Regeringskansliet
Faktapromemoria 2021/22:FPM78

# Förordning om informationssäkerhet i unionens institutioner, organ och byråer

2021/22:FPM78

Utrikesdepartementet

2022-04-29

## Dokumentbeteckning

COM(2022) 119
Förslag till Europaparlamentets och rådets förordning om informationssäkerhet i unionens institutioner, organ och byråer

## Sammanfattning

Kommissionen framför i förslag presenterat 22 mars 2022 åtgärder för att förbättra informationssäkerheten inom unionens institutioner, organ och byråer. Förslagets två huvudåtgärder består i ett införande av ett gemensamt och enhetligt säkerhetsregelverk för informationssäkerhet samt tillskapandet av en gemensam säkerhetsorganisation.

Den gemensamma säkerhetsorganisationen placeras under kommissionen, med representation från unionens institutioner, organ och byråer.
Förslaget till gemensamt regelverk omfattar såväl hanteringen av säkerhetsskyddsklassificerade EU-uppgifter som icke-säkerhetsskyddsklassificerade uppgifter och system. Förslagets regelverk för hantering av säkerhetsskyddsklassificerade EU-uppgifter utgår från befintligt regelverk i form av rådets säkerhetsföreskrifter som idag styr hanteringen i medlemsstaterna. För hantering av icke-säkerhetsskyddsklassificerad information inrättas ett nytt regelverk.

Förslaget till förordning avser enbart vara tillämpligt på informationssäkerheten internt inom och mellan unionens institutioner, organ och byråer.

Regeringen ställer sig positiv till förslagets grundtanke kring gemensamma säkerhetsregler och en samlad säkerhetsorganisation som ett led i ett fortsatt starkt och proaktivt EU-arbete på området men menar att ett mer detaljerat förslag behöver utarbetas. Detta förslag behöver utarbetas i samverkan med medlemsstaterna och utformas så att det säkerställer medlemsstaternas

# 1 Förslaget

## 1.1 Ärendets bakgrund

Informationssäkerheten vid unionens institutioner, organ och byråer (European Union Institutions Bodies and Agencys - EUIBA) är idag föremål för intern reglering i enlighet med respektive organisations instruktioner, interna regelverk och policys. Detta medför att information som delas mellan institutioner och organ och byråer omfattas av olika regelverk, hanteringskrav och säkerhetsnivåer vid olika tillfällen i hanteringskedjan. Detta är förhållanden som påverkar säkerheten inom institutionerna och även har påverkan på medlemsstaternas (MS) och den gemensamma säkerheten inom unionen.

Kommissionens (KOM) förslag är framtaget som en del av EU:s *Security Union Strategy*[1] som antogs av KOM den 24 juli 2020 och som fastställer dess åtagande att tillföra Europeiska unionens mervärde till de nationella insatserna på säkerhetsområdet. En del av detta engagemang är initiativet att effektivisera de interna rättsliga ramarna för informationssäkerhet i alla unionens institutioner och organ.

I enlighet med detta drog rådet (allmänna frågor) i december 2019 slutsatsen att EU:s institutioner och organ, med stöd av MS, bör utveckla och genomföra en omfattande uppsättning åtgärder för att säkerställa informations- och cybersäkerhet inom Europeiska unionens verksamhet. Detta återspeglar också en strävan från rådets säkerhetskommitté mot en enhetlig uppsättning säkerhetsregler för rådet, KOM och EEAS.

## 1.2 Förslagets innehåll

KOM framför i förslaget till reglering åtgärder för att förbättra informationssäkerheten inom EUIBA genom organisatoriska och regulatoriska förändringar.

Förslaget presenterar åtgärder inom två huvudområden:

[1] Communication on the EU Security Union Strategy, COM(2020) 605, 24 July 2020 (Strategic priority, A future-proof security environment).

1) en samordnad och enhetlig organisation för informationssäkerhet för EU:s institutioner och organisationer under ledning av KOM
2) ett gemensamt och enhetligt regelverk för informationssäkerheten vid unionens institutioner och organisationer vilket utgår från KOM och den föreslagna gemensamma säkerhetsorganisationen

Inom ramen för det föreslagna gemensamma regelverket för informationssäkerhet regleras också personalsäkerhet och industrisäkerhet. Regler kring personalsäkerhet innefattar bestämmelser avseende säkerhetsgodkännande för befattning med säkerhetsskyddsklassificerade EU-uppgifter (EUCI). Regler för industrisäkerhet innefattar bestämmelser för upphandling av tjänster och entreprenörers tillgång till EUCI.

