KOMMISSIONENS BESLUT (EU) 2021/2243

av den 15 december 2021

om interna regler för tillhandahållande av information till registrerade och begränsning av vissa av deras rättigheter i samband med Europeiska kommissionens behandling av personuppgifter, för att garantera den interna säkerheten för kommissionens institutioner

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 249.1, och

av följande skäl:

(1) När kommissionen utför sina uppgifter är den skyldig att respektera fysiska personers rättigheter i samband med den behandling av personuppgifter som erkänns i artikel 8.1 i Europeiska unionens stadga om de grundläggande rättigheterna och i artikel 16.1 i fördraget om Europeiska unionens funktionssätt. Den måste också respektera de rättigheter som fastställs i Europaparlamentets och rådets förordning (EU) 2018/1725 ([1]). Samtidigt måste kommissionen hantera säkerhetsincidenter på it-området i enlighet med bestämmelserna i artikel 15 i beslut (EU, Euratom) 2017/46 ([2]).

(2) För att säkerställa it-säkerheten, dvs. bevarande av konfidentialitet, integritet och tillgänglighet för kommunikations- och informationssystem och de dataset som de behandlar, när det gäller personer, tillgångar och information, har kommissionen, särskilt genom sitt generaldirektorat för informationsteknik, vidtagit åtgärder i enlighet med beslut (EU, Euratom) 2017/46 och beslut C (2017) 8841 final ([3]). Dessa åtgärder omfattar övervakning av it-säkerhetsriskerna och de it-säkerhetsåtgärder som genomförts, krav på systemägare att vidta specifika it-säkerhetsåtgärder för att minska it-säkerhetsriskerna för kommissionens kommunikations- och informationssystem samt hantering av säkerhetsincidenter på it-området.

(3) Generaldirektoratet för informationsteknik tillhandahåller it-säkerhet och it-säkerhetstjänster till kommissionen och behöver behandla flera kategorier av personuppgifter för att

— förmedla larm och varningar som rör it-säkerhetshändelser och it-säkerhetsincidenter,

— reagera på och begränsa it-säkerhetshändelser och it-säkerhetsincidenter,

— underlätta verktyg och insatser genom säkerhetsgranskningar, säkerhetsbedömningar och sårbarhetshantering,

— öka medvetenheten hos kommissionens personal på området cybersäkerhet,

— övervaka, upptäcka och förhindra att it-säkerhetshändelser och it-säkerhetsincidenter inträffar,

— granska privilegierade användarkonton.

(4) Säkerhetsincidenter på it-området som skulle kunna undergräva säkerheten i kommissionens informations- och kommunikationssystem kan inträffa i all behandling som utförs av kommissionen. De kan omfatta alla kategorier av personuppgifter som behandlas av kommissionen.

([1]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ 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 (EUT L 295, 21.11.2018, s. 39).

([2]) Kommissionens beslut (EU, Euratom) 2017/46 av den 10 januari 2017 om säkerheten i Europeiska kommissionens kommunikations- och informationssystem (EUT L 6, 11.1.2017, s. 40).

([3]) Kommissionens beslut C (2017) 8841 av den 13 december 2017 om tillämpningsföreskrifter för artiklarna 3, 5, 7, 8, 9, 10, 11, 12, 14 och 15 i kommissionens beslut 2017/46 om säkerheten i kommissionens kommunikations- och informationssystem.

(5) Under vissa omständigheter kan det visa sig vara nödvändigt att sammanjämka de registrerades rättigheter enligt förordning (EU) 2018/1725 med kommissionens behov av att utföra sina uppgifter för att säkerställa it-säkerheten för personer, tillgångar och information inom kommissionen enligt beslut (EU, Euratom) 2017/46, och med full respekt för andra registrerades grundläggande rättigheter och friheter. På grundval av artikel 25.1 i förordning (EU) 2018/1725 får kommissionen därför begränsa tillämpningen av artiklarna 14–17, 19, 20 och 35 i förordning (EU) 2018/1725 och av principen om öppenhet i artikel 4.1 a i den förordningen, i den mån de bestämmelserna motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 14–17, 19 och 20 i den förordningen.

