EUROPEISKA DATATILLSYNSMANNEN

Sammanfattning av Europeiska datatillsynsmannens yttrande om förslaget till en förordning om skydd för enskilda personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ, kontor och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG

(Den fullständiga texten till detta yttrande finns på engelska, franska och tyska på Europeiska datatillsynsmannens webbplats www.edps.europa.eu)

(2017/C 164/02)

En ny generation standarder för skyddet av personuppgifter håller på att utfärdas av Europeiska unionen. Antagandet för nästan ett år sedan av den allmänna dataskyddsförordningen och direktivet för den polisiära och den rättsliga sektorn representerar EU-lagstiftarnas mest ambitiösa strävan att säkerställa individens grundläggande rättigheter i den digitala eran. Det är nu dags för EU-institutionerna själva att föregå med gott exempel när det gäller de regler de tillämpar på sig själva som registeransvariga och behandlare av data. Under de senaste 18 månaderna har Europeiska datatillsynsmannen (EDPS) inlett en dialog på högsta nivå med EU-institutionerna för att förbereda dem för de nya utmaningarna när det gäller efterlevnaden av reglerna för skydd av personuppgifter, med betoning på den nya principen om ansvarsskyldighet för hur data behandlas. Med det här yttrandet vill EDPS med stöd i tolv års oberoende tillsyn, policyrådgivning och påverkansarbete föreslå förbättringar av förslaget till förordning om behandling av personuppgifter som utförs av unionens institutioner och organ.

Förordning (EG) nr 45/2001 har fungerat som ett rättesnöre som har tillhandahållit direkt tillämpliga skyldigheter för registeransvariga, rättigheter för de registrerade och ett tydligt oberoende tillsynsorgan. EU måste nu säkerställa enhetlighet med den allmänna dataskyddsförordningen genom en starkare betoning av ansvarsskyldighet och skyddsåtgärder för enskilda personer än av förfaranden. Vissa avvikelser i regler som gäller behandling av personuppgifter som utförs av EU-institutioner är motiverade, på samma sätt som undantag för offentliga sektorn har tagits med i den allmänna dataskyddsförordningen, men dessa måste hållas till ett minimum.

Ur den enskildes perspektiv är det dock av avgörande betydelse att den gemensamma principen för EU:s ramverk för uppgiftsskydd tillämpas konsekvent oberoende av vem som är registeransvarig. Det är också mycket viktigt att hela ramverket börjar tillämpas samtidigt, det vill säga i maj 2018, som är det datum då den allmänna dataskyddsförordningen börjar gälla fullt ut.

I linje med de arrangemang som sedan länge finns på plats mellan våra institutioner rådfrågade kommissionen EDPS om utkastet till förslag. Vi anser att kommissionen på det hela taget har uppnått en god balans mellan de olika intressen som står på spel. Det här yttrandet tar upp ett antal områden där förslaget skulle kunna förbättras ytterligare. Vi argumenterar för förbättringar av förslaget till förordning, i synnerhet när det gäller begränsningar av de registrerades rättigheter och möjligheten för EU-institutionerna att i vissa sammanhang använda certifieringsmekanismer. När det gäller EDPS egna arbetsuppgifter och befogenheter som oberoende organ förefaller förslaget ge en rimlig balans och återspegla de normala funktionerna för en oberoende datatillsynsmyndighet enligt stadgan om de grundläggande rättigheterna och i enlighet med vad som nyligen har bekräftats i domstolens rättspraxis, oavsett om funktionen är att verkställa, hantera klagomål eller ge råd till lagstiftaren om policyer som påverkar uppgiftsskydd och integritet.

Vi uppmuntrar EU-lagstiftarna att enas om förslaget så snabbt som möjligt så att EU-institutionerna får en rimlig övergångstid innan den nya förordningen kan bli tillämplig.

1. INLEDNING OCH BAKGRUND

1.1 Sammanhang

1. Den 10 januari 2017 antog Europeiska kommissionen ett förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ, kontor och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG ([1]) (nedan kallat *förslaget*).

([1]) COM(2017) 8 final; 2017/0002 (COD) (later, "the Proposal").

2. Den grundläggande rätten till skydd av personuppgifter behandlas i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) och artikel 16 i fördraget om Europeiska unionens funktionssätt (nedan kallat *EUF-fördraget*).

