

# JO-anmälan av Göteborgs Stad

**Anmälare:** Dataskydd.net

**Anmäld part:** Göteborgs Stad, inkl. Intraservice och Stadsledningskontoret

**Saken:** Legalitet i avtal med tjänsteleverantör, kränkning av rätten till privatliv och personlig integritet, röjande av sekretessreglerade uppgifter, överföring av personuppgifter till tredje land i strid med dataskyddsförordningen genom användande av publik molntjänst där lagring sker i tredje land och som omfattas av amerikansk lagstiftning som saknar effektiva rättsmedel för enskilda i Sverige.

## Bakgrund

Göteborgs Stad genomför sedan 2016 ett införande av tjänsten Office 365 som tillhandahålls av leverantören Microsoft. Under genomförandet har två bedömningar avseende röjande av sekretess genomförts av Stadsledningskontorets rättsliga experter. I november 2019 beslutade Göteborgs Stad att införandet ska genomföras för kommunens hela verksamhet.

## Saken

Göteborgs Stad hanterar sekretessreglerade uppgifter samt personuppgifter, inklusive känsliga personuppgifter i tjänsten Office 365. Efter slutförd realisering kommer stora delar av kommunens samlade digitala information att hanteras i tjänsten, även sekretessreglerade uppgifter och känsliga personuppgifter.

## Tjänsten Office 365

Office 365 är en s.k. molntjänst för hantering av dokument samt kommunikation. Uppgifterna lagras och hanteras i Microsofts egna datacenter på Irland och dessutom åtminstone i USA. Microsoft betraktas av amerikanska staten som ett amerikanskt företag, vilket innebär att Microsoft omfattas av tillämplig amerikansk lagstiftning.

För att en användare ska få tillgång till Office 365 krävs inloggning och alla användare tillhandahålls ett konto av Göteborgs Stad

I tjänsten har varje användare ett e-postkonto för inkommande och utgående e-post, inklusive bifogade filer. Möten och andra kalenderbokningar hanteras i tjänsten och användare har möjlighet att lagra kontaktuppgifter till externa kontakter. Dokument, kalkylark och presentationer skapas, redigeras och lagras i tjänsten.

Microsoft klassificerar Office 365 som en Online-tjänst och i Microsofts villkor (Dataskyddstillägg för Microsoft Onlinetjänster, januari 2020) anges att:

*Microsoft ska efterleva alla tillämpliga lagar och andra förordningar som rör deras tillhandahållande av onlinetjänsterna, inbegripet lagar om meddelande om säkerhetsincidenter och dataskyddskrav. Microsoft är dock inte skyldiga att efterleva lagar eller förordningar som är tillämpliga på kunden eller kundens bransch som inte också är allmänt tillämpliga på IT-tjänstleverantörer. Microsoft avgör inte huruvida kunddata omfattar information som lyder under någon särskild lag eller förordning. Alla säkerhetsincidenter regleras av nedanstående villkor för Meddelande om säkerhetsincidenter.*

*Kunden måste efterleva alla lagar och andra förordningar som gäller för dennas användning av onlinetjänster, inbegripet lagar som rör biometriska data, konfidentialitet för kommunikation och dataskyddskrav. Kunden ansvarar för att avgöra om onlinetjänsterna är lämpliga för lagring och behandling av information underkastat särskild lag eller förordning, och för att använda onlinetjänsterna på ett sätt som överensstämmer med kundens rättsliga och regleringsmässiga skyldigheter. Kunden ansvarar för att svara på eventuell begäran från tredje man angående kundens användning av en onlinetjänst, t.ex. en begäran om att ta bort innehåll enligt USA:s Digital Millennium Copyright Act eller andra tillämpliga lagar.*

Samt:

*Microsoft lämnar inte ut behandlade data, utom enligt följande: (1) På Kundens instruktioner. (2) Enligt beskrivning i detta DPA. (3) Så som krävs enligt lag.*

