfällen.

Enligt *första stycket* är sökanden skyldig att låta den utfärdande myndigheten ta sökandens ansiktsbild och fingeravtryck i samband med ansökan om statlig e-legitimation. Ansiktsbilden och fingeravtrycken ska sparas i ett lagringsmedium i bäraren av den statliga e-legitimationen. Detta framgår av 5 §, se författningskommentaren till den paragrafen.

Enligt *andra stycket* är sökanden skyldig att låta den utfärdande myndigheten ta sökandens ansiktsbild och fingeravtryck vid utlämnande av den statliga e-legitimationen om den utfärdande myndigheten begär det. Det finns dock ingen skyldighet för myndigheten att ta sökandens ansiktsbild och fingeravtryck vid utlämnande. Om uppgifterna tas får de användas vid kontroll enligt 6 §, se författningskommentaren till den paragrafen.

Den ansiktsbild, och de biometriska uppgifter som har tagits fram ur ansiktsbilden, som får tas enligt första stycket i denna paragraf får enligt 3 kap. 6 § 2 sparas i registret över ärenden om statlig e-legitimation. Av 3 kap. 9 § följer att det är förbjudet att som sökbegrepp använda ansiktsbilder och biometriska uppgifter som har tagits fram ur ansiktsbilder. Uppgifterna får dock användas vid sökning i registret i ett ärende om statlig e-legitimation. Sökning är då tillåten endast för att kontrollera sökandens identitet och innehav av en e-legitimation i samband med ansökan.

Av 12 § tredje stycket 2 följer att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om undantag från skyldigheten att lämna fingeravtryck.

5 § Ansiktsbilden som tas i samband med ansökan enligt 4 § första stycket ska sparas i ett lagringsmedium i bäraren av den statliga e-legitimationen. Om fingeravtryck har tagits ska även dessa sparas i lagringsmediet.

I paragrafen finns bestämmelser om utformningen av den statliga e-legitimationen. Övervägandena finns i avsnitt 8.3.

Den ansiktsbild som tas vid ansökan enligt 4 § första stycket ska sparas i ett lagringsmedium i bäraren av den statliga e-legitimationen. Om fingeravtryck har tagits ska även dessa sparas i lagringsmediet. Ansiktsbilden och de biometriska uppgifter som har tagits fram ur sådana bilder får sparas i registret över ärenden om statlig e-legitimation enligt 3 kap. 6 § 2, se författningskommentaren till den bestämmelsen.

Av 7 § första stycket framgår att fingeravtrycken och de biometriska uppgifter som tas fram ur dessa omedelbart ska förstöras när den statliga e-legitimationen har lämnats ut eller, om e-legitimationen inte har lämnats

ut, när det har gått 90 dagar från den dag då den utfärdades. Om ett ansökningsärende har avslutats på något annat sätt ska uppgifterna också förstöras omedelbart, se författningskommentaren till 7 § första stycket.

6 § Om sökanden styrker sin identitet med en identitetshandling som är försedd med en ansiktsbild eller innehåller ett lagringsmedium där ansiktsbild eller fingeravtryck är sparade, får den utfärdande myndigheten kontrollera att dessa motsvarar den ansiktsbild och de fingeravtryck som tas enligt 4 §.

Den utfärdande myndigheten får även kontrollera att ansiktsbild och fingeravtryck som tas i samband med utlämnande enligt 4 § andra stycket motsvarar de som finns lagrade i den statliga e-legitimationen.

Paragrafen innehåller bestämmelser om kontroll av ansiktsbilder och fingeravtryck. Övervägandena finns i avsnitt 9.4.

Av *första stycket* följer att om sökanden styrker sin identitet med en handling som är försedd med en ansiktsbild eller innehåller ett lagringsmedium där ansiktsbild eller fingeravtryck är sparade får den utfärdande myndigheten kontrollera att dessa motsvarar den ansiktsbild och de fingeravtryck som tas enligt 4 §, dvs. i samband med ansökan om och utlämnande av en e-legitimation. Jämförelsen av ansiktsbilderna kan vara okulär. Kontrollen kan också vara datorstödd genom att ansiktsbilden eller fingeravtrycken i identitetshandlingen jämförs biometriskt med ansiktsbilden och fingeravtrycken som har tagits med stöd av 4 § (jfr prop. 2004/05:119 s. 50).

Enligt *andra stycket* får den utfärdande myndigheten i samband med utlämnande av e-legitimationen även kontrollera att ansiktsbild och fingeravtryck som då tas med stöd av 4 § andra stycket motsvarar de som finns lagrade i den statliga e-legitimationen. Den utfärdande myndigheten avgör om ansiktsbild och fingeravtryck ska tas vid utlämnande enligt 4 § andra stycket och om en kontroll enligt denna bestämmelse i så fall ska göras.

I 3 kap. 10 § andra stycket 2 regleras behandlingen av känsliga personuppgifter vid denna typ av kontroll, se författningskommentaren till den paragrafen.

Av 7 § tredje stycket framgår att fingeravtrycken och de biometriska uppgifter som tas fram ur dessa omedelbart ska förstöras när kontrollen enligt denna paragraf har genomförts, se författningskommentaren till den bestämmelsen.

7 § De fingeravtryck som tas enligt 4 § första stycket och de biometriska uppgifter som tas fram ur dessa ska omedelbart förstöras när den statliga e-legitimationen har lämnats ut eller, om e-legitimationen inte har lämnats ut, när det har gått 90 dagar från den dag då den utfärdades. Om ett ansökningsärende har avslutats på något annat sätt ska uppgifterna också förstöras omedelbart.

Den ansiktsbild och de fingeravtryck som tas enligt 4 § andra stycket och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken ska omedelbart förstöras när kontrollen enligt 6 § andra stycket har genomförts.

Den ansiktsbild och de fingeravtryck som vid kontroll enligt 6 § tas fram ur ett lagringsmedium och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken ska omedelbart förstöras när kontrollen har genomförts.

Paragrafen innehåller bestämmelser om förstörelse av ansiktsbild, fingeravtryck och biometriska uppgifter. Övervägandena finns i avsnitt 9.4.

Enligt *första stycket* ska de fingeravtryck som tas av utfärdande myndighet i samband med ansökan om statlig e-legitimation enligt 4 § första stycket och de biometriska uppgifter som tas fram ur fingeravtrycken förstöras. Det ska göras omedelbart när e-legitimationen har lämnats ut eller, om e-legitimationen inte har lämnats ut, när det har gått 90 dagar från den dag då den utfärdades. Uppgifterna ska även förstöras omedelbart om ett ansökningsärende har avslutats på annat sätt. Med biometriska uppgifter avses detsamma som i artikel 4.14 i EU:s dataskyddsförordning, dvs. 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, exempelvis fingeravtryck. Biometriska uppgifter kan beskrivas som den information som är resultatet av en automatiserad mätning av t.ex. ett fingeravtryck utifrån en bild.

Ett ärende kan avslutas t.ex. genom att ansökan avslås eller skrivs av från vidare handläggning. Bestämmelsen innebär att fingeravtrycken och de biometriska uppgifter som tas fram ur dessa får behandlas under handläggningen av en ansökan om statlig e-legitimation. Efter att e-legitimationen har lämnats ut eller ansökningsärendet avslutats får uppgifterna inte sparas på något annat sätt än i den statliga e-legitimationen, se 5 § och författningskommentaren till den paragrafen. Det finns däremot inte något hinder mot att spara ansiktsbilder som har tagits vid ansökan enligt 4 § första stycket och de biometriska uppgifter som har tagits fram ur dessa i registret över ärenden om statlig e-legitimation, se 3 kap. 6 § 2 och författningskommentaren till den bestämmelsen.

Enligt *andra stycket* ska den ansiktsbild och de fingeravtryck som tas i samband med utlämnande av den statliga e-legitimationen och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken omedelbart förstöras när kontrollen enligt 6 § andra stycket har genomförts. Kontrollen enligt 6 § andra stycket innebär att utfärdande myndighet får kontrollera att ansiktsbild och fingeravtryck som tas i samband med utlämnande enligt 4 § andra stycket motsvarar de som finns lagrade i den statliga e-legitimationen.

Kontrollerna som utfärdande myndighet enligt 6 § får göra i samband med ansökan om och utlämnande av en statlig e-legitimation kan innefatta en jämförelse av ansiktsbild, fingeravtryck och de biometriska uppgifterna som tas fram ur ansiktsbilden och fingeravtrycken. Enligt *tredje stycket* ska den ansiktsbild och de fingeravtryck som vid en kontroll enligt 6 § tas fram ur ett lagringsmedium och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken förstöras. Det ska göras omedelbart efter att kontrollen har genomförts. Bestämmelsen omfattar ansiktsbild och fingeravtryck som tas fram ur ett lagringsmedium i en identitetshandling som en sökande styrker sin identitet med vid kontroll enligt 6 § första stycket. Den omfattar även ansiktsbild och fingeravtryck som tas fram ur den statliga e-legitimationen vid kontroll enligt 6 § andra stycket.

Avslag av ansökan och utfärdande av statlig e-legitimation

8 § En ansökan om en statlig e-legitimation ska avslås om de krav som framgår av denna lag eller de föreskrifter som har meddelats i anslutning till lagen inte är uppfyllda och sökanden inte har följt en uppmaning att rätta till bristen. I annat fall

ska den statliga e-legitimationen utfärdas och skyndsamt vara tillgänglig för utlämnande.

Paragrafen anger under vilka förutsättningar en ansökan om statlig e-legitimation ska avslås eller den statliga e-legitimationen ska utfärdas. Övervägandena finns i avsnitt 8.4.

En ansökan om statlig e-legitimation ska avslås om de krav som framgår av lagen, eller föreskrifter som har meddelats i anslutning till lagen, inte är uppfyllda och sökanden inte har följt en uppmaning att rätta till bristen. De krav som måste vara uppfyllda framgår av 2 kap. 1–4 §§, se författningskommentarerna till de paragraferna. Om kraven är uppfyllda ska den statliga e-legitimationen utfärdas och skyndsamt vara tillgänglig för att lämnas ut till sökanden.

Återkallelse och spärr av statlig e-legitimation

9 § En statlig e-legitimation ska återkallas och spärras om

1. det fanns hinder mot att utfärda en e-legitimation vid tiden för utfärdandet och hindret fortfarande består,
2. någon väsentlig uppgift som en e-legitimation innehåller är felaktig,
3. det är nödvändigt av säkerhetsskäl,
4. den är utfärdad på en fysisk identitetshandling som därefter har upphört att gälla, eller
5. innehavaren har avlidit.

En statlig e-legitimation får även återkallas och spärras på begäran av innehavaren. Om begäran avser ett barn under arton år krävs det vårdnadshavares medgivande, om det inte finns synnerliga skäl för återkallelsen och spärren.

Paragrafen anger grunderna för återkallelse och spärr av en statlig e-legitimation. Övervägandena finns i avsnitt 8.6.