Förordningen syftar till att skapa en gemensam ram av informationssäkerhetsregler tillämpliga vid samtliga EUIBA som omfattar hanteringen av såväl icke-säkerhetsskyddsklassificerade uppgifter som EUCI. Förordningen avser enbart att reglera informationssäkerhet och organisation internt inom EUIBA.

**Ett gemensamt och enhetligt regelverk för informationssäkerheten vid unionens institutioner och organ och byråer**

Varje institution och organisation ska upprätta en informationssäkerhets-policy som bygger på de minimikrav som fastställs i föreslagen förordning. Sådan policy avses reglera särskilda säkerhetsåtgärder för att skydda information i enlighet med resultaten av en intern riskbedömning och baserat på gemensamma minimikrav.

**Icke-säkerhetsskyddsklassificerade uppgifter**

I syfte att öka interoperabilitet och möjliggöra gemensamma hanteringsregler inom EUIBA föreslås ett enhetligt system för kategorisering och märkning.

Kategorisering av icke-säkerhetsskyddsklassificerade uppgifter avses ske i tre nivåer utifrån skyddsvärde. ”Uppgifter för allmänt bruk”, ”normala uppgifter” och ”känsliga icke-säkerhetsskyddsklassificerade uppgifter” (Sensitive Non Classified, SNC). Till varje enskild kategoriseringsnivå kopplas regler för hantering och märkning anpassade efter behov av säkerhet.

**Säkerhetsskyddsklassificerade uppgifter**

I syfte att öka interoperabilitet och etablera gemensamma hanteringsregler för EUCI inom och mellan EUIBA föreslås en enhetlig modell för klassificering och märkning av information i fyra klassificeringsnivåer baserat på den skada som kan uppstå vid röjande.

Föreslaget klassificeringssystem är identiskt med det som läggs fast i rådets säkerhetsföreskrifter.[2]

Regelverket avses utgöra lägsta gemensamma nivå för hantering inom EUIBA. Säkerhet vid delgivning och utbyte av EUCI till internationella organisationer och tredjeländer regleras också genom de regler och säkerhetsåtgärder som utgår från förordningen.

I förordningen föreslås att EUIBA, parallellt med ett gemensamt och enhetligt märkningssystem för information, också ska kunna upprätthålla sedan tidigare upprättade interna system för klassificering och märkning för interna ändamål eller för utbyte av information med sina särskilda motsvarigheter från andra EUIBA eller från MS.

**En samordnad och enhetlig informationssäkerhetsorganisation för EU:s institutioner och organisationer**

Genom förordningen bildas en interinstitutionell samordningsgrupp för informationssäkerhet. I samordningsgruppen representeras EUIBA av den organisation som är utsedd till huvudman för säkerhetsarbetet (Security Authority). Samordningsgruppen ska ha mandat att upprätta och implementera vägledande och styrande dokument om genomförandet av föreslagen förordning. Till samordningsgruppen skapas ett permanent sekretariat för att administrera samordningsgruppens arbete under säkerhetsavdelningen vid DG Human Resources and Security. Genom förordningen inrättas en Informationssäkerhetskommitté och permanenta tematiska undergrupper med representation från institutioner och organisationer.

Varje EUIBA som representeras i den föreslagna organisationen avses fortsatt förbli fullt ansvariga för informationssäkerheten inom respektive organisation.
Processen för att genomföra säkerhetsgodkännande för befattning med EUCI avseende EUIBA underställs föreslaget regelverk från KOM.

## 1.3 Gällande svenska regler och förslagets effekt på dessa

Förordningen avser enbart att reglera informationssäkerhet och organisation internt inom EUIBA. Förordningen hänvisar dock i flera frågor till framtida beslut om policys, regelverk och organisation som kan komma att påverka svenska regler på området. Sådana hänvisningar medför att det inte är möjligt att göra en fullständig och preciserad konsekvensanalys.

