Nulägesbeskrivning av Microsoft Teams ur ett integritetsskydds-perspektiv

Regionledningskontoret
Strategisk IT
Box 22550, 104 22 Stockholm
Telefon: 08-737 25 00
RS 2021-0840

Region Stockholm

Innehållsförteckning

1. Inledning

1.1 Sammanfattning

Region Stockholm (nedan kallad regionen) är kund till Microsoft, och regionens nämnder och bolag använder Microsoft Teams (nedan kallat Teams) för lagring av dokument samt intern och extern kommunikation. Efter att under ett flertal år fört löpande, strukturerade och mer eller mindre formella diskussioner med Microsoft kring hantering av personuppgifter, beslutade regionen att i juni 2021 genomföra en nulägesbeskrivning av lösningen Teams i projektform med informationsinsamling i dialog med Microsoft.

Nulägesbeskrivningen har genomförts *ur ett integritetsskyddsperspektiv* (att skilja från informationssäkerhetsperspektiv), det vill säga med beaktande av individers rätt till privatliv, och med särskild tyngdvikt på de krav som följer av svensk och europeisk integritetsskyddslagstiftning.[1] Nulägesbeskrivningen är vidare avgränsad till att *identifiera risker* som kan härledas till Teams design och villkor *oberoende av regionens planerade behandlingar*. Antagande görs således att identifierade risker skulle uppstå i nuläget oberoende av vilken eller vilka kategorier av behandlingar regionen planerar för i Teams, och är därmed relevanta att ta hänsyn till för samtliga verksamheter inom regionen vid bedömningar av för vilka typer av ändamål nyttjande av Teams skulle kunna vara lämpligt framöver.

1.2 Syften

Avsikten med denna rapport har varit att påbörja skriftlig dokumentation av identifierade risker för de registrerades rättigheter och friheter vid användning av Teams, så som Teams tillhandahålls sommaren 2021.

Rapporten har tagit avstamp i risker som följer av frågeställningen *”vilken information hanteras av vem, hur och varför inom ramen för respektive lösning som regionen nyttjar eller kan komma att nyttja?,* vilken varit den centrala frågeställningen i de dialoger som förts med Microsoft sedan 2019. Regionen anser att det med ett svar på den övergripande frågan finns goda förutsättningar att bedriva ett fortsatt systematiskt riskbaserat integritetsskyddsarbete, medan avsaknad av svar, vaga eller svårtolkade svar skulle peka på sämre förutsättningar att arbeta effektivt med integritetsskydd kopplat till Teams.

Syftet med rapporten har varit att fastställa en grund som eventuella förändringar av t.ex. villkor och/eller funktionalitet i Teams kan ställas i

[1] Till svensk och europeisk integritetsskyddslagstiftning hör bl.a. Förordning 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, i rapporten benämnd GDPR), samt Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

relation till i framtiden. Bedömningar och hantering av risker kan behöva justeras över tid, vilket kan effektiviseras om de kan ställas i relation till tidigare beslutad hanteringsplan inklusive faktiskt realiserade säkerhetsåtgärder.

Nulägesbeskrivningen ska även ligga till grund för att ta fram en långsiktig strategi kring ramar och förutsättningar för utkontraktering av de personuppgiftsbehandlingar, digitala förmågor och den funktionalitet som idag nyttjas och/eller potentiellt skulle kunna nyttjas genom Teams.

Riskerna kan med fördel även lyftas av regionens nämnder och bolag inom ramen för exempelvis konsekvensbedömningar, laglighetsbedömningar samt andra typer av risk- och lämplighetsanalyser för att effektivisera arbetet i de lägen där Teams är aktuellt som lösning för planerade behandlingar. Bedömning och hantering av de identifierade riskerna kommer således alltid behöva göras i förhållande till specifika verksamhetsändamål, tillgängliga medel och resurser samt utifrån omständigheter i de enskilda fallen.

1.3 Bakgrund

Microsoft har de senaste tio åren ändrat flertalet av sina leveransmodeller till att erbjuda fler funktioner som tjänster istället för som produkter. Denna förändring, i kombination med en mer omfattande lagstiftning som reglerar personuppgiftshantering inom EU och Sverige, har gjort att dessa frågor blivit ännu mer aktuella. Under 2018 trädde såväl GDPR[2] som den amerikanska lagstiftningen om datautlämning, Cloud Act[3], i kraft. Lagstiftningarnas ikraftträdande har bl.a. skapat ett större behov av administrativa expertresurser och utökade medel för att möjliggöra de löpande bedömningar, riskanalyser och den dokumentation som krävs när lösningar tillhandahålls av externa parter med dynamiska villkor, i synnerhet sådana lösningar som innebär tredjelandsöverföringar och/eller potentiella tredjelandsöverföringar till leverantörer som verkar i exempelvis USA.

Regionen har sedan 2017 på ett allt mer strukturerat och målinriktat sätt diskuterat integritetsskyddsfrågor med Microsoft och andra större mjukvaruleverantörer. Parallellt med diskussionerna med Microsoft har regionen löpande läst och analyserat den information rörande Teams och hantering av personuppgifter i lösningen som Microsoft publicerat för allmänheten och/eller sina kunder. Regionen har också bedrivit omvärldsbevakning i form av bl.a. deltagande i olika konferenser och utbildningar, granskning av samrådsyttranden från IMY och genomgång av uttalanden, vägledningar och rekommendationer från institutioner inom EU. Vidare har regionen fört diskussioner med andra regioner, kommuner och offentliga aktörer såsom SKR rörande de icke-konfidentiella (standardiserade) villkoren som tillhandahålls av Microsoft vid nyttjande av Teams.

[2] Förordning 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).

[3] Clarifying Lawful Overseas Use of Data Act (Cloud Act).

Sommaren 2020 meddelade EU-domstolen dom i det så kallade Schrems II-målet[4], angående giltiga respektive ogiltiga grunder för överföring av personuppgifter från EU till USA. I början av 2021 kom ett pressmeddelande från Microsoft som deklarerade intentioner att på central nivå investera stora summor för anpassning av globala tjänster – inklusive Teams – till den europeiska dataskyddslagstiftningen fram till hösten 2022.

1.4 Avgränsning

Denna rapport avgränsar sig till att *beskriva ett nuläge* genom att *identifiera och dokumentera risker* inom ramen för *integritetskyddsperspektivet* och har utförts genom informationsinsamling och observationer av *Teams* och *Microsoft som leverantör* av densamma.

Regionen har valt att göra ett antal avgränsningar också inom ramen för ett integritetsskyddsperspektiv på användning av Teams. Bland dessa ska framförallt risker hänförliga till den *geografiska platsen för behandlingen av personuppgifterna* nämnas. Skälet till denna avgränsning är att regionen identifierat ett behov av en djupare grundförståelse avseende Microsofts behandling av personuppgifter och de risker användningen av Teams kan medföra för regionens registrerade, oberoende av var personuppgifter behandlas. Regionen har bedömt att en sådan grundförståelse utgör förutsättning för att korrekt kunna bedöma laglighet och lämplighet av eventuella överföringar av personuppgifter utanför Sverige eller EU. Regionen avser att hantera frågan om den geografiska platsen för behandlingen av personuppgifter efter att genom detta projekt ha skapat sig den grundförståelse som krävs för en sådan analys.

