dataskydd.net
ORG.NR 802495-4797 – HTTPS://DATASKYDD.NET – INFO@DATASKYDD.NET

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Justitiedepartementet
103 33 Stockholm

Malmö 2017-03-03

EU-kommissionens förslag COM(2017) 10 – om dataskydd i elektroniska kommunikationsnät

Dataskydd.net är en svensk ideell förening som arbetar för dataskydd och informationssäkerhet för privatpersoner i tekniska och juridiska miljöer. Vi kombinerar tekniskt och juridiskt kunnande med ett tydligt fokus på att hjälpa privatpersoner hävda sin rätt, och att hjälpa myndigheter och företag etablera sådana lösningar som medverkar till att privatpersoner kan hävda sin rätt. Vi har särskild fokus på den positiva inverkan av EU:s dataskyddslagstiftning på svenska förhållanden.

Vi har lagt upp det här dokumentet på följande sätt. Den första delen innehåller kommentarer på delar av EU-kommissionen som vi bedömer är otillräckliga eller missgynnande för konsumenten. Den andra delen innehåller sådana förändringar eller sådant bevarande av status quo som EU-kommissionen föreslagit som vi bedömer är gynnsamma för konsumenten, och som svenska regeringen bör försvara. I en sista tredje del förtydligar vi de tillägg och ändringar som vi föreslagit i dokumentets första del.

Brister i lagförslaget

Allmän brist.

EU-kommissionens förslag är starkt fokuserat på *konfidentialitet*, en av tre möjliga mätbara måttstockar för dataskydd och datasäkerhet. Dataskydd.net hade gärna sett ett starkare fokus även på *tillförlitlighet*, i bemärkelsen att en kommunikationstjänst eller kommunikationsnät ska fungera på det sätt ur säkerhets- och dataskyddssynpunkt som en konsument rimligen kan förvänta sig. EU-kommissionens tidigare förslag på en europeisk elektronisk kommunikationskod[1] saknar även den ett fokus på *tillförlitlighet* i ovanstående bemärkelse.

Jfr. EECC, Art. 2.22 samt Art. 40, som antingen förbiser tillförlitlighet, överlåter på tillsynsmyndigheter att definiera tillförlitlighet och i detta senare fall i sådana fall riskerar överlåta på en tillsynsmyndighet som *inte* arbetar med just marknadsfrågor, utan snarare krisförberedande frågor, att genomföra en sådan definition. Den sist nämnda omständighet medför en hög risk att konsumenters rättmätiga förväntningar på leverantörer av för konsumenterna viktiga tjänster inte kommer att tillvaratas.

Artikel 2.2.d.

Vi är bekymrade över detta utökade undantag för brottsbekämpande myndigheter från att respektera vissa grundläggande funktioner i elektroniska kommunikationstjänster som används av allmänheten i förhållande till tidigare EU-lagstiftning. Art. 11.1 lämnar redan utrymme för för sådana avvikelser från

[1] COM (2016) 590.

förordningens allmänna bestämmelser som är nödvändiga för att tillgodose det intresse som uttrycks i texten.

I den svenska kontexten gäller detta särskilt de brottsbekämpande myndigheternas redan innevarande och, av allt att döma, omfattande bruk av tekniker som tillåter dem att ”stjäla” en kommunikationstjänstleverantörs identitet (t. ex. med IMSI-catchers).[2] När eDataskyddsdirektivet nu blir en förordning, för att underlätta synergier mellan detta regelverk och den redan antagna dataskyddsförordningen, riskerar det här att medföra att polisen antingen utsätts för ännu ett obehagligt trauma (jfr. datalagring) om EU-domstolen skulle besluta att polisen inte får stjäla identiteter från operatörer (eventuellt med undantag för situationer då identitetsstölden föregåtts av föregående oberoende prövning), eller att både svenska marknadsaktörer (konsumenter och företag) och marknadsaktörer i andra EU-länder berövas ett rimligt skydd mot att brottsbekämpande myndigheter ägnar sig åt identitetsstölder i elektroniska kommunikationsnät.

Notera att EU-domstolen i sitt utlåtande om datalagring från december 2016[3] hänvisat både till praxis från Europadomstolen[4] och till EU:s stadga för grundläggande mänskliga rättigheter. Direktiv (EU) 2016/680 om personuppgiftsbehandling i de brottsbekämpande myndigheternas verksamhet bör redan innebära att polisens och åklagarmyndighetens hantering av personuppgifter faller under EU:s stadga, och Europakonventionen är inskriven i svensk grundlag. Att skapa breda undantag för polisiära syften i eDataskyddsförordningen är alltså av mycket begränsad nytta för både EU och Sverige är redan bundna av andra dokument än den föreslagna förordningen som förhindrar att polisen kan efterfråga eller använda sig av generella datalagringsmetoder.

Vi föreslår att undantaget begränsas till sådana interaktioner mellan de brottsbekämpande myndigheter och elektroniska kommunikationstjänster som inte har tydligt lagstöd genom någon annan lag, till exempel genom att lägga till “*..., to the extent that such activities are otherwise regulated;*” i slutet av artikel 2.2.d.

Artikel 6.1.b

Det är mycket dåligt för konsumenter och för näringsidkare som är beroende av elektroniska kommunikationstjänster att innehållet i deras kommunikation (själva meddelandena och budskapen i kommunikationen enligt definitionen av *data från elektronisk kommunikation* i förordningens art. 4.3.a) går att bevara, utan privatpersonens eller näringsidkarens samtycke, med hänvisning till säkerhet. Säkerhet är ett ökänt flytande och föränderligt mål vars elasticitet i det här fallet lånar sig till att försätta den ekonomiskt beroende parten – kommunikationstjänstkunden - i en utsatt ställning gentemot den ekononiskt starka parten – kommunikationstjänstleverantören. Det är mycket osannolikt att någon tillsynsmyndighet kommer att kunna tillse hur den här bestämmelsen efterlevs på ett sådant sätt som balanserar förhållandet mer till den beroende partens fördel. Eftersom hotbilden inom IT-säkerhet ofta omtalas som att den förändras varje vecka, kan den starkare parten helt enkelt hitta på nya hotbilder i en sådan

[2] *Jfr*. Markus Naarttijärvi, Swedish police implementation of IMSI-catchers in a European law perspective, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.07.006

[3] ECLI:EU:C:2016:970.

[4] Zakharov mot Ryssland (Application no. 47143/06) och Szabo och Vissy mot Ungern (Application no. 37138/14).

rasande takt att ingen meningsfull maktbalans kan uppstå.

Vi föreslår att denna artikel flyttas till Art. 6.2, varigenom det förtydligas att bara metadata från elektronisk kommunikation (Art. 4.3.c) kan bevaras av säkerhetsskäl. Vi vill också påtala att detta inte förhindrar att kommunikationstjänster använder samtyckesbasen i Art. 6.3.b för att med de beroende parternas samtycke behandla innehållet i kommunikationen av specificerade säkerhetsskäl.

Artikel 7.3

Den engelska språkversionen av EU-kommissionens förslag innebär ett starkt försvagande av privatpersoners rätt till dataskydd jämfört med gällande lagstiftning. Privatpersoner har inga realistiska möjligheter att kontrollera om eller invända mot att en operatör eller annan elektronisk kommunikationsoperatör (vidare definition sedan EECC-förslaget) sparar trafikuppgifter som krävs för abonnentfakturering och betalning av samtrafikavgifter under betydligt längre tidsperioder än vad som krävs för att fakturan ska kunna utställas eller betalning krävas in. Vi föreslår att man bevarar samma bestämmelser som idag och kompletterar den svenska texten med ordet *bara* efter ordet *får*.

Artikel 8.1.d

Det är oklart varför artikel 8.1.b inte redan täcker detta fall. Dataskydd.net motsätter sig att *mätning av webbpublik* skulle utgöra någonting så speciellt och viktigt att konsumenter inte själva ska ges möjlighet att ta ställning till om de bidrar till sådan mätning. Konsumenter har ingen skyldighet att hjälpa apputvecklare, kommunikationstjänstutvecklare eller programmerare med dessa tre gruppers yrkesutövande.