(6) Detta beslut bör tillämpas på all behandling som utförs av kommissionen i egenskap av personuppgiftsansvarig vid utförandet av dess uppgifter för att säkerställa it-säkerheten för personer, tillgångar och information i kommissionen i enlighet med beslut (EU, Euratom) 2017/46. Det bör därför gälla de registrerade för de kategorier av personuppgifter som omfattas av all sådan behandling, dvs. enskilda personer som interagerar med något av kommissionens informations- och kommunikationssystem.

(7) Personuppgifterna lagras i en säker elektronisk miljö för att förhindra olaglig åtkomst av uppgifter av personer utanför kommissionen. Olika lagringstider gäller för olika behandlingar beroende på vilken typ av personuppgifter det rör sig om. Lagringen av akter i kommissionen regleras av den gemensamma lagringslistan på kommissionsnivå (SEC (2019) 900), som är ett regleringsdokument i form av en lagringsplan som anger lagringsperioderna för olika typer av kommissionsfiler för att begränsa datalagringen till vad som är nödvändigt.

(8) Kommissionen skulle kunna behöva begränsa tillämpningen av de registrerades rättigheter för att skydda sin inre säkerhet i enlighet med artikel 25.1 d i förordning (EU) 2018/1725 (dvs. för att bevara konfidentialiteten, integriteten och tillgängligheten i sina kommunikations- och informationssystem och de dataset som de behandlar, dess tillgångar och information). Kommissionen skulle framför allt kunna vara tvungen att göra detta när den

— förmedlar larm och varningar som rör it-säkerhetshändelser och it-säkerhetsincidenter,

— reagerar på och begränsar it-säkerhetshändelser och it-säkerhetsincidenter, underlättar verktyg och insatser genom säkerhetsgranskningar, säkerhetsbedömningar och sårbarhetshantering,

— ökar medvetenheten hos kommissionens personal på området cybersäkerhet,

— övervakar, upptäcker och förhindrar att it-säkerhetshändelser och it-säkerhetsincidenter inträffar,

— granskar privilegierade användarkonton.

(9) För hantering av säkerhetsincidenter på it-området som avses i artikel 15 i beslut (EU, Euratom) 2017/46 får generaldirektoratet för informationsteknik utbyta information med it-incidenthanteringsgruppen vid generaldirektoratet för personal och säkerhet.

(10) För att följa artiklarna 14, 15 och 16 i förordning (EU) 2018/1725 bör kommissionen informera alla enskilda personer om den verksamhet som inbegriper behandling av personuppgifter och som påverkar deras rättigheter. Den bör göra detta på ett öppet och konsekvent sätt genom att offentliggöra ett meddelande om skydd av personuppgifter på kommissionens webbplats. I förekommande fall bör den tillämpa ytterligare skyddsåtgärder för att informera de registrerade individuellt i ett lämpligt format.

(11) Efterlevnad av artiklarna 14, 15 och 16 i förordning (EU) 2018/1725 skulle kunna avslöja förekomsten av säkerhetsåtgärder, sårbarheter eller incidenter på it-området som vidtagits enligt artikel 15 i beslut (EU, Euratom) 2017/46. Om dessa säkerhetsåtgärder, sårbarheter och incidenter på it-området avslöjas ökar risken för att den exponerade säkerhetsåtgärden på it-området kringgås, för att den exponerade sårbarheten då skulle missbrukas och att en pågående analys av säkerhetsincidenter på it-området skulle kunna undergrävas eftersom objekt kan manipuleras oavsiktligt eller avsiktligt av en användare eller en skadlig aktör. Detta skulle allvarligt kunna försämra kommissionens förmåga att säkerställa dess it-säkerhet och i synnerhet att hantera säkerhetsincidenter på it-området på ett effektivt sätt i framtiden.

