Datum 2021-01-19

Diarienummer KS 2020/0435

E Hammerman, R Lycksell, H Meier

Kommunstyrelsen

Redovisning av pågående översyn av kommunens systemförvaltning ur ett dataskyddsperspektiv

Ärende

Behandling av personuppgifter regleras av den för hela EU gällande dataskyddsförordningen. För att personuppgifter ska få föras över till ett land utanför EU måste det landet ha bestämmelser som ger personuppgifterna ungefärligen samma skydd som de har i EU genom dataskyddsförordningen. I somras kom en dom från EU-domstolen där domstolen kommit fram till att europeiska personuppgifter inte har ett sådant skydd i USA, vilket påverkar många IT-tjänster. Det innebär att det är oklart dels under vilka förutsättningar personuppgifter får lagras i moln med amerikanska molntjänster, dels om amerikanska bolag, eftersom de som sådana alltid lyder under amerikansk lag, kan utföra drifts- och supportåtgärder som medför att de behandlar personuppgifter. Kommunledningskontoret redovisar i detta ärende hur kontoret har börjat kartlägga kommunens alla behandlingar av personuppgifter för att avgöra i vilken omfattning det kan förekomma sådana behandlingar där amerikanska bolag är involverade. Vardera nämnden är personuppgiftsansvarig och måste själv ta ställning till hur den ska göra om den använder program/system som innebär att amerikanska bolag behandlar personuppgifter som nämnden är ansvarig för.

Kommunledningskontorets förslag till beslut

Kommunstyrelsens beslut

Kommunstyrelsen noterar informationen till protokollet och överlämnar redovisningen till nämnderna.

E Hammerman, R Lycksell, H Meier

Bakgrund

Dataskyddsförordningen

Dataskyddsförordningen[1] har som ett av sina syften att skydda den personliga integriteten vid registrering och hantering av personuppgifter. I dataskyddsförordningen finns därför bestämmelser om skydd av personuppgifter i samband med överföring av data till tredje land, det vill säga länder utanför EU/EES-området.

Dataskyddsförordningen ställer bland annat krav på att det finns ett lagenligt syfte med att personuppgifter registreras, att uppgifterna inte används i annat syfte än avsett och att uppgifterna inte används för, icke lagenlig, samkörning av register. Dessutom har den enskilde rätt att begära ut och få ta del av vilka uppgifter som finns registrerade om den själv, att få felaktiga uppgifter korrigerade och att, med vissa begränsningar få sina personuppgifter borttagna.

Överföring av personuppgifter till tredje land är inte förenligt med dataskyddsförordningen om inte ovanstående lagstadgade rättigheter kan säkerställas genom motsvarande lagstiftning i det land som överföring görs till.

Lagstiftning i tredje land

Det finns länder utanför EU/EES som har en liknande lagstiftning som skyddar den personliga integriteten. I en del fall avser lagstiftningen endast landets egna medborgare. Det är EU-kommissionen som avgör om lagstiftningen ger ett skydd motsvarande dataskyddsförordningens.

En del länder har säkerhetslagstiftning som ger landets myndigheter rätt att begära ut personuppgifter från landets IT-leverantörer. USA har till exempel en lagstiftning, Cloud Act, som innebär att amerikanska säkerhetsmyndigheter med stöd av ett domstolsbeslut kan begära ut personuppgifter från alla företag som har sitt säte i USA. Detta gäller oavsett var de aktuella personuppgifterna finns registrerade, alltså även om data lagras inom EU och avser andra än amerikanska medborgare. Flera andra länder, däribland Kina, Ryssland och Indien, har liknande säkerhetslagstiftning.

Mellan EU och USA fanns först en överenskommelse med ett regelverk som kallades Safe Harbour, som innebar att USA bedömdes ha en skyddsnivå för personuppgifter motsvarande den europeiska. Den överenskommelsen

---

[1] På engelska General Data Protection Regulation, förkortat GDPR. Officiell beteckning: Förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

underkändes av EU-domstolen 2015. En ny överenskommelse med ett nytt regelverk togs därför fram 2016. Den kallas för Privacy Shield.

Ändrade förutsättningar för överföring av personuppgifter till USA

Under 2020 har EU-domstolen avgjort ett mål som gäller Facebook och överföring av personuppgifter till USA och som helt ändrar förutsättningarna för möjligheterna att föra över personuppgifter till USA – att göra personuppgifter tillgängliga för IT-företag som lyder under amerikansk rätt. Domen kallas Schrems II[2] eller Privacy Shield-domen.

I domen framgår tydligt hur domstolen resonerat och kommit fram till att Privacy Shield-överenskommelsen, som används som grund för många avtal om IT-tjänster saknar laglig grund. Det görs också tydligt att det ställs höga krav på personuppgiftsansvariga och tjänsteleverantörer att säkerställa efterlevnaden av EU:s lagstiftning om behandling av personuppgifter.

I en del avtal förbinder sig leverantören att följa standardklausuler som tagits fram av EU, Standard Contractual Clauses (SCC) om hantering av personuppgifter. Genom att hänvisa till dessa klausuler anser leverantören att de säkerställer dataintegriteten vid eventuell överföring till tredje land. Domstolens bedömning är att standardklausulerna är godkända och kan användas. Standardklausulerna kan dock överridas av nationell säkerhetslagstiftning.

Domstolen fastslår att det inte är lagligt att använda IT-tjänster baserat på en bedömning att det är låg risk för att personuppgifter begärs ut av tredje landsmyndigheter. Finns det en risk för att en myndighet kan få del av personuppgifter i en IT-tjänst måste skyddet för personuppgifterna säkerställas med ytterligare skyddsåtgärder. Om det inte är möjligt att införa skyddsåtgärder ska överföringen avbrytas. När det gäller USA kom EU-domstolen fram till att det faktum att endast amerikanska medborgare kan få en domstolsprövning av om en behandling av personuppgifter sker på korrekt sätt, vilket innebär att en avgörande säkerhetsfaktor saknas.