I *första stycket* anges i vilka fall en statlig e-legitimation ska återkallas och spärras på den utfärdande myndighetens initiativ. Med spärr avses den tekniska åtgärden som gör att e-legitimationen blir permanent obrukbar. En sådan spärr hindrar inte att föreskrifter meddelas med stöd av 1 kap. 11 § om att tillfälligt begränsa innehavarens användning av den statliga e-legitimationen, t.ex. vid upprepade felslagningar av inloggningsuppgifter.

Enligt *första stycket första punkten* ska en statlig e-legitimation återkallas och spärras om det fanns hinder mot att utfärda en e-legitimation vid tiden för utfärdandet och hindret fortfarande består. Återkallelse på denna grund aktualiseras exempelvis om innehavaren har fått en e-legitimation i en annan persons namn eller om något av de krav som gäller för att få en e-legitimation inte var uppfyllt vid utfärdandet och fortfarande inte är det (jfr prop. 1977/78:156 s. 48 och prop. 2015/16:28 s. 55).

I *första stycket andra punkten* anges att en statlig e-legitimation ska återkallas och spärras om någon väsentlig uppgift som en e-legitimation innehåller är felaktig. Bestämmelsen omfattar både rena felskrivningar och ändringar av uppgifter. Vilka uppgifter som ska finnas i en statlig e-legitimation framgår av 2 kap. 5 §. Vidare får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om det enligt 12 § andra stycket. Sådana uppgifter som krävs för att innehavaren ska kunna identifieras på ett korrekt sätt ska betraktas som väsentliga. Det kan vara t.ex. namn eller person- eller samordningsnummer. Om det visar sig att

någon sådan uppgift är felaktig eller inte längre gäller ska e-legitimationen återkallas och spärras.

Enligt *första stycket tredje punkten* ska en statlig e-legitimation återkallas och spärras om det är nödvändigt av säkerhetsskäl. Grund för återkallelse av säkerhetsskäl kan exempelvis finnas om den som e-legitimationen är utställd till eller någon annan kan misstänkas använda e-legitimationen i brottslig verksamhet. Det avser både fall där innehavaren själv har lämnat ut e-legitimationen till någon annan och sådana där e-legitimationen har hamnat i orätta händer på annat sätt.

Enligt *första stycket fjärde punkten* ska en statlig e-legitimation återkallas och spärras om e-legitimationen har utfärdats på en fysisk identitetshandling, exempelvis ett nationellt identitetskort, som inte längre gäller. Bestämmelsen gäller oavsett om den fysiska identitetshandlingen har upphört att gälla på grund av att giltighetstiden har gått ut eller att identitetshandlingen har återkallats.

Av *första stycket femte punkten* följer att en e-legitimation ska återkallas och spärras om innehavaren har avlidit.

Enligt *andra stycket* får en statlig e-legitimation återkallas och spärras på begäran av innehavaren. Det uppställs inte något krav på att ange några skäl för en sådan begäran. Om begäran om återkallelse och spärr avser ett barn under arton år krävs det vårdnadshavares medgivande, om det inte finns synnerliga skäl för att ändå återkalla och spärra e-legitimationen. Om föräldrarna har gemensam vårdnad om barnet, krävs medgivande från båda. Det kan exempelvis finnas synnerliga skäl om en av vårdnadshavarna är tillfälligt förhindrad att lämna sitt medgivande, t.ex. på grund av sjukdom, och det är uppenbart att dennes medgivande annars skulle ha lämnats (jfr 2 kap. 1 § andra stycket). Synnerliga skäl kan också finnas om e-legitimationen används i brottslig verksamhet och den enskilde skulle lida skada om återkallelsen eller spärren skulle dröja.

10 § En statlig e-legitimation ska, utöver i de fall som anges i 9 §, spärras
1. i samband med att en ny e-legitimation lämnas ut till sökanden, eller
2. när giltighetstiden har löpt ut.

Paragrafen reglerar ytterligare fall, utöver de som anges i 9 §, i vilka en statlig e-legitimation ska spärras. Övervägandena finns i avsnitt 8.6.

Av *första punkten* framgår att en statlig e-legitimation ska spärras i samband med att en ny lämnas ut till sökanden. Det kan t.ex. inträffa att en enskild ansöker om en ny e-legitimation innan giltighetstiden till en tidigare utfärdad e-legitimation har löpt ut.

Enligt *andra punkten* ska en statlig e-legitimation spärras när giltighetstiden har löpt ut.

Avgifter

11 § Utfärdande myndighet får ta ut avgifter för ansökan om statlig e-legitimation.

Paragrafen reglerar möjligheten för utfärdande myndighet att ta ut avgifter för ansökan om statlig e-legitimation. Övervägandena finns i avsnitt 8.9.

Av paragrafen framgår att utfärdande myndighet får ta ut avgifter för ansökan om statlig e-legitimation. Enligt 12 § tredje stycket 1 får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om avgifter för ansökan om statlig e-legitimation.

Rätt att meddela föreskrifter

12 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om förfarandet vid

1. ansökan,
2. utfärdande,
3. utlämnande, och
4. återkallelse och spärr.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen även meddela föreskrifter om den statliga e-legitimationens

1. innehåll, bärare och utformning i övrigt, och
2. aktivering.

Regeringen eller den myndighet som regeringen bestämmer får vidare meddela föreskrifter om

1. avgifter för ansökan om statlig e-legitimation, och
2. undantag från skyldigheten att lämna fingeravtryck enligt 4 §.

I paragrafen ges regeringen eller den myndighet som regeringen bestämmer möjlighet att meddela vissa föreskrifter. Övervägandena finns i avsnitt 8.2, 8.3, 8.6 och 8.9.

Första stycket första punkten avser en rätt att meddela ytterligare föreskrifter om förfarandet vid ansökan. Sådana föreskrifter kan t.ex. vara bestämmelser om kravet på styrkt identitet enligt 3 § eller om hur ansiktsbilden och fingeravtrycken ska tas enligt 4 §. Det kan också vara föreskrifter om var sökanden ska inställa sig vid ansökan om statlig e-legitimation.

Exempel på föreskrifter som avses i *första stycket andra punkten* är föreskrifter som bedöms som nödvändiga för förfarandet vid utfärdandet av den statliga e-legitimationen.

Föreskrifter enligt *första stycket tredje punkten* kan avse bestämmelser om tidpunkten för utlämnandet, t.ex. om utlämnandet ska göras i samband med ansökan eller vid ett senare tillfälle.

Föreskrifter som avses i *första stycket fjärde punkten* kan exempelvis reglera hur en begäran om återkallelse från innehavaren ska vara utformad.

Av *andra stycket första punkten* framgår att föreskrifter kan meddelas om e-legitimationens innehåll, bärare och utformning i övrigt. Det kan avse föreskrifter om vilka uppgifter som ska lagras i e-legitimationen, t.ex. uppgifter om sökanden, såsom namn och övriga personuppgifter. Vidare kan det avse föreskrifter om den statliga e-legitimationens bärare. Med bärare avses den fysiska handling som e-legitimationen placeras på. För svenska medborgare kan e-legitimationen t.ex. placeras på ett identitetskort utfärdat av en passmyndighet, dvs. för närvarande det nationella identitetskortet. För övriga personkategorier kan föreskrifterna exempelvis avse placering av e-legitimationen på ett kort som i fråga om utformning och innehåll motsvarar ett sådant identitetskort.

Av *andra stycket andra punkten* framgår att föreskrifter om aktivering av den statliga e-legitimationen kan meddelas. Att e-legitimationen aktiveras innebär att den rent praktiskt blir tillgänglig för innehavaren att använda, t.ex. genom en mobilapplikation.

Tredje stycket första punkten avser möjligheten att meddela föreskrifter om avgifter för ansökan om statlig e-legitimation. Bemyndigandet omfattar exempelvis frågan om avgifter ska tas ut och avgifternas storlek.

Tredje stycket andra punkten ger möjlighet att meddela föreskrifter om undantag från sökandens skyldighet att låta utfärdande myndighet ta sökandens fingeravtryck. Det kan t.ex. avse föreskrifter om att barn i en viss ålder eller personer som har skador på fingrarna inte är skyldiga att lämna fingeravtryck (jfr prop. 2008/09:132 s. 10 och 11).

3 kap. Behandling av personuppgifter

Ändamålen med behandlingen

1 § Personuppgifter får behandlas av utfärdande myndighet om det är nödvändigt för att

1. handlägga ärenden om statlig e-legitimation,
2. föra ett register över ärenden om statlig e-legitimation, och
3. vidta åtgärder för en säker användning av statliga e-legitimationer.

I paragrafen anges de primära ändamålen för personuppgiftsbehandling. Övervägandena finns i avsnitt 9.2.

Ändamålsbestämmelserna i paragrafen är s.k. primära ändamål, dvs. ändamål för vilka myndigheten både får samla in personuppgifter och behandla de uppgifter som har samlats in. Ändamålsbestämmelserna ger stöd för personuppgiftsbehandling i alla typer av ärenden om statlig e-legitimation. Bestämmelserna ger vidare stöd för att behandla personuppgifter vid alla åtgärder som är nödvändiga att vidta för ändamålen. Att behandlingen ska vara nödvändig innebär inte ett krav på att den ska vara oundgänglig. Behandlingen kan anses nödvändig om den leder till effektivitetsvinster (se prop. 2017/18:105 s. 189).

Enligt *första punkten* får utfärdande myndighet behandla personuppgifter om det är nödvändigt för att handlägga ärenden om statlig e-legitimation. Det gäller exempelvis för utfärdande, återkallelse och spärr eller någon annan åtgärd som har sin grund i lagen. De åtgärder som aktualiseras vid handläggning av ett ärende är exempelvis mottagande av uppgifter, diarieföring, kommunicering och utlämnande i samband med expediering.

Av *andra punkten* följer att utfärdande myndighet får behandla personuppgifter om det är nödvändigt för att föra ett register över ärenden om statlig e-legitimation. Enligt 5 § ansvarar Polismyndigheten för registret. Vilka uppgifter som får finnas i registret framgår av 6 §.

Åtgärder för en säker användning enligt *tredje punkten* kan vara åtgärder som den utfärdande myndigheten vidtar för att e-legitimationen ska användas på ett säkert sätt exempelvis i privata aktörers nättjänster, t.ex. genom villkor för användningen av den statliga e-legitimationen. Sådana villkor kan t.ex. ställas på aktörer som erbjuder identifiering med medel för elektronisk identifiering i sina nättjänster och innebära behandling av

personuppgifter, t.ex. uppgifter om en kontaktperson hos aktören som erbjuder nättjänsten.

2 § Personuppgifter som behandlas enligt 1 § får också behandlas av utfärdande myndighet

1. om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet, och

2. om det är nödvändigt för att lämna ut uppgifter i enlighet med lag eller förordning.

Personuppgifterna får även behandlas för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Paragrafen innebär att personuppgifter som behandlas enligt 1 § även får behandlas för vissa andra angivna ändamål, s.k. sekundära ändamål. Övervägandena finns i avsnitt 9.2.