(12) Enligt artikel 25.1 h i förordning (EU) 2018/1725 bemyndigas kommissionen också att begränsa tillämpningen av registrerades rättigheter för att skydda andra personers rättigheter och friheter i samband med säkerhetsincidenter på it-området som skulle kunna undergräva it-säkerheten.

(13) Kommissionen kan behöva begränsa tillhandahållandet av information till registrerade och tillämpningen av andra registrerades rättigheter när det gäller personuppgifter som mottagits från länder utanför EU eller internationella organisationer, för att fullgöra sin skyldighet att samarbeta med dessa länder eller organisationer. Detta är en del av kommissionens skyldighet att skydda ett viktigt mål av generellt allmänt intresse för EU, i enlighet med artikel 25.1 c i förordning (EU) 2018/1725. I vissa fall kan dock den registrerades intresse eller grundläggande rättigheter väga tyngre än intresset av internationellt samarbete.

(14) Kommissionen har därför identifierat de skäl som anges i artikel 25.1 c, d och h i förordning (EU) 2018/1725 som skäl för begränsningar som kan vara nödvändiga för uppgiftsbehandling som utförs av generaldirektoratet för informationsteknik i samband med tillhandahållande av it-säkerhet och säkerhetstjänster på it-området till kommissionen.

(15) Alla begränsningar som tillämpas enligt detta beslut bör vara nödvändiga och stå i proportion till risken för de registrerades rättigheter och friheter.

(16) Kommissionen bör hantera alla begränsningar på ett öppet sätt och registrera varje tillämpning av begränsningar i motsvarande registersystem.

(17) Enligt artikel 25.8 i förordning (EU) 2018/1725 får personuppgiftsansvariga skjuta upp, utelämna eller neka tillhandahållandet av information av samma skäl som gäller för att begränsa den registrerades rättigheter i de fall då tillhandahållandet av informationen skulle kunna undergräva syftet med begränsningen. Detta gäller särskilt begränsningarna av de skyldigheter som föreskrivs i artiklarna 16 och 35 i förordning (EU) 2018/1725. Kommissionen bör regelbundet se över införda begränsningar för att säkerställa att de registrerades rätt att bli informerade i enlighet med artiklarna 16 och 35 i förordning (EU) 2018/1725 begränsas endast så länge som är nödvändigt för att göra det möjligt för kommissionen att säkerställa sin säkerhet och i synnerhet hantera säkerhetsincidenter på it-området.

(18) Om kommissionen begränsar tillämpningen av andra rättigheter för registrerade än de som avses i artiklarna 16 och 35 i förordning (EU) 2018/1725, bör den personuppgiftsansvarige från fall till fall bedöma om meddelandet om begränsningen skulle undergräva dess syfte.

(19) Kommissionens dataskyddsombud bör göra en oberoende översyn av tillämpningen av begränsningar för att säkerställa efterlevnaden av detta beslut.

(20) För att kommissionen omedelbart ska kunna begränsa tillämpningen av vissa rättigheter och skyldigheter i enlighet med artikel 25 i förordning (EU) 2018/1725 bör detta beslut träda i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

(21) Europeiska datatillsynsmannen avgav ett yttrande den 16 september 2021.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Syfte och tillämpningsområde

1. I detta beslut fastställs de regler som kommissionen måste följa för att informera registrerade om behandlingen av deras uppgifter i enlighet med artiklarna 14, 15 och 16 i förordning (EU) 2018/1725, när den utför sina uppgifter enligt beslut (EU, Euratom) 2017/46.

Genom detta beslut regleras även villkoren för hur kommissionen får begränsa tillämpningen av artiklarna 4, 14–17, 19, 20 och 35 i förordning (EU) 2018/1725, i enlighet med artikel 25.1 c, d och h i den förordningen när den utför sina uppgifter enligt beslut (EU, Euratom) 2017/46.