3. Europeiska datatillsynsmannen (nedan kallad *EDPS*) är den oberoende tillsynsmyndighet som ansvarar för att säkerställa att unionens institutioner, organ, kontor och byråer (nedan kallade *EU-institutionerna*) följer lagstiftningen om uppgiftsskydd vid behandling av personuppgifter ([2]). Kravet på oberoende tillsyn i unionens system för skydd av personuppgifter behandlas i EU:s primärrätt, både i artikel 16.2 i EUF-fördraget och i artikel 8.3 i stadgan. Domstolen har konsekvent betonat att kontroll från en oberoende myndighet är av avgörande betydelse för rätten till skydd av personuppgifter och har fastställt kriterier för oberoendet ([3]). Bland annat ska tillsynsmyndigheten agera med fullständigt oberoende, vilket innebär beslutanderätt oberoende av något direkt eller indirekt externt inflytande ([4]) och frihet från misstankar om partiskhet ([5]).

4. Det huvudsakliga rättsinstrumentet som är tillämpligt på behandling av personuppgifter som utförs av EU-institutionerna är förordning (EG) nr 45/2001 ([6]) (nedan kallad *förordning (EG) nr 45/2001*), kompletterad av beslut nr 1247/2002/EG ([7]).

5. Efter slutförandet den 27 april 2016 av de långdragna förhandlingarna om EU:s nya ramverk för uppgiftsskydd – den allmänna dataskyddsförordningen (nedan kallad *GDPR*) och direktivet för den polisiära och den rättsliga sektorn – markerar detta förslag (tillsammans med kommissionens förslag till en förordning om integritet och elektronisk kommunikation ([8])) början på en avgörande fas i processen med att slutföra detta EU-ramverk för uppgiftsskydd. Syftet är att anpassa bestämmelserna i förordning (EG) nr 45/2001 till de regler som fastställs i den allmänna dataskyddsförordningen för att skapa ett starkare och mer sammanhängande ramverk för uppgiftsskydd i unionen och göra båda instrumenten tillämpliga samtidigt ([9]). Dessutom innehåller förslaget nya regler för skydd av slutanvändares terminalutrustning som fastställs i kommissionens förslag till den nya förordningen om integritet och elektronisk kommunikation.

6. I sin strategi för 2015–2019 åtog sig EDPS att samarbeta med Europaparlamentet, rådet och kommissionen för att se till att de gällande reglerna i förordning (EG) nr 45/2001 anpassas till GDPR och att ett ändrat ramverk träder i kraft senast i början av 2018. EDPS välkomnar att ha blivit rådfrågad informellt av kommissionen före antagandet av förslaget och att kommissionen i förslaget verkar ha tagit hänsyn till många aspekter som EDPS hittills har tagit upp i sina informella bidrag. EDPS finner att det aktuella förslaget är mer tillfredsställande med tanke på största möjliga anpassning till GDPR, förutom om en restriktiv tolkning av specifika särdrag i EU:s offentliga sektor motiverar något annat, och uppskattar i synnerhet den balans mellan olika intressen som kommissionen har lyckats uppnå.

7. Det här yttrande tar upp ett antal områden där förslaget skulle kunna förbättras ytterligare, men EDPS uppmuntrar EU-lagstiftarna att enas om förslaget så snart som möjligt så att EU-institutionerna får en rimlig övergångsperiod innan den nya förordningen kan bli tillämplig fullt ut.

1.2 **Förslagets mål och tidsfrister**

8. Tidigare har EDPS rekommenderat att de väsentliga reglerna för EU-institutionerna skulle ingå i det (dåvarande) förslaget till allmän dataskyddsförordning ([10]). Nu väljer EU-lagstiftarna ett annat alternativ: ett separat rättsinstrument som är tillämpligt på EU-institutionerna, är i linje med den allmänna dataskyddsförordningen och blir

([2]) Article 286 EC rendered the (then) Community rules on data protection applicable to EU institutions and bodies and mandated the creation of a dedicated independent supervisory authority (later, the EDPS).
([3]) Case C-518/07 *Commission v Germany*, EU:C:2010:125; Case C-614/10 *Commission v Austria*, EU:C:2012:631; Case C-288/12 *Commission v Hungary*, EU:C:2014:237; Case C-362/14 *Maximilian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650.
([4]) Case C-518/07 *Commission v Germany*, *supra* para. 19.
([5]) Case C-288/12 *Commission v Hungary*, *supra* para. 53.
([6]) See *supra* note 3.
([7]) Decision No 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties (OJ L 183, 12.7.2002, p. 1).
([8]) Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 2017/0003 (COD).
([9]) See Article 98 and recital 17 of the GDPR.
([10]) See e.g. the EDPS Opinion of 7 March 2012 on the data protection reform package (OJ C 192, 30.6.2012, p. 7).