Rapporten är vidare avgränsad till att *beskriva* de risker användningen av Teams kan innebära för de registrerades fri- och rättigheter. Det innebär att *bedömning* och *hantering* av de identifierade riskerna, däribland bedömning av specifika lämpliga säkerhetsåtgärder utifrån omständigheter i det enskilda verksamhetsfallet och om det är realiserbart att vidta dessa säkerhetsåtgärder på ett effektivt och hållbart sätt, exkluderats. Dessa aspekter planerar regionen att, med utgångspunkt i denna nulägesbeskrivning, istället belysa i ett senare skede av arbetet.

1.5 Genomförande

Upplägget för projektet som regionen och Microsoft inledningsvis enades om skulle genomföras i form av två stycken 1-2 timmars workshoppar för informationsinsamling. Under dessa möten skulle 14 frågor rörande integritetsskydd kopplat till Teams diskuteras och besvaras. Frågorna hade utformats av regionen utifrån lärdomar, kunskap och behov av förtydliganden

[4] Mål C-311/18.

till följd av tidigare dialoger med Microsoft. Regionen skulle därefter internt ta fram en nulägesbeskrivning i form av en rapport som överblickar de risker regionen identifierat med Teams sett ur ett integritetsskyddsperspektiv. Från regionen deltog egna och externa resurser kopplat till integritetsskydd, licenshantering, riskhantering och molnlösningar. Från Microsoft deltog kundansvariga, tjänstespecialister, jurister, avtalsspecialister och informationssäkerhetsspecialister, antingen direkt i mötena eller som resurser i bakgrunden.

Microsoft fick ta del av de ursprungliga frågorna innan den första workshoppen och valde genomgående att, utöver muntliga redogörelser, presentera sin syn på respektive fråga i form av en skriftlig presentation som regionen senare fick ta del av. Vid de första två workshopparna diskuterades de svar som Microsoft presenterade, bl.a. huruvida det fanns en gemensam syn på frågeställningarna, om svaren Microsoft gav på respektive fråga var tydliga och lättbegripliga eller inte, samt om svaren kunde styrkas skriftligt t.ex. genom garantier i avtalsvillkor eller i Microsofts information till de registrerade. I samband med dessa två workshoppar uppkom två ytterligare frågor utifrån Microsofts önskan att några av de ursprungliga frågorna skulle förtydligas. Parterna enades om att vidga projektets omfattning med en tredje workshop med fler och nya mötesdeltagare i syfte att ge parterna ytterligare möjligheter att tydliggöra och diskutera tidigare svar utöver det som redan framförts under de första två workshopparna. Vid den tredje workshoppen deltog bl.a. en jurist, en avtalsspecialist och chefen för hälso- och sjukvård för Microsoft Sverige. Två dagar efter detta tredje möte presenterade regionen några preliminära identifierade risker och övergripande feedback.

Regionen har under projektet gjort observationer och tagit del av information och dokument från Microsoft, som granskats i syfte att identifiera och förstå eventuella risker med användning av Teams utifrån ett integritetsskyddsperspektiv.

1.6 Målgrupp

Rapporten riktar sig först och främst till nämnder och bolag inom Region Stockholm. Målgruppen inkluderar verksamhetschefer, jurister, dataskyddsombud, integritetsskyddshandläggare, liksom stöd- och kontrollfunktioner inom dataskydd, informationssäkerhet och IT samt övrig personal som arbetar med verksamhetsutveckling i form av digitalisering.

I andra hand kan rapporten fungera som del av leverantörsstyrnings- och samverkansprocesser med Microsoft. Målgrupp är således även personal hos Microsoft som i huvudsak arbetar med integritetsskyddsfrågor och/eller personal som kan facilitera vidare diskussioner internt inom Microsoft i syfte att utveckla leverantörens insikt, organisation och mognad avseende krav på personuppgiftsbehandling i förhållande till såväl europeiska som specifikt svenska offentliga kunder och kunder inom hälso- och sjukvård.

2. Om Teams

Teams är en samarbetsplattform som möjliggör extern och intern kommunikation samt fildelning mellan dess användare. Teams är en klient/server-lösning som lanserades år 2018 och är en vidareutveckling av bl.a. Skype och Yammer samt bygger vidare på funktionalitet som tidigare introducerats inom ramen för bl.a. OneDrive (såsom fillagring), Sharepoint (såsom fildelning och anslagstavlor) och Outlook (såsom kalender). Teams är en integrerad del av Microsoft 365 vilket innebär att den har många och starka beroende till bl.a. andra Officelösningar och såväl Azure-AD som andra infrastrukturkomponenter från Microsoft.

Teams är en molntjänst som ligger inom ramen för en SaaS-lösning (Software as a Service) och är därmed i grunden byggd som en s.k. ”evergreen”, en tjänst som ständigt utvecklas och där gränser och omfattning av tjänsten kontinuerligt förändras i takt med lansering av t ex ny funktionalitet, förändring av priser och/eller justering av villkor. Nya uppdateringar aviseras löpande av Microsoft vilket ställer krav på att regionen löpande sätter sig in i redan realiserade och/eller aviserade förändringar och i varje enskilt fall bedömer på vilka sätt dessa förändringar kan komma att påverka bl.a. befintliga identifierade risker för de registrerade och behandlingar av personuppgifter som pågår och/eller planeras att påbörjas inom ramen för lösningen.

2.1 Behandling av personuppgifter i Teams

Vid användning av Teams är viss behandling[5] av personuppgifter[6] ofrånkomlig, då den utgör en förutsättning för tjänsten i sitt grundinförande som innehåller bl.a. användarbaserad inloggning och autentisering. Integritetsskyddslagstiftningen kommer därigenom alltid i någon utsträckning vara tillämplig vid användningen av lösningen. Behandling av personuppgifter påbörjas av Microsoft, både i egenskap av personuppgiftsbiträde och personuppgiftsansvarig, redan vid uppsättningen av Teams - med eller utan faktisk aktivitet eller nyttjande.

När en medarbetare eller användare får ett konto i regionens uppsättning av Teams, sker alltid en behandling av förnamn, efternamn, e-postadress, telefonnummer (om uppgiften finns tillgänglig), medarbetarens/användarens

[5] Definition enligt GDPR (art 4) av *behandling*: ”en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,”

[6] Definition enligt GDPR (art 4) av *personuppgifter*: ”varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,”

organisationstillhörighet, kostnadsställe samt vissa uppgifter om användarens enhet. Vilka övriga kategorier av personuppgifter som kan behandlas i Teams utöver de som följer av grundinförandet, är upp till regionen att besluta om genom instruktioner till användarna.