2. Detta beslut ska tillämpas på behandling av personuppgifter antingen av kommissionen eller på dess vägnar med avseende på eller i fråga om den verksamhet som bedrivs för att garantera it-säkerheten för personer, tillgångar och information inom kommissionen enligt beslut (EU, Euratom) 2017/46.

Artikel 2

Tillämpliga undantag och begränsningar

1. Kommissionen ska, vid fullgörandet av sina skyldigheter med avseende på de registrerades rättigheter enligt förordning (EU) 2018/1725, överväga om några av de undantag som anges i den förordningen är tillämpliga.

2. Om utövandet av de rättigheter och skyldigheter som föreskrivs i artiklarna 14–17, 19, 20 och 35 i förordning (EU) 2018/1725 i fråga om personuppgifter som behandlas av kommissionen skulle undergräva syftet att tillhandahålla it-säkerhet och säkerhetstjänster på it-området, om inte annat följer av artiklarna 3–7 i detta beslut, bland annat genom att avslöja kommissionens utredningsverktyg, sårbarheter och metoder, eller negativt skulle påverka andra registrerades rättigheter och friheter och säkerhet, särskilt när det gäller behandling av personuppgifter, i syfte att

— förmedla larm och varningar som rör it-säkerhetshändelser och it-säkerhetsincidenter,

— reagera på och begränsa it-säkerhetshändelser och it-säkerhetsincidenter,

— underlätta verktyg och insatser genom säkerhetsgranskningar, säkerhetsbedömningar och sårbarhetshantering,

— öka medvetenheten hos kommissionens personal på området cybersäkerhet,

— övervaka, upptäcka och förhindra att it-säkerhetshändelser och it-säkerhetsincidenter inträffar,

— granska privilegierade användarkonton,

får kommissionen begränsa tillämpningen av

a) artiklarna 14–17, 19, 20 och 35 i förordning (EU) 2018/1725, och

b) den öppenhetsprincip som fastställs i artikel 4.1 a i förordning (EU) 2018/1725 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som anges i artiklarna 14–17, 19 och 20 i förordning (EU) 2018/1725.

Kommissionen får göra detta i enlighet med artikel 25.1 c, d och h i förordning (EU) 2018/1725.

3. Om inte annat följer av artiklarna 3–7 får kommissionen begränsa de rättigheter och skyldigheter som avses i punkt 2 i denna artikel i följande fall:

a) Om utövandet av dessa rättigheter och skyldigheter med avseende på personuppgifter som erhålls från EU:s övriga institutioner, organ eller byråer skulle kunna begränsas av dessa på grundval av de rättsakter som anges i artikel 25 i förordning (EU) 2018/1725 eller i enlighet med kapitel IX i den förordningen, i enlighet med Europaparlamentets och rådets förordning (EU) 2016/794 ([4]) eller i enlighet med rådets förordning (EU) 2017/1939 ([5]).

b) Om utövandet av dessa rättigheter och skyldigheter med avseende på de personuppgifter som erhålls från den behöriga myndigheten i en medlemsstat skulle kunna begränsas av den myndigheten på grundval av lagstiftningsåtgärder som avses i artikel 23 i Europaparlamentets och rådets förordning (EU) 2016/679 ([6]) eller enligt nationella bestämmelser som införlivar artiklarna 13.3, 15.3 eller 16.3 i Europaparlamentets och rådets direktiv (EU) 2016/680 ([7]).

([4]) Europaparlamentets och rådets förordning (EU) 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF (EUT L 135, 24.5.2016, s. 53).

([5]) Rådets förordning (EU) 2017/1939 av den 12 oktober 2017 om genomförande av fördjupat samarbete om inrättande av Europeiska åklagarmyndigheten (EUT L 283, 31.10.2017, s. 1).

([6]) 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) (EUT L 119, 4.5.2016, s. 1).

([7]) 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/RIF (EUT L 119, 4.5.2016, s. 89).

c) Om utövandet av dessa rättigheter och skyldigheter skulle undergräva kommissionens samarbete med länder utanför EU eller internationella organisationer om gemensamma cybersäkerhetshot.