*Microsoft ska inte lämna ut behandlade data till rättsvårdande myndighet såvida inte detta krävs enligt lag. Om rättsvårdande myndighet skulle kontakta Microsoft med en begäran om behandlade data ska Microsoft försöka hänvisa den rättsvårdande myndigheten till att begära dessa data direkt från Kunden. Om Microsoft är tvungna att lämna ut behandlade data till rättsvårdande myndighet ska Microsoft omgående meddela Kunden och tillhandahålla en kopia av begäran, såvida inte Microsoft är förhindrade enligt lag att göra så.*

*Vid mottagande av tredje mans begäran om behandlade data ska Microsoft omgående meddela kunden, såvida inte detta är förbjudet enligt lag. Microsoft ska avvisa begäran utom då uppfyllelse krävs enligt lag. Om begäran är giltig ska Microsoft försöka hänvisa tredje man direkt till Kunden med sin begäran om data.*

I det övergripande affärsavtalet, "volymavtal", mellan å ena sidan Microsoft och å andra sidan Statens inköpscentral och SKL Kommentus inköpscentral anges:

*Kompletterande Avtal som ingåtts med något av Microsofts Koncernbolag utanför Europa ska regleras av och tolkas enligt delstaten Washingtons lagar och USA:s federala lagar. Kompletterande Avtal som ingåtts med något av Microsofts Koncernbolag i Europa ska regleras av och tolkas enligt irländsk lag. Om tvist uppstår på grund av eller i samband med Professionella tjänster ska lagen i den jurisdiktion där det av Microsofts Koncernbolag som utför relevant Statement of Services har sitt registrerade säte tillämpas. FN:s konvention från den 11 april 1980 angående avtal om internationell handel av varor och tillhörande instrument gäller inte för detta avtal.*

Samt:

*Om parterna väcker talan med anledning av detta avtal förbinder parterna sig att använda följande exklusiva jurisdiktioner:*

*(i) om Microsoft väcker talan ska talan väckas i den jurisdiktion där Kundens Koncernbolag, som är part i avtalet, har sitt huvudkontor*

*(ii) om Kunden väcker talan med anledning av ett Statement of Services skall talan väckas i den jurisdiktion där det Microsoft-koncernbolag som utför Statement of Services har sitt registrerade säte För all annan talan gäller att (1) om Kunden väcker talan mot ett av Microsofts koncernbolag utanför Europa har statliga eller federala domstolar i King County i delstaten Washington i USA jurisdiktion och (2) om Kunden väcker talan mot ett av Microsofts koncernbolag i Europa, och inte också mot ett av Microsofts koncernbolag utanför Europa, har Irland jurisdiktion.*

*Parterna samtycker till att domstolen i den överenskomna jurisdiktionen har domsrätt. Detta val av jurisdiktion hindrar inte någon av parterna från att söka interimistiska åtgärder i lämplig jurisdiktion avseende brott mot immateriella rättigheter eller sekretessskyldigheter.*

Den amerikanska lagen CLOUD Act, som trädde i kraft i mars 2018, innebär bland annat att leverantörer av elektroniska kommunikationstjänster och molntjänster som är underkastade amerikansk jurisdiktion, ska under vissa omständigheter bevara samt lämna ut data som är under leverantörens kontroll. Det spelar i sammanhanget inte någon roll om informationen lagras eller hanteras i eller utanför USA. En sådan begäran ska – något förenklat – ske genom en s.k. ”warrant” (en form av husrannsakan) som utfärdats av amerikansk domstol, ett administrativt föreläggande eller ett föreläggande av s.k. ”grand jury” (en speciell form av amerikansk domstol). En tjänsteleverantör kan bestrida begäran i domstol men beslutet om begäran ska beviljas beslutas av amerikansk rättsinstans och varken kunden eller annat berört lands myndigheter behöver involveras. CLOUD Act ger också USA:s justitieminister möjlighet att genom ett verkställighetsavtal med andra stater reglera möjligheten för dessa stater att direkt hos amerikanska leverantörer begära information i syfte att bekämpa allvarlig brottslighet.

