

Sammanfattning av Europeiska datatillsynsmannens yttrande om förslagen till två förordningar om inrättande av en ram för interoperabilitet mellan EU:s storskaliga informationssystem

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

(2018/C 233/07)

Dagens angelägna utmaningar när det gäller säkerhet och gränsförvaltning kräver en smartare användning av den information som de behöriga offentliga myndigheterna redan har tillgång till. Europeiska kommissionen har därför inlett en process för att skapa interoperabilitet mellan EU:s (befintliga och framtida) storskaliga informationssystem inom områdena migration, asyl och säkerhet. I december 2017 utfärdade kommissionen två förslag till förordningar som syftar till att inrätta en rättslig ram för interoperabilitet mellan EU:s storskaliga informationssystem.

Interoperabilitet kan – förutsatt att den genomförs på ett väl genomtänkt sätt och i full överensstämmelse med de grundläggande rättigheterna, inbegripet rätten till integritet och skydd av personuppgifter – vara ett användbart verktyg för att tillgodose legitima behov hos de behöriga myndigheter som använder sig av de storskaliga informationssystemen och för att bidra till utvecklingen av ett effektivt och ändamålsenligt informationsutbyte. Interoperabilitet är inte endast eller huvudsakligen ett tekniskt val, utan snarare ett politiskt val som kan ha djupgående rättsliga och samhällsliga verkningar som inte kan gömmas bakom påstått tekniska förändringar. EU-lagstiftarens beslut att göra de storskaliga it-systemen interoperabla kommer inte endast att ha en permanent och djupgående inverkan på deras struktur och deras sätt att fungera, utan kommer också att förändra det sätt på vilket rättsliga principer inom detta område hittills har tolkats och kommer därigenom att utgöra en ”punkt utan återvändo”.

Även om interoperabilitet kanske ursprungligen planerades endast som ett verktyg för att underlätta användningen av systemen, införs genom förslagen nya åtkomstmöjligheter och möjligheter att använda uppgifterna i de olika systemen, i syfte att bekämpa identitetsbedrägerier, underlätta identitetskontroller och rationalisera de brottsbekämpande myndigheternas åtkomst till informationssystem som inte är utformade för brottsbekämpning.

Genom förslagen kommer framför allt en ny centraliserad databas att skapas som kommer att innehålla information om miljontals tredjelandsmedborgare, inbegripet deras biometriska uppgifter. På grund av databasens storlek och karaktären av de uppgifter som kommer att lagras i den kan ett eventuellt dataintrång leda till allvarlig skada för ett potentiellt mycket stort antal personer. Om sådan information faller i fel händer, kan databasen bli ett farligt verktyg mot de grundläggande rättigheterna. Det är därför nödvändigt att upprätthålla starka rättsliga, tekniska och organisatoriska skyddsåtgärder. Särskild vaksamhet krävs också både när det gäller databasens syften och när det gäller användningsvillkor och användningsföreskrifter.

EDPS betonar i detta sammanhang vikten av att ytterligare klargöra omfattningen av problemet med identitetsbedrägerier bland tredjelandsmedborgare, i syfte att säkerställa att den föreslagna åtgärden är lämplig och proportionerlig. Möjligheten att söka i den centraliserade databasen för att underlätta identitetskontroller på medlemsstaternas territorium bör avgränsas närmare.

EDPS förstår att de brottsbekämpande myndigheterna behöver få tillgång till bästa möjliga verktyg för att snabbt identifiera gärningsmännen bakom terroristattentat och andra grova brott. Att underlätta de brottsbekämpande myndigheternas åtkomst till informationssystem som inte är utformade för brottsbekämpning (dvs. till information som erhållits av myndigheter för andra syften än brottsbekämpning), om så bara i begränsad utsträckning, är emellertid långt ifrån en obetydlig fråga ur ett grundläggande rättighetsperspektiv. Rutinmässig åtkomst utgör de facto ett allvarligt åsidosättande av principen om ändamålsbegränsning. EDPS uppmanar därför till att verkliga skyddsåtgärder ska upprätthållas för att skydda tredjelandsmedborgares grundläggande rättigheter.