Innan begränsningar tillämpas under de omständigheter som avses i första stycket, led a och b ska kommissionen samråda med EU:s berörda institutioner, organ, byråer eller myndigheter i medlemsstaterna om de möjliga skälen för att införa begränsningar och om bedömningen av nödvändigheten av begränsningarna och deras proportionalitet, såvida detta inte skulle undergräva kommissionens verksamhet och såvida det inte är uppenbart för kommissionen att tillämpningen av en begränsning föreskrivs i någon av de rättsakter som avses i dessa punkter eller att samrådet skulle undergräva syftet med kommissionens verksamhet enligt beslut (EU, Euratom) 2017/46.

Första stycket led c ska inte tillämpas om den registrerades intressen eller grundläggande fri- och rättigheter väger tyngre än kommissionens intresse av att samarbeta med länder utanför EU eller internationella organisationer.

4. Punkterna 1, 2 och 3 ska inte påverka tillämpningen av andra kommissionsbeslut om interna regler som styr tillhandahållande av information till registrerade och begränsningen av tillämpningen av vissa rättigheter enligt artikel 25 i förordning (EU) 2018/1725.

5. Alla begränsningar av rättigheter och skyldigheter enligt punkt 2 i denna artikel ska vara nödvändiga och stå i proportion till riskerna för de registrerades rättigheter och friheter.

6. En bedömning av nödvändigheten och proportionaliteten ska göras från fall till fall innan begränsningar tillämpas, och begränsningar ska inskränkas till vad som är absolut nödvändigt för att uppnå det avsedda syftet.

Artikel 3

Tillhandahållande av information till registrerade

1. Kommissionen ska på sin webbplats offentliggöra ett meddelande om skydd av personuppgifter som informerar alla registrerade om dess verksamhet som inbegriper behandling av personuppgifter när kommissionen fullgör sina uppgifter enligt beslut (EU, Euratom) 2017/46, inklusive en beskrivning av de kategorier av personuppgifter som berörs. När så är möjligt, och utan att it-säkerheten äventyras, ska kommissionen se till att de registrerade informeras individuellt på lämpligt sätt.

2. Om kommissionen, helt eller delvis, begränsar informationen till registrerade, vars personuppgifter behandlas i dess verksamhet i enlighet med förordning (EU, Euratom) 2017/46, ska den dokumentera och registrera skälen till begränsningen i enlighet med artikel 6 i det här beslutet.

Artikel 4

Registrerades rätt till tillgång till, radering av eller begränsning av databehandlingen

1. När kommissionen, helt eller delvis, begränsar de registrerades rätt till tillgång till, radering av eller begränsning av behandlingen av deras personuppgifter såsom avses i artiklarna 17, 19 och 20 i förordning (EU) 2018/1725 ska den informera den berörda registrerade i sitt svar på begäran om tillgång, radering eller begränsning av databehandling,

a) om den begränsning som tillämpas och om de huvudsakliga skälen till detta, och

b) om hur man kan inge klagomål till Europeiska datatillsynsmannen eller begära rättslig prövning vid Europeiska unionens domstol.

2. Kommissionen får skjuta upp, utelämna eller neka tillhandahållande av information av skälen till den begränsning som avses i punkt 1 om detta skulle undergräva begränsningens verkan.

3. Kommissionen ska dokumentera och registrera skälen till begränsningen i enlighet med artikel 6.

4. När rätten till tillgång helt eller delvis begränsas, kan de registrerade utöva sin rätt till tillgång genom att kontakta Europeiska datatillsynsmannen, i enlighet med artikel 25.6, 25.7 och 25.8 i förordning (EU) 2018/1725.

