Regeringskansliet
Faktapromemoria 2016/17:FPM64

Dataskyddsförordning för EU:s institutioner

2016/17:FPM64

Justitiedepartementet

2017-02-13

Dokumentbeteckning

KOM(2017) 8
Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

Sammanfattning

Den 10 januari 2017 presenterade kommissionen ett förslag till ny dataskyddsförordning för EU:s institutioner, organ, kontor och byråer. Syftet är att slutföra inrättandet av ett starkt och sammanhängande dataskyddsregelverk inom EU. Förslaget innebär en anpassning av den befintliga dataskyddsförordningen för EU:s institutioner och organ till principerna och bestämmelserna i den allmänna dataskyddsförordningen som antogs i april 2016.

Regeringen välkomnar kommissionens förslag. Det är angeläget att enskilda ges ett likvärdigt integritetsskydd inom hela unionen, oavsett om behandling av den enskildes personuppgifter sker i medlemsstaterna eller inom EU:s institutioner, organ, kontor eller byråer. Ett starkt skydd för enskildas uppgifter inom EU är även av stor vikt för ett fritt flöde av personuppgifter inom unionen och därmed en välfungerande inre marknad.

1 Förslaget

1.1 Ärendets bakgrund

Den behandling av personuppgifter som sker i EU:s institutioner och organ regleras i dag av Europaparlamentets och rådets förordning (EG) nr 45/2001

av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (dataskyddsförordning för EU:s institutioner). De närmare villkoren för den Europeiska datatillsynsmannen, som utövar tillsyn enligt dataskyddsförordningen för EU:s institutioner, regleras för närvarande i Europaparlamentets, rådets och kommissionens beslut nr 1247/2002/EG av den 1 juli 2002 om tjänsteföreskrifter och allmänna villkor för utövande av funktionen som europeisk datatillsynsman.

Den 25 maj 2018 börjar 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) tillämpas. Enligt artikel 2.3 i denna förordning ska dataskyddsförordningen för EU:s institutioner anpassas till principerna och bestämmelserna i den allmänna dataskyddsförordningen i enlighet med den allmänna dataskyddsförordningens artikel 98. Av sistnämnda artikel följer att kommissionen ska lägga fram lagstiftningsförslag för att säkerställa att dataskyddsförordningen för EU:s institutioner ger samma skyddsnivå för enskilda som den allmänna dataskyddsförordningen.

Kommissionen lade den 10 januari 2017 fram ett förslag till en ny förordning som ska ersätta dataskyddsförordningen för EU:s institutioner samt beslutet om tjänsteföreskrifter och allmänna villkor för den Europeiska datatillsynsmannen.

1.2 Förslagets innehåll

Det huvudsakliga syftet med kommissionens förslag är att slutföra inrättandet av ett starkt och sammanhängande dataskyddsramverk inom EU. EU:s institutioner, organ, kontor och byråer behandlar t.ex. uppgifter om sina anställda och besökare. Förslaget innebär en anpassning av den befintliga dataskyddsförordningen för EU:s institutioner till principerna och bestämmelserna i den allmänna dataskyddsförordningen.

Förslaget till ny förordning baseras således i stor utsträckning på strukturen och regleringen i den allmänna dataskyddsförordningen. Dessutom har huvuddragen i beslutet om tjänsteföreskrifter och allmänna villkor för den Europeiska datatillsynsmannen tagits in i förslaget.

I det följande redogörs för de huvudsakliga förändringar som förslaget medför. Redogörelsen är inte avsedd att ge en heltäckande beskrivning av förslaget.

1.2.1 Samtycke

När samtycke utgör grund för personuppgiftsbehandling ska EU:s institutioner och organ be den enskilde om dennes samtycke med användning av ett tydligt och enkelt språk innan behandlingen inleds. Samtycke måste inhämtas för varje typ av personuppgiftsbehandling, dvs. det är inte tillåtet att inhämta ett samlat samtycke för flera olika typer av behandling. Den registrerade kommer även ha rätt att när som helst ta tillbaka ett tidigare lämnat samtycke.