EDPS vill slutligen betona att förslagen såväl rättsligt som tekniskt fogar ännu ett lager av komplexitet till de befintliga systemen, liksom till de system som fortfarande håller på att utarbetas, och att de exakta verkningarna är svåra att bedöma i detta skede. Denna komplexitet kommer att inverka inte endast på dataskyddet, utan också på styrningen och övervakningen av systemen. Det är svårt att i detta skede göra en fullständig bedömning av den exakta inverkan på de rättigheter och friheter som utgör själva grunden för EU-projektet. Av dessa skäl uppmanar EDPS till en bredare diskussion om framtiden för informationsutbytet inom EU, styrningen av det och på vilka sätt de grundläggande rättigheterna kan skyddas i detta sammanhang.

1. INLEDNING

1.1 Bakgrund

1. I april 2016 antog kommissionen sitt meddelande *Starkare och smartare informationssystem för gränser och säkerhet* ⁽¹⁾ och inledde därmed en diskussion om hur Europeiska unionens informationssystem bättre kan förstärka gränsförvaltningen och den inre säkerheten.
2. Som en uppföljning av meddelandet inrättade kommissionen i juni 2016 en expertgrupp för informationssystem och interoperabilitet. Expertgruppen fick i uppgift att ta itu med rättsliga, tekniska och operativa utmaningar i syfte att uppnå interoperabilitet mellan EU:s centrala system för gränser och säkerhet ⁽²⁾.
3. Expertgruppen lade först fram sina rekommendationer i en interimrapport i december 2016 ⁽³⁾ och därefter i en slutrapport i maj 2017 ⁽⁴⁾. EDPS uppmanades att delta i expertgruppens arbete och utfärdade ett uttalande om begreppet interoperabilitet inom området migration, asyl och säkerhet. Uttalandet finns med i expertgruppens slutrapport.
4. Med utgångspunkt i meddelandet från 2016 och expertgruppens rekommendationer förslög kommissionen en ny strategi för att göra alla EU:s centraliserade informationssystem för säkerhet, gränsförvaltning och migrationshantering driftskompatibla ⁽⁵⁾. Kommissionen meddelade sin avsikt att arbeta för inrättandet av en europeisk sökportal, en gemensam biometrisk matchningstjänst och en gemensam databas med identitetsuppgifter.
5. Den 8 juni 2017 välkomnade rådet kommissionens synpunkter och den föreslagna vägen för att uppnå interoperabilitet mellan informationssystemen senast 2020 ⁽⁶⁾. Den 27 juli 2017 inledde kommissionen ett offentligt samråd om interoperabilitet mellan EU:s informationssystem för gränser och säkerhet ⁽⁷⁾. Samrådet åtföljdes av en inledande konsekvensbedömning.
6. Den 17 november 2017 utfärdade EDPS, som ett ytterligare bidrag, ett diskussionsunderlag om interoperabiliteten mellan informationssystemen inom området med frihet, säkerhet och rättvisa ⁽⁸⁾. I detta dokument medgav EDPS att interoperabilitet – när den genomförs på ett väl genomtänkt sätt och i överensstämmelse med de centrala kraven på nödvändighet och proportionalitet – kan vara ett användbart verktyg för att tillgodose legitima behov hos de behöriga myndigheter som använder sig av de storskaliga informationssystemen och för att förbättra informationsutbytet.
7. Den 12 december 2017 offentliggjorde kommissionen två lagförslag (nedan kallade *förslagen*) avseende
 - Europaparlamentets och rådets förordning om inrättande av en ram för interoperabilitet mellan EU-informationssystem (gränser och viseringar) och om ändring av rådets beslut 2004/512/EG, förordning (EG) nr 767/2008, rådets beslut 2008/633/RIF, förordning (EU) 2016/399 och förordning (EU) 2017/2226 (nedan kallat *förslaget om gränser och viseringar*),
 - Europaparlamentets och rådets förordning om inrättande av en ram för interoperabilitet mellan EU-informationssystem (polissamarbete och rättsligt samarbete, asyl och migration) (nedan kallat *förslaget om polissamarbete och rättsligt samarbete, asyl och migration*).