Som ett positivt motexempel vill vi anföra Mozilla Corporations webbläsare för mobiler, som ger nya användare ett tydligt val om man vill bidra med statistik och rapporter om webbläsarhälsa, krascher och dylikt för att hjälpa Mozilla med vidareutvecklingen av deras produkter. Företag som vill göra *mätningar av webbpublik* kan rimligen med motsvarande inställningsfunktionaliteter ge användare ett val.

Ingen skyldighet att bli mätt

Att det är lätt att genomföra mätningar av webbpublik samtidigt som det är svårt för webbpubliken att förstå eller förhindra att den blir mätt kan ha medfört en falsk uppfattning att privatpersoner som ingår i en webbpublik har en skyldighet att bli mätt. Detta är uppenbarligt orimligt att förutsätta.

Artikel 10.

Dataskydd.net är mycket bekymrade över att EU-kommissionen tagit bort presumtionen att *dataskydd som standard* (privacy-by-default) i själva verket inte ska vara standard. Vi föredrog formuleringen som fanns i en påstådd läcka av förordningen som publicerades av tidskriften Politico i december 2016, och som utgick ifrån att tjänster och produkter ska ha dataskydd som standard.

Elektroniska kommunikationstjänster mer än andra tjänster skapar förutsättningar för andra tjänster att på ett enkelt sätt som möjligt upprätthålla konfidentialitet, tillförlitlighet och dataskydd. Standardisering och tydliga standardiseringsmandat uppmuntrar konkurrens, teknisk utveckling och, i det innevarande fallet, ett starkt dataskydd.

De tidigare erfarenheterna av EU-lagstiftning om standardisering och dataskydd (till exempel art. 3.3.e i Direktiv 2014/53/EU (RED)) visar tydligt att det inte räcker att man öppnar för möjligheten att tillsynsmyndigheter någon gång skulle kunna ta ett initiativ om någon näringslivsaktör orkar initiera det paneuropeiska lobby-projekt det innebär att få med sig tillräckligt många sådana myndigheter för att eventuellt så småningom upprätta någon sorts utredande

Nej till Nja!

Nja-linjen kring dataskydd skadar allas intressen. Det orsakar höga kostnader, stor ekonomisk och juridisk osäkerhet, det underminerar meningsfull tillsynsverksamhet, minskar möjligheten till förutsägbarhet för konsumenter och ger en fördel till andra regioner i världen som kanske inte på samma sätt försöker äta och ha kakan kvar samtidigt.

kommitté på EU-kommissionens direktorat för industrifrågor. Ett tydligt mandat i artikel 10 skulle ge tillsynsmyndigheterna klarhet över sina befogenheter och möjlighet att agera på desamma, konsumenter skulle få en tydligare bild av vad de kan förvänta sig för standard, och näringslivsaktörerna slipper hamna i situationen att de bara jagar efter en affärsmodell och som eftersläntrare implementerar standarder som utvecklas i USA och i Kina. "Nja-linjen" till dataskydd orsakar i det här fallet bara höga byråkratiska och juridiska kostnader och osäkerhet, utan att ge några uppenbara fördelar. Det ligger inte i Sveriges intresse att gulla med EU-kommissionen när den velar.

Artikel 16.4

Telefonförsäljning har varit föremål för klagomål under flera årtionden och de nuvarande självregleringssystemen (NIX-Telefon) har gång på gång visats fungera så pass dåligt att Konsumentverket nu avbrutit sitt samarbete med registret.[5] I frånvaron av några som helst incitament för telefonförsäljningsindustrin att självreglera behövs lagstiftning. Det här är inte rätt tillfälle att på den europeiska nivån permanenta ett redan dåligt fungerande system, som sedan kommer bli än svårare för lagstiftare att förändra. EU-kommissionen motiverar dessutom bestämmelsen med att det inte finns någon kostnad för konsumenter av telefonförsäljning (föreslaget skäl 36). Åratal av frustrerade postningar på sociala medier, klagomål i hushåll och arga insändare borde indikera att det i alla fall finns en kostnad i att många blir störda.

Bra delar i förslaget

Artikel 4.3.c

Dataskydd.net stödjer införandet av en särskilt definition för metadata (data om data).

Artikel 8.

