Expedierad via e-post 140619 / cs

9 b 5

Datainspektionen

Datum
2014-06-19

Diarienr
1858-2013

Personuppgiftsombudet Anna Trulsson
Anna.trulsson@msb.se

Samråd om detekteringstjänst

Ni har i begäran om samråd efterfrågat Datainspektionens synpunkter på en tjänst som Myndigheten för samhällsskydd och beredskap (MSB) har för avsikt att erbjuda olika aktörer som ett led i ett effektivt informationssäkerhetsarbete.

Datainspektionen lämnar följande synpunkter.

Bakgrund

Av er redogörelse i ärendet framgår bland annat följande.

MSB har för avsikt att erbjuda en detekteringstjänst som syftar till att förstärka organisationers möjligheter att identifiera, verifiera och utreda IT-säkerhetsincidenter orsakade av skadliga adresser och skadlig kod. Detekteringstjänsten kompletterar en organisations befintliga kommersiella IT-säkerhetslösningar i form av bland annat brandväggar, virusskydd och intrångsdetekteringssystem. Organisationerna får tillgång till detekteringstjänsten genom att teckna ett anslutningsavtal med MSB. Ett sådant avtal tecknas endast med organisationer som MSB bedömer ha ett tydligt behov av det fördjupade IT-säkerhetsstöd som detekteringstjänsten ger.

Inom ramen för detekteringstjänsten kommer olika typer av information att hanteras, däribland personuppgifter. De personuppgifter som man avser att behandla består i huvudsak av IP-adresser. Men det finns också ett önskemål om att lagra all den kommunikation som passerar en organisations brandvägg i en särskild databas för närmare analys då en IT-incident har konstaterats. Ni bedömer att respektive ansluten organisation är personuppgiftsansvarig för den behandling av personuppgifter som detekteringstjänsten aktualiserar och att MSB utgör personuppgiftsbiträde i dessa fall.

Utöver denna personuppgiftsbehandling behandlar MSB personuppgifter i form av IP-adresser i en särskild databas (i det följande MSB:s databas). MSB:s databas innehåller en sammanställning av identifierade och verifierade skadliga IP-adresser och skadlig kod som MSB får tillgång till genom bland annat de tekniska nätverk som CERT.se deltar i, egen analys och samarbetspartners. Ni har uppgett att MSB är personuppgiftsansvarig för behandlingen av personuppgifter i MSB:s databas.

Datainspektionens synpunkter

Myndigheter och organisationer behöver vidta olika organisatoriska och tekniska åtgärder till skydd för personuppgifter och annan information. Sett som en helhet framstår det dock som att den aktuella detekteringstjänsten inbegriper åtgärder som går långt utöver vad som normalt är påkallat utifrån myndigheters och organisationers egna behov. Detekteringstjänsten kan möjliggöra en omfattande och närgången kartläggning av enskildas förehavanden på Internet, till exempel enskildas kontakt med myndigheter. Tillåtligheten av en sådan tjänst är därför diskutabel.

För att kunna göra den proportionalitetsbedömning som det ytterst blir fråga om i detta fall måste behovet och de positiva effekterna av detekteringstjänsten vägas mot den förlust i integritetshänseende som tjänsten ger upphov till. Det kräver ingående kunskap om de närmare förutsättningarna för tjänsten i fråga. Datainspektionen kan på befintligt underlag inte bedöma vare sig tillåtligheten av tjänsten eller de lagringstider som ni önskat få bedömda i er samrådsbegäran. Inspektionen lämnar dock följande allmänna synpunkter på den aktuella tjänsten.

Såvitt Datainspektionen känner till finns det idag inte någon rättslig reglering som specifikt tar sikte på den behandling av personuppgifter som en detekteringstjänst av nu aktuellt slag ger upphov till, utan behandlingen måste i huvudsak prövas utifrån personuppgiftslagen. I förekommande fall måste också bestämmelser i särskild registerförfattning beaktas. Datainspektionen utesluter inte att en detekteringstjänst av den modell ni beskrivit går att förena med befintlig lagstiftning. Inspektionen vill dock flagga för några omständigheter som förefaller problematiska.