Av *första punkten* framgår att personuppgifter som behandlas enligt 1 § även får behandlas om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet. Bestämmelserna utformas med regleringen i 2 kap. 1 § första stycket 1 lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område som förebild. Vägledning för hur bestämmelserna ska tillämpas kan därför hämtas från förarbetena till de bestämmelserna (prop. 2017/18:269 s. 292 och prop. 2018/19:65 s. 192). Vid den fortsatta behandlingen för dessa ändamål gäller brottsdatalagen (2018:1177) och lagen om polisens behandling av personuppgifter inom brottsdatalagens område (prop. 2017/18:232 och prop. 2017/18:269).

Enligt *andra punkten* får personuppgifter som behandlas enligt 1 § även behandlas om det är nödvändigt för att lämna ut uppgifter i enlighet med lag eller förordning. Det kan handla om att myndigheten behöver lämna ut uppgifter till enskilda eller till andra myndigheter enligt exempelvis 6 kap. 4 och 5 §§ offentlighets- och sekretesslagen (2009:400).

Bestämmelsen i *andra stycket* tillåter att personuppgifter som behandlas enligt 1 § behandlas för andra ändamål enligt den s.k. finalitetsprincipen. Bestämmelsen är utformad enligt artikel 5.1 b i EU:s dataskyddsförordning och bör tolkas på samma sätt. Det innebär bl.a. att behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i förordningen inte ska anses vara oförenlig med insamlingsändamålen. Det innebär också att de omständigheter som anges i artikel 6.4 a–e i förordningen ska beaktas vid bedömningen av om behandlingen är förenlig med insamlingsändamålen. Exempel på omständigheter som den personuppgiftsansvarige ska beakta är personuppgifternas art och eventuella konsekvenser för registrerade av den planerade fortsatta behandlingen.

Begränsning av rätten att göra invändningar

3 § Artikel 21.1 i EU:s dataskyddsförordning om rätten att göra invändningar gäller inte vid sådan behandling som är tillåten enligt denna lag eller föreskrifter som har meddelats i anslutning till lagen.

I paragrafen görs undantag från den rätt som registrerade har att invända mot behandling av personuppgifter enligt artikel 21.1 i EU:s dataskyddsförordning. Övervägandena finns i avsnitt 9.8.

Undantaget avser rätten för den registrerade att när som helst, av skäl som hänför sig till den registrerades specifika situation, göra invändningar mot behandlingen av personuppgifter. Vid sådan behandling av personuppgifter som är tillåten enligt lagen, eller föreskrifter som har meddelats i anslutning till den, gäller därmed inte rätten enligt artikel 21.1 i EU:s dataskyddsförordning att göra invändningar mot behandlingen.

Säkerhetsåtgärder

4 § Tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter i verksamheten med den statliga e-legitimationen.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om

1. begränsningen av tillgången till personuppgifter enligt första stycket, och
2. säkerhetsåtgärder till skydd för personuppgifter.

Paragrafen reglerar tillgången till personuppgifter för utfärdande myndighets personal. Övervägandena finns i avsnitt 9.7.

Anställda och andra som utför uppgifter i den utfärdande myndighetens verksamhet med den statliga e-legitimationen ska enligt *första stycket* inte ges tillgång till fler personuppgifter än det som behövs med hänsyn till deras arbete. Det är den utfärdande myndigheten som i egenskap av personuppgiftsansvarig ansvarar för att avgöra vilka personuppgifter som varje person behöver ha tillgång till för att kunna fullgöra sina arbetsuppgifter. Tillgången till personuppgifter kan begränsas genom tekniska och organisatoriska åtgärder. Uttrycket var och en inkluderar såväl tillsvidareanställd personal som t.ex. personal med tidsbegränsad anställning.

Andra stycket ger regeringen eller den myndighet som regeringen bestämmer möjlighet att meddela ytterligare föreskrifter om begränsningar av tillgången till personuppgifter och om säkerhetsåtgärder till skydd för personuppgifter.

Föreskrifter som kan meddelas med stöd av *andra stycket första punkten* kan t.ex. vara föreskrifter om vilka uppgifter en handläggare ska få tillgång till i ett ärende om ansökan om statlig e-legitimation eller om återkallelse av statlig e-legitimation.

Med stöd av *andra stycket andra punkten* kan exempelvis föreskrifter meddelas om att en viss typ av teknisk lösning ska användas för att skydda och begränsa tillgången till enskildas personuppgifter i myndighetens verksamhet.

5 § Polismyndigheten ska med hjälp av automatiserad behandling föra ett register över ärenden om statlig e-legitimation.

I paragrafen anges att Polismyndigheten ska föra ett register över ärenden om statlig e-legitimation. Övervägandena finns i avsnitt 9.3.

Av bestämmelsen följer att registret ska avse ärenden om statlig e-legitimation. Det innebär att registret även får innehålla uppgifter om ärenden där någon e-legitimation inte har utfärdats.

Med automatiserad behandling avses behandling med hjälp av tekniska hjälpmedel, såsom datorer, till skillnad från manuell behandling som avser t.ex. renodlad pappershantering (jfr prop. 2017/18:105 s. 47).

Vilka uppgifter som registret får innehålla regleras i 6 §. Hur länge uppgifterna får behandlas framgår av 7 §. Behandlingen av personuppgifter i registret omfattas även av övriga bestämmelser i kapitlet. Det innebär att bestämmelserna om exempelvis ändamål i 1 och 2 §§, säkerhetsåtgärder i 4 § och sökbegränsningar i 8 och 9 §§ även gäller när personuppgifter behandlas i registret, se författningskommentarerna till de paragraferna.

6 § Registret över ärenden om statlig e-legitimation får endast innehålla

1. namn, personnummer, samordningsnummer, medborgarskap, födelsedatum och kontaktuppgifter till sökanden,
2. ansiktsbilder som har tagits vid ansökan enligt 2 kap. 4 § första stycket och biometriska uppgifter som har tagits fram ur sådana bilder,
3. handlingar eller uppgifter från handlingar som har kommit in eller upprättats i ärenden om statlig e-legitimation,
4. uppgifter som rör handläggningen av ärenden om statlig e-legitimation, och
5. uppgifter om utfärdade statliga e-legitimationer.

I paragrafen regleras vad registret över ärenden om statlig e-legitimation får innehålla. Övervägandena finns i avsnitt 9.3.

Paragrafen innehåller en uppräkning av det som registret får innehålla. Uppräkningen är uttömmande.

Enligt *första punkten* får registret innehålla namn, personnummer, samordningsnummer, medborgarskap, födelsedatum och kontaktuppgifter till sökanden.

Av *andra punkten* framgår att registret får innehålla ansiktsbilder som har tagits vid ansökan enligt 2 kap. 4 § första stycket och biometriska uppgifter som har tagits fram ur sådana bilder. Med biometriska uppgifter avses detsamma som i artikel 4.14 i EU:s dataskyddsförordning, dvs. 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, exempelvis ansiktsbilder. Biometriska uppgifter kan beskrivas som den information som är resultatet av en automatiserad mätning av t.ex. ett ansikte utifrån ett fotografi. Möjligheten att söka i registret med hjälp av ansiktsbilder och biometriska uppgifter regleras i 9 §.

I *tredje punkten* anges att registret får innehålla handlingar eller uppgifter från handlingar som har kommit in eller upprättats i ärenden om statlig e-legitimation. Det kan t.ex. avse medgivanden som ska lämnas av vårdnadshavare enligt 2 kap. 1 §, kopior av handlingar som använts för att

styrka identiteten enligt 2 kap. 3 § och beslut om beviljade eller avslagna ansökningar eller återkallelse och spärr av e-legitimationer.

Enligt *fjärde punkten* får registret innehålla uppgifter som rör handläggningen av ärenden om statlig e-legitimation. Det kan t.ex. avse uppgift om när ansökan gjordes, vilken handläggare som tog emot ansökan eller som är ansvarig för ett ärende och vilka åtgärder som har vidtagits i ärendet.

Av *femte punkten* följer att registret får innehålla uppgifter om utfärdade statliga e-legitimationer. Sådana uppgifter kan t.ex. avse e-legitimationens serienummer eller annan identifierare, aktiveringskod, utfärdandedatum och giltighetstid.

Längsta tid som personuppgifter i registret får behandlas

7 § Personuppgifter i registret över ärenden om statlig e-legitimation får inte behandlas längre än tio år från utgången av det kalenderår som det ärende som uppgifterna hänför sig till avslutades.

Paragrafen reglerar hur länge personuppgifter får behandlas i registret över ärenden om statlig e-legitimation. Övervägandena finns i avsnitt 9.6.

I paragrafen anges den längsta tid som personuppgifter får behandlas i registret. Om det vid en tidigare tidpunkt står klart att personuppgifterna saknar betydelse i verksamheten med den statliga e-legitimationen ska de upphöra att behandlas redan då. Det är den personuppgiftsansvarige som bedömer hur länge personuppgifter behöver behandlas i registret. Bestämmelsen om längsta tid för behandling av personuppgifter hindrar inte att handlingar arkiveras och gallras enligt arkivlagens (1990:782) bestämmelser. Ett ärende kan avslutas t.ex. genom att ansökan avslås eller skrivs av från vidare handläggning.

Av 12 § framgår att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgifter ska fortsätta behandlas för vissa ändamål, se författningskommentaren till den paragrafen.

Förbud mot vissa sökningar

8 § Det är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller sådana personuppgifter om lagöverträdelser som avses i artikel 10 i EU:s dataskyddsförordning.

Paragrafen förbjuder sökningar i vissa syften. Övervägandena finns i avsnitt 9.5.

Enligt paragrafen är det förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller sådana personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning, dvs. personuppgifter om fällande domar i brottmål och lagöverträdelser som innefattar brott. Vad som avses med känsliga personuppgifter framgår av författningskommentaren till 10 §. Förbudet gäller oavsett om en sökning utförs i registret över ärenden om statlig e-legitimation eller bland andra uppgifter som behandlas enligt lagen. Det gäller vidare när personuppgifter behandlas för såväl primära ändamål enligt 1 § som sekundära ändamål enligt 2 §.

Förbudet i paragrafen omfattar alla tekniska åtgärder som innebär att känsliga personuppgifter eller sådana personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning används för att strukturera eller systematisera information i syfte att få fram ett urval av personer. Därmed förbjuds sökningar som görs för att få fram ett urval av personer som t.ex. har ett visst etniskt ursprung eller som har dömts för brott. Däremot hindrar bestämmelsen inte sökningar som görs i ett annat syfte än att identifiera ett urval av individer, t.ex. för att ta fram verksamhetsstatistik, för registervård eller vid tillsyn.

9 § Det är förbjudet att som sökbegrepp använda

1. ansiktsbilder, biometriska uppgifter som har tagits fram ur ansiktsbilder och andra känsliga personuppgifter som avses i 10 §, och
2. uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden.

Trots förbuden i första stycket får den ansiktsbild som tas enligt 2 kap. 4 § första stycket och de biometriska uppgifter som tas fram ur ansiktsbilden användas vid sökning i registret över ärenden om statlig e-legitimation i ett ärende om statlig e-legitimation. Sökning är då tillåten endast för att kontrollera sökandens identitet och innehav av en e-legitimation i samband med ansökan.