[2] COUNCIL DECISION of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU)

Förslaget tar inte hänsyn till att MS, inom området för den gemensamma säkerheten inom EU, sammanträder och beslutar inom ramen för rådets verksamhet. Denna verksamhet regleras av rådets säkerhetsföreskrifter och det multilaterala säkerhetsskyddsavtalet mellan MS. Om denna verksamhet som hanterar frågor kring såväl gemensam som nationell säkerhet skulle komma att regleras via KOMs gemensamma regelverk för EUIBA, medför detta att MS verksamhet i frågor med direkt påverkan på såväl nationell som gemensam säkerhet också omfattas av KOM interna regelverk för EUIBA. Ett regelverk över vilket MS inte har rådighet.

Även då förordningen syftar till ett internt regelverk för EUIBA kan de förslag på regler kring industrisäkerhet och personalsäkerhet som föreligger komma att ha påverkan på MS regelverk. Sådan påverkan kan uppkomma bl.a. då föreslaget regelverk avses omfatta även industriprojekt såsom Horizon Europe, EDF m.fl. Detta kan komma att medföra problem gentemot gällande lagstiftning i landet där företaget har sitt säte. MS möjlighet att vara suveräna avseende bedömningar kring frågor som rör nationell säkerhet enligt TFEU art. 4.2. riskerar också att påverkas.

Likaså kan förslaget kring gemensamt regelverk för hantering av icke-säkerhetsklassificerade uppgifter medföra påverkan på svenska regler. Sådana hanteringsregler ska respekteras av mottagaren och det är idag okänt hur detta kan komma att påverka svenska regler, offentlighetslagstiftning och svenska entiteters förutsättningar för samverkan med EUIBA.

Hanteringen av säkerhetsskyddsklassificerade EU-uppgifter och nationellt säkerhetsskyddsklassificerade uppgifter inom ramen för MS samverkan inom EU regleras idag genom rådets säkerhetsföreskrifter och det multilaterala säkerhetsskyddsavtalet mellan EU:s medlemsstater[3]. Ett kompletterande regelverk liksom kompletterande organisationsstruktur för EUIBAs interna verksamhet kan komma att medföra påverkan på MS informationshantering gentemot EUIBA liksom på befintligt säkerhetsskyddsavtal och på nationella förhållanden som omfattas av säkerhetsskyddslagen.

## 1.4 Budgetära konsekvenser / Konsekvensanalys

Då en utförlig konsekvensanalys av förslaget saknas är det svårt att i detalj bedöma de budgetära konsekvenserna. KOM bedömer att genomförandet kräver inrättande och tillsättning av två tjänster för att upprätthålla verksamheten i det föreslagna permanenta sekretariatet för samordningsgruppen.

[3]Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union, 6 November 2009, 13886/09

KOM förväntar sig kostnadsbesparingar genom en samordnad och gemensam verksamhet, främst genom ett effektivare utnyttjande av personella resurser inom EUIBAs säkerhetsverksamhet. Det är dock oklart om sådana effekter kan uppnås. Därtill tillgodoräknar sig KOM också minskade ekonomiska skador till följd av säkerhetsincidenter, genom att ett effektivare säkerhetsarbete kan bedrivas som ett resultat av förslagen reglering och de förändringar i regelverk och organisation som avses. Man bedömer också att eventuella ekonomiska insatser som krävs för genomförandet av den nya lagstiftningen, kan täckas inom ramen för de befintliga programmen för förbättring av informationssäkerheten i varje enskild unionsinstitution och organisation.

Även om det inte framgår av KOMs förslag kan det inte uteslutas att förslaget medför ökad administration och får andra konsekvenser för MS och deras expertmyndigheter. Vidare kan förslaget kring införande av kategorisering och hanteringsregler för ej klassificerad information komma att medföra kostnader såväl genom ökad administration som genom framställande av lösningar för att hantera denna information. Eventuella kostnader som förslagen kan leda till för den nationella budgeten ska finansieras i linje med de principer om neutralitet för statens budget som riksdagen beslutat om (prop. 1994/95:40, bet. 1994/95:FiU5, rskr. 1994/95:67). Utgiftsdrivande åtgärder på EU-budgeten behöver finansieras genom omprioriteringar i den fleråriga budgetramen (MFF).