<u>Det finns osäkerheter kring informationsflödet och personuppgiftsansvaret</u>

Det är i och för sig en rimlig utgångspunkt att personuppgiftsansvaret för användningen av detekteringstjänsten ligger hos respektive organisation som väljer att använda sig av tjänsten och att MSB utgör personuppgiftsbiträde i dessa fall. Att en myndighet anlitar en utomstående part för att utföra behandling av personuppgifter för sin räkning är vanligt förekommande och fullt i linje med personuppgiftslagen.

Det kan dock ifrågasättas om detekteringstjänsten enbart har funktionen att tillgodose respektive organisations informationssäkerhetsbehov eller om den också har till uppgift att ge MSB ökad förmåga att utföra de uppgifter inom informationssäkerhetsområdet som följer av myndighetens instruktion. Det kan i så fall bli aktuellt att också betrakta MSB som personuppgiftsansvarig för den personuppgiftsbehandling som sker inom ramen för detekteringstjänsten. Om avsikten till exempel är att uppgifter om skadliga IP-adresser och skadlig kod som upptäcks med hjälp av detekteringstjänsten i en organisation ska tillfogas MSB:s databas ligger det nära till hands att betrakta MSB som personuppgiftsansvarig för denna behandling.

Ur integritetssynpunkt är det viktigt att det klart framgår för alla inblandade vem som är att betrakta som personuppgiftsansvarig i alla led av informationshanteringen. Det förefaller i detta fall finnas oklarheter kring placeringen av personuppgiftsansvaret, vilket innebär en risk för otillbörliga integritetsintrång.

Man måste också beakta de grundläggande kraven i 9 § personuppgiftslagen som gäller för all behandling av personuppgifter. Bland annat får behandlingen inte strida mot den så kallade finalitetsprincipen, som kommer till uttryck i 9 § punkten d) personuppgiftslagen. Principen innebär att personuppgifter inte får användas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Principen begränsar på ett påtagligt sätt möjligheterna att sprida personuppgifter mellan myndigheter, företag och organisationer.

Om en överföring av personuppgifter från en organisation till en annan inte direkt omfattas av de ursprungliga ändamålen ska det alltså prövas om ändamålet med behandlingen är oförenligt med de ursprungliga ändamålen. Enligt Datalagskommittén får vad som är oförenligt med de ursprungliga ändamålen bestämmas genom praxis och de mera preciserade regler som regeringen och Datainspektionen kan komma att utfärda. Det saknas dock närmare praxis och föreskrifter på området. Däremot har vissa uttalanden gjorts i utredningsbetänkanden. Socialdatautredningen har anfört följande i betänkandet Behandling av personuppgifter inom socialtjänsten (SOU 1999:109):

> Enligt utredningens uppfattning bör man vid denna "oförenlighetsprövning", hypotetiskt utgå från hur en registrerad typiskt sett (inte den registrerade i det enskilda fallet) skulle se på saken. Kommer man vid en sådan bedömning fram till att den registrerade rimligen måste räkna med att de insamlade uppgifterna också får behandlas för det nya ändamålet, kan det nya ändamålet inte anses vara oförenligt med det ursprungliga ändamålet. Detta är, menar utredningen, en rimlig utgångspunkt med tanke på syftet

> bakom EG-direktivet, dvs. att skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatlivet, i samband med behandling av personuppgifter. Vid sådant förhållande blir det fråga om en restriktiv tillämpning av bestämmelsen i 9 § första stycket d personuppgiftslagen och utrymmet för att behandla redan insamlade personuppgifter för andra ändamål blir följaktligen litet. (s. 160)

Enligt Datainspektionen finns det mot ovan angivna bakgrund anledning att uttrycka tveksamhet med ett eventuellt förfarande som innebär att trafikdata i form av IP-nummer som samlats in i en specifik myndighets verksamhet också sprids till och lagras hos MSB för det övergripande syftet att stödja och samordna samhällets informationssäkerhet.

Informationsskyldigheten är svår att uppfylla

Såvitt Datainspektionen kan förstå innebär detekteringstjänsten att den personuppgiftsansvarige organisationen samlar in och lagrar data som passerar till och från organisationens brandvägg. Sådana uppgifter får, i den mån de kvalificerar sig som personuppgifter, anses insamlade direkt från den registrerade enligt 23 § personuppgiftslagen.