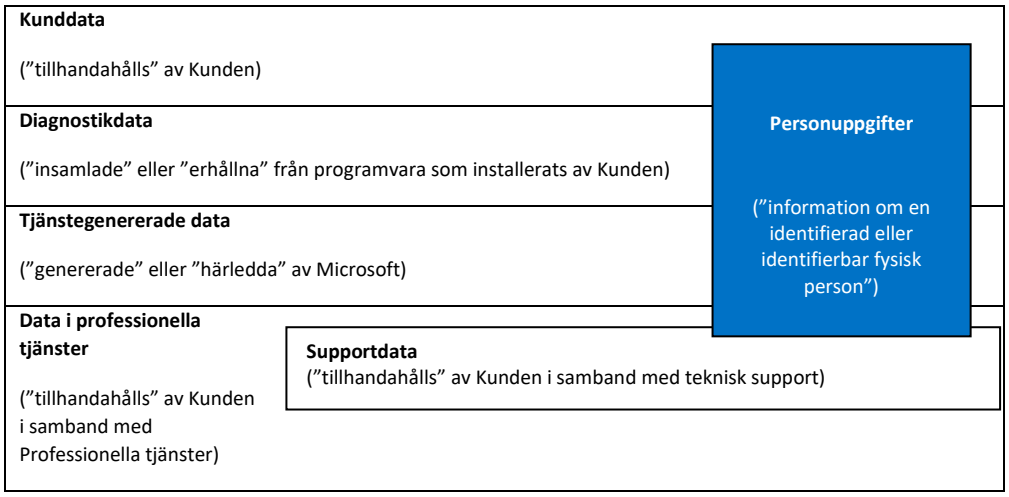
2.2 Personuppgiftsbiträdesavtal

Regionen och Microsoft har ingått ett personuppgiftsbiträdesavtal som reglerar Microsofts skyldigheter beträffande behandling av och säkerhet för kunddata och personuppgifter i samband med tillhandahållande av bl.a. Teams till regionens nämnder och bolag (”Personuppgiftsbiträdesavtalet”)[7]. Enligt Personuppgiftbiträdesavtalet, ska Microsoft enbart behandla personuppgifter enligt regionens dokumenterade instruktioner för att a) tillhandahålla regionen Onlinetjänsterna och Professionella tjänster, däribland Teams, samt för b) Microsofts berättigade verksamhetsutövning i samband med leverans av dessa tjänster.

Regionens volymlicensieringsavtal, inbegripet Personuppgiftsbiträdesavtalet, i kombination med produktdokumentationen och regionens användning och konfigurering av funktioner i Onlinetjänsterna anges utgöra regionens fullständiga dokumenterade instruktioner till Microsoft för behandling av Personuppgifter.

I Personuppgiftsbiträdesavtalet förekommer begreppen kunddata, diagnostikdata, tjänstegenererade data, data i professionella tjänster och supportdata, vilka anges utgöra ”datatyper”. Samtliga datatyper anges kunna innehålla både personuppgifter och övrig information. Det framgår emellertid inte vilka följder det har att personuppgifter av Microsoft kategoriseras i dessa datatyper, eller kopplingen mellan uppdelningen i datakategorier och kraven på behandling av personuppgifter som följer av GDPR. Datakategorierna beskrivs översiktligt nedan.

[7] Microsoft Onlinetjänster - Dataskyddstillägg, senast uppdaterat 9 december 2020.



2.3 Särskilt om fördelningen av personuppgiftsansvar i Teams

Enligt Personuppgiftsbiträdeavtalet, är regionen personuppgiftsansvarig och Microsoft personuppgiftsbiträde och/eller underbiträde. Däremot anges, att i den mån Microsoft använder eller i övrigt behandlar personuppgifter för Microsofts berättigade verksamhetsutövning, gör Microsoft detta i egenskap av självständig personuppgiftsansvarig. De ändamål som anges falla under Microsofts berättigade verksamhetsutövning är följande:

(1) Fakturering och kontohantering. (2) Ersättning (t.ex. beräkning av personalens provision eller partnerincitament). (3) Intern rapportering och företagsmodellering (t.ex. prognostisering, intäkter, kapacitetsplanering, produktstrategi). (4) Bekämpning av bedrägeri, cyberbrott eller cyberangrepp som kan påverka Microsoft eller Microsoft-produkter. (5) Förbättra kärnfunktionerna för hjälpmedel, integritet eller energieffektivitet. (6) Ekonomisk rapportering och efterlevnad av skyldigheter enligt lag (underkastat nedanstående begränsningar avseende utlämnande av Behandlade data).

Av Personuppgiftsbiträdsavtalet framgår uttryckligen att Microsoft vid tillhandahållandet av tjänsterna inte ska använda eller på annat sätt behandla personuppgifter för: (a) Användarprofilering. (b) Annonsering eller liknande kommersiella ändamål. (c) Marknadsundersökning i avsikt att skapa nya funktioner, tjänster eller produkter, eller i något annat syfte, såvida inte sådan behandling är förenlig med Kundens dokumenterade instruktioner.

I Personuppgiftsbiträdesavtalet saknas närmare beskrivning av vilka personuppgifter som behandlas för dessa ändamål av Microsoft som personuppgiftsansvarig, eller i vilken omfattning sådan behandling sker.

Oberoende av fördelningen av personuppgiftsansvar för de behandlingar som utförs av regionen och Microsoft vid regionens användning av Teams, har regionen en skyldighet att göra en helhetsbedömning avseende risker för de

registrerades rättigheter och friheter och då kan hantering av personuppgifter inom ramen för de kategorier Microsoft är personuppgiftsansvarig för också bli föremål för regionens bedömning av lösningens laglighet och lämplighet i senare skede. Vidare är regionen enligt kap. 21 7§ OSL skyldig att tillse att sekretess råder för personuppgifter om det kan antas att uppgifterna efter ett utlämnande kan komma att behandlas i strid med GDPR. Frågan om Microsofts efterlevnad av GDPR är därför också i de fall Microsoft utgör personuppgiftsansvarig viktig för att säkerställa regionens lagstadgade krav på sekretess.

I nuläget saknas dokumentation om och insikt i frågan huruvida ett gemensamt personuppgiftsansvar kan anses föreligga mellan Microsoft och regionen för någon av de datakategorier som omnämns, varför det i nuläget inte antas förekomma.

3. Observationer

Nedan presenteras en lista på relevanta observationer och risker avseende integritetsskydd som regionen har identifierat i dialogen med Microsoft. Listan är ej heltäckande eller uttömmande. Under respektive risk påtalas ett urval av konsekvenser som kan uppstå om risken realiseras d.v.s. skador eller avvikelser som kan uppstå vid påbörjade behandlingar och/eller nyttjande av tjänsten i nuläget om inte risken kan hanteras effektivt över tid.

Observationerna har följande teman:

3.1 Bristande transparens avseende Microsofts egna behandlingar

a) Otydlighet avseende innebörden av Microsofts egna behandlingar i Teams
Av Personuppgiftsbiträdesavtalet framgår att utöver den kunddata Microsoft behandlar såsom personuppgiftsbiträde till regionen, behandlar Microsoft personuppgifter i rollen som personuppgiftsansvarig med stöd av sin berättigade verksamhetsutövning. Det innebär att personuppgifter som regionen för in i Teams direkt eller indirekt behandlas för ytterligare ändamål utöver de som regionen instruerar Microsoft att utföra.