Dataskydd.net tror att förtydligandena i denna artikel är av nytta för privatpersoner och konsumenter. Det är tyvärr fortfarande inte klart hur eller om ansvariga tillsynsmyndigheter kan utarbeta riktlinjer eller delta i standardiseringsprocesser.

Artikel 15.

Dataskydd.net är mycket positiva till att EU-kommissionen föreslår en begränsning av spridningen av identitetsuppgifter på ett sådant sätt att bara frivilliga fysiska eller juridiska personer behöver ingå i sådana allmänt tillgängliga förteckningar. Lättillgängliga identitetsuppgifter möjliggör telefon-phiske, nät-phiske, bedrägerier och identitetsstöld. Att förlita sig enbart på polisens möjlighet att verka avskräckande på sådana verksamheter, genom att till exempel utöka brottskatalogen, tror inte Dataskydd.net är en tillräcklig åtgärd för att skydda svenska privatpersoner och småföretagare. Det är helt enkelt för lätt idag för den som vill göra dumma saker att hitta rätt information för vara framgångsrik med dumheten.

Skydd mot ID-kapning och bedrägeri!

Informationssäkerhet för enskilda privatpersoner, eller privatpersoner som agerar genom till exempel egen firma, behöver inte vara komplicerat. Men det kräver perspektiv på de olika sätt identitetsuppgifter kan missbrukas av aktörer med ont uppsåt.

[5] Konsumentverket, *KO har ordet: Branschens egenåtgärder räcker inte – lagändring krävs*, 7 februari 2017.

ARTIKEL 16.5

Dataskydd.net välkomnar EU-kommissionens krav på ett förtydligande av bestämmelserna om berättigade intressen i förhållande till marknadsföring.

ARTIKEL 17

Dataskydd.net är mycket positiva till att konsumenter ges tillräckligt med information för att utvärdera leverantörer ur säkerhetssynpunkt.

ARTIKEL 18

Dataskydd.net är mycket positiva till att man fokuserar tillsynsverksamheten till samma myndighet som ansvarar för dataskyddsfrågor i övrigt. Vi hoppas att det är en sorts lagstöd för samarbete mellan myndigheter som kan inkludera kontaktvägar även mellan konsumentmyndigheter och tillsynsverksamheten.

Sammanfattning av ändringsyrkanden

Art. 2.2.d activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;	Art. 2.2.d activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, to the extent that such activities are otherwise regulated;

SKÄL: Detta säkerställer att brottsbekämpande myndigheter bara kan interferera med säkerheten, konfidentialiteten, tillförlitligheten eller tillgängligheten i elektroniska kommunikationstjänster och elektroniska kommunikationsnät i den utsträckning det finns lagstöd för sådana åtgärder. Förslaget är rimligt både i Sverige och i EU i stort, och ökar det europeiska regelverkets förmåga att stå emot instabila administrationers på lokal nivå i unionen samtidigt som det inte begränsar de brottsbekämpande myndigheternas befogenheter utifrån en rimlig definition av rättssäkerhetsbegreppet.

Art. 6.1.b Providers of electronic communications networks and services may process electronic communications data if: /.../ ~~it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.~~	(Flytta till ->) Art. 6.2.d (NY!) Providers of electronic communications services may process electronic communications metadata if: /.../ it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.

SKÄL: Det här säkerställer att leverantörer av elektroniska kommunikationstjänster med hänvisning till omständigheter som är snabbt föränderliga och långt bortanför kundernas och tillsynsmyndigheternas rimliga förmåga till kontroll, inte kan kränka konfidentialiteten för innehållet i elektronisk kommunikation. Om en leverantör av elektroniska kommunikationstjänster vill tillhandahålla tjänster till sina kunder som innebär att innehållet i elektronisk kommunikation måste granskas å kundens vägnas, finns alla möjligheter att göra detta med kundens samtycke. Presumtionen för kunderna måste vara att lagstiftningen garanterar rätten till konfidentiell kommunikation så som angiven i den föreslagna förordningen Art. 5.