Artikel 5

Information till den registrerade om en personuppgiftsincident

När kommissionen begränsar den information som tillhandahålls en registrerad om en personuppgiftsincident, såsom avses i artikel 35 i förordning (EU) 2018/1725, ska kommissionen dokumentera och registrera skälen till begränsningen i enlighet med artikel 6 i detta beslut. Kommissionen ska överlämna dokumentationen till Europeiska datatillsynsmannen vid tidpunkten för anmälan av personuppgiftsincidenten.

Artikel 6

Dokumentation och registrering av begränsningar

1. Kommissionen ska dokumentera skälen till varje begränsning som tillämpas enligt detta beslut, inbegripet en hänvisning till den rättsliga grunden som tillämpas för begränsningen och en bedömning av nödvändigheten av begränsningen och dess proportionalitet, med beaktande av relevanta delar av artikel 25.2 i förordning (EU) 2018/1725.

2. I dokumentationen ska det anges hur den registrerades utövande av rättigheten skulle undergräva syftet med att tillhandahålla kommissionen it-säkerhet och säkerhetstjänster på it-området i linje med beslut (EU, Euratom) 2017/46 eller av begräsningar som tillämpas i enlighet med artikel 2.2 eller 2.3 i detta beslut, eller skulle inverka negativt på andra registrerades rättigheter och friheter.

3. Kommissionen ska registrera denna dokumentation och alla handlingar som innehåller underliggande faktiska och rättsliga omständigheter. Denna information ska på begäran ställas till Europeiska datatillsynsmannens förfogande.

Artikel 7

Begränsningarnas varaktighet

1. De begränsningar som avses i artiklarna 3, 4 och 5 ska fortsätta tillämpas så länge skälen för dem är fortsatt giltiga.

2. Om skälen för en sådan begränsning som avses i artiklarna 3, 4 och 5 inte längre är giltiga ska kommissionen

a) häva begränsningen,

b) informera den registrerade om de huvudsakliga skälen till begränsningen,

c) informera den registrerade om hur man när som helst kan inge klagomål till Europeiska datatillsynsmannen eller begära rättslig prövning vid Europeiska unionens domstol.

Artikel 8

Skyddsåtgärder och lagringsperioder

1. Kommissionen ska se över tillämpningen av de begränsningar som avses i artiklarna 3, 4 och 5 var sjätte månad efter deras antagande samt vid avslutandet av den enskilda it-säkerhetsverksamheten. Därefter ska kommissionen på årsbasis övervaka behovet av att behålla en eventuell begränsning.

I översynen ska ingå en bedömning av nödvändigheten av begränsningen och dess proportionalitet, med beaktande av relevanta delar av artikel 25.2 i förordning (EU) 2018/1725.

2. Kommissionen har antagit tekniska och organisatoriska åtgärder för att undvika oavsiktlig eller olaglig förstörelse, förlust, ändring, obehörigt röjande av eller obehörig åtkomst till personuppgifter som överförts, lagrats eller på annat sätt behandlats, såsom förvaltning av åtkomsträttigheter, backup-policy och andra åtgärder i enlighet med beslut (EU/Euratom) 2017/46.

3. Kommissionen ska registrera de tillämpliga lagringsperioderna i enlighet med den gemensamma bevarandeförteckningen för kommissionens akter och ska i sitt meddelande om skydd av personuppgifter göra de relevanta lagringsperioderna för denna behandling tillgängliga för de registrerade.

Artikel 9

Omprövning via kommissionens dataskyddsombud

1. Kommissionens dataskyddsombud ska utan onödigt dröjsmål underrättas när registrerades rättigheter begränsas i enlighet med det här beslutet. På begäran ska dataskyddsombudet ges tillgång till registret och alla handlingar som innehåller underliggande faktiska och rättsliga omständigheter.

2. Dataskyddsombudet får begära en översyn av begränsningarna och ska informeras om resultatet av den begärda översynen.

3. Kommissionen ska dokumentera dataskyddsombudets deltagande när de registrerades rättigheter begränsas i enlighet med det här beslutet.

Artikel 10

Ikraftträdande

Detta beslut träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Bryssel den 15 december 2021.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande