2021-03-23 Personuppgiftshantering: Schrems II och skolans molntjänster

Frågor från chatten

Vi publicerar presentationerna efter seminariet på webbplatsen: www.skolfederation.se under respektive seminarie.

https://www.skolfederation.se/2021-03-23-personuppgiftshantering-schrems-ii/

- Spelar det någon roll om lagring sker inom EU/EES även om det är en amerikansk molntjänst?

Jurist svarar: Nej det gör det tyvärr inte.

Jurist svarar: Även sådan behandling påverkas av Schrems II -domen pga hur den amerikanska lagstiftningen ser ut.

-Jag läste precis om ett beslut som fattats av domstol i Frankrike, där man beaktar att lagring sker inom EU och därutöver har en säker hantering av krypteringsnycklar (underbiträdet hade inte åtkomst till nycklarna, utan det var utlagt på tredje part). Domstolen kom fram till att det amerikanska bolaget, i detta fall, klarade av att efterleva kraven i gdpr om tredjelandsöverföring.

-Jag har hört att översättningen av vad som skett i Frankrike är felaktigt :(

- Skulle spontant svara att det är helt beroende av vart nycklarna i sig ligger förvarade. Ingår det i tjänsten som tex tillhandahåller nycklarna och är ett amerikanskt bolag så har de tillgång till nycklarna och således informationen.

Jurist svarar: Jag håller med -- enl. huvudregeln är det handlar inte om var personuppgifterna är lagrade utan även åtkomst på distans räknas som en tredjelandsöverföring.

- Knäckfrågan är väl om det amerikanska bolaget har tillgång till personuppgifterna eller inte.

- Kan man komma runt detta genom att upprätta lokala "förhållningsregler/riktlinjer" hur vi skall använda tjänsten inom skolan - dvs t ex lagra lokalt , begränsa vilka uppgifter som får hanteras (även om plattformen/tjänsten är amerikansk)?

Jurist svarar: Jag skulle inte säga att man ”kommer runt” det men det är absolut ett steg i rätt riktning.

- Om det lagras via ett amerikanskt bolag så har de rättighet att ha tillgång till datan, detta kan lösas genom att tex använda ett svenskt bolag, med servers i Sverige och svensk lagstiftning. Eller med Data maskering där nyckeln ligger tex via HSM i ett land som Sverige lokalt.

- Kommer vi i dag att få möjlighet att få hjälp med att hantera detta? Dvs hur fortsätter vi använda t ex Google Workspace for Education.

- Privasy shield ej tillåtet

- art 49 kan man använda det i skolan för att elever vill skicka videohälsningar till en skola som är utanför EU/EES?

Jurist svarar: det är the million dollar question. Vi kommer försöka ge vägledning och tips på hur man kan ta sig an situationen men men det kommer inte kunna ges ett enkelt svar på hur man kan fortsätta använda de tjänsterna.

- Spelar det någon roll om servrarna står inom EU eller utanför? Eller är det bara leverantörens nationalitet som har betydelse?

- Vad kan vara ytterligare skyddsåtgärder?

- Spelar ingen roll var servrarna står

- Cloud act kom till just för att de amerikanska moln-leverantörerna inte kom åt datan som lagrades inom EU. med cloud act har nu USA rättighet att hämta data så länge det är ett amerikanskt bolag som hanterar datan, oavsett var servrarna står.

(så har jag tolkat det)

- *sorry, amerikanska myndigheten kom inte åt datan lagrad hos tex AWS inom EU

- Alla länder i Europa tillämpar samma princip som diskuteras här genom budapestkonventionen om it-brott

- även USA har ratificerat it-brottskonventionen

- CloudACT går alltså att klara genom en tredjeparts krypteringsnyckel i GWSE?

Jurist svarar: art 49 ska användas restriktivt och endast i undantagsfall. Antingen måste några villkor vara uppfylla (se art. 46.1) eller får det ske om det bla inte är repetitivt, nödvändig för berättigade intressen, endast gäller begränsat antal registrerade osv. Finns en specifik vägledning från EDPB kring just Art 49 så rekommenderar att man läser den om man bill använda sig av art. 49

- Kan man efterfråga samtycke från anställda inom en kommun för att deras personuppgifter (endast epost) kan komma att föras över till tredje land? E-post är väl trots allt en offentlig uppgift för kommuner.

