

EUROPEISKA DATATILLSYNSMANNEN

Sammanfattning av Europeiska datatillsynsmannens yttrande om kommissionens meddelande "Att frigöra de molnbaserade datortjänsternas potential i Europa"

(Den fullständiga texten till detta yttrande finns på EN, FR och DE på Europeiska datatillsynsmannens webbplats <http://www.edps.europa.eu>)

(2013/C 253/03)

I. Inledning

I.1 Yttrandets syfte

1. Mot bakgrund av de molnbaserade datortjänsternas betydelse för det framväxande informationssamhället och den pågående politiska debatten inom EU om molntjänster har datatillsynsmannen beslutat att avge det här yttrandet på eget initiativ.

2. Detta yttrande är ett svar till kommissionens meddelande "Att frigöra de molnbaserade datortjänsternas potential i Europa" av den 27 september 2012 (nedan kallat "meddelandet")⁽¹⁾ där centrala åtgärder och beslut anges för att påskynda användningen av molnbaserade datortjänster i Europa. Datatillsynsmannen har rådfrågats informellt innan meddelandet antogs och har lämnat informella kommentarer. Datatillsynsmannen ser positivt på att hänsyn har tagits till vissa av hans kommentarer i meddelandet.

3. Med tanke på omfattningen av och tyngden i den pågående debatten om förhållandet mellan molntjänster och dataskyddets rättsliga ramar är dock inte yttrandet begränsat till de frågor som behandlas i meddelandet.

4. Yttrandet kretsar framför allt kring de utmaningar molntjänsterna medför för dataskyddet och hur de kan hanteras i förslaget till dataskyddsförordning (nedan kallad "förslaget till förordning")⁽²⁾. I yttrandet finns också synpunkter på de områden som enligt meddelandet kräver ytterligare åtgärder.

I.2 Bakgrund

5. Inom den allmänna politiska debatten i EU om molntjänster är följande händelser och dokument av särskild vikt:

— Efter att 2010 ha lagt fram sitt meddelande om en digital agenda för Europa⁽³⁾ höll kommissionen ett offentligt samråd om molntjänster i Europa mellan den 16 maj och den 31 augusti 2011 och offentliggjorde resultaten den 5 december 2011⁽⁴⁾.

— Den 1 juli 2012 antog artikel 29-gruppen⁽⁵⁾ ett yttrande om molnbaserade datortjänster (nedan kallat "artikel 29-gruppens yttrande")⁽⁶⁾ med en analys av hur gällande dataskyddsbestämmelser i direktiv 95/46/EG tillämpas på de leverantörer inom EES-området som tillhandahåller molnbaserade datortjänster och på deras kunder⁽⁷⁾;

— Den 26 oktober 2012 antog ombudsmännen för dataskydd och personuppgifter en resolution om molntjänster vid sin 34:e internationella konferens⁽⁸⁾.

⁽¹⁾ COM(2012) 529 final.

⁽²⁾ COM(2010) 11 final.

⁽³⁾ KOM(2010) 245 slutlig.

⁽⁴⁾ http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf

⁽⁵⁾ Artikel 29-gruppen är ett rådgivande organ som tillsatts i enlighet med artikel 29 i direktiv 95/46/EG. Gruppen består av företrädare för nationella tillsynsmyndigheter och datatillsynsmannen samt en företrädare för kommissionen.

⁽⁶⁾ Artikel 29-gruppens yttrande 05/2012 om molnbaserade datortjänster, finns på http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_sv.pdf

⁽⁷⁾ På nationell nivå har dessutom dataskyddsmyndigheter i flera medlemsstater tagit fram egna riktlinjer för molnbaserade datortjänster, till exempel i Italien, Sverige, Danmark, Tyskland, Frankrike och Storbritannien.

⁽⁸⁾ Resolution om molnbaserade datortjänster, antagen vid den 34:e internationella konferensen om dataskydd och skydd av personuppgifter i Uruguay den 26 oktober 2012.

I.3 Meddelande om molnbaserade datortjänster

6. Datatillsynsmannen välkomnar meddelandet. I meddelandet anges följande tre särskilda nyckelåtgärder som måste vidtas på EU-nivå för att följa och gynna användningen av molntjänster i Europa:

— Nyckelåtgärd 1: Bringa reda i standarddjungeln

— Nyckelåtgärd 2: Säkra och rättvisa avtals- och kontraktsvillkor

— Nyckelåtgärd 3: Inrätta ett europeiskt partnerskap för molntjänster som kan göra den offentliga sektorn till en drivkraft bakom innovation och tillväxt

7. Ytterligare politiska åtgärder anges också, till exempel insatser för att stimulera användningen av molntjänster genom att gynna forskning och utveckling eller informationskampanjer, liksom behovet av att med hjälp av en förstärkt internationell dialog hantera centrala teman i anslutning till molntjänster, däribland dataskydd, tillgång för rättsvårdande instanser, säkerhet samt tjänsteleverantörernas ansvar.

8. Dataskyddet omnämns i meddelandet som ett viktigt inslag för att användningen av molnbaserade datortjänster ska bli framgångsrika i Europa. I meddelandet konstaterar man ⁽¹⁾ att förslaget till förordning tar upp många av de problem som leverantörer och användare av molntjänster har rapporterat ⁽²⁾.

I.4 Yttrandets inriktning och struktur

9. Detta yttrande har tre mål.

10. Det första målet är att belysa betydelsen av personuppgiftsskydd och dataskydd i dagens diskussioner om molnbaserade datortjänster. Yttrandet betonar framför allt att dataskyddet i molntjänstmiljöerna inte får ha en lägre nivå än skyddet i andra databehandlingssammanhang. Rutiner för molnbaserade datortjänster kan bara utvecklas och tillämpas legalt om det finns garantier för att denna nivå på dataskyddet efterlevs (se avsnitt III.3). I yttrandet beaktas den vägledning som ges i artikel 29-gruppens yttrande.

11. Det andra målet är att ytterligare analysera de viktigaste utmaningarna som molntjänsterna innebär för dataskyddet i relation till förslaget till dataskyddsförordning, särskilt svårigheten att entydigt fastställa de olika aktörernas ansvarsområden och begreppen registeransvarig respektive registerförare. I yttrandet (framför allt i avsnitt IV) analyseras hur förslaget till förordning i dess nuvarande utformning ⁽³⁾ skulle kunna bidra till att garantera en hög nivå på dataskyddet i molnbaserade datortjänster. Det bygger därför på de synpunkter som datatillsynsmannen utvecklat i sitt yttrande över dataskyddsreformen (nedan kallat "tillsynsmannens yttrande över dataskyddsreformen") ⁽⁴⁾ och kompletterar det med att särskilt ta upp molntjänstmiljöerna. Datatillsynsmannen betonar att hans yttrande om dataskyddsreformen är fullt tillämpligt även på molntjänster och måste betraktas som en plattform för detta yttrande. Vissa av de frågor som tas upp där – till exempel hans analys av de nya bestämmelserna om den registrerades rättigheter ⁽⁵⁾ – är tillräckligt klargjorda och behandlas därför inte ytterligare i detta yttrande.

12. Det tredje målet är att fastställa områden inom data- och personuppgiftsskyddet som kräver ytterligare åtgärder på EU-nivå mot bakgrund av den molnstrategi som kommissionen lägger fram i meddelandet. Här ingår bland annat ytterligare vägledning, standardiseringsinsatser, ytterligare riskbedömningar för specifika sektorer (till exempel offentlig sektor), standardiserade kontraktsvillkor, internationell dialog om problem kring molntjänster och effektiva metoder för internationellt samarbete (ämnet utvecklas mer i avsnitt V).

⁽¹⁾ Se sidan 8 i meddelandet, avsnittet om "Digitala agendans åtgärder för uppbyggnad av det digitala förtroendet".

⁽²⁾ Begreppet "molnkunder" används överlag i detta yttrande för att beteckna kunder som agerar i egenskap av företag, och konsumenter som agerar i egenskap av enskilda slutanvändare.

⁽³⁾ Hänsyn bör tas till att förslaget till förordning för närvarande diskuteras i rådet och Europaparlamentet enligt det ordinarie lagstiftningsförfarandet.

⁽⁴⁾ Yttrandet finns på <http://www.edps.europa.eu>

⁽⁵⁾ Se datatillsynsmannens yttrande, framför allt punkterna 140–158.

13. Yttrandet har följande struktur: Avsnitt II innehåller en översikt över de molnbaserade datortjänsternas främsta egenskaper och tillhörande dataskyddsproblem. I avsnitt III granskas de mest relevanta inslagen i EU:s befintliga rättsliga ram och i förslaget till förordning. Avsnitt IV innehåller en analys av hur förslaget till förordning kan bidra till att bemöta de dataskyddsutmaningar som uppstår vid användningen av molnbaserade datortjänster. I avsnitt V analyseras kommissionens förslag till hur den politiska ramen kan utvecklas och fastställs områden där det kan krävas ytterligare insatser. Avsnitt VI innehåller slutsatserna.

14. Många av synpunkterna i detta yttrande gäller alla miljöer där molntjänster används men yttrandet behandlar inte specifikt EU-institutionernas eller EU-organens användning av molntjänster av det slag som omfattas av datatillsynsmannens övervakning enligt förordning (EG) nr 45/2001. Datatillsynsmannen kommer att lägga fram riktlinjer till dessa institutioner och organ i ärendet separat.

VI. Slutsatser

121. Enligt beskrivningen i meddelandet innebär molnbaserade datortjänster många nya möjligheter för företag, konsumenter och offentlig sektor vid hanteringen av data med hjälp av externa IT-resurser. Samtidigt medför tekniken många utmaningar, framför allt i fråga om lämplig nivå på skyddet av de uppgifter som behandlas i molnen.

122. Om kriterierna för tillämpligheten av EU:s dataskyddslagstiftning inte är tillräckligt tydliga och om molntjänstleverantörernas roll och ansvarsområden definieras eller betraktas i ett alltför snävt perspektiv – eller inte genomförs effektivt – så finns det en stor risk för att ansvaret vid molntjänstleverantörernas bearbetningar tunnans ut när molnbaserade datortjänster används. Datatillsynsmannen betonar att användningen av molnbaserade datortjänster inte kan motivera lägre dataskyddsnormer än de som är tillämpliga vid traditionell databehandling.

123. Dataskyddsförordningen skulle i det hänseendet och i sin nuvarande utformning bidra med många klagöranden och verktyg som kan bidra till att garantera att molntjänstleverantörerna ger en tillfredsställande nivå på dataskyddet, framför allt till kunder baserade i Europa.

- I artikel 3 förtydligas och breddas det territoriella tillämpningsområdet av EU:s dataskyddsbestämmelser så att även molnbaserade datatjänster omfattas.
- I artikel 4(5) införs ett nytt inslag i registeransvaret, det vill säga "villkor". Detta ligger i linje med den framväxande trenden som mot bakgrund av den IT-relaterade komplexiteten bakom tillhandahållandet av molntjänster visar att villkoren för när en molntjänstleverantör kan betraktas som registeransvarig måste breddas. Detta skulle bättre återspegla den rätta nivån av inflytande på databehandlingen.
- Med förslaget till förordning ökar ansvaret på och ansvarsskyldigheten för registeransvariga och registerförare genom införandet av särskilda skyldigheter, till exempel inbyggt uppgiftsskydd och uppgiftsskydd som standard (artikel 23), anmälan om personuppgiftsbrott (artiklarna 31 och 32) och konsekvensbedömning avseende uppgiftsskydd (artikel 33). Dessutom åläggs registeransvariga och registerförare att införa mekanismer för att visa att de införda dataskyddsåtgärderna är effektiva (artikel 22).
- Genom artiklarna 42 och 43 i förslaget till förordning kan internationella dataöverföringsmekanismer användas mer flexibelt för att hjälpa molnkunder och molntjänstleverantörer att återopa lämpliga dataskyddsgarantier vid överföringen av personuppgifter till datacenter eller servrar i tredjeland.
- Genom artiklarna 30, 31 och 32 i förslaget till förordning klagörs de registeransvarigas och registerförarnas skyldigheter ifråga om säker databehandling; även informationskrav vid eventuella dataintrång klagörs vilket utgör grunden för ett heltäckande och samarbetsinriktat synsätt på hur säkerheten i molnmiljön olika aktörer emellan ska hanteras.

- Genom artiklarna 55–63 i förslaget till förordning stärks samarbetet mellan tillsynsmyndigheter och deras samordnade övervakning av gränsöverskridande databehandling, vilket är särskilt viktigt i miljökring molnbaserade datortjänster.