Som angetts ovan, innehåller Personuppgiftsbiträdesavtalet en uttömmande lista över de *ändamål* för vilka Microsoft behandlar personuppgifter såsom personuppgiftsansvarig, nämligen

> *”(1) Fakturering och kontohantering. (2) Ersättning (t.ex. beräkning av personalens provision eller partnerincitament). (3) Intern rapportering och företagsmodellering (t.ex. prognostisering, intäkter, kapacitetsplanering, produktstrategi). (4) Bekämpning av bedrägeri, cyberbrott eller cyberangrepp som kan påverka Microsoft eller Microsoft-produkter. (5) Förbättra kärnfunktionerna för hjälpmedel, integritet eller energieffektivitet. (6) Ekonomisk rapportering och efterlevnad av skyldigheter enligt lag (underkastat nedanstående begränsningar avseende utlämnande av Behandlade data)”.*

Det anges särskilt att kunddata eller personuppgifter inte behandlas för användarprofilering, marknadsföring eller liknande kommersiella syften, eller för andra ändamål som inte framgår av personuppgiftsbiträdesavtalet.

Av art. 5.1 led b GDPR följer att personuppgifter ska samlas in för särskilda, uttryckligt och angivna ändamål. Av skäl 39 GDPR följer vidare att de specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Av Integritetsskyddsmyndighetens (IMY) vägledning på området[8], framgår att ”Ändamålen måste vara specifika och konkreta, inte luddiga eller otydliga. [..] Det räcker normalt inte heller att ert ändamål enbart är att "förbättra användarnas upplevelse", "it-säkerhet" eller "framtida forskning". Det är alltför brett uttryckt, och de registrerade kan inte bedöma vad sådan personuppgiftsbehandling kan innebära.”

Mot bakgrund av de krav på tydlighet avseende ändamål som följer av GDPR, anser regionen att flera av de ändamål som anges för Microsofts egna behandlingar inte är tillräckligt specifika och konkreta. Det är exempelvis inte möjligt för regionen eller de registrerade att förstå den närmare innebörden av att personuppgifter, om än efter att ha sammanställts på aggregerad nivå, behandlas för prognostisering, produktstrategi och för bekämpning av bedrägeri, cyberbrott eller cyberangrepp.

[8] IMY:s vägledning avseende ändamålsbegränsning (hämtad 9/9-21).

Risk

Regionen är föremål för omfattande lagkrav avseende sin behandling av personuppgifter, och måste för att kunna använda Teams ha insikt i hur personuppgifter som delas med Microsoft behandlas. Vid anlitande av en leverantör med vilken personuppgifter delas, är det helt avgörande att förstå vilka personuppgifter som delas och hur uppgifterna sedermera behandlas av leverantören. Utan insikt i den närmare innebörden av de ytterligare behandlingar som utförs av Microsoft i egenskap av personuppgiftsansvarig, är det inte möjligt för Region Stockholm att utvärdera om användningen av Teams uppfyller kraven i GDPR på t.ex. ändamålsbegränsning och säkerhet för personuppgifterna, samt OSL:s krav på sekretess.

b) Personuppgiftsbehandlingar utöver villkoren

Microsoft har tagit kontakt direkt med användare (medarbetare) inom regionen med förfrågan om att tillhandahålla s.k. ”Valfria anslutna upplevelser”9. Såväl utskick till användare med förfrågan om anslutning till Valfria anslutna upplevelser, som ingående av avtal med användare för detta ändamål, innebär att användarens personuppgifter behandlas. Det innebär att Microsoft, i egenskap av personuppgiftsansvarig och med stöd av samtycke, avtal och/eller berättigat intresse10, behandlat personuppgifter som regionen överfört till Microsoft för ändamål som inte framgår av Personuppgiftsbiträdesavtalet, för att ingå avtal om eller inhämta samtycke till ytterligare behandlingar av personuppgifter som inte heller de följer av Personuppgiftsbiträdesavtalet.

Risk

Regionen behöver ha insikt i hur personuppgifter som delas med Microsoft inom Teams behandlas. Microsofts behandling av personuppgifter som delats av regionen, för ändamål som går utöver de som anges i Personuppgiftsbiträdesavtalet, kräver att regionen informeras om dessa behandlingar och godkänner dem i behörig ordning. Den behandling av personuppgifter som sker när Microsoft kontaktar användare inom regionen med erbjudande om att ingå ”Valfria anslutna upplevelser” angränsar mot att utgöra marknadsföring, vilket är ett av de ändamål som Microsoft enligt Personuppgiftsbiträdesavtalet uttryckligen inte ska behandla personuppgifter

[9] ”Valbara anslutna upplevelser” beskrivs här *https://docs.microsoft.com/sv-se/deployoffice/privacy/optional-connected-experiences* medan ”Valbara tjänster” (”Connected Experiences”) har villkor som omfattas av Microsoft Service Agreement *https://www.microsoft.com/servicesagreement* och Microsoft Privacy Statement *https://privacy.microsoft.com/*. Avtalet accepteras i samband med att användaren första gången använder tjänsten genom användarens samtycke.

[10] Den rättsliga grunden för utskick med förfrågan om anslutning till Valfria anslutna upplevelser kan antas vara berättigat intresse (då detta angetts för samtliga behandlingar för vilka Microsoft är personuppgiftsansvarig i dialogen), medan behandling av personuppgifter inom ramen för tillhandahållandet av Valfria Anslutna Upplevelser beskrivs på ett sätt som skulle antyda att det rör sig om samtycke och/eller avtal med den registrerade. Följande text har hämtats från *https://docs.microsoft.com/sv-se/deployoffice/privacy/optional-connected-experiences* (hämtad 26/8-2021): *”Det är viktigt att känna till att dessa valfria molnbaserade tjänster inte omfattas av organisationens licens med Microsoft. I stället är de licensierade direkt till dig. Genom att använda de valfria molnbaserade tjänsterna godkänner du också Villkor för Microsoft-tjänster och sekretesspolicyn. Ytterligare villkor kan också gälla beroende på vilken tjänst du använder. Det tas i de flesta fall inte ut någon avgift för att använda tjänsterna. Om en avgift tas ut (vilket kan vara fallet med vissa tillägg som är tillgängliga för nedladdning via Office Store), kommer du att bli tydligt informerad innan du använder dem.”*

för. Regionens avtalsansvariga, som har behörighet att diskutera avtalsändringar, har inte informerats om behandlingen på förhand utan gjorts medvetna om den först i samband med erbjudandet de mottagit i egenskap av medarbetare.