Telemetridata är mätdata som hämtas och hanteras av leverantören och som kan omfatta både faktiskt innehåll och s.k. metadata. Telemetridata kan teoretiskt bli föremål för utlämnande i enlighet med amerikansk lagstiftning, men hanteras främst av leverantören i syfte att förbättra och underhålla tjänsten. Intressant i detta sammanhang är att molntjänst som affärsmodell i sig ofta rymmer en inneboende drivkraft att använda kundernas data för egna ändamål, t.ex. för att utveckla nya tjänster, och att dela med sig av uppgifterna till andra företag, t.ex. som annonsunderlag. Även om vissa inställningar kan begränsa mängden telemetridata som hanteras av Microsoft kan kunderna inte styra detta helt. Standardavtalet från Microsoft ger leverantören möjlighet att hantera uppgifter för egna ändamål, även om sådana avtal strider mot dataskyddsregleringen. I en utredning genomförd av nederländska staten konstateras att leverantörer av bland annat molntjänster utan

lagligt stöd hämtar in potentiellt känsliga data, även metadata, och att de lämnar ut telemetridata till länder utanför EU.

## Uppfyller avtalet med Microsoft de krav som gällande rätt ställer på Göteborgs Stad att agera under lagarna?

I 1 kap. 1 § tredje st. regeringsformen anges att den offentliga makten utövas under lagarna. Här fastslås alltså principen om all maktutövning lagbundenhet. En svensk kommunal myndighet eller politisk församling agerar således under den svenska lagen (arkivhantering kan inte ske enligt exempelvis amerikansk eller irländsk rätt). En svensk kommunal myndighet kan inte heller fransäga sig ansvaret för skyddet av sina allmänna handlingar genom att utkontraktera hela eller delar av denna hantering.

I en utredning om Statliga myndigheters avtal (SOU 1994:136) anges det att i kravet på god hushållning med statliga medel även ligger ett krav på att de avtal som ingås får ett sådant innehåll och en sådan utformning att det finns betryggande klarhet om alla parter rättigheter och skyldigheter enligt avtalen (s. 146). För att uppfylla krav på god hushållning med statliga medel måste myndigheterna se till att de avtal som de ingår också har en sådan kvalitet som behövs för att trygga statens ekonomiska intressen i vid mening (s. 167). Det finns inga bärande skäl för att motsvarande synsätt inte skulle gälla för kommunala myndigheters avtal (jfr 11 kap. 1 § kommunallagen).

I den mån det avtal som Göteborgs Stad tecknat med Microsoft inte innehåller något om en viss fråga av betydelse för hur Microsoft ska utföra en uppgift för Göteborgs Stads räkning torde avtalet enligt vanliga tolkningsregler fyllas ut av de regler som gäller enligt den rättsordning som parterna avtalat ska gälla mellan dem, exempelvis amerikansk eller irländsk rätt. Skulle irländsk rätt gälla mellan Göteborgs Stad och Microsoft kan det emellertid visa sig ge verkningar i Office 365, som inte har stöd i svenska regler om ärendehandläggning eller offentlighet och sekretess.

För en myndighet är det avgörande att verksamhetssystem, t.ex. kontorsstöd, hanteras i enlighet med svensk rätt. I avtal kan knappast varje situation regleras uttryckligen, jämför t.ex. det ovan nämnda avtalsvillkoret för Office 365 om att Microsoft inte är skyldig att efterleva lagar eller förordningar som är tillämpliga på kunden eller kundens bransch som inte också är allmänt tillämpliga på leverantörer av IT-tjänster. Det framstår dessutom som märkligt att tvister som rör Office 365 inte ska prövas av svensk domstol utan av en utländsk domstol som dessutom ska tillämpa en främmande rättsordning, jämför t.ex. med det ovan nämnda avtalsvillkoret för Office 365 att Microsoft inte ska lämna ut behandlade data till rättsvårdande myndighet såvida inte detta krävs enligt lag.

Till skillnad från en privaträttslig aktör torde alltså Göteborgs Stads avtalsfrihet vara begränsad genom att Göteborgs Stad måste uppfylla kraven i svensk lag. Hit hör att Göteborgs Stad inte får avhända sig kontrollen över sina allmänna handlingar och att den hantering som sker samt parternas avtal ska vara förenliga med svensk rätt.