Åtgärder på EU- och nationell nivå efter domslutet

Domen får stora praktiska konsekvenser för såväl privata som offentliga aktörer inom EU och USA och det har inletts förhandlingar mellan EU och USA. Om eller när en ny överenskommelse med ett nytt regelverk kan

[2] Efter personen som anförde klagomålet mot Facebook. Det är dom nummer två då samma person hade anfört de klagomål som ledde till att överenskommelsen kallad Safe Harbour underkändes av EU-domstolen (Schrems I).

komma till går i dagsläget inte att säga. Det har inletts ett antal granskningar av hur amerikanska bolag får tillgång till personuppgifter genom att leverera IT-tjänster, av såväl Integritetsskyddsmyndigheten (förut kallad Datainspektionen) som andra EU-länders tillsynsmyndigheter. Granskningarna samordnas av den europeiska dataskyddstyrelsen European Data Protection Board, EDPB.

De problem med överföring av personuppgifter till USA som avsaknaden av jämförbara skyddsåtgärder medför kan inte lösas på nationell nivå eftersom det är fråga om en EU- och amerikansk lagstiftning. EDPB har utarbetat en vägledning baserad på olika scenarier. Samtliga dataskyddsmyndigheter inom EU samverkar för att etablera likartade bedömningar i de eventuella tillsynsärenden som kommer in.

Sveriges kommuner och regioner, SKR, för en dialog och ett påverkansarbete med Datainspektionen och regeringen. SKR rekommenderar sina medlemmar att kartlägga befintliga avtal avseende IT-tjänster och att upprätta en handlingsplan baserad på den vägledning EDPB har tagit fram för hur personuppgiftsansvariga nu kan agera. Vägledningen rekommenderar att de personuppgiftsansvariga ska göra en kartläggning och analys av alla överföringar. Vägledningen ger också rekommendationer för olika scenarier. I scenarierna beskrivs flera olika typer av dataöverföringar från rena transfereringstjänster mellan sändare och mottagare inom EU/EES till överföringar med mottagare utanför EU/EES där lokal behandling av data sker. Vägledningen hanterar också frågeställningar om det är nödvändigt eller inte nödvändigt för ett personuppgiftsbiträde att ta del av personuppgifterna för att kunna leverera IT-tjänster. I de fall det inte är nödvändigt rekommenderas att kompletterande skyddsåtgärder vidtas.

Åtgärder som påbörjats i Danderyd

Danderyds kommun var tidigt ute med att påbörja en planering av åtgärder efter EU-domstolens dom. Kommunledningskontoret har initierat en kartläggning av IT-tjänster kopplade till kommunens avtal om olika IT-tjänster. I bedömningen granskas såväl den huvudleverantör som står bakom avtalet som eventuella underleverantörer. Kartläggningen pågår fortfarande och alla förvaltningar är delaktiga i arbetet.

Kommunledningskontoret och de andra förvaltningarna kommer därefter att analysera varje IT-tjänst för att avgöra ifall det behöver vidtas några åtgärder avseende den aktuella IT-tjänsten. Åtgärder kan vara att byta till en alternativ IT-tjänst, omförhandla avtal, ta fram nya interna regelverk och rutiner för användning av tjänsten, vidta ytterligare skyddsåtgärder eller att

avveckla användningen av IT-tjänsten. Därefter kan en översiktlig handlingsplan med förslag till åtgärder sammanställas.

Parallellt med ovanstående arbete bevakar kommunledningskontoret händelseutvecklingen på såväl nationell nivå som på EU-nivå. Leverantörerna av IT-tjänster har också ansvar för att vidta åtgärder som kan påverka situationen. Kommunledningskontoret bevakar naturligtvis även detta och kan välja att föra dialog med en del leverantörer.

Kommunen följer också hur frågan hanteras i andra kommuner. Göteborgs stad har t.ex. valt ett liknande förfarande som Danderyds kommun.

Nuläget i Danderyds kommun

Kommunen använder, liksom flertalet kommuner i landet, IT-tjänster där huvudleverantör och/eller underleverantörer är amerikanska företag. Det gäller inte minst Microsoft 365 med tjänster som Outlook, Office, Teams, Sharepoint med mera som används av alla nämnder och därmed inom alla förvaltningar. Det gäller också Google for Education (Workspace) som används inom bildningsförvaltningen.

Dessa IT-tjänster har en stor och central betydelse för kommunens verksamheter. Tjänsterna är i nuläget väsentliga för att kommunen ska kunna bibehålla en väl fungerande verksamhet under den pågående pandemin. Kommunledningskontoret bedömer att det idag saknas godtagbara alternativ som kan erbjuda motsvarande funktionalitet och där leverantören inte är ett amerikanskt företag.

En kortsiktig, fullständig, avveckling av dessa molntjänster skulle allvarligt påverka kommunens verksamheter. Kommunledningskontoret bedömer att ifall en avveckling av dessa tjänster skulle komma att krävas så kan det endast ske med en långsiktig och väl genomtänkt planering.

I övrigt är det för tidigt att uttala sig om i vilken omfattning det förekommer andra IT-tjänster där kommunen behöver vidta åtgärder.

Johan Lindberg
Kommundirektör

Johan Nordenmark
Administrativ chef

Handlingar i ärendet
Tjänsteutlåtande, Redovisning av pågående översyn av kommunens systemförvaltning ur ett dataskyddsperspektiv

E Hammerman, R Lycksell, H Meier

Expedieras
Samtliga nämnder