tillämpligt samtidigt som denna. EDPS stödjer detta tillvägagångssätt: det skulle vara oacceptabelt om Europeiska kommissionen och övriga EU-institutioner inte skulle vara bundna av regler motsvarande dem som snart blir tillämpliga på medlemsstatsnivå. Vidare skulle det inte vara önskvärt att EDPS ansvarar för tillsynen av att EU-institutionerna efterlever väsentliga regler som skulle vara underlägsna de regler som EDPS motsvarigheter på nationell nivå utövar tillsyn över, i synnerhet med tanke på att EDPS kommer att vara medlem i den framtida dataskyddsstyrelsen (nedan kallad *EDPB*) ([11]).

9. De framtida regler som är tillämpliga på personuppgifter som behandlas av EU-institutionerna bör därför anpassas till bestämmelserna i den allmänna dataförordningen förutom i de fall då restriktivt tolkade specifika förhållanden för offentliga sektorn motiverar något annat. I det avseendet välkomnar EDPS skäl 5 i förslaget, som betonar att största möjliga enhetlighet behövs och förtydligar att ”[n]är en bestämmelse i denna förordning bygger på samma koncept som en bestämmelse i [den allmänna dataskyddsförordningen] bör dessa båda bestämmelser tolkas enhetligt, särskilt eftersom den systematik som denna förordning bygger på bör uppfattas som en motsvarighet till systematiken bakom [den allmänna dataskyddsförordningen]”.

10. Samtidigt kan harmoniseringen med den allmänna dataskyddsförordningen varken vara fullständig eller automatisk. Den allmänna dataskyddsförordningen innehåller många klausuler som tillåter medlemsstaterna att upprätthålla eller införa specifik lagstiftning inom vissa områden, bland annat offentliga myndigheter. ([12]) I de fall där GDPR innehåller specifika regler för offentliga myndigheter ([13]) eller lämnar utrymme för medlemsstaterna att genomföra bestämmelserna, kan förslaget anses spela en roll som är jämförbar med nationell lagstiftnings ”genomförande” av GDPR. Det gäller till exempel artikel 9 ”Överföring av personuppgifter till andra mottagare än unionens institutioner och organ” eller artikel 66 ”Administrativa sanktionsavgifter” i förslaget (se avsnitt 2.8.1 nedan). Det är dessutom viktigt att se till att den höga grad av skydd som i dagsläget gäller för EU-institutionerna upprätthålls. Därför behöver vissa särdrag i förordning (EG) nr 45/2001, såsom i artikel 25 ”Begränsningar” (se avsnitt 2.3.1 nedan) och artikel 44 ”Utnämning av dataskyddsombudet” (se avsnitt 2.4.5.1 nedan).

11. Utöver den väsentliga anpassningen till GDPR är det viktigt att de ändrade reglerna blir tillämpliga fullt ut samtidigt som GDPR, dvs. den 25 maj 2018. I det befintliga nätverket av uppgiftsskyddsombud (nedan kallat *DPO*) finns en effektiv kanal för informationsdelning och samarbete. EDPS känner sig därför säker på att efterlevnad kan uppnås efter en relativt kort övergångstid, t.ex. tre månader.

12. Den princip om ansvarsskyldighet som GDPR bygger på – samt det här förslaget – går ett steg längre än enkel efterlevnad av reglerna och innebär en ny kultur. För att underlätta övergången har EDPS satt igång ett ”ansvarsskyldighetsprojekt”. I det sammanhanget har EDPS under 2016 och 2017 varit i kontakt med sju viktiga EU-institutioner och -organ för att hjälpa dem att förbereda sig i god tid för genomförandet av GDPR.

1.3 **Tillämpningsområde och förhållande till andra rättsinstrument**

13. EDPS har vid flera tidigare tillfällen uppmanat kommission att föreslå ett bärkraftigt och *övergripande* system som skulle vara ambitiöst och göra uppgiftsskyddet i EU effektivare och mer *sammanhängande*, så att en sund miljö skapas för vidareutveckling under kommande år ([14]). Kommissionen valde ett annat tillvägagångssätt och föreslog ett separat rättsinstrument för uppgiftsskydd inom brottsbekämpningsområdet ([15]). Ett antal förslag till rättsakter som införde separata ”fristående” system för uppgiftsskydd följde ([16]).

([11]) EDPS Opinion of 7 March 2012 on the data protection reform package, p. 6.