124. Med tanke på molntjänsternas särskilda egenskaper föreslår datatillsynsmannen dock att följande aspekter ytterligare klargörs:

- Beträffande det territoriella tillämpningsområdet i förslaget till förordning föreslår datatillsynsmannen att artikel 3.2a ändras enligt följande: "utbudande av varor eller tjänster som innebär behandling av personuppgifter om sådana registrerade i unionen", eller att ett nytt led infogas där det specificeras att registerförare som är baserade utanför EU och behandlar personuppgifter om registrerade i unionen och som erbjuder tjänster till juridiska personer inom EU också ska omfattas av det territoriella tillämpningsområdet i förslaget till förordning.
- Begreppet "överföring" bör tydligt definieras, vilket datatillsynsmannens också påpekade i sitt yttrande över dataskyddsreformen.
- En särskild bestämmelse bör införas som klargör villkoren för när rättsvårdande myndigheter i länder utanför EES-området kan få tillgång till uppgifter som lagras via en molntjänst. Sådana bestämmelser kan också innehålla krav på att den som mottar en begäran om tillgång i särskilda fall ska informera och samråda med behörig tillsynsmyndighet i EU.

125. Datatillsynsmannen betonar också att ytterligare vägledning kommer att krävas från kommissionen och/eller tillsynsmyndigheter (framför allt via den framtida europeiska dataskyddsstyrelsen) i följande frågor:

- Klargöra vilka mekanismer som bör införas för att kunna kontrollera att dataskyddsåtgärderna i praktiken är effektiva.
- Hjälpa registerförare vid utnyttjandet av bindande företagsregler och med hur de kan följa tillämpliga krav.
- Ta fram bästa praxis i frågor som registeransvariga/registerförarens ansvar, lämpligt bevarande av uppgifter i molnmiljöerna, uppgiftsportabilitet och de registrerades utövande av sina rättigheter.

126. Datatillsynsmannen inser dessutom att uppförandekoder som utarbetas av branschen och godkänns av relevanta tillsynsmyndigheter kan vara ett användbart verktyg för att öka efterlevnaden och höja tilliten bland de olika aktörerna.

127. Datatillsynsmannen ger sitt stöd till att kommissionen i samråd med tillsynsmyndigheterna tar fram standarder för avtalsvillkor vid tillhandahållandet av molnbaserade datortjänster som uppfyller kraven på dataskydd, framför allt till

- att ta fram mallar för avtalsvillkor som ska infogas i affärsvillkoren vid erbjudanden om molnbaserade datortjänster,
- att utveckla gemensamma upphandlingsvillkor- och krav för den offentliga sektorn där hänsyn tas till att känsliga uppgifter ska behandlas,
- att formge ytterligare internationella dataöverföringsmekanismer till molnmiljöerna, särskilt genom att uppdatera nuvarande standardvillkor och lägga fram standardiserade avtalsvillkor för överföringen av data från registerförare i EU till registerförare utanför EU.

128. Datatillsynsmannen betonar att vederbörlig hänsyn måste tas till dataskyddskraven vid utvecklingen av standarder och certifieringssystem, framför allt

- att tillämpa principerna om inbyggt uppgiftsskydd och uppgiftsskydd som standard vid utvecklingen av nya standarder,
- att i standarderna integrera dataskyddskrav såsom begränsning av syfte och begränsning av lagring,
- att kräva att leverantörer ger sina kunder nödvändig information så att de kan göra en underbyggd riskbedömning och att de informerar om vilka säkerhetsåtgärder de har infört samt slår larm vid händelser som påverkar säkerheten.

129. Datatillsynsmannen betonar slutligen behovet av att ta itu med de utmaningar molnbaserade dator-tjänster medför på internationell nivå. Han uppmuntrar kommissionen att föra en internationell dialog kring de problem som uppstår kring molntjänsterna, däribland rättskipning och tillgång för rättsvårdande myndigheter, och föreslår att många av frågorna hanteras genom olika internationella eller bilaterala avtal, till exempel avtal om ömsesidigt bistånd och handelsavtal. Världsomfattande standarder bör tas fram på internationell nivå för att ange minimivillkor och principer för rättsvårdande myndigheters tillgång till uppgifter. Datatillsynsmannen stöder också att tillsynsmyndigheterna utvecklar verkningsfulla internationella samarbetsmetoder, framför allt sådana som handlar om molntjänster.

Utfärdat i Bryssel den 16 november 2012.

Peter HUSTINX
Europeiska datatillsynsmannen