- Samtycke är inte en rättslig grund för myndigheter normalt sett. Den anställde anses vara i en beroendeställning gentemot myndigheten och samtycket kan inte anses vara frivilligt

- Om leverantören hänvisar till standardavtalsklausuler. Skall man teckna detta separat?

- Angående standardavtalsklausuler så är det ju en sak att resonera om tredje land mer allmänt, ställt i förhållande till att resonera om enbart USA. Standardavtalsklausulerna i sig kan ju likt "Privacy Shield" inte åsidosätta amerikansk lagstiftning.

- Är det inte skillnad på kommersiella produkter som Facebook, Gmail, privata Office365 osv och hur personuppgifter hanteras där med de produkter som t ex en skolkommun har som Google Workspace for Education eller A3-licenser i ett företagsägt Office365.

- Jag håller med. Jag uppfattar inte att avtal i form av standardklausuler kan vara ett alternativ till att kunna överföra personuppgifter genom amerikanska molntjänster.

Jurist svarar: Om jag förstår din fråga rätt: Ja, standardavtalsklausulerna är separata handlingar som inte får ändras (bara fyllas i och kompletteras så länge kompletteringarna inte står i strid med standardavtalsklausulerna. Så SCC:erna kompletterar era andra tjänsteavtal med leverantören.

Jurist svarar : Standardavtalsklausulerna binder inte amerikanska myndigheter och är inget frikort för amerikanska bolag att slippa undan amerikansk lagstiftning. Det är alltså svårt att använda standardavtalsklausulerna för amerikanska molntjänster idag.

Jurist svarar: Jag kan inte se att det finns någon skillnad där rättsligt tyvärr.

- Vad gäller om en huvudman vill avbryta ett avtal med en leverantör i förtid på grund av att leverantören direkt eller indirekt använder molntjänster i tredje land?

Jurist svarar: Det stämmer att standardavtalsklausuler inte är något frikort för amerikanska molntjänster. Som -- sa, möjligheten att använda amerikanska molntjänster är rätt begränsat. Kan man inte avsluta den behandlingen är mitt tips att vidta åtgärder för att skademinimera.

Jurist svarar: - utifrån ett dataskyddsperspektivv är det just det som rekommenderas, men du kanske menar rent praktiskt och då kan förhoppningsvis andra i chatten ge bättre tips!

- Hur ska man hantera användning av O365 Education? Är det godkänt att använda om man minimera personuppgifter? Som liten skola finns ingen förhandlingsmöjlighet med Microsoft.

: - Vi har en nordisk leverantör som nu i vår vill flytta lagring från Norge till Amazonservrar i Tyskland. De påstår att all data är krypterad och att bara de har tillgång till krypteringsnycklarna. Hur ska vi förhålla oss till detta, räcker kryptering?

Jurist svarar: inte ”godkänt” tyvärr men att minimera personuppgifterna är ett steg i rätt riktning.

Jurist svarar: Min bedömning är att man som beställare har goda avtalsmässiga grunder att säga upp ett avtal där en leverantör behandlar personuppgifter i USA i strid med gällande lag. Den typen av avtal finns inget skyddsintresse för i svensk lagstiftning, även om man avtalsmässigt sitter fast i långa avtalstider.

- Informationen som presenteras just nu är inkorrekt.

- utveckla gärna.

Jurist svarar: kryptering är ett kompletterande åtgärd och är det en bra/korrekt kryptering ska det räcka. Jag är ingen IT-säkerhetsspec men har förstått att det i verkligheten är det rätt svårt att kryptera hela vägen så det är svårt att svara på om det räcker i praktiken men min personliga åsikt är att det låter som att ni är på god väg

- men stänger inte SOU2021:1 dörren för ytterligare skyddsåtgärder? Vi har mot denna bakgrund svårt att se att det i en situation som gäller tredjelandsöverföring vid utkontraktering av it-drift finns några ytterligare skyddsåtgärder som kan vidtas som läker de brister som EU-domstolen i Facebook Ireland och Schrems bedömer finns i amerikansk lagstiftning.”