⁽¹⁾ Meddelande från kommissionen till Europaparlamentet och rådet: *Starkare och smartare informationssystem för gränser och säkerhet*, 6.4.2017, COM(2016) 205 final.

⁽²⁾ Idem, s. 15.

⁽³⁾ *Interim report by the chair of the high-level expert group on information systems and interoperability set up by the European Commission* (interimsrapport från ordföranden för expertgruppen för informationssystem och interoperabilitet, inrättad av Europeiska kommissionen), december 2016, tillgänglig på: <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435>.

⁽⁴⁾ *Final report of the high-level expert group on information systems and interoperability set up by the European Commission* (slutrapport från expertgruppen för informationssystem och interoperabilitet, inrättad av Europeiska kommissionen), 11 maj 2017, tillgänglig på <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435>.

⁽⁵⁾ Meddelande från kommissionen till Europaparlamentet, Europeiska rådet och rådet av den 16 maj 2017 – *Sjunde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion*, COM(2017) 261 final.

⁽⁶⁾ Rådets slutsatser om vägen till ett förbättrat informationsutbyte och säkerställande av interoperabiliteten mellan EU:s informationssystem, 8 juni 2017: <http://data.consilium.europa.eu/doc/document/ST-10151-2017-INIT/sv/pdf>.

⁽⁷⁾ Det offentliga samrådet och konsekvensbedömningen finns på: https://ec.europa.eu/home-affairs/content/consultation-interoperability-eu-information-systems-borders-and-security_en.

⁽⁸⁾ https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf.

1.2 Syftena med förslagen

8. Förslagen syftar allmänt till att förbättra förvaltningen av Schengenområdets yttre gränser och bidra till Europeiska unionens inre säkerhet. För att uppnå detta kommer enligt förslagen en ram att inrättas för att säkerställa interoperabilitet mellan EU:s befintliga och framtida storskaliga informationssystem inom områdena gränskontroll, asyl och immigration, polissamarbete och rättsligt samarbete i brottmål.
9. De föreslagna interoperabilitetskomponenterna utgörs av följande:
 - Tre befintliga system: Schengens informationssystem (SIS), Eurodacsystemet och Informationssystemet för viseringar (VIS).
 - Tre föreslagna system som fortfarande håller på att utarbetas eller utvecklas:
 - Ett som EU-lagstiftarna nyligen har kommit överens om och som behöver utvecklas: in- och utresesystemet ⁽¹⁾.
 - Två som fortfarande är under förhandling: det föreslagna EU-systemet för reseuppgifter och resetillstånd (Etias) ⁽²⁾ och det föreslagna europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris-TCN-systemet) ⁽³⁾.
 - Interpols databas över stulna och förkomna resehandlingar.
 - Europols databaser ⁽⁴⁾.
10. Interoperabiliteten mellan dessa system säkerställs genom fyra komponenter, nämligen
 - en europeisk sökportal,
 - en gemensam biometrisk matchningstjänst,
 - en gemensam databas för identitetsuppgifter (CIR), och
 - en detektor för multipla identiteter (MID).
11. Den europeiska sökportalen är avsedd att fungera som en meddelandehanterare. Den är avsedd att utgöra ett enkelt gränssnitt som tillhandahåller snabba sökresultat på ett öppet sätt. Den kommer att göra det möjligt att samtidigt söka i de olika systemen med användning av identitetsuppgifter (både biografiska och biometriska). Slut-användaren kommer med andra ord att kunna utföra en enda sökning och erhålla resultat från alla de system i vilka han eller hon är bemyndigad att söka, i stället för att söka i varje enskilt system för sig.
12. Den gemensamma biometriska matchningstjänsten är ett tekniskt verktyg för att underlätta identifieringen av personer som kan ha registrerats i olika databaser. Den kommer att lagra mallar av de biometriska uppgifter (fingeravtryck och ansiktsbilder) som finns i EU:s centraliserade informationssystem (dvs. SIS, Eurodacsystemet, in- och utresesystemet, VIS och Ecris-TCN). Den kommer att göra det möjligt att dels samtidigt söka i de olika systemen efter biometriska uppgifter, dels jämföra dessa uppgifter.
13. CIR kommer att underlätta identifieringen av personer, även på medlemsstaternas territorium, och kommer också att bidra till att rationalisera de brottsbekämpande myndigheternas åtkomst till informationssystem som inte är utformade för brottsbekämpning. CIR kommer att lagra biografiska och biometriska uppgifter som har registrerats i VIS, Ecris-TCN, in- och utresesystemet, Eurodacsystemet och Etias. CIR kommer att lagra uppgifterna, logiskt åtskilda, enligt det informationssystem från vilket uppgifterna härrör.