# Ges tillräckligt skydd för den personliga integriteten i Göteborg Stads tillämpning av Microsoft Office 365?

Skyddet för rätten till privatliv och den personliga integriteten framgår av Europakonventionen, regeringsformen, Europeiska Unionens stadga om de grundläggande rättigheterna (EU-stadgan) samt av dataskyddsförordningen (GDPR).

I Europakonventionen, artikel 8 ”Rätt till skydd för privat- och familjeliv” föreskrivs följande:

*Var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens.*

Regeringsformen anger följande i 2 kap. 6 § 2 st. angående intrång i den personliga integriteten:

*Utöver vad som föreskrivs i första stycket är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.*

Av EU-stadgan följer följande av artikel 7 ”Respekt för privatlivet och familjelivet”:

*Var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer.*

Till detta kommer bestämmelsen i artikel 47 under rubriken ”Rätt till ett effektivt rättsmedel och till en opartisk domstol”:

*Var och en vars unionsrättsligt garanterade fri- och rättigheter har kränkts har rätt till ett effektivt rättsmedel inför en domstol, med beaktande av de villkor som föreskrivs i denna artikel. Var och en har rätt att inom skälig tid få sin sak prövad i en rättvis och offentlig rättegång och inför en oavhängig och opartisk domstol som har inrättats enligt lag. Var och en ska ha möjlighet att erhålla rådgivning, låta sig försvaras och företrädas. Rätts hjälp ska ges till personer som inte har tillräckliga medel, om denna hjälp är nödvändig för att ge dem en effektiv möjlighet att få sin sak prövad inför domstol.*

Dataskyddsförordningen anger följande i artikel 28, punkt 1:

*Om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas.*

Den myndighet som vill anlita ett personuppgiftsbiträde är således, både för sina egna anställda samt för medborgare, skyldig att säkerställa att personuppgiftsbiträdet garanterar att varje personuppgiftsbehandling innebär att personerna har rätt till både privatliv och effektiva rättsmedel.

Integritetskommittén konstaterade att de största riskerna för den personliga integriteten när det gäller molntjänster hänger ihop med den förlust av insyn och

kontroll som användning av sådana tjänster i regel innebär. Utöver de risker som redan nämnts ovan kan sägas att denna förlust medför risker för obehörig åtkomst hos leverantörer och underleverantörer och för att uppgifterna hamnar i länder där lagstiftningen ger ett otillräckligt skydd. Uppgifterna riskerar också att hamna hos underleverantörer som är okända för kunden, vilket i sin tur kan göra det svårt för en personuppgiftsansvarig att uppfylla sin skyldighet att se till att uppgifterna hanteras i enlighet med dataskyddsregleringen.

## Är behandling av sekretessreglerad information i enlighet med Offentlighets- och sekretesslagen i Göteborg Stads tillämpning av Microsoft Office 365?

Innan en myndighet gör sekretessreglerad information tillgänglig för en extern leverantör, måste myndigheten bl.a. analysera om detta innebär ett röjande av uppgifter i den mening som avses i OSL. Den rättsliga expertgruppen inom eSamverkansprogrammet (eSam) gjorde 2018 ett rättsligt uttalande som tog sikte på röjandebegreppet vid användande av molntjänster. Det rättsliga uttalandet har därefter ansetts vara korrekt av t.ex. Kammarkollegiet, Pensionsmyndigheten och Försäkringskassan.

*Först* ska en prövning göras om leverantören enligt avtal med uppdragsgivaren inte får ta del av eller vidarebefordra den information som görs tekniskt tillgänglig för leverantören. Detta innebär att det ska finnas en juridiskt bindande och sanktionerad avtalssekretess för leverantören. Leverantören får inte heller vara bunden av regler i främmande rätt om att lämna ut information utan en föregående sekretessprövning eller annan laglig grund enligt svensk rätt för ett utlämnande. Om detta första villkor är uppfyllt, ska i ett *andra steg* en bedömning göras av om omständigheterna i övrigt medför att det är osannolikt att leverantören ändå tar del av eller vidarebefordrar informationen.