# 2 Ståndpunkter

## 2.1 Preliminär svensk ståndpunkt

Informations- och cybersäkerhet är ett viktigt område för regeringen, som ställer sig generellt positiv till fortsatta åtgärder på området som medverkar till ett fortsatt starkt och proaktivt EU-arbete på området. Regeringen bejakar därför förslagets grundtanke med gemensamma säkerhetsregler och en samlad organisation.

Regeringen anser att utvecklingen av cyber- och informationssäkerheten inom unionens organisationer och institutioner, till följd av det utbredda samberoende som finns i dessa frågor, behöver ske i nära samverkan med MS och utgå ifrån att de behöver ha insyn och inflytande.
Regeringen vill framhålla vikten av att de åtgärder som påkallas av förordningens genomförande inte avleder resurser från det pågående arbetet med NIS2-direktivet eller andra initiativ som avser höja cyber- och informationssäkerheten inom unionen.

Eftersom föreslaget regelverk för hantering av EUCI avses utgå från rådets säkerhetsföreskrifter vilka idag är föremål för revidering och uppdatering,

anser regeringen att det aktuella förslaget bör invänta beslut om uppdaterade säkerhetsföreskrifter från rådet.

Föreslagen förordning hänvisar ett antal lösningar och åtgärder med möjlig påverkan på såväl det interna säkerhetsarbetet inom EUIBA, som det gemensamma säkerhetsarbetet inom EU och på MS till framtida beslut om policys, regelverk och organisation. KOM har under det förberedande arbetet inte fullt ut identifierat och redogjort för de konsekvenser som föreslagna åtgärder skulle kunna ge upphov till inom såväl institutioner som MS. Regeringen kommer därför att i de kommande förhandlingarna begära konsekvensbeskrivningar som möjliggör beslut i frågan.

Den föreslagna placeringen under KOM medför begränsade möjligheter till insyn och inflytande från MS. Även då förordningen avser vara tillämplig enbart för EUIBA interna verksamhet finns det områden inom vilka ett sådant internt regelverk kan antas ställa krav på eller på annat sätt påverka MS, bl.a. då ett sådant regelverk kommer omfatta MS verksamhet under rådet. Ett gemensamt regelverk bör därför utgå från rådet eller på annat sätt konstrueras i syfte att garantera MS insyn och inflytande.

Den organisationsstruktur som föreslås inrättas under KOM skulleges samma utformning som befintlig organisationsstruktur som finns inrättad under rådets säkerhetskommitté. Ett samutnyttjande av befintlig organisationsstruktur och verksamhet under rådet bör därför övervägas av såväl resurs- som av samordningsskäl.

Föreslaget regelverk för hantering av EUCI avser att i mångt bygga på rådets säkerhetsföreskrifter. Ett sådant parallellt regelverk motsäger förordningens mål avseende gemensamt och likalydande regelverk för samtliga EUIBA. Likaså föreslås samtliga EUIBA att bibehålla ev. befintliga interna regelverk. Även detta motverkar förordningens syfte kring gemensamt regelverk.

Det finns goda skäl att införa gemensamma regelverk för hanteringen av icke-säkerhetsskyddsklassificerade uppgifter. Ett gemensamt regelverk medför ökad interoperabilitet och ökar förutsättningarna att upprätthålla en dimensionerad säkerhet i hela hanteringskedjan inom EUIBA.
Det finns dock anledning att förhålla sig även till frågan om hanteringen av det gemensamma informationskapitalet i MS. Det kan inte bortses ifrån att ett införande av ett sådant regelverk unilateralt inom EUIBA skulle komma att medföra påverkan även på MS hantering.

## 2.2 Medlemsstaternas ståndpunkter

Trots konsensus bland MS kring behovet av gemensamma regelverk och en tydlig och samlad säkerhetsorganisation för samtliga EUIBA är KOM förslag till förordning ifrågasatt. MS har inom ramen för de nationella säkerhetsmyndigheterna (National Security Authority, NSA) under rådets

säkerhetskommitté i ett gemensamt uttalande framfört villkor med avseende på förslagets utformning, tolkning och genomförande som ska vara styrande för vidare förhandlings- och lagstiftningsprocess.