⁽¹⁾ Europaparlamentets och rådets förordning av den 30 november 2017 om inrättande av ett in- och utresesystem för registrering av in- och utreseuppgifter och av uppgifter om nekad inresa för tredjelandsmedborgare som passerar medlemsstaternas yttre gränser, om fastställande av villkoren för åtkomst till in- och utresesystemet för brottsbekämpande ändamål och om ändring av konventionen om tillämpning av Schengenavtalet och förordningarna (EG) nr 767/2008 och (EU) nr 1077/2011 (EUT L 327, 9.12.2017, s. 20).

⁽²⁾ Förslag till Europaparlamentets och rådets förordning om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias) och om ändring av förordningarna (EU) nr 515/2014, (EU) 2016/399, (EU) 2016/794 och (EU) 2016/1624, COM(2016) 731 final, 16.11.2016.

⁽³⁾ Förslag till Europaparlamentets och rådets förordning om inrättande av ett centraliserat system för identifiering av medlemsstater som innehar uppgifter om fällande domar mot tredjelandsmedborgare och statslösa personer för att komplettera och stödja det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister (Ecris-TCN-systemet) och om ändring av förordning (EU) nr 1077/2011, COM(2017) 344 final, 29.6.2017.

⁽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).

14. MID är ett verktyg som kommer att göra det möjligt att länka identiteter i CIR och SIS och kommer att lagra länkar mellan uppgifter. MID kommer att lagra länkar som tillhandahåller information när en eller flera definitiva eller möjliga matchningar upptäcks och/eller när en falsk identitet används. MID kommer att kontrollera huruvida sökta uppgifter eller införda uppgifter förekommer i mer än ett av systemen i syfte att upptäcka multipla identiteter (dvs. samma biometriska uppgifter länkade till olika biografiska uppgifter eller samma/liknande biografiska uppgifter länkade till olika biometriska uppgifter). MID kommer att visa de biografiska identitetsuppgifter som har en länk i de olika systemen.
15. Förslagen syftar till att genom dessa fyra interoperabilitetskomponenter
 - ge bemyndigade användare snabb, smidig, systematisk och kontrollerad åtkomst till relevanta informationssystem,
 - underlätta identitetskontroller av tredjelandsmedborgare på medlemsstaternas territorium,
 - spåra multipla identiteter som används med samma biometriska uppgifter, och
 - rationalisera de brottsbekämpande myndigheternas åtkomst till informationssystem som inte är utformade för brottsbekämpning.
16. Enligt förslagen kommer dessutom en central databas för rapporter och statistik (CRRS) och ett universellt meddelandeformat (UMF) att inrättas och automatiska mekanismer för kontroll av uppgifternas kvalitet kommer att införas.
17. Offentliggörandet av två lagstiftningsförslag i stället för ett beror på behovet att ta hänsyn till skillnaden mellan system som rör
 - Schengenregelverket om gränser och viseringar (dvs. VIS, in- och utresesystemet, Etias och SIS, vilka regleras genom förordning (EG) nr 1987/2006),
 - Schengenregelverket om polissamarbete, eller system som inte är relaterade till Schengenregelverket (Eurodac-systemet, Ecris-TCN och SIS, vilka regleras genom rådets beslut 2007/533/RIF).
18. De två förslagen är "syskonförslag" och ska läsas tillsammans. Numreringen av artiklarna är i stort sett likadan i båda förslagen, liksom innehållet. När vi hänvisar till en viss artikel avses därför, om inte annat anges, nämnda artikel i båda förslagen.