I paragrafen förbjuds användningen av vissa sökbegrepp i en utfärdande myndighets verksamhet med den statliga e-legitimationen. Övervägandena finns i avsnitt 9.4 och 9.5.

Första stycket innebär förbud mot att använda vissa typer av uppgifter som sökbegrepp i verksamheten med den statliga e-legitimationen. Med sökbegrepp avses sådana begrepp som används för att söka igenom en informationsmängd i syfte att hitta och välja ut de poster eller uppgiftskonstruktioner där begreppet förekommer (jfr prop. 2022/23:34 s. 211). Förbudet gäller oavsett om en sökning utförs i registret över ärenden om statlig e-legitimation eller bland andra uppgifter som behandlas enligt lagen. Förbudet gäller när personuppgifter behandlas för såväl primära ändamål enligt 1 § som sekundära ändamål enligt 2 §. Förbudet är absolut i den meningen att syftet med sökningen saknar betydelse. Förbudet medför att sökningar inte får göras ens för att tillmötesgå en begäran om utlämnande av allmän handling. Enligt 2 kap. 7 § tryckfrihetsförordningen anses en sammanställning inte förvarad hos en myndighet om den innehåller personuppgifter och myndigheten enligt lag eller förordning saknar befogenhet att göra den tillgänglig. Sammanställningen är alltså i sådana fall inte en allmän handling.

Enligt *första stycket första punkten* gäller ett förbud mot att som sökbegrepp använda ansiktsbilder, biometriska uppgifter som har tagits fram ur sådana bilder och andra känsliga personuppgifter enligt 10 §. Bestämmelsen innebär att det är förbjudet att exempelvis i ett datorprogram göra en sökning med utgångspunkt i en ansiktsbild eller biometriska uppgifter som har tagits fram ur en sådan bild. Se även författningskommentaren till 10 §.

Enligt *första stycket andra punkten* gäller ett förbud mot användningen av uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden som sökbegrepp. Bestämmelsen utformas med 17 § (2015:899) lagen om

identitetskort för folkbokförda i Sverige som förebild (jfr prop. 2017/18:95 s. 64–67 och 122).

I *andra stycket* finns ett undantag från förbuden i första stycket. Den ansiktsbild som tas vid en ansökan om statlig e-legitimation och de biometriska uppgifter som tas fram ur ansiktsbilden får användas vid sökning i registret över ärenden om statlig e-legitimation. Sökning tillåts endast i samband med ansökan och för att kontrollera sökandens identitet och innehav av statlig e-legitimation.

Behandling av känsliga personuppgifter

10 § Personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) får behandlas endast om det är absolut nödvändigt för ändamålet med behandlingen.

Känsliga personuppgifter får dock behandlas

1. i registret när det är tillåtet enligt 6 § 2,
2. vid kontroller som är tillåtna enligt 2 kap. 6 §, och
3. vid sökningar som är tillåtna enligt 9 § andra stycket.

I paragrafen regleras i vilka fall känsliga personuppgifter får behandlas i en utfärdande myndighets verksamhet med den statliga e-legitimationen. Övervägandena finns i avsnitt 9.2, 9.3 och 9.4.

Enligt *första stycket* får personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning behandlas endast om det är absolut nödvändigt för ändamålet med behandlingen. De uppgifter som avses är sådana som betecknas som känsliga personuppgifter enligt 3 kap. 1 § lagen med kompletterande bestämmelser till EU:s dataskyddsförordning. Med känsliga personuppgifter avses uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i en fackförening. Även genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa och uppgifter om en fysisk persons sexualliv eller sexuella läggning är känsliga personuppgifter. En kombination av t.ex. ansiktsbild och uppgifter om namn, medborgarskap och födelseort kan i vissa fall anses avslöja en persons etniska ursprung. Enligt bestämmelsen får sådana uppgifter behandlas om det är absolut nödvändigt för ändamålet med behandlingen. Att behandlingen ska vara absolut nödvändig innebär att behovet av att behandla uppgifterna måste prövas noggrant i varje enskilt fall.

Av *andra stycket* framgår i vilka fall som känsliga personuppgifter får behandlas utan någon prövning av om behandlingen är absolut nödvändig för ändamålet.

Enligt *andra stycket första punkten* får känsliga personuppgifter behandlas i registret över ärenden om statlig e-legitimation när det är tillåtet enligt 6 § 2. Det avser alltså behandling av ansiktsbilder som har tagits vid ansökan enligt 2 kap. 4 § första stycket och biometriska uppgifter som har tagits fram ur bilderna.

Av *andra stycket andra punkten* framgår att känsliga personuppgifter får behandlas vid kontroller som är tillåtna enligt 2 kap. 6 §. Den paragrafen reglerar möjligheten till jämförande kontroller av bl.a. biometriska uppgifter när en sökande ska styrka sin identitet i ett ärende om statlig e-legitimation, se författningskommentaren till den paragrafen.

Enligt *andra stycket tredje punkten* får känsliga personuppgifter behandlas vid sådana sökningar som är tillåtna enligt 9 § andra stycket. Enligt den bestämmelsen får biometriska uppgifter användas vid sökning i registret över ärenden om statlig e-legitimation i ett ärende om statlig e-legitimation för att kontrollera sökandens identitet och innehav av en e-legitimation i samband med ansökan, se författningskommentaren till den paragrafen.

Personuppgiftsansvar

11 § Varje utfärdande myndighet är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten själv utför.

Polismyndigheten är personuppgiftsansvarig för behandling av personuppgifter i registret över ärenden om statlig e-legitimation.

Paragrafen innehåller bestämmelser om personuppgiftsansvaret i verksamheten med den statliga e-legitimationen. Övervägandena finns i avsnitt 9.1.

Av *första stycket* framgår att varje utfärdande myndighet är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten själv utför. Det innebär att varje myndighet ansvarar för den personuppgiftsbehandling som sker inom ramen för myndighetens egen verksamhet.

Enligt *andra stycket* är Polismyndigheten personuppgiftsansvarig för behandlingen av personuppgifter i registret över ärenden om statlig e-legitimation. Den som exempelvis vill begära rättelse enligt artikel 16 i EU:s dataskyddsförordning av uppgifter i registret ska därför vända sig till Polismyndigheten.

Rätt att meddela föreskrifter

12 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter som avses i 7 § får fortsätta att behandlas under en viss tid för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, och
2. avskiljande och begränsningar av åtkomsten till personuppgifter som behandlas enligt 1.

I paragrafen finns en upplysningsbestämmelse om att regeringen eller den myndighet som regeringen bestämmer kan meddela vissa föreskrifter. Övervägandena finns i avsnitt 9.6.

Enligt *första punkten* kan regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om att personuppgifter i registret över ärenden om statlig e-legitimation får fortsätta behandlas under en viss tid för arkivändamål av allmänt intresse eller vetenskapliga, statistiska eller historiska ändamål under längre tid än det som regleras i 7 §. Föreskrifterna får alltså tillåta att uppgifter för sådana ändamål behandlas under längre tid än tio år från utgången av det kalenderår som det ärende som uppgifterna hänför sig till avslutades.

Av *andra punkten* framgår att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om avskiljande och

begränsningar av åtkomsten till personuppgifter i registret över ärenden om statlig e-legitimation som behandlas för sådana ändamål som anges i första punkten. Med avskiljande menas att personuppgifter tas bort från registret över ärenden om statlig e-legitimation.

4 kap. Erkännande av medel för elektronisk identifiering

Krav på erkännande av medel för elektronisk identifiering

1 § När medel för elektronisk identifiering krävs för att få tillgång till en nättjänst som tillhandahålls av en offentlig aktör, och tjänsten helt eller delvis riktar sig till enskilda, ska medel erkännas för autentisering för tjänsten om

1. medlet för elektronisk identifiering tillhandahålls inom ramen för ett auktorisationssystem i enlighet med lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post, och
2. tillitsnivån för medlet motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga aktören kräver för åtkomst till nättjänsten.

I paragrafen uppställs ett krav på offentliga aktörer att erkänna vissa medel för elektronisk identifiering. Övervägandena finns i avsnitt 10.

Paragrafen innebär att offentliga aktörer är skyldiga att erkänna medel för elektronisk identifiering för autentisering i en nättjänst när ett sådant medel krävs för att få tillgång till en nättjänst som tillhandahålls av aktören och tjänsten helt eller delvis riktar sig till enskilda. Vad som avses med medel för elektronisk identifiering, nättjänst och autentisering framgår av 1 kap. 3 §, se författningskommentaren till den paragrafen. Vilka som anses vara offentliga aktörer framgår av 1 kap. 4 §, se författningskommentaren till den paragrafen. Att tjänsten helt eller delvis riktar sig till enskilda innebär att kravet inte omfattar nättjänster som används inom ramen för en persons arbete eller utbildning, där identifiering sker med medel som uteslutande används i tjänsten eller i utbildningen.

Kravet gäller enligt *första punkten* endast sådana medel för elektronisk identifiering som tillhandahålls inom ramen för ett auktorisationssystem enligt lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post. Det innebär att leverantören och medlet ska ha godkänts inom ramen för ett auktorisationssystem enligt lagen.

Vidare måste enligt *andra punkten* tillitsnivån på medlet motsvara minst den tillitsnivå som den offentliga aktören kräver för åtkomst till nättjänsten.

Kravet i denna paragraf att erkänna vissa medel för elektronisk identifiering innebär inte ett krav på att den offentliga aktören ska ingå avtal med leverantörer genom ett auktorisationssystem enligt lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post.

Bemyndiganden

2 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. undantag från kravet i 1 §, och
2. hur kravet i 1 § ska fullgöras.

I paragrafen ges regeringen eller den myndighet som regeringen bestämmer rätt att meddela vissa föreskrifter om kravet på erkännande av medel för elektronisk identifiering. Övervägandena finns i avsnitt 10.

Möjligheten att enligt *första punkten* föreskriva om undantag från kravet att erkänna medel för elektronisk identifiering kan t.ex. aktualiseras av hänsyn till rikets säkerhet. Det kan också avse föreskrifter om undantag från kravet i förhållande till medel för elektronisk identifiering om det t.ex. finns flera överlappande auktorisationssystem med delvis likartade tjänster.

Föreskrifter enligt *andra punkten* kan avse inom vilken tid ett medel för elektronisk identifiering som har tillkommit i ett auktorisationssystem ska erkännas av en offentlig aktör för autentisering i aktörens nättjänst.

5 kap. Överklagande och verkställighet

1 § Beslut enligt denna lag eller enligt föreskrifter som har meddelats i anslutning till lagen får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

I paragrafen finns bestämmelser om överklagande av beslut enligt lagen. Övervägandena finns i avsnitt 11.

Enligt *första stycket* får beslut enligt lagen eller enligt föreskrifter som har meddelats i anslutning till lagen överklagas till allmän förvaltningsdomstol. Ytterligare bestämmelser om överklagande, bl.a. vem som får överklaga ett beslut, hur man överklagar ett beslut och tiden för överklagande finns i förvaltningslagen (2017:900).

