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

Lund 2015-11-04

Skrivelse till riksdagen angående dom i mål nr 1356-14

Delning av personuppgifter mellan Försäkringskassan och socialnämnder

Hej ledamot i Konstitutionsutskottet,

Tidigare i år har Dataskydd.net kontaktat dig för att anmärka på vissa brister i regeringens proposition 2015/16:28 om behandling av personuppgifter och regleringen av id-kortsverksamheten hos Skatteverket, regeringens propositon 2014/15:143 om ändringar i lagen om vägtrafikregister och regeringens proposition 2014/15:148 om en ny domstolsdatalag. Dataskydd.net:s invändningar har nu aktualiserats av en ny dom från Högsta förvaltningsdomstolen (HFD)[1]. HFD har uttalat att begreppet "direktåtkomst" bara omfattar allmänna handlingar. Denna omdefinition av begreppet direktåtkomst tar bort många av de specifika krav på teknisk säkerhet vid dataöverföringar som lagstiftaren tidigare föreställt sig. HFD:s dom flyttar spridning av uppgifter från regler om direktåtkomst till den allmänna regleringen om säkerhet under 31§ Personuppgiftslagen (PUL). Där anges att "lämpliga tekniska och organistoriska säkerhetsåtgärder ska vidtas" för att skydda de uppgifter som behandlas och sprids.

Dom i mål nr 1356-14, HFD.

För det första är Dataskydd.net positiva till att man förenklar lagstiftningen om databehandling. Specialregleringen av direktåtkomst har i många fall inneburit svårbegriplig och mångfaldig lagstiftning, som ställer sinsemellan olika krav på de IT-system som utvecklas och gör det svårt för både myndigheter och privatpersoner att i fall från fall hålla isär vad som gäller.

HFD:s dom accentuerar dock behovet av en bättre transparens kring IT-system i Sverige. Det är till exempel olyckligt att särskilda skyddskrav bara formuleras för sådana IT-system som behandlar offentligt material. Rimligen bör myndigheterna skydda sekretessbelagt material på ett mer stringent sätt än det ej sekretessbelagda materialet skyddas. Samtidigt har lagstiftaren sällan har de tekniska kunskaper och praktiska erfarenheter som krävs för att förutspå vilken sorts säkerhetsproblem som kan uppstå i ett IT-system. Den detaljreglering av säkerhetskrav som "direktåtkomst" medfört har inneburit att IT-system binds till vissa funktionaliteter som inte nödvändigtvis är annat än juridiskt ändamålsenliga.

Dataskydd.net har tidigare framhållit vikten av individcentrisk incident- och sårbarhetsrapportering - information riktad till privatpersoner som berörs av ett säkerhetsproblem då säkerhetproblemet upptäcks. Vi har också förespråkat ett krav på samtycke inför spridning av uppgifter mellan myndigheter för att underlätta privatpersoners förståelse för hur data sprids mellan olika IT-system i myndighetsvärlden. Om privatpersoner, både i egenskap av individer och i egenskap av allmänheten, inte får reda på eller kan tillgodogöra sig information

[1] Se http://www.hogstaforvaltningsdomstolen.se/Om-Hogsta-forvaltningsdomstolen/Nyheter-fran-Hogsta-forvaltningsdomstolen/Dom-i-mal-om-personuppgiftslagen/

om tekniska och organisatoriska säkerhetsåtgärder på myndigheter, har de i praktiken inga möjligheter att verifiera att deras rättigheter faktiskt skyddas på det sätt lagen kräver. 31§ PUL är i dagsläget ett betydligt svagare skydd än specialregleringen om direktåtkomst i bemärkelsen att det är svårt om inte omöjligt att säkerställa dess efterlevnad.

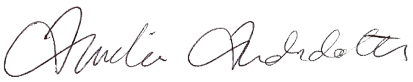
Datainspektionen har bara knapphändig praxis kring 31§ PUL. Privatpersoner har inga möjligheter att utvärdera tekniska och organisatoriska åtgärder hos myndigheter. I flera förslag det senaste året har Justitiedepartementet drivit på för att myndigheter ska förhindras från att lämna ut information till privatpersoner som låter dem uppskatta huruvida de tekniska och organisatoriska åtgärderna hos myndigheten alls har förutsättning att uppfylla kraven i 31§ PUL. I grunden verkar ligga en bevisligen felaktig föreställning om att öppenhet kring säkerhetsåtgärder är dåligt. I förslaget om en ny domstolsdatalag föreslås ett regelrätt förbud mot att informa om säkerhetsåtgärder (Proposition 2014/15:148, §12) och detta återkommer i utredningen om en ny myndighetsdatalag (SOU 2015:39, förslagen §23, s. 42). Av förhoppningsvis uppenbara skäl omöjliggör sådana bestämmelser för privatpersoner att utkräva ansvar av myndigheter som inte följer kraven i 31§ PUL. Vidare saknas möjligheter för privatpersoner att kräva skadestånd om myndigheter bryter mot bestämmelserna.

Dataskydd.net har samlat omfattande material om nyttan av transparens och öppenhet kring säkerhetsåtgärder i näringslivet och från forskningen i sina remissyttranden på utredningarna om en ny säkerhetsskyddsförordning (SOU 2015:25) och om en informationssäkerhetsstrategi (SOU 2015:23). Se https://dataskydd.net/vara-remissvar

Ju fler tjänstemän som i sin arbetsvardag använder säkerhetsmässigt undermåliga tekniska och organisatoriska lösningar för att göra sitt jobb, desto svårare är det att skapa en motivation till att förändra de undermåliga lösningarna. Justitiedepartementet förslag och HFD:s dom spelar sådan förändringsovilja i händerna om inte riksdagen tar initiativ till bättre transparens mot privatpersoner angående säkerhetsåtgärder.

Dataskydd.net har i remissyttranden på utredningen om informations- och cybersäkerhet i Sverige (SOU 2015:23)[2] och utredningen om personuppgiftsbehandling på utlännings- och medborgarskapsområdet[3] gjort mer utförliga resonemang om meriterna med individcentrisk incident- och sårbarhetsrapportering och samtycke.

Bättre transparens kring datahantering och dataspridning, samt en grundläggande princip att individen själv måste ges effektiva medel att tillgodose de rättigheter individen har i lag, är grundpelare i den europeiska dataskyddsrätten. Detta har bekräftats av EU-domstolen vid ett antal uppmärksammade rättsfall de senaste åren, och är också grunden för EU-kommissionens förslag om en ny dataskyddsförordning från 2012.



Amelia Andersdotter
Ordförande, Dataskydd.net

[2] https://dataskydd.net/nyheter/2015/09/11/dataskyddnet-lamnar-remissyttrande-pa-sou-201523-om-informationssakerhet
[3] https://dataskydd.net/nyheter/2015/09/30/dataskyddnet-lamnar-remissyttrande-pa-sou-201573-om-personuppgiftsbehandling-pa