Jurist svarar: - ett annat tips är att fråga om det har fått några begäranden om utlämnanden från amerikanska myndigheter och om de då har lämnat ut och isf vad…

Jurist svarar: jag håller tyvärr med. Men jag inser också hur verkligheten ser ut för många och ger därför tips på hur man kan skademinimera i väntan på långsiktig lösning.

- du har rätt. Det gäller då ha en kryptering som kan följa datan från dess att den skapas/uppmärksammas till att den inte ska finnas längre inom organisationen. Många organisationer brottas även med att man behöver ha tillgång till stor del av informationen varför Format preserving Encryption/hashing är en viktig del att ha i beaktning för att minska riskerna för spridning av känslig data men samtidigt kunna använda datan/informationen man hanterar inom sin organisation.

- Utan Google och Microsoft så hade den svenska skolan rasat fullständigt under pandemin.

Då hade vi brutit mot skollagen. Vilken lag trumfar?

- Återgång till Exchange-server?

- Vi har avtal med Prorenata och i pub-avtalet så finns en del leverantörer i bl a USA där de hänvisar till Privacy shield, hur kan man lösa det?

Jurist svarar: bra poäng… Det finns inget tydligt svar kring vilket lag trumfar men i skollagen står det ju inte att man ska använda just de tjänsterna så antar att man inte har laglig rätt att göra det. MEN verkligheten är ju en annan…

- Hur klarar vi en pandemi till utan denna typen av tjänster i skolväsendet

- Sen finns det en Nationell digitaliseringsstrategi för skolväsendet samt lokala IT-strategier som vi förväntas följa.

- Att tro att det finns kapacitet för Sverige som nation eller på EU-nivå för att skapa produkter som kan mäta sig med t ex GWSE eller o365 är väldigt naivt imo.

- Säkra videotjänster börjar ju erbjudas (Inera,Compodium, Iver mfl) som inte använder US-molntjänster och som lagrar i Sverige

- Vi har i vår kommun påbörjat ett informationssäkerhets arbete på strategisk nivå med vår grannkommun, med hjälp av Stratsys, Digframe, som ledningssystem för att kartlägga och säkerställa. Vi är i uppstarten, men vi hoppas på att det ska kunna hjälpa oss

- Stämmer det att FISA endast är tillämpbar för data lagrad eller överförd till USA? Så om datan lagras inom EU/EES sär är inte FISA tillämpbar?

- Nulla regula sine exceptione, en gammal latinsk sentens som visar på problematiken mellan juridik och praktik, detta är alltså inget nytt under solen. Någon sa att Juridik och praktik har aldrig varit så lång ifrån varann som nu, det gör att denna sentens kanske aldrig varit så aktuell som nu.

Vi behöver titta på detta med proportionalitetsprincip också! Med detta vill jag inte säga att vi ska strunta i juridiken men tycker att SKR har en mer rimlig och pragmatisk syn på det hela.

Är det rimligt att det blir full halt eller som juristen varit inne på dvs inte stoppa huvudet i sanden men göra så mycket man kan under tiden.

- Men Cloud Act är

- Ja, men då krävs iaf ett domstolsbeslut.

- Skulle vara intressant att veta vilka alternativa lösningar förutom Google o Microsoft som några kommuner verkar ha kännedom om/använda?

- Välj de frågor ni tycker är mest intressanta att diskutera.

Vilka konsekvenser och problem ser ni till följd av Schrems II-domen?

Hur kan huvudmännen nu bäst förbereda sig inför eventuella tillsynsärenden avseende skolans hantering av elevuppgifter i molntjänster?

Hur fungerar dialogen mellan huvudmän och leverantörer rörande GDPR:s krav på skolans molntjänster och hur kan den förbättras?

Vilka samarbetsmöjligheter har huvudmännen för att möta GDPRs krav på användning av molntjänster?

- Amerikansk server på Irland. Kan det vara tillräckligt skydd för personuppgifter?

- Samverkan borde drivas av SKR/Skolverket. Detta berör alla huvudmän i hela Sverige och även Europa

- Som jag tolkat det så kan servrarna inte ägas av Amerikanskt bolag

Jurist svarar: har amerikanska myndigheter tillgång till personuppgifter? Om ja (troligtvis) då nej, inte tillräckligt skydd.