Av *andra stycket* framgår att prövningstillstånd krävs vid överklagande till kammarrätten.

2 § Beslut enligt denna lag gäller omedelbart, om inte annat anges i beslutet.

Av paragrafen framgår att beslut enligt lagen gäller omedelbart, om inte något annat anges i beslutet. Övervägandena finns i avsnitt 11.

Att ett beslut gäller omedelbart innebär att beslutet får verkställas även om det har överklagats eller om överklagandetiden inte har gått ut. Det innebär t.ex. att en e-legitimation fortsätter att vara spärrad om ett beslut om återkallelse och spärr, som gäller omedelbart, överklagas.

Sammanfattning av delbetänkandet En säker och tillgänglig statlig e-legitimation (SOU 2023:61)

Uppdraget i korthet

Att föreslå utformning av en statlig e-legitimation

Rådets kompromissförslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet (den reviderade eIDAS-förordningen), COM(2021) 281, innebär bl.a. att det ska bli obligatoriskt för varje medlemsstat att anmäla en e-legitimation på den högsta tillitsnivån enligt ett förfarande för gränsöverskridande identifiering.[2] Tillitsnivån på e-legitimationen avgör hur tillförlitligt det är att personen som identifierar sig är den man utger sig för att vara.

Med anledning av bl.a. förslagen i den reviderade eIDAS-förordningen har utredningen getts i uppdrag att, för det första, lämna förslag på hur en kostnadseffektiv statlig e-legitimation på högsta tillitsnivå kan utformas och tillhandahållas av Myndigheten för digital förvaltning och att, för det andra, analysera och föreslå förändringar som följer av den reviderade eIDAS-förordningen. Syftet är att stärka samhällets säkerhet och robusthet, motverka bedrägerier som begås med hjälp av e-legitimationer och underlätta för så många som möjligt att kunna få tillgång till en e-legitimation.

I detta delbetänkande redovisas utredningens förslag avseende det första deluppdraget.

Problem- och behovsbild

Tillgänglighet, säkerhet och redundans

En statlig e-legitimation som komplement till de kommersiella som redan finns i Sverige, har efterfrågats även av andra anledningar än de förväntade kraven i den reviderade eIDAS-förordningen. I våra direktiv anges att ett statligt alternativ till befintliga e-legitimationer bör utredas ur fler perspektiv, särskilt i fråga om tillgänglighet, säkerhet och redundans.

I synnerhet bland äldre personer, personer med funktionsnedsättningar och personer utan svenskt personnummer råder ett mer eller mindre stort digitalt utanförskap. Även svenskar i utlandet kan i vissa fall ha svårt att få tillgång till en svensk e-legitimation. Staten har ett ansvar att säkerställa att e-legitimationer blir tillgängliga för så många som möjligt. I likhet med vad som framförts i tidigare utredningar om en statlig e-legitimation anser vi att en grundidentifiering (se nedan) som uppfyller kraven för den högsta

[2] Ständiga representanternas kommitté (Coreper I), 25 november 2022, Förslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet – Allmän riktlinje, s. 55 eIDAS-förordningen är den vanligen förekommande benämningen av Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

tillitsnivån och utförs av staten, medför att också andra e-legitimationer, som baseras på den statliga, kan bli säkrare. I förening med andra säkerhetshöjande åtgärder vid e-legitimationens användande kan riskerna för identitetsrelaterad brottslighet då minskas.

Id-växling, dvs. att kunna skaffa en alternativ e-legitimation för vissa specifika ändamål, kan komma att underlättas genom en statlig e-legitimation på högsta tillitsnivån. En statlig e-legitimation skulle alltså inte bara stärka den civila beredskapen genom att utgöra ett komplement till befintliga e-legitimationer; den kan också underlätta för andra aktörer att erbjuda e-legitimationer och betrodda tjänster, vilket i sin tur också kan stärka beredskapen och även bidra till ökad konkurrens på e-legitimationsmarknaden. I kapitel 6 redovisas problem- och behovsbilden närmare.

En statlig e-legitimation för så många som möjligt

Myndigheten för digital förvaltning ska utfärda den statliga e-legitimationen

I enlighet med vårt uppdrag föreslår vi att en statlig e-legitimation på tillitsnivå hög enligt eIDAS-förordningen ska utfärdas av Myndigheten för digital förvaltning (avsnitt 7.6).

Enligt våra förslag ska den statliga e-legitimationen tillhandahållas efter ansökan till den som, vid personlig inställelse hos en identitetskontrollerande myndighet, har styrkt sin identitet och har svenskt personnummer, alternativt ett samordningsnummer för personer med styrkt identitet vilket inte är vilandeförklarat. Vi föreslår också en minimiålder. Den statliga e-legitimationen får utfärdas från och med det kalenderår sökanden fyller nio år. För barn under arton år krävs att barnets vårdnadshavare har lämnat skriftligt medgivande (avsnitt 7.4). Den statliga e-legitimationen ska ha en giltighetstid om högst fem år (avsnitt 7.7).

Delat myndighetsansvar

Polismyndigheten och Skatteverket bedöms var och en vara lämpliga som identitetskontrollerande myndighet

Vårt uppdrag omfattar att bl.a. föreslå vilken eller vilka myndigheter som ska ansvara för grundidentifieringen i samband med utfärdandet av den statliga e-legitimationen, och vilka kontroller av sökandens identitet som ska genomföras vid en sådan grundidentifiering.

Med grundidentifiering avses i detta betänkande ett förfarande som leder fram till att en identitetshandling utfärdas, innefattande en process i vilken det ingår personlig inställelse för sökanden vid såväl ansökan om som utlämnandet av identitetshandlingen, att sökanden styrker sin identitet på ett tillförlitligt sätt, och att vissa fysiska kännetecken av sökanden dokumenteras. Vårt förslag om ansöknings- och utgivningsprocess för den statliga e-legitimationen innefattar samtliga dessa moment (avsnitt 7.5).

Vår tolkning av uppdraget är att grundidentifieringen ska utföras av en annan myndighet än Myndigheten för digital förvaltning. Vi gör bedömningen att det är antingen Polismyndigheten eller Skatteverket som

kan komma i fråga för att genomföra grundidentifieringen på ett tillräckligt säkert, effektivt och tillgängligt sätt, och att regeringen ska bemyndigas att bestämma vilken myndighet som ska ansvara för uppgiften (avsnitt 7.6).

Vi förordar Polismyndigheten framför Skatteverket. Polismyndigheten har redan i dag en utbredd närvaro i samhället och har till antalet närmare dubbelt så många utgivningsställen för identitetshandlingar som Skatteverket. Vidare har Polismyndigheten en i omfattning och tid större erfarenhet beträffande identitetskontroller. Att polisen utses som identitetskontrollerande myndighet för den statliga e-legitimationen bedömer vi sammantaget vara den mest kostnadseffektiva lösningen. Därtill menar vi att Polismyndigheten vid identitetskontrollerna – i sin egenskap av brottsbekämpande myndighet – bättre kan motverka utmaningar kopplade till den identitetsrelaterade brottsligheten.

Utlandsmyndigheterna och Utrikesdepartementet bedöms ha erforderliga förutsättningar att hantera grundidentifiering i samband med ansökningar om statlig e-legitimation utanför riket (avsnitt 7.6).

Utformningen av den statliga e-legitimationen

Den statliga e-legitimationen ska tillhandahållas på ett kontaktlöst aktivt kort som även är eller kan certifieras som en anordning för att skapa kvalificerade elektroniska underskrifter

Den statliga e-legitimationen ska tillhandahållas på en bärare som utformats på ett sätt som uppfyller kraven för nivå hög enligt eIDAS-regelverket. Bäraren av e-legitimationen ska vara ett kontaktlöst aktivt kort som ska skyddas mot obehörig användning, läsning och kopiering av uppgifter som e-legitimationen innehåller (avsnitt 7.2).

E-legitimationen bör dock, enligt vår bedömning, finnas även på ett statligt utfärdat identitetskort så snart som möjligt (avsnitt 7.6). Skatteverkets identitetskort för folkbokförda i Sverige får utfärdas enbart till personer som har fyllt tretton år och är folkbokförda i landet enligt folkbokföringslagen (1991:481). Det nationella identitetskortet får utfärdas av Polismyndigheten till endast svenska medborgare. Dessa statliga identitetshandlingar kan därmed för närvarande inte utgöra bärare för den statliga e-legitimationen, om den ska kunna tillhandahållas till hela den föreslagna personkretsen (avsnitt 7.2).

I våra direktiv konstateras dels att det är tidskrävande att ta fram ett kombinerat identitetskort och e-legitimation, dels att förslagen i den reviderade eIDAS-förordningen, i kombination med ett förändrat säkerhetsläge, kan medföra vissa krav på skyndsamhet att ta fram en statlig e-legitimation på högsta tillitsnivån. Vårt förslag kan mot den bakgrunden ses som en alternativ lösning för att möta skyndsamhetskraven. En e-legitimation på ett separat kort tillgodoser samtidigt behovet av att personer som saknar svenskt personnummer men har tillräcklig anknytning till Sverige för att tilldelas ett samordningsnummer, kan få en svensk e-legitimation, oberoende av om personkretsen för exempelvis Skatteverkets identitetskort även fortsättningsvis omfattar enbart folkbokförda personer.

Den statliga e-legitimationen ska innehålla de attribut som behövs i e-legitimationer som ges ut till privatpersoner, dvs. innehavarens namn och

personnummer, alternativt samordningsnummer för personer med styrkt identitet. Därutöver ska den statliga e-legitimationen i ett lagringsmedium på bäraren innehålla innehavarens ansiktsbild och fingeravtryck (avsnitt 7.2).

Vi bedömer att den statliga e-legitimationen bör kunna användas för att framställa kvalificerade elektroniska underskrifter. Bäraren för e-legitimationen ska därför antingen vara eller kunna certifieras som en anordning för att framställa kvalificerade elektroniska underskrifter (avsnitt 7.3).

Finansiering

Ansökningsavgift och förstärkta anslag till berörda myndigheter

En ansökan om statlig e-legitimation ska förenas med en ansökningsavgift. Den kan finansiera delar av det arbete som fordras för att utföra grundidentifieringen. Uppbyggnaden av detta arbete, liksom det som krävs för verksamheten att utfärda den statliga e-legitimationen, förutsätter dock anslagsfinansiering. Det är vidare en förutsättning för att skapa långsiktighet i dessa verksamheter (avsnitt 7.9).

Krav på offentlig sektor att godta vissa e-legitimationer för identifiering i digitala tjänster

Godkända e-legitimationer måste kunna användas

Vi föreslår att det ska ställas lagkrav på offentliga aktörer att för sina digitala tjänster tillåta identifiering med de e-legitimationer som utfärdas av leverantörer som är godkända enligt ett auktorisationssystem för elektronisk identifiering och för digital post.[3] Utöver statliga myndigheter, kommuner och regioner omfattas sådana företag som yrkesmässigt bedriver verksamhet, vilken till någon del är offentligt finansierad, inom förskola, skola, hälso- och sjukvård samt omsorg. Enligt vår bedömning krävs denna reglering bl.a. för att uppnå de i våra direktiv uppställda målen om ökad tillgänglighet och ökad redundans genom en mer diversifierad marknad för e-legitimationer.