Om det brister i någon av dessa två förutsättningar, ska informationen anses röjd när den tillgängliggörs för leverantören. Om information är sekretessbelagd krävs i så fall att den myndighet som röjer informationen har stöd i lag eller förordning för att lämna ut dem.

JO uttalade i beslut den 9 september 2014 allvarlig kritik mot vissa vårdgivare inom bland annat Västra Götalandsregionen för att ha ingått avtal om journalföring med ett företag trots att detta inte varit förenligt med regelverket om sekretess inom hälso- och sjukvården. JO:s beslut avsåg dock svenska nationella förhållanden. När eSamverkansprogrammets juridiska expertgrupp i ett rättsligt uttalande år 2015 bedömde att ett röjande under vissa förutsättningar kunde undgås var det fråga om en relativt smal ”spång” för vissa tjänster inom Sverige, utan kopplingar till utländskt ägande eller annan grund för att kräva en tillämpning av ett annat lands rättsordning. Globala leverantörer började emellertid åberopa detta uttalande för att tillhandahålla ”motorvägsbroar” för svenska myndigheters uppgifter till utlandet. Därmed aktualiserades helt andra rättsfrågor än dem eSamverkansprogrammets

rättsliga expertgrupp tagit upp. Detta gäller särskilt när villkor om lagval och prorogationsklausuler exkluderar svensk rätt mellan parterna och undandrar tjänsten från svenska domstolars jurisdiktion såvitt avser parternas mellanhavanden. En svensk myndighet som anlitar en sådan tjänst hindras från att kunna uppfylla sina skyldigheter enligt 8 kap. 3 § OSL.

Den juridiska expertgruppen inom eSamverkansprogrammet gjorde ett förtydligt rättsligt uttalande år 2018 om att en myndighet inte får lämna en uppgift för vilken sekretess gäller till en utländsk myndighet utan att den svenska myndigheten först har gjort en prövning av att uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och att det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten.

Denna sekretessprövning, som redan på grund av rekvisitens utformning knappast kan göras på förhand, får inte överlämnas till en leverantör av exempelvis molntjänster eller en utländsk myndighet (se dessutom Outsourcing 2.0, en vägledning av eSamverkansprogrammet från december 2019 om sekretess och dataskydd, s. 65 ff.). Genom att använda Office 365 röjer således Göteborgs Stad sekretessbelagda uppgifter för Microsoft. Röjandet är – i avsaknad av sekretessbrytande bestämmelser – i strid med OSL. Det blir särskilt tydligt när villkorens närmare utformning granskas. Eftersom utländsk rätt ska gälla mellan parterna kan den rättsordningen innehålla regler om utlämnande som inte kan förenas med svensk rätt. Samtidigt följer det av avtalsvillkoren mellan parterna att undantag gäller för Microsoft från förbudet att lämna ut kunddata utanför Microsoft, om ett utlämnande krävs enligt lag, dvs. enligt den utländska rättsordning som enligt avtalet ska tillämpas mellan parterna.

## Är hanteringen av personuppgifter i enlighet med GDPR i Göteborg Stads tillämpning av Microsoft Office 365?

Amerikanska myndigheter är bundna att följa och verkställa amerikansk rättsordning. En amerikansk myndighet är inte part i eller bundna av villkoren i ett personuppgiftsbiträdesavtal, standardavtalsklausuler, uppförandekoder eller bindande företagsbestämmelser varför användning av dessa i sig inte möjliggör överföring till USA. Om en överföring till USA ska vara godtagbar måste det finnas tillgång till lagstadgade rättigheter och effektiva rättsmedel för de individer vars personuppgifter behandlas. Komplexiteten i olika länders regelverk för personuppgiftsbehandling kan skilja sig åt men varje personuppgiftsansvarig har alltid ett ansvar för att en tredjelandsoverföring är rättsligt korrekt.