Art. 7.3 ~~Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.~~	Art. 7.3 Electronic communications metadata processed for the purpose of billing in accordance with point (b) or Article 6(1), is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

SKÄL: Denna text speglar lydelsen av Art. 6.2 i direktiv 2002/58/EU, konsoliderad version efter förändringarna som genomfördes genom direktiv 2009/136/EU. Genom att bevara de redan befintliga rättigheterna försvagas inte privatpersoners rättigheter när direktivet blir till förordning. Teleoperatörer har ingen gudagiven rätt att konkurrera med leverantörer av mobila operativsystem och mobilappar, och särskilt är det underligt om lagstiftaren ger dem möjlighet att försöka konkurrera med sådana leverantörer genom att slippa bry sig om ifall konsumenterna vill ha deras tjänster.

Art. 8.1.d The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: /.../ (d) ~~if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end- user.~~	Art. 8.1.d TA BORT

SKÄL: En användare/konsuments av en tjänst för informationssamhället har ingen skyldighet att bli mätt eller på något annat sätt bidra till att tjänsten kan förbättras eller konsumentens beteende kartläggas. Tillhandahållare av tjänster för informationssamhället bör istället försöka erhålla konsumentens samtycke enligt Art. 8.1.b, till exempel genom att erbjuda konsumenten att bidra till produktens förbättring.

Art. 10	Art. 10
1. ~~Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.~~	1. The settings of all the components of the terminal equipment placed on the market shall be configured to, by default, prevent third parties from storing information, processing information already stored in the terminal equipment and preventing use by third parties of the equipment's processing capabilities.
2. ~~Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.~~	2. Software placed on the market permitting electronic communications, including the retrieval and presentation of information from the Internet or the Web, shall be configured to prevent third parties from storing information on the terminal equipment of the end-user or processing information already stored on that equipment by default.
3. ~~In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.~~	3. Supervisory authorities should have the capacity and authority to interact with standard setting organisations, including such standard setting as is made possible under directive 2014/53/EC, to ensure that they can effectively supervise and facilitate adherence to data protection by default principles.

SKÄL: I en tidig läcka, publicerad av tidningen Politico i december 2016, förekom den alternativa formuleringen av artikel 10 som här återges med ett tillägg om tillsynsmyndighetens möjlighet att interagera med standardorganisationer. De presumtivt tidigare formuleringarna av Art. 10(1) och Art. 10(2) har fördelarna att de är teknikneutrala, tydliga, och möjliga att tillse. I kommissionens faktiskt föreslagna Art. 10 har den teknikneutrala tydligheten bytts ut mot vad som förefaller vara en manual för att installation av något vanligare konsumentoperativsystem för hemdatorer. För att motivera vårt egna tillägg i Art. 10(3), är det ett sedan länge känt problem att europeiska tillsynsmyndigheter inte har kapaciteten eller förmågan att interagera med standardorgan på ett sätt som är meningsfullt för både medborgarna och de andra deltagarna i sådana organ. Det här öppnar möjligheten för en tillsynsmyndigheten att säga både A och B, istället för att säga A och sedan strosa iväg.

Recital 36. ~~Voice-to-voice direct marketing calls that do not involve the use of automated calling and communication systems, given that they are more costly for the sender and impose no financial costs on end-users. Member States should therefore be able to establish and or maintain national systems only allowing such calls to end-users who have not objected.~~ Art. 16.4 ~~Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications.~~	Recital 36 TA BORT Art. 16.4 TA BORT

SKÄL: Självregleringen av telefonförsäljning har fungerat väldigt dåligt och skapar varje år massor med irritation, huvudbry eller direkta problem för både småföretagare och privatpersoner. Att småföretagare och privatpersoner inte betalar för att ta emot ett telefonsamtal, innebär inte att telefonsamtalet inte orsakar en kostnad i form av förlorad arbetstid, ökad stress eller bara irritation. Att det är så lätt att utsätta privatpersoner för ofrivillig telefonreklam och telefonförsäljning gör att legitim telefonreklam och telefonförsäljning får ett mer negativt rykte än vad det skulle ha om konsumenter alltid upplevde att det var tydligt vem de hade godkänt får ringa dem med kommersiella budskap. Kravet på föregående samtycke i artikel 16.1 borde alltså vara tillräckligt.