Den föreslagna skyldigheten gäller endast om tillitsnivån för e-legitimationen motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga aktören kräver för åtkomst till den digitala tjänsten.

Statliga myndigheter, kommuner och regioner som har behov av tjänster för elektronisk identifiering ska använda de tjänster som tillhandahålls genom auktorisationssystem. Närmare bestämmelser om vilken typ av tjänster som kravet avser, och om hur skyldigheten ska fullgöras, meddelas genom myndighetsföreskrifter (avsnitt 7.13).

[3] Prop. 2023/46:6. I propositionen föreslås att valfrihetssystem enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering ska ersättas av auktorisationssystem för sådana tjänster.

Författningsreglering

En ny lag och förordning om elektronisk identifiering

Den lagreglering som är nödvändig med anledning av förslaget om en statlig e-legitimation samlas i en ny lag. I den lagen regleras också det föreslagna kravet om att godta vissa e-legitimationer. För övriga bestämmelser, bl.a. sådana som behövs för verkställigheten av lagen, föreslås en förordning (avsnitt 7.1).

I lagen tas in centrala bestämmelser om den uppgifts- och ansvarsfördelning som aktualiseras mellan berörda myndigheter i den gemensamma utgivningsprocessen, bl.a. personuppgiftsansvar och behandling av personuppgifter (avsnitt 7.11). Vidare införs bestämmelser om kraven för att tillhandahålla en statlig e-legitimation (avsnitt 7.4), om återkallelse och spärr av utfärdad e-legitimation (avsnitt 7.7), om överklagande och verkställbarhet av beslut, och om användning av vissa e-legitimationer (avsnitten 7.8 och 7.13).

Våra förslag medför behov av följdändringar i bl.a. offentlighets- och sekretessförordningen (2009:641) samt regeringens förslag till lag om auktorisationssystem i fråga om tjänster för elektronisk identifiering och digital post.

Ny och ändrad reglering föreslås träda i kraft den 1 mars 2026.

Delbetänkandets lagförslag

Förslag till lag om elektronisk identifiering

Härigenom föreskrivs följande.

Lagens innehåll och förhållande till annan reglering

1 § Denna lag innehåller bestämmelser om medel för elektronisk identifiering som utfärdas av staten samt krav på erkännande av vissa medel för elektronisk identifiering.

Bestämmelser om medel för elektronisk identifiering finns också i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direkt 1999/93/EG, här benämnd EU:s förordning om elektronisk identifiering, samt i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Ord och uttryck i lagen

2 § Med elektronisk identifiering, medel för elektronisk identifiering, nättjänst och autentisering avses i denna lag detsamma som i EU:s förordning om elektronisk identifiering.

3 § Med en offentlig aktör avses i denna lag

1. en statlig eller kommunal myndighet, eller en beslutande församling i en kommun eller region,

2. en sammanslutning som inrättats särskilt för att tillgodose behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär, och som består av en eller flera myndigheter eller församlingar som anges i 1,

3. en privat aktör som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad och som

a) aktören bedriver i egenskap av enskild huvudman inom skolväsendet eller huvudman för en sådan internationell skola som avses i 24 kap. skollagen (2010:800),

b) utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen (2017:30) eller tandvård enligt tandvårdslagen (1985:125),

c) bedrivs enligt socialtjänstlagen (2001:453), lagen (1988:870) om vård av missbrukare i vissa fall, lagen (1990:52) med särskilda bestämmelser om vård av unga eller lagen (1993:387) om stöd och service till vissa funktionshindrade, eller

d) utgör personlig assistans som utförs med assistansersättning enligt 51 kap. socialförsäkringsbalken, eller

4. en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina, och som tillstörsta delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller av utbildning på forskarnivå.

4 § Statligt medel för elektronisk identifiering får, efter ansökan, utfärdas av den myndighet som regeringen bestämmer (utfärdande myndighet).

5 § Statliga medel för elektronisk identifiering får utfärdas till en person som innevarande kalenderår är eller ska fylla nio år och som har antingen ett svenskt personnummer enligt folkbokföringslagen (1991:481) eller ett sådant samordningsnummer som tilldelats personer som styrkt sin identitet enligt lagen (2022:1697) om samordningsnummer, som inte är förklarat vilande.

För den som är under arton år krävs vårdnadshavares skriftliga medgivande.

6 § Den sökande är skyldig att styrka sin identitet och övriga personuppgifter.

7 § Kontroll av att sökandens identitet är styrkt ska göras av den eller de myndigheter som regeringen bestämmer (identitetskontrollerande myndighet).

8 § I samband med ansökan är sökanden skyldig att låta den identitetskontrollerande myndigheten ta ett fingeravtryck och en ansiktsbild i digitalt format.

9 § Fingeravtrycken och ansiktsbilden enligt 8 § ska sparas i ett lagringsmedium i bäraren av det statliga medlet för elektronisk identifiering.

Fingeravtrycken och de biometriska data som tas fram ur dessa ska omedelbart förstöras när det statliga medlet för elektronisk identifiering har lämnats ut eller en ansökan om sådant medel har återkallats eller avslagits.

10 § En ansökan ska avslås om förutsättningarna i 5 och 6 §§ inte är uppfyllda. Detsamma gäller det som anges i 8 § eller som föreskrivits i enlighet med 11 § andra stycket 1 inte har iakttagits, och sökanden inte har följt en uppmaning att avhjälpa bristen.

11 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om undantag från skyldigheten att lämna fingeravtryck när det gäller minderåriga och personer som av fysiska skäl är permanent förhindrade att lämna fingeravtryck.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om

1. ansökan om samt utfärdande och utlämnande av ett statligt medel för elektronisk identifiering, och
2. utformningen av det statliga medlet för elektronisk identifiering.

Återkallelse och spärr av statligt medel för elektronisk identifiering

12 § Ett statligt medel för elektronisk identifiering ska återkallas och spärras om

1. det fanns hinder mot att utfärda ett sådant medel vid tiden för utfärdandet och hindret fortfarande består,
2. någon väsentlig uppgift som ett sådant medel innehåller är felaktig eller inte längre gäller,
3. det är nödvändigt av säkerhetsskäl för att någon annan än den som ett sådant medel är utställt till kan misstänkas obehörigt förfoga över det, eller om innehavaren av medlet på annat sätt förlorat kontrollen över det,
4. ett sådant medel inte har aktiverats inom sex månader efter att ansökan gjordes, eller
5. innehavaren av ett sådant medel har avlidit.

På begäran av innehavaren får ett statligt medel för elektronisk identifiering återkallas och spärras.

13 § Om ett statligt medel för elektronisk identifiering tidigare har utfärdats till sökanden ska det spärras senast i samband med att ett nytt sådant medel utfärdas.

14 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om förfarandet vid spärr av statligt medel för elektronisk identifiering.

Behandling av personuppgifter

15 § Bestämmelserna i 16, 17, 19–23 och 25 §§ samt föreskrifter som meddelats enligt 18 och 24 §§ i 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 EU:s dataskyddsförordning.

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 16–25 §§ eller föreskrifter som har meddelats i anslutning till dessa paragrafer.

Databas över statliga medel för elektronisk identifiering

16 § Den utfärdande myndigheten ska med hjälp av automatiserad behandling föra en databas med en samling uppgifter om statliga medel för elektronisk identifiering som myndigheten har utfärdat.

17 § En kopia av den ansiktsbild som enligt 9 § ska finnas i ett lagringsmedium i bäraren av det statliga medlet för elektronisk identifiering, och de biometriska uppgifter som tas fram ur ansiktsbilden får behandlas i databasen.

18 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om

1. vilka uppgifter databasen ska eller får innehålla, och
2. den längsta tid som personuppgifter får behandlas i databasen.

Personuppgiftsansvar

19 § Den utfärdande myndigheten är personuppgiftsansvarig för den behandling av personuppgifter som sker i samband med ansökan om och utfärdande av ett statligt medel för elektronisk identifiering.

Den identitetskontrollerande myndigheten är personuppgiftsansvarig för den behandling av personuppgifter som sker i samband med att myndigheten kontrollerar att sökandens identitet är styrkt enligt 7 §.

Ändamål

20 § Personuppgifter får behandlas av den utfärdande myndigheten om det är nödvändigt för att

1. handlägga ärenden om statligt medel för elektronisk identifiering,
2. administrera en databas över innehavare av statliga medel för elektronisk identifiering, och
3. möjliggöra en säker användning av statliga medel för elektronisk identifiering.

Personuppgifter får behandlas av den identitetskontrollerande myndigheten om det är nödvändigt för att, i samband med ansökan, kunna kontrollera den sökandes identitet.

Personuppgifter som har samlats in enligt första stycket får också behandlas av den utfärdande myndigheten

1. om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet,
2. om det är nödvändigt för att fullgöra uppgiftsutlämnande som sker i överensstämmelse med lag eller förordning, och
3. för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Behandling av känsliga personuppgifter

21 § Personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) får behandlas endast om det är absolut nödvändigt för ändamålet med behandlingen.

Känsliga personuppgifter får dock behandlas

1. i databasen när det är tillåtet enligt 17 § och föreskrifter som meddelats enligt 18 §, och
2. vid sökning som är tillåten enligt 22 §.

Integritetshöjande och säkerhetshöjande åtgärder

22 § Det är förbjudet att använda ansiktsbilder samt biometriska uppgifter som har tagits fram ur sådana bilder som sökbegrepp. Trots förbudet får den ansiktsbild som tas enligt 8 §, och de biometriska uppgifter som tas fram ur ansiktsbilden, användas vid sökning i databasen i samband med ansökan om medel för elektronisk identifiering. Sökning är då tillåten endast för att kontrollera sökandens identitet och innehav av sådant medel.

Sådana övriga känsliga personuppgifter som avses i 21 § och uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden får inte användas som sökbegrepp.

23 § Tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter.

24 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela

1. närmare föreskrifter om tillgången till personuppgifter, och
2. ytterligare föreskrifter om säkerhetsåtgärder till skydd för personuppgifter.

Rätten att göra invändningar

25 § Artikel 21.1 i EU:s dataskyddsförordning om rätten att göra invändningar gäller inte vid sådan behandling som är tillåten enligt denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Krav på erkännande av vissa medel för elektronisk identifiering

26 § När medel för elektronisk identifiering krävs för att få tillgång till en nättjänst som tillhandahålls av en offentlig aktör, och tjänsten helt eller delvis riktar sig till privatpersoner, ska medel erkännas för autentisering för tjänsten om

1. medlet för elektronisk identifiering tillhandahålls av leverantör som är godkänd i enlighet med lagen (20XX:XXX) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post, och
2. tillitsnivån för medlet för elektronisk identifiering motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga aktören kräver för åtkomst till nättjänsten.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. vilka typer av tjänster för elektronisk identifiering som kravet i första stycket avser,
2. hur skyldigheten ska fullgöras, och
3. undantag från kraven.