De personuppgiftsbehandlingar som sker när en användare ingått avtal om Valfria anslutna upplevelser är förvisso baserade på avtal med användarens eller med stöd av dennes samtycke, och föremål för ett eget avtal mellan användaren och Microsoft. Behandlingarna är likväl problematiska ur ett flertal aspekter:

- Det finns en risk att användaren inte uppfattar att Valfria anslutna upplevelser är ett avtal som ingås mellan användaren och Microsoft, utan istället tror att det är en del av de arbetsverktyg regionen tillhandahåller. Det påverkar användarnas förmåga att fatta informerade och välgrundade beslut om hur deras personuppgifter behandlas.
- Genom användares anslutning till Valfria anslutna upplevelser kan personuppgifter om andra registrerade inom regionen komma att behandlas och delas med externa parter, t.ex. genom omnämnandefunktionen eller funktionen för att koppla externa listor till Outlook, för ändamål som dessa registrerade inte samtyckt till eller avtalat om.
- Möjligheten för användare att ansluta sig till Valfria anslutna upplevelser styrs genom tekniska konfigurationer av Microsofts Onlinetjänster. Det innebär att det är tekniska administratörer inom regionen som styr över vilka registrerade som kan kontaktas för att ansluta sig till Valfria anslutna upplevelser, och sedermera genom en sådan anslutning dela sina egna och andras personuppgifter inom ramen för Teams. I praktiken innebär det att beslut om Microsofts möjlighet till personuppgiftsbehandlingar som går utöver de personuppgiftsbehandlingar som parterna kommit överens om genom personuppgiftsbiträdesavtalet lämnas till personer utan behörighet att ingå eller godkänna ändringar av avtal.

3.2 Otydlig fördelning av personuppgiftsansvar

Enligt Personuppgiftsbiträdesavtalet, är regionen personuppgiftsansvarig för de behandlingar som utförs av Microsoft för att tillhandahålla Teams. Dessa behandlingar utgörs av de behandlingar av personuppgifter som utförs i syfte att:

- Leverera fungerande resurser enligt Kundens och dess användares licens, konfiguration och användning, inbegripet tillhandahållande av personligt anpassade användarupplevelser.
- Felsökning (förebyggande, detektion och åtgärdande av problem).
- Fortlöpande förbättring (installera de senaste uppdateringarna och göra förbättringar för användarproduktivitet, tillförlitlighet, effektivitet och säkerhet).

Microsoft har angivit att det innebär att regionen är personuppgiftsansvarig för behandlingen av personuppgifter i de datakategorier Microsoft benämner Diagnostiska data och Tjänstegenererade data, under förutsättning att dessa behandlingar sker i led att tillhandahålla Teams. Diagnostiska data utgörs enligt information på Microsofts hemsida av ”*alla de data som ’samlas in’ eller ’erhålls’ från programvara du installerar lokalt för användning i samband med Microsofts onlinetjänster för företag. Det används för att hjälpa Microsoft säkerställa att klientprogramvaran är säker och fungerar på korrekt sätt. Microsoft samlar till exempel in information om hur lång tid det tar att starta en app, om ett tillägg har kraschat och hur många inloggningsförsök som har gjorts. Diagnostiska data kallas även telemetridata. Det innehåller inte namn, e-postadresser eller filinnehåll.*”. Tjänstegenererade data beskrivs omfatta '*alla de data som ’genereras’ eller ’härleds’ av Microsoft via en onlinetjänst. Microsoft samlar in dessa data från våra onlinetjänster och använder dem för att säkerställa att prestanda, säkerhet, skalning och andra tjänster som påverkar kundupplevelsen fungerar på den nivå som våra kunder kräver. För att till exempel förstå hur datacenterkapaciteten ska utökas i takt med att en kunds användning av Microsoft Teams ökar, bearbetar vi loggdata av deras Teams-användning. Vi går därefter igenom loggarna för att hitta högbelastningstider och bestämmer vilka datacenter som ska läggas till för att tillmötesgå denna kapacitet.*”

För regionen är det inte tydligt i vilken utsträckning behandlingen av dessa datakategorier sker som ett led i att tillhandahålla Teams till regionen, och i vilken utsträckning de sker för Microsofts berättigade verksamhetsutövning. Eftersom denna fråga är avgörande för vilken av parterna som enligt Personuppgiftsbiträdesavtalet utgör personuppgiftsansvarig, innebär denna otydlighet att regionen har svårt att avgöra hur och i vilket skede personuppgiftsansvaret övergår till Microsoft. Det leder i sin tur till att regionen har svårt att bedöma om de krav som åligger regionen i egenskap av personuppgiftsansvarig upprätthålls vid dessa behandlingar.

Med beaktande av att personuppgiftsansvar ska bedömas utifrån de faktiska omständigheterna vid varje behandling av personuppgifter, och inte kan regleras genom avtal, kan det också ifrågasättas om regionen har en tillräcklig insikt i och inflytande över de behandlingar som sker för andra ändamål än ren teknisk lagring och bearbetning av regionens personuppgifter. Detta gäller särskilt de behandlingar av personuppgifter som utförs i syfte att förbättra tjänsten, då regionen saknar inflytande avseende såväl ändamål och medel för dessa behandlingar på det sätt som anges som kriterier för personuppgiftsansvar i art. 4.7 GDPR.

Otydligheten har också visat sig ha effekt på de registrerades möjligheter att utöva sina rättigheter enligt GDPR. Det har förekommit att medarbetare i regionen, i egenskap av registrerade, kontaktat Microsoft med förfrågningar avseende behandlingen av deras personuppgifter inom ramen för de behandlingar för vilka Microsoft är personuppgiftsansvarig. De registrerade har

då hänvisats till att kontakta Microsoft via formulär på hemsidan[11]. Vid förfrågningar som sedermera gjorts via hemsidan har det visat sig att den personal hos Microsoft som besvarar dessa förfrågningar i flertalet mejl hänvisat de registrerade tillbaka till regionen för att utöva sina rättigheter – trots att den registrerade klargjort att förfrågan endast avser behandlingar för vilka Microsoft är personuppgiftsansvarig.

Risk

En osäkerhet kring fördelningen av personuppgiftsansvar såväl som bristen på insikt och inflytande rörande behandlingar som Region Stockholm är personuppgiftsansvarig för, medför svårigheter att säkerställa att personuppgifterna behandlas i enlighet med kraven i GDPR. Det skapar också en otydlighet i fråga om rättslig grund för behandling av personuppgifterna, då regionen och Microsoft har olika rättsliga grunder för sina respektive behandlingar. Eftersom ansvaret för de behandlingar som sker inom ramen för Teams inte har kunnat fastställas fullt ut är det inte möjligt för regionen att föra en fullständig förteckning över behandlingar enligt artikel 30 GDPR. Osäkerheten innebär även att såväl regionen som Microsoft riskerar att den personuppgiftsansvariges skyldigheter inte fullgörs eftersom de ”faller mellan stolarna”, inte minst skyldigheten att upprätthålla transparens i förhållande till de registrerade.