## 2.3 Institutionernas ståndpunkter

Vissa i förslaget ingående delar har i sin nuvarande form avstyrkts av rådets säkerhetskommitté, samt av rådets rättstjänst liksom av EEAS rättstjänst. Som skäl har angivits bl.a. rättsliga förhållanden som skulle begränsa möjligheterna för föreslagen organisation att upprätthålla efterlevnaden och säkerställa ett konsekvent och sammanhängande genomförande av förordningen utan att inkräkta på institutionernas autonomi. Det har också åberopats skäl kopplade till MS inflytande och ställning. Rådets har i sina synpunkter framfört en önskan att vidare bearbetning av förslaget sker i samverkan mellan institutionerna.

## 2.4 Remissinstansernas ståndpunkter

Förslaget har inte varit föremål för remiss.

# 3 Förslagets förutsättningar

## 3.1 Rättslig grund och beslutsförfarande

KOM har som rättslig grund angett fördraget om Europeiska unionens funktionssätt, särskilt artikel 298, och fördraget om upprättande av Europeiska atomenergigemenskapen, särskilt artikel 106a.

Beslut fattas enligt ordinarie lagstiftningsförfarande, d.v.s. Europaparlamentet och rådet fattar beslut gemensamt. KOM har som rättslig grund angett artikel 298 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) och artikel 106a i fördraget om upprättandet av Europeiska atomenergigemenskapen.

Artikel 298 i EUF-fördraget infördes genom Lissabonfördraget och gör det möjligt för lagstiftarna att fastställa bestämmelser i syfte att skapa en effektiv och oberoende förvaltning som kommer att stödja institutionerna, organen, kontoren och byråerna i att utföra sitt uppdrag.

Då förslaget också omfattar information som relaterar till och härrör från verksamheten inom Europeiska atomenergigemenskapen och uppgifter som inte klassificerats som Euratom Classified Information, men som hanteras av unionens institutioner, organ och byråer hanteras enligt regler för hantering av EUCI, behövs ytterligare rättslig grund. Denna ytterligare rättsliga grund utgörs av artikel 106a i fördraget om upprättandet av Europeiska

atomenergigemenskapen, som gör artikel 298 i EUF-fördraget tillämplig även på ovan nämnda Euratom-verksamhet.

## 3.2 Subsidiaritets- och proportionalitetsprincipen

Eftersom endast unionen kan anta regler avseende hantering och säkerhet avseende det gemensamma informationskapitalet inom unionens verksamhet, såväl klassificerad som icke-klassificerad information, anser KOM att subsidiaritetsprincipen inte är tillämplig.

KOM menar att förslaget inte går utöver vad som är nödvändigt för att åstadkomma ett gemensamt och enhetligt regelverk för informationssäkerhet eftersom förslaget lämnar utrymme för EU:s institutioner att införa specifika åtgärder anpassade för den varierande säkerhetsmognadsnivån vid varje unionsinstitution. KOM anser därför proportionalitetsprincipen vara uppfylld.

Regeringen gör ingen annan bedömning baserat på de ramar för tillämpning som anges i förslaget och som innebär att förordningen enbart avser reglera informationssäkerheten inom EU:s institutioner och organisationer.
Det kan dock inte bortses från att förslaget, bl.a. inom områdena industrisäkerhet, personalsäkerhet och hantering av såväl klassificerad som icke-klassificerad information, kan komma att medföra påverkan på MS regelverk och lagstiftning beroende på hur förslag till förordning utformas och implementeras. Därför bör en vidare prövning av förslagets proportionalitet anstå tills förslaget analyserats ytterligare.

# 4 Övrigt

## 4.1 Fortsatt behandling av ärendet

Förhandlingar i ärendet har aviserats att inledas i april och förväntas pågå under tre år. Förhandlingar som sker enligt de villkor som framställts från MS kommer medföra en sådan högre grad av detaljering och konkretisering som medför att nödvändiga analyser för ställningstagande kan framställas som underlag för vidare beslut.

## 4.2 Fackuttryck/termer

EUCI – European Union Classified Information. Säkerhetsskyddsklassificerad information. Motsvaras av säkerhetsskyddsklassificering enligt säkerhetsskyddslagen.

EUIBA - European Union Institutions Bodies and Agencys. De institutioner och organisationer som utgör parterna i det interna EUsamarbetet.

SNC – Sensitive Non-Classified Information. Känslig information som ej omfattas av säkerhetsskyddsklassificering.

NIS2-direktivet – EU-direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (faktapromemoria 2020/21:FPM71)

NSA – National Security Authority, Nationell säkerhetsmyndighet