Användning av statligt medel för elektronisk identifiering

27 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om villkor för när och hur ett statligt medel för elektronisk identifiering får användas.

Övriga bestämmelser

28 § Beslut enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

29 § Beslut enligt denna lag gäller omedelbart, om inte något annat anges i beslutet.

Denna lag träder i kraft den 1 mars 2026.

Förslag till lag om ändring i lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post

Härigenom föreskrivs att 2 § lagen om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post

dels ska ha följande lydelse,

dels att det i lagen ska införas en ny paragraf, 23 §, av följande lydelse.

Nuvarande lydelse enligt proposition 2023/24:6	*Föreslagen lydelse*
2 §	
Med ett ***auktorisationssystem*** avses i denna lag ett system där	
1. den myndighet som tillhandahåller systemet godkänner att leverantören av tjänster för elektronisk identifiering av enskilda eller för digital post får ingå ett avtal inom systemet och ingår avtal med var och en av de godkända leverantörerna om utförande av sådana tjänster,	
2. en enskild har rätt att välja den leverantör som ska utföra tjänsterna för den enskildes räkning, *och*	2. en enskild har rätt att välja den leverantör som ska utföra tjänsterna för den enskildes räkning,
3. en offentlig aktör *kan* använda tjänsterna i sin verksamhet enligt avtal med den tillhandahållande myndigheten.	3. en *sådan* offentlig aktör *som avses i 4 § första stycket 1–3 a ska använda tjänsterna för elektronisk identifiering och kan använda tjänsterna för digital post* i sin verksamhet enligt avtal med den tillhandahållande myndigheten, *och*
	4. en sådan offentlig aktör som avses i 4 § första stycket 3 b–5 och andra stycket kan använda tjänsterna i sin verksamhet enligt avtal med den tillhandahållande myndigheten.
	23 §
	Regeringen eller den myndighet som regeringen bestämmer får besluta om undantag från skyldigheten i 2 § 3.

Denna lag träder i kraft den 1 mars 2026.

Förteckning över remissinstanserna

Efter remiss har yttranden över delbetänkandet En säker och tillgänglig e-legitimation (SOU 2023:61) kommit in från AB Svenska pass, Afasiförbundet i Sverige, Arbetsförmedlingen, Barnombudsmannen, Bolagsverket, Boverket, Brottsförebyggande rådet, Brottsoffermyndigheten, Centrala studiestödsnämnden, Chalmers tekniska högskola AB, Dals-Eds kommun, Diskrimineringsombudsmannen, Domstolsverket, E-hälsomyndigheten, Ekobrottsmyndigheten, Ekonomistyrningsverket, Falköpings kommun, Finansiell ID-Teknik BID AB, Finansinspektionen, Freja eID Group AB, Funktionsrätt Sverige, Föreningen för svenskar i världen, Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Försäkringskassan, Gislaveds kommun, Göteborgs kommun, Helsingborgs kommun, Hogia Signit AB, Hovrätten över Skåne och Blekinge, Huddinge kommun, Härnösands kommun, Inera AB, Integritetsskyddsmyndigheten, International Air Transport Association, Internetstiftelsen i Sverige, Justitiekanslern, Kalix kommun, Kammarkollegiet, Kammarrätten i Stockholm, Kommerskollegium, Konkurrensverket, Kriminalvården, Kronofogdemyndigheten, Kungliga tekniska högskolan, Kungälvs kommun, Lantmäteriet, Lessebo kommun, Luleå tekniska universitet, Länsstyrelsen i Blekinge län, Länsstyrelsen i Gävleborgs län, Länsstyrelsen i Norrbottens län, Länsstyrelsen i Skåne län, Länsstyrelsen i Stockholms län, Länsstyrelsen i Uppsala län, Länsstyrelsen i Västra Götalands län, Malmö kommun, Migrationsverket, Myndigheten för delaktighet, Myndigheten för digital förvaltning, Myndigheten för civilt försvar (tidigare Myndigheten för samhällsskydd och beredskap), Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Post- och telestyrelsen, Regelrådet, Region Stockholm, Riksarkivet, Riksdagens ombudsmän, Riksförbundet för barn, unga och vuxna med intellektuell funktionsnedsättning, Sameskolstyrelsen, Scrive AB, Skatteverket, Skolforskningsinstitutet, Skolväsendets överklagandenämnd, Socialstyrelsen, Sorsele kommun, Specialpedagogiska skolmyndigheten, SPF Seniorerna, Statens servicecenter, Statens skolinspektion, Statens skolverk, Statens tjänstepensionsverk, Statistiska centralbyrån, Statskontoret, Stockholms kommun, Styrelsen för ackreditering och teknisk kontroll, Svensk Handel, Svenska bankföreningen, Svenska institutet för standarder, Sveriges advokatsamfund, Sveriges akademikers centralorganisation, Sveriges ambassad i Bangkok, Sveriges ambassad i Belin, Sveriges ambassad i Canberra, Sveriges ambassad i London, Sveriges ambassad i Washington, Sveriges generalkonsulat Hongkong, Sveriges Kommuner och Regioner, Sveriges riksbank, Synskadades riksförbund, Säkerhets- och försvarsföretagen, Säkerhetspolisen, Tanums kommun, TechSverige, Telia Sverige AB, Tierps kommun, Tillväxtverket, Totalförsvarets forskningsinstitut, Transportstyrelsen, Trelleborgs kommun, Umeå kommun, Universitets- och högskolerådet, Upphandlingsmyndigheten, Uppsala kommun, Verket för innovationssystem, Vetenskapsrådet, Vännäs kommun, Växjö kommun och Åklagarmyndigheten.

Därutöver har yttrande inkommit från Elöverkänsligas riksförbund, Föreningen för digitala fri- och rättigheter, Föreningen mot nätbedrägerier, Föreningen Sveriges överförmyndare, Idnow Gmbh, Institutet för mänsk-

liga rättigheter, Kirei AB, Kommunalförbundet Lystkom, Riksföreningen JAG, Svenska kommunalpensionärernas förbund, Sparbankernas riksförbund och Yubico AB.

Följande remissinstanser har inbjudits att lämna synpunkter, men avstått från att yttra sig eller inte kommit in med något yttrande. Bodens kommun, Borgholms kommun, CGI Sverige AB, Comfact AB, Cybercom Group AB, Fintech Sverige, Föreningen Begripsam, Föreningen för arkiv och informationsförvaltning, Företagarna, Förvaltningsrätten i Härnösand, Gotlands kommun, Ideella föreningen teknikföretagen i Sverige, Knowit AB, Landsorganisationen i Sverige, Nordanstigs kommun, Norrköpings kommun, Pensionärernas riksorganisation, Region Gävleborg, Region Skåne, Signicat AB, Sundsvalls kommun, Svenska e-identitet, Svenskt näringsliv, Sveriges ambassad i Madrid, Tingsryds kommun, Tjänstemännens centralorganisation, Uddevalla kommun, Vimmerby kommun, ZealiD AB och Ödeshögs kommun.

Förslag till lag om statlig e-legitimation och elektronisk identifiering

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Lagens innehåll och förhållande till annan reglering

1 § Denna lag innehåller bestämmelser om en statlig e-legitimation och krav på erkännande av vissa medel för elektronisk identifiering.

Bestämmelser om medel för elektronisk identifiering finns i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, här benämnd EU:s förordning om elektronisk identifiering, och i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

2 § Denna lag kompletterar, i den del den avser behandling av personuppgifter, 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 EU:s dataskyddsförordning.

Vid behandlingen 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 föreskrifter som regeringen har meddelat i anslutning till denna lag.

Ord och uttryck

3 § Med autentisering, elektronisk identifiering, medel för elektronisk identifiering och nättjänst avses i denna lag detsamma som i EU:s förordning om elektronisk identifiering.

4 § Med en offentlig aktör avses i denna lag

1. en statlig eller kommunal myndighet, eller en beslutande församling i en kommun eller region,
2. en sammanslutning som inrättats särskilt för att tillgodose behov i det allmännas intresse, under förutsättning att behovet inte är av industriell eller kommersiell karaktär, och som består av en eller flera myndigheter eller församlingar som anges i 1,
3. en privat aktör som yrkesmässigt bedriver verksamhet som till någon del är offentligt finansierad och som

a) aktören bedriver i egenskap av enskild huvudman inom skolväsendet eller huvudman för en sådan internationell skola som avses i 24 kap. skollagen (2010:800),

b) utgör hälso- och sjukvård enligt hälso- och sjukvårdslagen (2017:30) eller tandvård enligt tandvårdslagen (1985:125),

c) bedrivs enligt socialtjänstlagen (2025:400), lagen (1988:870) om vård av missbrukare i vissa fall, lagen (1990:52) med särskilda bestämmelser om vård av unga eller lagen (1993:387) om stöd och service till vissa funktionshindrade, eller

d) utgör personlig assistans som utförs med assistansersättning enligt 51 kap. socialförsäkringsbalken, eller

4. en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina, och som till största delen har statsbidrag som finansiering av högskoleutbildning på grundnivå eller avancerad nivå eller av utbildning på forskarnivå.

En statlig e-legitimation

5 § Den statliga e-legitimationen är ett medel för elektronisk identifiering.

Utfärdande myndighet

6 § Den statliga e-legitimationen utfärdas av utfärdande myndighet.

Polismyndigheten är utfärdande myndighet inom riket.

Utom riket fullgör beskickningar och karriärkonsulat uppgifter som utfärdande myndighet i den utsträckning som beslutas av regeringen eller den myndighet som regeringen bestämmer.

7 § Utfärdande myndighet ska fullgöra de uppgifter som anges i denna lag och i föreskrifter som har meddelats i anslutning till lagen.

Vem som kan få en statlig e-legitimation

8 § En statlig e-legitimation får utfärdas till en svensk medborgare som har fyllt eller som innevarande kalenderår ska fylla nio år.

9 § En statlig e-legitimation får utfärdas till en utlänning som har fyllt eller som innevarande kalenderår ska fylla nio år och som

1. är folkbokförd i Sverige enligt folkbokföringslagen (1991:481), eller

2. har tilldelats ett personnummer enligt 18 b § samma lag och som omfattas av lagen (1976:661) om immunitet och privilegier i vissa fall.

Giltighetstiden

10 § En e-legitimation ska utfärdas med en giltighetstid om fem år. Om sökanden inte har fyllt tolv år ska giltighetstiden vara tre år.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att den statliga e-legitimationen i särskilt angivna fall ska ha en kortare giltighetstid.

Villkor för användningen av den statliga e-legitimationen

11 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om villkor för användningen av den statliga e-legitimationen.

2 kap. Ansökan, utfärdande och återkallelse

En ansökan krävs

1 § Den statliga e-legitimationen utfärdas efter ansökan.

Om sökanden är under arton år krävs det vårdnadshavares medgivande, om det inte finns synnerliga skäl för utfärdandet.

Personlig inställelse

2 § Den som ansöker om en statlig e-legitimation ska lämna ansökan vid personlig inställelse.