5. SLUTSATSER

142. EDPS medger att interoperabilitet – när den genomförs på ett väl genomtänkt sätt och i överensstämmelse med de centrala kraven på nödvändighet och proportionalitet – kan vara ett användbart verktyg för att tillgodose legitima behov hos de behöriga myndigheter som använder sig av de storskaliga informationssystemen och för att förbättra informationsutbytet.
143. EDPS betonar att interoperabilitet inte huvudsakligen är ett tekniskt val, det är först och främst ett politiskt val som ska göras, med betydande rättsliga och samhällsliga verkningar under de kommande åren. Mot bakgrund av den tydliga trenden att blanda EU:s olika lagstiftningsområden och politiska mål (dvs. gränskontroller, asyl och immigration, polissamarbete och nu också rättsligt samarbete i brottmål) samt att rutinmässigt ge brottsbekämpande myndigheter åtkomst till informationssystem som inte är utformade för brottsbekämpning, kommer ett beslut av EU-lagstiftaren om att göra de storskaliga it-systemen interoperabla inte endast att ha en permanent och djupgående inverkan på deras struktur och deras sätt att fungera, utan kommer också att förändra det sätt på vilket rättsliga principer inom detta område hittills har tolkats och kommer därigenom att utgöra en "punkt utan återvändo". Av dessa skäl uppmanar EDPS till en bredare diskussion om framtiden för informationsutbytet inom EU, styrningen av det och på vilka sätt de grundläggande rättigheterna kan skyddas i detta sammanhang.
144. Även om förslagen, såsom de lagts fram, kan ge intrycket att interoperabilitet är den slutliga komponenten i redan fullt fungerande informationssystem (eller åtminstone system vilkas grundrättsakter redan är "stabila" och i slutskedet av lagstiftningsprocessen), önskar EDPS erinra om att detta inte är fallet. I realiteten är det så att tre av de sex EU-informationssystem som förslagen är avsedda att koppla samman inte ännu existerar (Etias, Ecris-TCN och in- och utresesystemet), två är för närvarande föremål för en översyn (SIS och Eurodac) och ett ska ses över senare i år (VIS). Att bedöma exakt hur ett så komplext system med så många "rörliga delar" kommer att inverka på integriteten och dataskyddet är så gott som omöjligt. EDPS erinrar om vikten av att säkerställa överensstämmelse mellan förslagen och de rättsakter som redan är (eller snart kommer att vara) föremål för förhandlingar, i syfte att säkerställa en enhetlig rättslig, organisatorisk och teknisk miljö för all verksamhet som innebär behandling av personuppgifter inom unionen. I detta sammanhang vill EDPS betona att detta yttrande inte påverkar ytterligare interventioner som kan följa när lagstiftningsprocessen kring de olika sammankopplade rättsinstrumenten går framåt.