3.3 Otydlighet kring datastadier

Microsoft har angett att de personuppgifter som behandlas i Teams befinner sig antingen i stadiet data at rest, eller i stadiet data in transit. Eftersom Teams är en klient/server-lösning utgår regionen från att personuppgifter för vilka Microsoft är personuppgiftsvarig till viss del befinner sig i data at rest i regionens miljö, för att sedan överföras till Microsoft där de landar i data at rest. I diskussion med Microsoft har det framkommit att Microsoft ej anser sig behandla personuppgifter i stadiet data in use, vilket utifrån regionens förståelse är ett begrepp/ett stadium som Microsoft inte använder sig av eller tar hänsyn till i sina lösningar. För att kunna förstå hur personuppgifter flödar i Teams, särskilt vid vilket stadie personuppgifter överförs till Microsoft, är regionen av uppfattningen att det är nödvändigt att klargöra var personuppgifterna befinner sig när de är i vad regionen i bl.a. sitt arbete med integritetsskydd hänvisar till som stadiet data in use[12]. Detta är framför allt viktigt för att förstå vilka säkerhetsåtgärder som vidtas, och omfattningen av Microsofts ansvar i detta stadie.

[11] Microsoft-Report a Privacy Concern (hämtad 10/9-21).

[12] Data som befinner sig i tillståndet "data in use" är data som aktivt används och behandlas av en användare i en applikation. Data i detta tillstånd kan förändras av användaren och för att detta ska vara möjligt behöver data vara dekrypterad, vilket innebär att data i detta tillstånd är mer sårbar.

Risk

I nuläget har regionen och Microsoft inte nått en samsyn kring de olika datastadier som personuppgifter befinner sig vid användning av Teams. Denna osäkerhet innebär att regionen inte kan bedöma vilka säkerhetsåtgärder som vidtas för personuppgifter som befinner sig i vad regionen hänvisar till som data in use, och om dessa säkerhetsåtgärder är tillräckliga för de behandlingar som sker i Teams.

3.4 Avsaknad av förmåga att motta instruktioner

Microsoft har angett att de enbart kan motta instruktioner avseende personuppgiftsbehandlingar de utför som personuppgiftsbiträde åt regionen, om instruktionen återspeglar Teams tekniska funktionalitet. Regionen ges därmed inte möjlighet att dela instruktioner som innehåller information om bl.a. ändamålet med behandlingen, vilka personuppgifter som behandlas samt vilka som utgör de registrerade. Istället hänvisar Microsoft till att regionen kan påverka säkerhetsåtgärderna genom konfigurationer av tjänsten, men anger samtidigt att skyddet är detsamma oaktat typen av data som regionen lägger in i Teams.

Kärnan i förhållandet mellan en personuppgiftsansvarig och ett personuppgiftsbiträde är att behandlingen av personuppgifter utförs av personuppgiftsbiträdet och/eller underbiträden för den personuppgiftsansvariges intresse och på dennes instruktioner. Instruktioner ska ges för varje behandlingsaktivitet.[13] I Europeiska Dataskyddstyrelsens riktlinjer avseende begreppen personuppgiftsansvarig och personuppgiftsbiträde anges följande: "*In the case of data protection law, a processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means".*[14] Vidare anges: *"Even if the processor offers a service that is preliminary defined in a specific way, the controller has to be presented with a detailed description of the service and must make the final decision to actively approve the way the processing is carried out and request changes if necessary."*[15]

Enligt Personuppgiftsbiträdesavtalet, ska regionens instruktioner till Microsoft i sin helhet utgöras av volymlicensieringsavtalet (inbegripet DPA-villkoren och eventuella tillämpliga uppdateringar) tillsammans med produktdokumentationen samt regionens användning och konfigurering av funktioner i Teams. Med denna nuvarande ordning, där regionen i hög grad är

[13] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, punkt 116.
[14] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, punkt 80.
[15] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, punkt 30.

förpassad till Microsofts standardutformning av Teams, saknar regionen möjlighet att anpassa användningen av Teams efter sina förändrade behov.

Risk

Bristen på möjlighet att ge Microsoft instruktioner avseende behandlingen, särskilt rörande ändamål och medel, innebär att varje förändrat behov av åtgärder som uppstår inom regionen kan leda till att regionen tvingas upphöra med användningen av Teams. Det skapar i sin tur svårigheter för regionen att upprätthålla långsiktighet och kontinuitet i användningen av Teams. Denna svårighet förstärks av såväl tjänstens som villkorens dynamiska karaktär. Det faktum att Microsoft har en omfattande kontroll över personuppgiftsbehandlingen, på ett sätt som påminner om en personuppgiftsansvarigs, innebär också en risk att Personuppgiftsbiträdesavtalet inte återspeglar den faktiska fördelningen av personuppgiftsansvar som föreligger enligt definitionerna i GDPR, och att parterna därmed agerar utifrån felaktiga ansvarsroller.

3.5 Avtalsvillkor

a) Avtalsvillkoren är dynamiska och uppdateras ensidigt med hög frekvens
Villkoren för Teams, inklusive till vilka länder personuppgifter överförs och omfattningen av överföringarna, uppdateras löpande utan särskilt godkännande från regionen. Sett utifrån Microsofts perspektiv, anses godkännande ske genom fortsatt användning av tjänsten. Under det senaste året har cirka fem till tio uppdateringar på funktionell nivå rapporterats per vecka inom ramen för Office365. Dessa uppdateringar kan ha en direkt eller indirekt påverkan på Teams och skyddet för de registrerades fri- och rättigheter. Till uppdateringarna följer dock inte med någon beskrivning av vilka eventuella förändringar som uppdateringarna medför i fråga om hur personuppgifter behandlas i just Teams och i förhållande till de ändamål som regionen avser nyttja lösningen för.

Risk

De frekventa uppdateringarna av villkoren kräver omfattande resurser och kompetens för hantering hos regionen, och försvårar för regionen att bevaka att personuppgifterna som överförs till Microsoft genom Teams behandlas på ett sätt som uppfyller de krav som åligger regionen vid utkontraktering av informationsbehandling. Detta kan i förlängningen innebära att personuppgifter behandlas i strid med GDPR eller annan integritetsskyddande lagstiftning.

b) Avtalsvillkoren är inte transparenta
Villkoren för Teams och instruktionerna för Microsofts behandling av personuppgifter är reglerade i flertalet dokument, däribland volymlicensieringsavtalet (inbegripet Personuppgiftsbiträdesavtalet och

eventuella tillämpliga uppdateringar), produktdokumentationen och regionens användning och konfigurering av funktioner i Teams.