1.2.2 Den registrerades rättigheter

Genom förslaget införs principen om transparens i förhållande till den registrerade, bl.a. genom att EU:s institutioner och organ åläggs att använda ett tydligt och enkelt språk vid sin kommunikation samt att göra information till den registrerade lätt tillgänglig.

Det införs en rätt till att bli bortglömd. Rättigheten innebär att den registrerade, under vissa förutsättningar, kan begära att få sina personuppgifter raderade av en EU-institution eller ett EU-organ. Det införs även en skyldighet för institutionen eller organet att underrätta andra som behandlar de aktuella personuppgifterna, t.ex. sökmotorer, om den registrerades begäran.

1.2.3 Underrättelse om personuppgiftsincidenter till den Europeiska datatillsynsmannen och den registrerade

Vid en personuppgiftsincident kommer EU:s institutioner och organ vara skyldiga att underrätta den Europeiska datatillsynsmannen och den registrerade om incidenten. Underrättelse till den Europeiska datatillsynsmannen ska lämnas utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar från det att den personuppgiftsansvarige fått vetskap om incidenten. Underrättelseskyldigheten gäller emellertid inte om det är osannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter. En underrättelse ska även lämnas till den registrerade om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Detta ska ske utan onödigt dröjsmål. En underrättelse krävs dock inte om t.ex. den personuppgiftsansvarige redan vidtagit åtgärder som säkerställer att risken sannolikt inte längre kommer att uppstå eller det skulle innebära en oproportionerlig ansträngning. I det senare fallet ska i stället allmänheten informeras eller en liknande åtgärd vidtas som informerar de registrerade på ett lika effektivt sätt.

1.2.4 Den personuppgiftsansvariges ansvar

Genom förslaget införs en skyldighet för den personuppgiftsansvarige att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa,

och för att denne ska kunna visa, att behandlingen sker i enlighet med förordningen. Den personuppgiftsansvarige ska i detta sammanhang beakta behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter. Förslaget innebär även att regler om inbyggt dataskydd (”by design”) och dataskydd som standard (”by default”) införs. Detta innebär bl.a. att den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder – såsom pseudonymisering – för ett effektivt genomförande av dataskyddsprinciper, t.ex. principen om uppgiftsminimering. Det innebär även att den personuppgiftsansvarige ska genomföra åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas.

Den skyldighet som i dag finns att, under vissa förhållanden, begära förhandskontroll av den Europeiska datatillsynsmannen tas bort genom förslaget.

Vidare införs en skyldighet för den personuppgiftsansvarige att utföra konsekvensbedömningar avseende dataskydd om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

1.2.5 Samarbete och ömsesidigt bistånd

Enligt förslaget ska den Europeiska datatillsynsmannen samarbeta med bl.a. de nationella tillsynsmyndigheterna i den utsträckning som krävs för att de ska kunna fullgöra sina respektive uppgifter. Det införs även en skyldighet för den Europeiska datatillsynsmannen att, om det föreskrivs i en EU-rättsakt, samarbeta med de nationella tillsynsmyndigheterna för att säkerställa en effektiv övervakning av stora IT-system eller EU-organ.

1.2.6 Administrativa sanktionsavgifter

Det införs en möjlighet för den Europeiska datatillsynsmannen att under vissa förutsättningar påföra institutioner och organ en administrativ sanktionsavgift när dessa underlåter att följa ett föreläggande från den Europeiska datatillsynsmannen. Sanktionsavgifterna kommer att tillfalla EU:s allmänna budget.

1.3 Gällande svenska regler och förslagets effekt på dessa

Förslaget syftar till att reglera behandling av personuppgifter som sker i EU:s institutioner och organ och inte sådan behandling som sker i medlemsstaterna. Förslaget bedöms bl.a. mot den bakgrunden i nuläget inte ha några effekter på svenska regler.

1.4 Budgetära konsekvenser / Konsekvensanalys

Förslaget bedöms inte innebära några konsekvenser för den svenska statsbudgeten.