EU-kommissionen skrev i sin andra årliga rapport om avtalet mellan EU-kommissionen och USA gällande överföring av personuppgifter till USA, ”Privacy Shield”, att den lagstiftning som var viktigast i förhållande till amerikanska myndigheters åtkomst till personuppgifter gällde sektion 702 av Foreign Intelligence Surveillance Act, FISA. FISA sektion 702 möjliggör för amerikanska underrättelsemyndigheter att samla information om icke-amerikanska medborgare

som rimligen kan antas befinna sig utanför USA. Den domstol som handlägger dessa ärenden är Foreign Intelligence Surveillance Court, FISC. Enligt den irländska domstolen High Court är alla förhandlingar i FISC som utgångspunkt hemliga, dock finns en teoretisk möjlighet till beslut om offentliggörande. High Court angav vidare att amerikanska myndigheter enligt FISA kan inhämta och spara en EU-medborgares personuppgifter utan att bevisa sannolika skäl till FISC relaterade till motiven till inhämtningen om EU-medborgaren. High Court angav att när FISC fattar hemliga beslut om övervakning innebärande att även företag som ska verkställa besluten måste hemlighålla sin delaktighet, saknas juridiska eller administrativa vägar för individer vars personuppgifter inhämtas att få kännedom om inhämtningen. Det saknas därmed också möjlighet för individer att få tillgång till, korrigera eller radera personuppgifter, likaså saknas en rätt till administrativ eller rättslig prövning.

Irländska High Court berörde också Executive Order 12333, EO 12333, utfärdad av presidentämbetet i USA. Det är inte en lag utan en exekutiv order som presidenten när som helst kan återkalla eller ändra. Enligt High Court är det huvudsakligen från EO 12333 som den amerikanska signalspaningsmyndigheten NSA hämtar sitt mandat för underrättelseinhämtning från utlandet. High Court uppger vidare att NSA inte behöver inhämta förhandstillstånd för övervakning enligt EO 12333, att NSA:s agerande enligt EO 12333 inte regleras genom lagstiftning, inte är föremål för rättslig tillsyn och inte kan bli föremål för domstolsprövning.

High Court noterade också de svårigheter som finns för individer, i synnerhet individer utan anknytning till USA, att få talerätt i amerikansk domstol avseende överträdelse relaterade till personuppgiftsbehandling. En individ måste med framgång göra gällande att den har talerätt för att över huvud taget kunna inleda en rättsprocess och det noterades att detta är en mycket komplex fråga när det gäller hemlig myndighetsövervakning. High Court angav att på grundval av alla bevis som granskats är just frågan om talerätt ett extraordinärt svårt hinder för en individ att övervinna i fall som gäller amerikanska myndigheters hemliga övervakning.

Göteborgs Stad har genom sitt beslut tillåtit behandling av känsliga personuppgifter i USA. Detta innebär att Göteborgs Stad brutit mot artikel 28 i dataskyddsförordningen genom att Göteborgs Stad som personuppgiftsansvarig har anlitat ett personuppgiftsbiträde som varken ger eller kan ge tillräckliga garantier som säkerställer att den registrerades rättigheter skyddas.

## Göteborg Stads egen bedömning om uppfyllande av Offentlighets- och sekretesslagen, GDPR och skyddet för den personliga integriteten

Av de publicerade utlåtandena från Stadsledningskontorets rättsliga experter hanteras sekretessreglerad information i Göteborgs Stads implementation av Office 365.

Stadsledningskontorets jurister har två gånger, 2017 och 2019, skrivit bedömningar rörande OSL i förhållande till Office 365. I promemorian från 2017 är slutsatsen att



sekretessreglerade uppgifter är att anse som röjda i OSL:s mening, men att Göteborgs Stad genom en tilläggstjänst från Microsoft kan säkerställa att anställda hos Microsoft inte tar del av sekretessreglerade uppgifter utan att Göteborgs Stad på förhand godkänt detta. Stadsjuristerna noterar dock att avtalet med Microsoft innehåller undantag där Microsoft kan åläggas av amerikanska myndigheter att lämna ut information, inkl. yppandeförbund om att ett utlämnande skett. Stadsjuristerna anser också att bedömningen av frågan om röjande ska ses i en bredare kontext på så sätt att en uppgift ska anses röjd bara om en utomstående ges faktisk åtkomst till uppgifterna, till skillnad från att ett röjande anses ha skett redan när det gjorts tekniskt och juridiskt möjligt att åtkomst kan komma att ges.