Av art. 28 GDPR framgår vad ett personuppgiftsbiträdesavtal måste innehålla. Av artikeln följer bl.a. att avtalet ska ange föremålet för behandlingen, samt behandlingens varaktighet, art och ändamål. Innebörden av kraven i art. 28 GDPR har utvecklats av den Europeiska Dataskyddsstyrelsen, som i sina riktlinjer avseende begreppen personuppgiftsansvarig och personuppgiftsbiträde bl.a. anger att:

- Föremålet för behandlingen ska formuleras tillräckligt specifikt för att det ska vara tydligt vilket som är det huvudsakliga föremålet för behandlingen.
- Arten och ändamålen med behandlingen ska vara så utförlig som möjligt, så att externa parter ska kunna förstå innehållet och riskerna med behandlingarna som utförs av personuppgiftsbiträdet.
- Kategorierna av personuppgifter som behandlas ska specificeras så detaljerat som möjligt, och det är inte tillräckligt att enbart ange att ”personuppgifter” eller ”särskilda kategori av personuppgifter” behandlas.[16]

Villkoren och instruktionerna för Microsofts behandling av personuppgifter beskrivs för närvarande inte på ett sätt som fullt ut möjliggör för regionen att förstå hur Microsoft behandlar personuppgifter och med stöd av vilka bedömningar. Till exempel görs listor på dotterbolag och/eller underbiträden tillgängliga, men dessa förtydligas inte avseende vilka kategorier av behandlingar som utförs av respektive part över tid. Det specificeras inte heller vilka kategorier av personuppgifter respektive dotterbolag/underbiträde behandlar, utöver att ange att underbiträdena ges tillgång till ”kunddata”. Med hänsyn till att kunddata enligt Microsofts klassificering utgörs av all data regionen för in i Teams, ges regionen inte möjlighet att bedöma lämpligheten och lagligheten i dessa överföringar.

Risk

Det nuvarande personuppgiftsbiträdesavtalet möter inte de krav på transparens avseende behandlingarna av personuppgifter som följer av art. 28 GDPR och Europeiska Dataskyddsstyrelsens riktlinjer. Det finns vidare en risk för att personuppgifter överförs utanför EU/EES, utan att adekvata kompletterande säkerhetsåtgärder vidtagits för överföringen.

3.6 Ineffektivt organiserad hantering av personuppgifter ur ett integritetsskyddsperspektiv

Som aktör inom offentlig sektor samt tillhandahållare av hälso- och sjukvård, är regionen föremål för omfattande och komplexa krav på integritetsskydd vid

[16] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, punkt 114.

utkontraktering av personuppgiftsbehandlingar. För att kunna bedriva ett effektivt, hållbart, systematiskt och riskbaserat integritetskyddsarbete ställs höga krav på kompetens, resurser och rutiner inom dessa områden hos såväl regionen som dess leverantörer. I dialogen med Microsoft upplever regionen att Microsoft har lång erfarenhet och branschledande organisatorisk mognad i arbetet med bl.a. informationssäkerhet och i att utveckla attraktiva, användarvänliga och lättillgängliga programvarutjänster. I frågor som rör integritetsskydd upplever regionen att denna kompetens förvisso finns inom Microsoft, men att den inte är representerad i samma utsträckning som övriga kompetenser i den löpande dialogen med regionen som kund.

Det systematiska riskbaserade integritetsskyddsarbetet - som ska bedrivas både enskilt och gemensamt hos regionen som personuppgiftsansvarig och Microsoft i egenskap av både personuppgiftsbiträde och/eller underbiträde - ska ske i förhållande till behandlingarnas art och nyttjande av den aktuella tjänsten i den omfattning och med de avgränsningar som regionen planerar. Vidare ska Microsoft i egenskap av personuppgiftsansvarig säkerställa att de registrerades fri- och rättigheter skyddas och att ansvar och skyldigheter tillgodoses.

Medan regionen upplever ett professionellt bemötande från Microsofts kundnära personal, är dessa i frågor om integritetsskydd beroende av att involvera specialister i arbetet. Dessa specialister ingår inte i kundteamets standardutformning utan tillfrågas vid specifika frågeställningar, vilket påverkar specialisternas förutsättningar att sätta sig in i regionens särskilda förutsättningar. Specialisterna har vidare visat sig vara tillgängliga i begränsad omfattning för såväl kundteam som enskilda kunder. Detta arbetssätt skapar en tröskel för en kontinuerlig dialog anpassad utifrån regionens behov inom integritetsskyddsområdet, och försvårar möjligheten att med korta kommunikationsvägar kunna behandla dessa frågor inom det team som har bäst kunskap om regionen verksamhet och användning av Teams. Många gånger behöver svar på regionens frågors hanteras globalt, trots att frågan i sig berör förhållanden som uppkommer till följd av att de träffas av den unika kombinationen av europeisk och svensk lagstiftning. Det leder också till att svaren på de frågor regionen ställer till Microsoft ofta lämnas utan kontextuell hänsyn, vilket gör det svårt för regionen att omsätta svaren i praktiken, tillämpa dem över tid eller utgå från på en mer principiell nivå. Sammantaget leder detta till att regionen upplever en brist på helhetsansvar och tydlighet.

Det är viktigt att de personer som bedömer och vidtar säkerhetsåtgärder för de personuppgifter som behandlas i Teams – eventuellt inkluderat drift- och supportpersonal hos Microsoft - har god kunskap om både integritetsskydd och regionens olika typer av behandlingar av personuppgifter. Regionen upplever sammantaget att Microsoft som helhet - sannolikt till följd av strategiska beslut utanför Sveriges gränser som påverkat och fortsatt påverkar hur arbete kan fördelas och organiseras - brister i det grundläggande stöd som krävs av personuppgiftsbiträden enligt art. 28.3 led h GDPR.

Risk

Beaktat de omfattande och komplexa krav på integritetsskydd som åligger offentlig sektor generellt och hälso- och sjukvård specifikt är det en förutsättning att varje leverantör av tjänster till sådana kunder har en god förståelse för och organisation för att möta dessa krav. Om detta inte är på plats finns det risk att samarbetet kring tjänsterna försvåras, nödvändiga åtgärder för att skydda de registrerades rättigheter och friheter fördröjs, samt att personuppgifterna oavsiktligt behandlas i strid med de krav som åligger regionen och/eller Microsoft som personuppgiftsansvarig eller personuppgiftbiträde. Utöver bedömningar riskerar även nödvändig dokumentation, såsom registerförteckning och tillhandahållande av information till de registrerade bli lidande och eventuella personuppgiftsincidenter riskerar att inte uppmärksammas och åtgärdas. Givet de mycket omfattande personuppgiftsbehandlingar som Microsoft utför åt ett stort antal kunder, men även för egen räkning i egenskap av personuppgiftsansvarig, ser regionen en risk att den kompetens och de resurser som krävs för att i varje enskilt fall kunna göra relevanta bedömningar i fråga om bl.a. rättslig grund, lagringstider och säkerhetsåtgärder inte på ett betryggande sätt upprätthålls över tid.

3.7 Register över personuppgiftsbehandlingar

I egenskap av personuppgiftsansvarig är regionen ansvarig för att bedöma huruvida de säkerhetsåtgärder som vidtas av personuppgiftsbiträdet är tillräckliga, samt att påvisa att de har bedömt dessa åtgärder. För att kunna leva upp till dessa krav, krävs i regel att relevant dokumentation utbyts mellan parterna, däribland registerförteckning.[17] Regionen har efterfrågat att få ta del av det register över personuppgiftsbehandlingar Microsoft utför för regionens räkning, och som Microsoft enligt art. 30.2 GDPR är skyldiga att föra för varje personuppgiftsansvarig. Microsoft har inte, trots förfrågan, delat detta register med regionen[18]. Microsoft har under arbetet med denna rapport angett att de avser publicera information på sin hemsida som möjliggör för kunder att ta del av information som motsvarar vad som ska ingå i registerförteckningen. Regionen noterar dock att denna information inte finns tillgänglig i dagsläget, samt att sådan information på hemsidan inte kan vara kundspecifik på det sätt som regionen efterfrågar.