Den personuppgiftsansvarige är under dessa förhållanden skyldig att i samband med insamlingen på eget initiativ informera de registrerade om behandlingen av uppgifterna. Det enda tillämpliga undantaget från informationsskyldigheten i dessa fall är om den registrerade känner till behandlingen i fråga (25 § personuppgiftslagen). Datainspektionen har i sina allmänna råd ansett att bestämmelsen innebär att information inte behöver lämnas om sådant som den registrerade kan förutsättas känna till.

En registrerad får normalt räkna med att en myndighet av verksamhets- och IT-säkerhetsskäl hanterar uppgifter om datatrafik som passerar till och från myndigheten. Den aktuella detekteringstjänsten innebär dock en omfattande och potentiellt integritetskänslig behandling av personuppgifter som en registrerad inte nödvändigtvis kan förutsättas känna till. Utgångspunkten bör därför vara att den personuppgiftsansvarige ska informera den registrerade om den aktuella behandlingen. Hur en myndighet rent faktiskt ska kunna uppfylla denna långtgående informationsskyldighet förefaller oklart.

Datainspektionen efterlyser en rättslig reglering

Personuppgiftslagens tillämpningsområde är vidsträckt och regleringen bygger till stor del på grundläggande principer. Det skapar i sig en otydlighet om de närmare gränserna för hur personuppgifter får hanteras inom ramen för den aktuella detekteringstjänsten. Både integritets- och rättsäkerhetsskäl talar därför för att en dylik presumtivt mycket integritetskänslig insamling och hantering av personuppgifter ges en särskild författningsreglering.

Med hänsyn till det integritetsskydd som var och en är tillförsäkrad gentemot det allmänna i 2 kap. 6 § andra stycket regeringsformen behöver integritetsskyddet lyftas fram särskilt vid utformningen av en sådan författningsreglering. Regelverket måste utformas så att det bedömda behovet och effektiviteten av åtgärderna står i rimlig proportion till intrånget i enskildas personliga integritet. Det förutsätter en noggrann och tydligt redovisad integritetsanalys. En sådan analys bör bland annat innehålla följande beståndsdelar:

1. En utförlig beskrivning av vilka slags uppgifter eller sammanställningar av information som kan komma att hanteras inom ramen för den aktuella detekteringstjänsten;
2. En redogörelse för de aktörer som är inblandade i den aktuella informationshanteringen;
3. En precisering av konkreta behov och ändamål för den behandling av personuppgifter som kan komma att aktualiseras;
4. En analys av hur åtkomsten till och hanteringen av personuppgifter är tänkt att ske. Vem behöver informationen? Vilken information rör det sig om och varför behövs den? Hur är åtkomsten till personuppgifter tänkt att ske?
5. En redogörelse för hur personuppgiftsansvaret är tänkt att se ut i alla led av informationskedjan;
6. En noggrann analys av hur länge personuppgifter behöver sparas inom ramen för detekteringstjänsten. Lagringstiderna måste ställas i förhållande till uppgifternas känslighet och de ändamål för vilka de behandlas;
7. En bedömning av om det finns anledning att avvika från bestämmelserna om information till de registrerade enligt personuppgiftslagen och hur ett sådant undantag i så fall bör utformas;
8. En beskrivning och analys av de integritetsrisker som är förknippade med den aktuella personuppgiftsbehandlingen.

Avslutande synpunkter

Synpunkterna ovan är några exempel på områden som behöver bli föremål för analys och godtagbara författningsförslag. Integritetsanalysen kan dock inte stanna där. Det krävs också bland annat en närmare analys av behovet av ändringar i offentlighets- och sekretesslagen och hur en detekteringstjänst av nu aktuellt slag förhåller sig till särskild registerförfattning.

Datainspektionen beklagar avslutningsvis att ni fått vänta så länge på svar i detta ärende.

Detta samrådsyttrande har beslutats av generaldirektören Kristina Svahn Starrsjö efter föredragning av juristen Oskar Öhrström. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom, enhetschefen Britt-Marie Wester och IT-säkerhetsspecialisten Mikael Ejner deltagit.

Kristina Svahn Starrsjö

Oskar Öhrström