- Det har lyfts önskningar om ytterligare stöd från SKR. Be er kommunledning att kontakta SKR och framför denna önskan.

- SKR har väl varit väldigt anonyma i denna fråga...

- Hur har Google definierat denna juridiska del i standardklausulerna? Microsoft skriver att de är underordnade Amerikans lag så.....

Jurist svarar: EDPB - European Data Protection Board (Europeiska dataskyddsstyrelsen på svenska)

- vi har också tänkt så. Om servern är i EU-land men leverantör i USA så har de tillgång. Vet inte om det är rätt tolkning?

- Fråga från grupp 6: går verksamhetskritiska uppdrag före?

Jurist svarar: Svar till grupp 6: nej

- Tänkte det... Tack!

Jurist svarar: Allt är lika viktigt… otillfredsställande svar men så är det tyvärr.

- det är så jag tolkat det också. oavsett var lagring sker, är det ett amerikanskt bolag som äger servrarna så har USA möjlighet att få tillgång till datan som ligger lagrad där. Detta skapar såklart större risk att uppgifter hamnar i fel händer/ får spridning.

- Orimligt att lägga det ansvaret på en nämnd. Där finns inte kompetensen att ens börja nysta i detta.

- Om nämnden är personuppgiftsansvarig så har de bollen, kanske kan de delegera ansvaret??

- Vilka lagar är det egentligen man bryter om man har en leverantör i Sverige som lagrar på t.ex. amerikanska servrar? (Utgår ifrån att man har tjänsteavtal, PUB-avtal och DPIA på plats)

- men den kompetensen är det väl vi som ska ha och informera nämnden (dso eller annan utpekad person)

- Kraven bör i rimlighetens namn ställas på leverantörerna. I nuläget levererar de en olaglig produkt som gör huvudmännen föremål för viten.

Jurist svarar: Man bryter mot GDPR.

- Varför sägs det inte rakt ut att vi inte får använda AWS/GWSE/O365 pga ägande i USA? Dvs att alla offentliga verksamheter i Sverige måste starta ett arbete att rulla ur dessa molnlösningar och backa 10-20 i IT-utveckling.

Om allt faller med ägandet i USA så spelar det ju ingen roll hur många riskanalyser vi gör eller om vi uppgiftsminimerar eller likande. Det har ju gjorts klart i dag att vi inte kan nå compliance.

- om vi kravställer enligt lagen och omförhandlar avtal eller avbryter avtal kommer marknaden att börja erbjuda lösningar tänker jag.

- Jag tänker vi får kunna påvisa vid en eventuell granskning av IMY att vi är medvetna och jobbar systematiskt med frågan, som ju också hanterar om var vi har personuppgifterna och måste de hanteras i tjänsten eller finns det annat arbetsätt

Jurist svarar: jag tror att det inte sägs rakt ut för det råder fortfarande lite osäkerhet men jag håller med om att mycket talar för att det inte är tillåtet att använda de tjänsterna. Jag håller dock inte med om att det inte spelar någon roll vad man gör. Jag tror på att vidta kortsiktiga riskminimerade åtgärder tills dess att man har en långsiktig lösning på plats.

- Mycket talar för att man hamnar i den slutsatsen som du beskriver NN. Men att vi arbetar metodiskt. Jag tror inte att någon annan än vi själva ta ansvaret.

- Jag vill passa på att tacka Internetstiftelsen och alla som närvarat för ett väl genomfört 3h-pass och tack för alla som delat sina tankar, den här tiden sprang iväg. :)

- Fast det sägs utan att sägas rakt ut? Det är det som blir mitt problem. De jurister som pratat i dag har sagt detta som jag tolkar det utan att säga det i klartext.

- Problemet här är som jag förstår det att alldeles oavsett vilka avtal och säkerhetsklausuler och krypteringar man har så har amerikanska säkerhetstjä tillgång till uppgifterna och det är inte ok?

Jurist svarar: Jag tackar också för alla frågor. Jag har försökt svara så gott jag kan men som ni har märkt sitter inte jag på alla svar. Lycka till med ert fortsatta arbete!