Styrkande av identitet

3 § Sökanden ska vid ansökan styrka sin identitet och övriga personuppgifter som krävs för att en statlig e-legitimation ska utfärdas.

Ansiktsbild och fingeravtryck

4 § Sökanden ska låta den utfärdande myndigheten ta sökandens ansiktsbild och fingeravtryck i samband med ansökan om statlig e-legitimation.

Sökanden ska även låta den utfärdande myndigheten ta sökandens ansiktsbild och fingeravtryck vid utlämnande av den statliga e-legitimationen, om den utfärdande myndigheten begär det.

5 § Ansiktsbilden som tas i samband med ansökan enligt 4 § första stycket ska sparas i ett lagringsmedium i bäraren av den statliga e-legitimationen. Om fingeravtryck har tagits ska även dessa sparas i lagringsmediet.

6 § Om sökanden styrker sin identitet med en identitetshandling som är försedd med en ansiktsbild eller innehåller ett lagringsmedium där ansiktsbild eller fingeravtryck är sparade, får den utfärdande myndigheten kontrollera att dessa motsvarar den ansiktsbild och de fingeravtryck som tas enligt 4 §.

Den utfärdande myndigheten får även kontrollera att ansiktsbild och fingeravtryck som tas i samband med utlämnande enligt 4 § andra stycket motsvarar de som finns lagrade i den statliga e-legitimationen.

7 § De fingeravtryck som tas enligt 4 § första stycket och de biometriska uppgifter som tas fram ur dessa ska omedelbart förstöras när den statliga e-legitimationen har lämnats ut eller, om e-legitimationen inte har lämnats ut, när det har gått 90 dagar från den dag då den utfärdades. Om ett ansökningsärende har avslutats på något annat sätt ska uppgifterna också förstöras omedelbart.

Den ansiktsbild och de fingeravtryck som tas enligt 4 § andra stycket och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken ska omedelbart förstöras när kontrollen enligt 6 § andra stycket har genomförts.

Den ansiktsbild och de fingeravtryck som vid kontroll enligt 6 § tas fram ur ett lagringsmedium och de biometriska uppgifter som tas fram ur ansiktsbilden och fingeravtrycken ska omedelbart förstöras när kontrollen har genomförts.

Avslag av ansökan och utfärdande av statlig e-legitimation

8 § En ansökan om en statlig e-legitimation ska avslås om de krav som framgår av denna lag eller de föreskrifter som har meddelats i anslutning till lagen inte är uppfyllda och sökanden inte har följt en uppmaning att rätta till bristen. I annat fall ska den statliga e-legitimationen utfärdas och skyndsamt lämnas ut till sökanden.

Återkallelse och spärr av statlig e-legitimation

9 § En statlig e-legitimation ska återkallas och spärras om

1. det fanns hinder mot att utfärda en e-legitimation vid tiden för utfärdandet och hindret fortfarande består,
2. någon väsentlig uppgift som en e-legitimation innehåller är felaktig,
3. det är nödvändigt av säkerhetsskäl,
4. den är utfärdad på en fysisk identitetshandling som därefter har upphört att gälla, eller
5. innehavaren har avlidit.

En statlig e-legitimation får även återkallas och spärras på begäran av innehavaren. Om begäran avser ett barn under arton år krävs det vårdnadshavares medgivande, om det inte finns synnerliga skäl för återkallelsen och spärren.

10 § En statlig e-legitimation ska, utöver i de fall som anges i 9 §, spärras

1. i samband med att en ny e-legitimation lämnas ut till sökanden, eller
2. när giltighetstiden har löpt ut.

Avgifter

11 § Utfärdande myndighet får ta ut avgifter för ansökan om statlig e-legitimation.

Rätt att meddela föreskrifter

12 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om förfarandet vid

1. ansökan,
2. utfärdande,
3. utlämnande, och
4. återkallelse och spärr.

Regeringen eller den myndighet som regeringen bestämmer kan även med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om den statliga e-legitimationens

1. innehåll, bärare och utformning i övrigt, och
2. aktivering.

Regeringen eller den myndighet som regeringen bestämmer får vidare meddela föreskrifter om

1. avgifter för ansökan om statlig e-legitimation, och
2. undantag från skyldigheten att lämna fingeravtryck enligt 4 §.

3 kap. Behandling av personuppgifter

Ändamålen med behandlingen

1 § Personuppgifter får behandlas av utfärdande myndighet om det är nödvändigt för att

1. handlägga ärenden om statlig e-legitimation,
2. föra ett register över ärenden om statlig e-legitimation, och
3. vidta åtgärder för en säker användning av statliga e-legitimationer.

2 § Personuppgifter som har samlats in enligt 1 § får också behandlas av utfärdande myndighet

1. om det är nödvändigt för att tillhandahålla information som behövs i Polismyndighetens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet, och
2. om det är nödvändigt för att lämna ut uppgifter i enlighet med lag eller förordning.

Personuppgifterna får även behandlas för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Begränsning av rätten att göra invändningar

3 § Artikel 21.1 i EU:s dataskyddsförordning om rätten att göra invändningar gäller inte vid sådan behandling som är tillåten enligt denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Säkerhetsåtgärder

4 § Tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter i verksamheten med den statliga e-legitimationen.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om

1. begränsningen av tillgången till personuppgifter enligt första stycket, och
2. säkerhetsåtgärder till skydd för personuppgifter.

Register över ärenden om statlig e-legitimation

5 § Polismyndigheten ska med hjälp av automatiserad behandling föra ett register över ärenden om statlig e-legitimation.

6 § Registret över ärenden om statlig e-legitimation får innehålla

1. namn, personnummer, samordningsnummer, medborgarskap, födelsedatum och kontaktuppgifter till sökanden,
2. ansiktsbilder som har tagits vid ansökan enligt 2 kap. 4 § första stycket och biometriska uppgifter som har tagits fram ur sådana bilder,
3. handlingar eller uppgifter från handlingar som har kommit in eller upprättats i ärenden om statlig e-legitimation,
4. uppgifter som rör handläggningen av ärenden om statlig e-legitimation, och
5. uppgifter om utfärdade statliga e-legitimationer.

Längsta tid som personuppgifter i registret får behandlas

7 § Personuppgifter i registret över ärenden om statlig e-legitimation får inte behandlas längre än tio år från utgången av det kalenderår som det ärende som uppgifterna hänför sig till avslutades.

Förbud mot vissa sökningar

8 § Det är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter eller sådana personuppgifter om lagöverträdelser som avses i artikel 10 i EU:s dataskyddsförordning.

9 § Det är förbjudet att som sökbegrepp använda

1. ansiktsbilder, biometriska uppgifter som har tagits fram ur ansiktsbilder och andra känsliga personuppgifter som avses i 10 §, och
2. uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden.

Trots förbuden i första stycket får den ansiktsbild som tas enligt 2 kap. 4 § första stycket och de biometriska uppgifter som tas fram ur ansiktsbilden användas vid sökning i registret över ärenden om statlig e-legitimation i ett ärende om statlig e-legitimation. Sökning är då tillåten endast för att kontrollera sökandens identitet och innehav av en e-legitimation i samband med ansökan.

Behandling av känsliga personuppgifter

10 § Personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) får behandlas endast om det är absolut nödvändigt för ändamålet med behandlingen.

Känsliga personuppgifter får dock behandlas

1. i registret när det är tillåtet enligt 6 § 2,
2. vid kontroller som är tillåtna enligt 2 kap. 6 §, och
3. vid sökningar som är tillåtna enligt 9 § andra stycket.

Personuppgiftsansvar

11 § Varje utfärdande myndighet är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten själv utför.

Polismyndigheten är personuppgiftsansvarig för behandling av personuppgifter i registret över ärenden om statlig e-legitimation.

Rätt att meddela föreskrifter

12 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter som avses i 7 § får fortsätta att behandlas under en viss tid för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål, och
2. avskiljande och begränsningar av åtkomsten till personuppgifter som behandlas enligt 1.

4 kap. Erkännande av medel för elektronisk identifiering

Krav på erkännande av medel för elektronisk identifiering

1 § När medel för elektronisk identifiering krävs för att få tillgång till en nättjänst som tillhandahålls av en offentlig aktör, och tjänsten helt eller delvis riktar sig till enskilda, ska medel erkännas för autentisering för tjänsten om

1. medlet för elektronisk identifiering tillhandahålls inom ramen för ett auktorisationssystem i enlighet med lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post, och
2. tillitsnivån för medlet motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga aktören kräver för åtkomst till nättjänsten.

Bemyndiganden

2 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. undantag från kravet i 1 §, och
2. hur kravet i 1 § ska fullgöras.

5 kap. Överklagande och verkställighet

1 § Beslut enligt denna lag eller enligt föreskrifter som har meddelats i anslutning till lagen får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

2 § Beslut enligt denna lag gäller omedelbart, om inte annat anges i beslutet.

Denna lag träder i kraft den 1 december 2026.

Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att 22 kap. 1 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
22 kap.	
1 §	
Sekretess gäller för uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men om uppgiften röjs och uppgiften förekommer i verksamhet som avser	
1. folkbokföringen eller annan liknande registrering av befolkningen och, i den utsträckning regeringen meddelar föreskrifter om det, i annan verksamhet som avser registrering av en betydande del av befolkningen, eller	
2. förande av eller uttag ur sjömansregistret.	
Sekretess gäller i verksamhet som avses i första stycket 1 för uppgift i form av fotografisk bild av den enskilde, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.	Sekretess gäller i verksamhet som avses i första stycket 1 för uppgift i form av fotografisk bild av den enskilde *och biometrisk uppgift som har tagits fram ur bilden*, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.
För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.	

Denna lag träder i kraft den 1 december 2026.

Lagrådets yttrande

Utdrag ut protokoll vid sammanträde 2026-01-30

Närvarande: F.d. justitieråden Kerstin Calissendorff och Mats Melin samt justitierådet Martin Nilsson

En statlig e-legitimation

Enligt en lagrådsremiss den 22 januari 2026 har regeringen (Finansdepartementet) beslutat inhämta Lagrådets yttrande över förslag till

1. lag om statlig e-legitimation och elektronisk identifiering,
2. lag om ändring i offentlighets- och sekretesslagen (2009:400).

Förslagen har inför Lagrådet föredragits av rättssakkunniga Marzia Isaksson, biträdd av rättssakkunnige Dante Olason Hallberg och departementssekreteraren Sophie Ankarcrona Thelin.

Lagrådet lämnar förslagen utan erinran.

Finansdepartementet

Utdrag ur protokoll vid regeringssammanträde den 7 maj 2026

Närvarande: statsrådet Busch, ordförande, och statsråden Edholm, Waltersson Grönvall, Jonson, Strömmer, Forssmed, Tenje, Slottner, Wykman, Malmer Stenergard, Kullgren, Liljestrand, Bohlin, Carlson, Rosencrantz, Dousa, Larsson, Britz, Lann

Föredragande: statsrådet Slottner

Regeringen beslutar proposition 2025/26:250 En statlig e-legitimation