145. EDPS noterar att även om interoperabilitet kanske ursprungligen planerades endast som ett verktyg för att underlätta användningen av systemen, införs genom förslagen nya åtkomstmöjligheter och möjligheter att använda uppgifterna i de olika systemen, i syfte att bekämpa identitetsbedrägerier, underlätta identitetskontroller och rationalisera de brottsbekämpande myndigheternas åtkomst till informationssystem som inte är utformade för brottsbekämpning.
146. EDPS betonar, liksom han redan gjorde i diskussionsunderlaget, vikten av att först ytterligare klargöra omfattningen av problemet med identitetsbedrägerier bland tredjelandsmedborgare, i syfte att säkerställa att den föreslagna åtgärden är lämplig och proportionerlig.
147. Vad gäller användningen av uppgifter i de olika systemen för att underlätta identitetskontroller på medlemsstaternas territorier, betonar EDPS att syftena med sådan användning, dvs. att bekämpa olaglig invandring och bidra till en hög säkerhetsnivå, är för brett formulerade och att syftena bör vara "strängt begränsade" och "noggrant avgränsade" i förslagen, i enlighet med praxis från Europeiska unionens domstol. Han anser särskilt att åtkomst till CIR för att fastställa en tredjelandsmedborgares identitet i syfte att säkerställa en hög säkerhetsnivå endast bör tillåtas när åtkomst för samma syften till liknande nationella databaser (t.ex. register över medborgare/i landet bosatta etc.) föreligger och på samma villkor. Han rekommenderar att detta tydliggörs i förslagen. I annat fall kan det förefalla som om det i förslagen fastställs en presumtion om att tredjelandsmedborgare per definition utgör ett säkerhetshot. Han rekommenderar även att det säkerställs att åtkomst till uppgifterna i syfte att identifiera en person under en identitetskontroll tillåts
- i princip, i närvaro av personen, och
 - om han eller hon är oförmögen att samarbeta och inte har några handlingar som fastställer hans eller hennes identitet, eller
 - vägrar att samarbeta, eller
- om det finns motiverade eller välgrundade skäl att tro att de handlingar som visas fram är falska eller att personen inte talar sanning om sin identitet.
148. EDPS förstår att de brottsbekämpande myndigheterna behöver få tillgång till bästa möjliga verktyg för att snabbt identifiera gärningsmännen bakom terroristattentat och andra grova brott. Det är emellertid inte godtagbart att verkliga skyddsåtgärder som införts för att skydda de grundläggande rättigheterna undanröjs huvudsakligen i syfte att skynda på ett förfarande. EDPS rekommenderar därför att det i artikel 22.1 i förslagen införs som villkor att rimliga skäl ska föreligga, att en föregående sökning i nationella databaser ska ha genomförts och att en sökning i övriga medlemsstaters system för automatisk identifiering av fingeravtryck ska ha inletts enligt beslut 2008/615/RIF, innan en sökning görs i den gemensamma databasen för identitetsuppgifter. EDPS anser dessutom att det alltid också ska kontrolleras att villkoren för åtkomst till begränsad information (exempelvis i form av träff/ingen träff) är uppfyllda, oavsett om vidare åtkomst medges till uppgifterna i det system som gav träffen.
149. EDPS anser att det tydligare bör visas att användningen av uppgifter som lagrats i Ecris-TCN för att upptäcka multipla identiteter och underlätta identitetskontroller är nödvändig och proportionerlig, och kräver också ett klargörande vad gäller dess förenlighet med principen om ändamålsbegränsning. Han rekommenderar därför att det i förslagen säkerställs att åtkomst till och användning av de uppgifter som lagrats i Ecris-TCN endast medges för de ändamål för vilka Ecris-TCN inrättats, vilka anges i rättsakten om dess inrättande.
150. EDPS välkomnar att förslagen syftar till att skapa en harmoniserad teknisk miljö för system som kommer att arbeta tillsammans för att tillhandahålla en snabb, smidig, kontrollerad och systematisk åtkomst till den information de olika aktörerna behöver för att utföra sina uppgifter. Han erinrar om att de grundläggande dataskyddsprinciperna bör beaktas i alla skeden av genomförandet av förslagen och rekommenderar följaktligen att det i förslagen införs en skyldighet för eu-LISA och medlemsstaterna att följa principerna om inbyggt dataskydd och dataskydd som standard.
151. Utöver de allmänna kommentarer och huvudsakliga problem som identifierats ovan lämnar EDPS ytterligare rekommendationer avseende följande aspekter av förslaget:
- Funktionaliteten hos den europeiska sökportalen, den gemensamma biometriska matchningstjänsten, CIR och MID.
 - Perioderna för lagring av uppgifter i CIR och MID.
 - Den manuella verifieringen av länkar.
 - Den centrala databasen för rapporter och statistik.

- Uppdelningen av roller och ansvarsområden mellan eu-LISA och medlemsstaterna.
 - Säkerheten hos interoperabilitetskomponenterna.
 - Rättigheterna för registrerade personer.
 - Åtkomsten för anställda vid eu-LISA.
 - Övergångsperioden.
 - Loggarna.
 - De nationella tillsynsmyndigheternas och EDPS roll.
152. Europeiska datatillsynsmannen är fortsatt tillgänglig för att ge ytterligare råd avseende förslagen, även vad gäller eventuella delegerade akter eller genomförandeakter som antas i enlighet med de föreslagna förordningarna och som kan ha en inverkan på behandlingen av personuppgifter.

Bryssel den 19 mars 2018.

Giovanni BUTTARELLI
Europeisk datatillsynsman