Enligt kommissionens bedömning är förslagets inverkan begränsad till utgifterna för EU:s institutioner och organ. Det bedöms emellertid inte skapas några betydande tillkommande utgifter för institutionerna och organen.

Vidare anger kommissionen att effekterna av de nya skyldigheter som följer av den allmänna dataskyddsförordningen, som förslaget innebär en anpassning till, redan har bedömts vid arbetet med denna. En specifik konsekvensanalys för förslaget till dataskyddsförordning för EU:s institutioner bedöms i och med det vara överflödig.

2 Ståndpunkter

2.1 Preliminär svensk ståndpunkt

Regeringen välkomnar kommissionens förslag. Det är angeläget att enskilda ges ett likvärdigt integritetsskydd inom hela unionen, oavsett om behandling av den enskildes personuppgifter sker i medlemsstaterna eller i EU:s institutioner, organ, kontor eller byråer. Ett starkt skydd för personuppgifter inom unionen är av stor vikt för ett fritt flöde av personuppgifter och därmed en välfungerande inre marknad. Det kan förutses att frågor om förhållandet mellan dataskyddsförordningen för EU:s institutioner samt Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (öppenhetsförordningen) kan uppkomma. För regeringen är det en prioriterad fråga att öppenhetsaspekterna beaktas i tillräcklig utsträckning vid utformningen av förordningen. Beträffande förslagets budgetära konsekvenser, kommer regeringen att verka för att eventuella sådana konsekvenser finansieras genom omprioriteringar inom befintliga ramar.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaternas ståndpunkter till förslaget är ännu inte kända.

2.3 Institutionernas ståndpunkter

Institutionernas ståndpunkter är ännu inte kända.

2.4 Remissinstansernas ståndpunkter

Förslaget har inte remitterats.

3 Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Förslaget har sin rättsliga grund i artikel 16 i fördraget om Europeiska unionens funktionssätt (FEUF).

Förslaget antas genom det ordinarie beslutsförfarandet, vilket i enlighet med artikel 294 FEUF betyder att det krävs kvalificerad majoritet i rådet samt enighet med Europaparlamentet.

3.2 Subsidiaritets- och proportionalitetsprincipen

Eftersom endast EU kan anta regler som styr hur EU:s institutioner och organ behandlar personuppgifter omfattas förslaget till anpassning av EU:s exklusiva kompetens. Av denna anledning behöver någon subsidiaritetsprövning inte ske.

Kommissionen bedömer att förslaget även är förenligt med proportionalitetsprincipen av i huvudsak följande skäl. För att uppnå det grundläggande målet att tillförsäkra enskilda ett likvärdigt skydd inom hela unionen i fråga om behandling av personuppgifter och fri rörlighet för personuppgifter är det nödvändigt och ändamålsenligt att reglera behandling av personuppgifter inom EU:s institutioner och organ. Förslaget går inte utöver vad som är nödvändigt för att uppnå detta mål. Ett starkt skydd av personuppgifter inom EU är av stor vikt för ett fritt flöde av personuppgifter och därmed en välfungerande inre marknad. Förslaget syftar till att anpassa den nuvarande dataskyddsförordningen för EU:s institutioner till den allmänna dataskyddsförordningen, för att säkerställa enskilda ett starkt och sammanhängande integritetsskydd inom hela unionen. Regeringen har inte funnit skäl att göra någon annan bedömning än den kommissionen har gjort vad gäller förslagets förenlighet med proportionalitetsprincipen.

4 Övrigt

4.1 Fortsatt behandling av ärendet

Den första behandlingen av förslaget skedde den 19 januari 2017 i rådsarbetsgruppen DAPIX. Det maltesiska ordförandeskapet har som ambition att nå en allmän inriktning vid rådet för rättsliga och inrikes frågor (RIF) i juni 2017. Målsättningen är att en ny förordning ska vara på plats och börja tillämpas när den allmänna dataskyddsförordningen börjar tillämpas den 25 maj 2018.

-