([12]) See in particular Article 6(3) and recital 10 to the GDPR: “Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data (‘sensitive data’). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.”

([13]) E.g. last sentence of Article 6(1), Article 20(5), Article 27, Article 37, Article 41 or Article 46(2)(a) of the GDPR.

([14]) See in particular the EDPS Opinion of 14 January 2011 on the Communication “A comprehensive approach on personal data in the European Union”, OJ L 181, 22.6.2011, p. 1.

([15]) See *supra* note 5.

([16]) Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final, now adopted as Regulation 2016/794 and published in OJ L 135 24.05.2016, p. 53; Proposal for a Council Regulation on the establishment of the European Public Prosecutor’s Office, COM(2013) 534 final. See also the Council General approach [First reading] on the Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) available at: http://data.consilium.europa.eu/doc/document/ST-6643-2015-INIT/en/pdf.

14. EDPS erkänner att det aktuella rättsliga ramverket för uppgiftsskydd, om än fragmenterat, är det bästa resultat som går att uppnå i dagsläget ([17]). EDPS förstår att det här förslaget skulle fortsätta gälla för de EU-institutioner som i dag omfattas av förordning (EG) nr 45/2001 ([18]) (i huvudsak alla tidigare institutioner, organ, kontor och byråer inom första och andra ”pelaren”) ([19]) men inte som sådant påverka befintliga system eller ”fristående” system som väntar på godkännande ([20]). Sådana system kommer att påverkas av det aktuella förslaget endast om och beroende på i vilken grad detta uttryckligen anges i det relevanta rättsinstrumentet. EDPS noterar detta tillvägagångssätt men föreslår att det beskrivs mer ingående i ingressen till förslaget och eventuellt även i dess artikel 2 ”Tillämpningsområde”. Samtidigt skulle EDPS vilja betona att fragmenteringen och den ökade komplexiteten i det rättsliga ramverket för databehandling som utförs av de olika EU-institutioner som är verksamma inom den tidigare första och tredje ”pelaren” inte är ett helt tillfredsställande resultat och kan behöva åtgärdas av EU-lagstiftarna på medellång sikt.

15. Förordning (EG) nr 45/2001 innehåller åtgärder för att skydda rätten till privatliv och konfidentialitet för kommunikation i fall när EU-institutionerna har kontrollen över infrastruktur som används för kommunikation. För det ändamålet innehåller förordningen vissa bestämmelser som täcker delar av bestämmelserna i direktiv 2002/58/EG (nedan kallat *direktivet om integritet och elektronisk kommunikation*) ([21]) och fastställer principen att regler för skydd av grundläggande rättigheter bör tillämpas på ett sammanhängande och harmoniskt sätt i hela unionen, med hänvisning till direktivet om integritet och elektronisk kommunikation ([22]). Behovet av att säkerställa samma nivå av skydd för privatlivet och konfidentialitet vid kommunikation som involverar EU-institutioner kvarstår oförändrat och därför bör principen om en sammanhängande och harmonisk tillämpning upprätthållas. EDPS anser därför att förslaget bör säkerställa att relevanta regler i GDPR och framtida förordningar om integritet och elektronisk kommunikation gäller på motsvarande sätt för EU-institutionerna. Detta bör innefatta såväl att skydda konfidentialitet och privatliv när det gäller kommunikationstjänster som kontrolleras EU-institutionerna som andra principer i den framtida förordningen om integritet och elektronisk kommunikation, så som skyddet av terminalenheter, t.ex. när det gäller spårning och skräppost.

16. Slutligen gäller att även om EU-lagstiftningen om uppgiftsskydd även omfattar Europeiska ekonomiska samarbetsområdet och deltagande EFTA-länder är skyldiga att upprätta oberoende tillsynsmyndigheter enligt GDPR är EFTA-institutioner inte föremål för några särskilda regler eller tillsyn när det gäller uppgiftsskydd, trots att de utbyter personuppgifter med EU-institutioner. EDPS anser att det aktuella förslaget kan vara en möjlighet att ta itu med denna fråga.

3. **SLUTSATSER**

90. Generellt anser EDPS att förslaget lyckas anpassa reglerna för EU-institutioner till GDPR samtidigt som det tar hänsyn till särdragen hos EU:s offentliga sektor. Den höga graden av skydd när det gäller behandling som utförs av EU-institutionerna bevaras i allmänhet i förslaget. EDPS uppskattar särskilt den balans kommissionen har uppnått mellan de olika intressen som står på spel.