I promemorian från 2019 är slutsatsen att amerikanska myndigheter inte bedöms ges någon åtkomst till Göteborgs Stads information bara genom att uppgifterna förs över till Office 365. Dessutom bedöms det osannolikt att åtkomst ges inom ramen för CLOUD Act, varför stadsjuristerna anser att något röjande i OSL:s mening inte sker till amerikanska myndigheter genom överföring av uppgifter till Office 365. I de fall amerikanska myndigheter får tillgång till uppgifter som är sekretessreglerade skulle ett utlämnande enligt 8 kap. 3 § OSL ändå vara tillåtet eftersom informationen i motsvarande fall sannolikt skulle lämnas ut till en svensk myndighet. Hur den myndighet som är ansvarig enligt OSL skulle ha fullgjort sin prövningskyldighet enligt 8 kap. 3 § OSL framgår inte.

Göteborgs Stad har inte heller i någon allmänt tillgänglig promemoria bedömt dataskyddsförordningen (GDPR) i förhållande till Office 365 eller gjort någon bedömning av huruvida användandet av Office 365 innebär intrång i den personliga integriteten för personer vars uppgifter hanteras i Office 365 eller om det finns effektiva rättsmedel att tillgå för de vars personliga integritet kan komma att kränkas.

## Vikten av tillsyn

I regeringens digitala agenda för Sverige betonas vikten av att privata och offentliga aktörer agerar ansvarsfullt. Digitala system ska vara säkra och den personliga integriteten ska värnas. Regeringen framhåller även den ökade sårbarhet som följer av teknikberoendet, att allmänhetens tillit är beroende av teknikens säkerhet samt att allt fler statliga, regionala och kommunala myndigheter hanterar uppgifter i molntjänster. Göteborgs Stads användning av Office 365 är ett exempel.

Myndigheter som Pensionsmyndigheten, Kammarkollegiet och Försäkringskassan samt den myndighetsgemensamma föreningen eSamverkansprogrammet synes göra bedömningen att beskriven hantering av sekretessreglerade uppgifter samt personuppgifter är oförenlig med svensk grundlag, dataskyddsförordningen och internationell rätt. Samma bedömning gör Europeiska dataskyddsombudet. Privata leverantörer samt Sveriges Kommuner och Regioner hävdar att rättsläget är oklart medan andra aktörer som Göteborgs Stad förefaller göra bedömningen att villkoren i svensk och europeisk rätt inte är uppfyllda men att detta inte hindrar användande av Office 365.

En allt större andel av de uppgifter som är känsliga för individer och myndigheter samt för offentlig sektor i stort, hanteras i molntjänster. Detta har av flera bedömts vara både olagligt och olämpligt. Det är därför angeläget att det rättsliga läget klargörs snarast. Riskerna och konsekvenserna främst på lång sikt för vår nation är omöjliga att överblicka. Det är särskilt allvarligt om myndigheter, ivrigt påhejade av utländska kommersiella intressen, anser sig ha mandat att bortse från svensk grundlag för att det inte passar kortsiktiga ekonomiska intressen.

Det är därför angeläget att klargöra:

1. Utövar Göteborgs Stad sin verksamhet under lagarna så som det krävs enligt grundlag när staden hanterar uppgifter i Office 365?
2. Är rätten till privatliv och den personliga integriteten tillräckligt skyddad för de personer vars uppgifter hanteras i Göteborgs Stads användande av Office 365?
3. Följer Göteborgs Stad offentlighets- och sekretesslagstiftningen när sekretessreglerade uppgifter hanteras i Office 365?
4. Följer Göteborgs Stad EU:s dataskyddsförordning när personuppgifter hanteras i Office 365?
5. Finns det effektiva rättsmedel att tillgå för enskilda vars rättigheter kränks eller riskerar att kränkas genom att Göteborgs Stad hanterar enskildas uppgifter i Office 365?