91. EDPS anser att förslaget bör förbättras ytterligare, främst när det gäller metoderna för begränsning i artikel 25. För att säkerställa efterlevnaden av kvalitetskraven enligt ovan skulle artikel 25.1 i förslaget behöva ändras på så sätt att endast rättsakter som antas på grundval av fördragen kan begränsa grundläggande rättigheter, vilket skulle innebära att samma standarder skulle krävas för EU-institutioner som de som gäller för medlemsstaterna enligt GDPR. Om begränsningar av artikel 34 ”Konfidentialitet för elektronisk kommunikation” övervägs, uppmanar EDPS EU-lagstiftarna att säkerställa att eventuella begränsningar som EU-institutionerna gör i sin egen verksamhet av den grundläggande rättigheten till skydd av personlig integritet vid kommunikation följer samma standarder som de som fastställs i unionslagstiftningen inom detta område enligt domstolens tolkning.

92. EDPS välkomnar att förslaget innehåller en separat artikel om EDPS roll som rådgivare till EU-institutionerna (artikel 42 i förslaget). Däremot är EDPS bekymrad över att lydelsen ”[e]fter antagandet av förslag” (i motsats till ”[n]är kommissionen antar ett lagförslag” i artikel 28.2 i förordning (EG) nr 45/2001) kan innebära ett ifrågasättande av det långvariga åtagandet från kommissionens sida att rådfråga EDPS informellt om utkast till

([17]) EDPS Opinion 3/2015 “Europe’s big opportunity - EDPS recommendations on the EU’s options for data protection reform”, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-10-09_GDPR_with_addendum_EN.pdf.

([18]) See the list of EU institutions and bodies available at: http://publications.europa.eu/code/en/en-390500.htm.

([19]) Regulation (EC) No 45/2001 already today applies to, *inter alia*, the European Defence Agency, European Union Institute for Security Studies, and the European Union Satellite Centre.

([20]) Europol, Eurojust, EPPO, *supra* note 21.

([21]) Directive 2002/58/EC of the European Parliament and of theCouncil of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications (OJ L 201, 31.7.2002, p. 37), as amended (later, “the ePrivacy Directive”).

([22]) Recitals 10–12 ePrivacy Directive.

förslag, vanligen i det stadium när samrådet inom kommissionen sker. Med tanke på den informella rådfrågningens betydelse skulle EDPS välkomna ett skäl där kommissionen upprepar sitt åtagande när det gäller denna sedan länge etablerade praxis. EDPS skulle också önska att förslaget bevarar lydelsen från artikel 28.2 i förordning (EG) nr 45/2001 (”när kommissionen antar”), vilket skulle ge större handlingsfrihet i detta avseende. EDPS anser att artikel 42 i den föreslagna formen är tillräckligt klargörande när det gäller respektive uppgifter för EDPS och EDPB för att undvika onödigt dubbelarbete i framtiden.

93. EDPS anser att möjligheten att lägga ut DPO:s funktion inte är lämplig för myndighetsutövande EU-institutioner. Därför bör det andra alternativet i artikel 44.4 (”eller utföra uppgifterna på grundval av ett tjänsteavtal”) strykas.

94. EDPS välkomnar artikel 66 i förslaget, som skulle ge EDPS rätt att ålägga sanktionsavgifter. Han anser att EU-institutionerna skulle få en privilegierad ställning jämfört med den offentliga sektorns institutioner i många medlemsstater om EU:s tillsynsmyndighet skulle berövas möjligheten att ålägga sanktionsavgifter.

95. EDPS anser att certifieringsmekanismer kan vara ett mycket användbart instrument för EU-institutionerna, och de används redan i vissa sammanhang, t.ex. för certifiering av efterlevnad av allmänt accepterade standarder. Hänvisningar till användning av certifiering (men inte uppförandekoder) bör därför läggas till i artikel 26 ”Den personuppgiftsansvariges ansvar”, artikel 27 ”Inbyggt dataskydd och dataskydd som standard”, samt artikel 33 ”Säkerhet i samband med behandlingen”.

96. Det här yttrandet tar upp ett antal områden där förslaget skulle kunna förbättras ytterligare, men EDPS skulle uppmuntra EU-lagstiftarna att enas om förslaget så snart som möjligt så att EU-institutionerna får åtnjuta en rimlig övergångsperiod innan den nya förordningen blir tillämplig samtidigt med GDPR, i maj 2018.

Bryssel den 15 mars 2017.

Giovanni BUTTARELLI

Europeiska datatillsynsmannen