Risk

Att inte få ta del av Microsofts behandlingsregister, försvårar regionens möjlighet att följa upp vilka konkreta behandlingar Microsoft utför för regionens räkning, och skilja dem från de behandlingar Microsoft utför som självständig personuppgiftsansvarig. Det försvårar vidare identifiering, bedömning, uppföljning och dokumentation av de säkerhetsåtgärder som vidtas

[17] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, punkt 95.

[18] Frågan framfördes muntligt och skriftligt av regionen till Microsoft i juni 2021.

för respektive behandling, uppfyllande av kravet på information till de registrerade, och uppfyllande av ansvarsskyldigheten överlag.

3.8 Otydlighet avseende säkerhetsåtgärder

Enligt art. 32 GDPR ska den personuppgiftsansvarige säkerställa att lämpliga tekniska och organisatoriska säkerhetsåtgärder vidtas med beaktande av behandlingens art, omfattning, sammanhang och ändamål. Denna skyldighet åligger den personuppgiftsansvarige också vid anlitande av ett personuppgiftsbiträde. Det är därför högst väsentligt att regionen både ges tillräckligt med underlag för att bedöma om de säkerhetsåtgärder som vidtas av Microsoft är tillräckliga i förhållande till de planerade behandlingarna, och ges möjlighet att löpande följa upp säkerhetsåtgärdernas effektivitet.

Microsoft delar in personuppgifterna i Teams i fyra datakategorier, där kunddata anges vara en av datakategorierna. Logiken kring kategoriseringen av data i dessa kategorier är till viss del oklar för Region Stockholm. Microsoft åtar sig ansvaret för säkerheten av kunddata och i Tillägg A i Personuppgiftsbiträdesavtalet anges följande: ”Microsoft har implementerat och ska för kunddata i de centrala onlinetjänsterna upprätthålla säkerhetsåtgärderna som, tillsammans med säkerhetsåtaganden i detta DPA, är Microsofts enda ansvar vad gäller säkerheten för dessa data”. Enligt Personuppgiftsbiträdesavtalet ska de implementerade säkerhetsåtgärder och leva upp till de krav som anges i SS-EN ISO/IEC 27001, och SS-EN ISO/IEC 27018. De implementerade säkerhetsåtgärderna kan ur ett informationssäkerhetsperspektiv anses vara effektiva, dock saknas en tydlig koppling till de behandlingar av personuppgifter som sker i Teams, vilket gör det svårt att bedöma om de vidtagits med hänvisning till behandlingens art, ändamål, sammanhang och omfattning vid bedömning av säkerheten i samband med behandlingen. Information om säkerhetsåtgärder för övriga datakategorier, utöver kunddata, har inte delats med regionen.

I Personuppgiftsbiträdesavtalet redogörs inte för huruvida eller på vilket sätt behandlingens art, omfattning eller ändamål har tagits i beaktan eller haft inverkan på de implementerade säkerhetsåtgärderna. Microsoft har angett att de enbart kan motta instruktioner avseende personuppgiftsbehandlingen de utför som personuppgiftsbiträde åt Region Stockholm, om instruktionen återspeglar Teams tekniska funktionalitet. Det är därför inte möjligt för Region Stockholm som personuppgiftsansvarig att implementera önskade säkerhetsåtgärder. Sammantaget innebär detta att regionen vid användning av Teams är förpassad till de säkerhetsåtgärder som framgår av Personuppgiftsbiträdesavtalet, vilka regionen saknar närmare insikt i samt möjlighet att påverka. Detta innebär svårigheter för Region Stockholm att genomföra bedömningar av huruvida säkerhetsåtgärderna är lämpliga, och därmed säkerställa regelefterlevnad av art. 32 GDPR.

Utöver de allmänna kraven på säkerställande av att lämpliga tekniska och organisatoriska säkerhetsåtgärder vidtas vid behandling av personuppgifter,

följer av art. 25 GDPR ett krav på inbyggt dataskydd och dataskydd som standard, vilket innebär att säkerhetsåtgärderna ska implementeras utifrån ett integritetsskyddsperspektiv där bl.a. behandlingens art, omfattning och ändamål tas i beaktande vid implementering och upprätthållande av säkerhetsåtgärder. Enligt Europiska Dataskyddsstyrelsens riktlinjer innebär kravet inte att vissa specifika säkerhetsåtgärder ska vidtas, utan att de säkerhetsåtgärder som vidtas är anpassade efter de särskilda behandlingarna i fråga.[19] Varken i Personuppgiftsbiträdesavtalet eller i annan information som regionen tagit del av, anges hur behandlingens art, ändamål och för de enskilda fallen vid implementering eller upprätthållande av säkerhetsåtgärder.

Risk

Region Stockholm har, som personuppgiftsansvarig för kunddata, ett ansvar att utvärdera och bedöma de säkerhetsåtgärder som Microsoft vidtar. Regionens avsaknad av möjlighet att lämna instruktioner avseende säkerhetsåtgärder innebär svårigheter för Region Stockholm att påverka vilka säkerhetsåtgärder som vidtas. Det kan i sin tur innebära att regionens användning av Teams begränsas till sådana behandlingar som kan utföras med de standardiserade säkerhetsåtgärder som vidtas i Teams.

3.9 Bristande dokumentation av rättslig grund

Microsoft behandlar enligt egna uppgifter personuppgifter baserat på berättigat intresse enligt art. 6.1 led f. Det ska noteras att det i Personuppgiftsbiträdesavtal inte uttryckligen anges med vilket lagstöd behandlingen av personuppgifter sker, utan att denna information förtydligats efter förfrågan från regionen. Varje enskild typ av behandling som utförs på denna grund kräver att intresseavvägningen är dokumenterad i fråga om intressets legitimitet, samt behandlingens nödvändighet och proportionalitet i förhållande till intresset. Den dokumentation som delats med regionen avseende Microsofts behandling av personuppgifter med stöd av berättigat intresse[20] berör till viss del hur intresseavvägningen gjorts, men innehåller inte några utförliga bedömningar i fråga om legitimitet, nödvändighet och proportionalitet. Dokumentationen avser vidare enbart ett urval av de intressen/ändamål för vilka personuppgifter behandlas, och inte samtliga.

Risk

Då regionen inte har tagit del av någon utförlig dokumentation av på vilken rättslig grund Microsoft behandlar personuppgifter, saknar Region möjlighet att bedöma rimligheten och lagligheten i dessa behandlingar. Det kan leda till att

[19] Guidelines 4/2019 Data Protection by Design and by Default, punkt 14.
[20] Microsoft Data Protection & Security Terms for Online Services: Legitimate Business Operations.

regionen delar personuppgifter med Microsoft som sedan behandlas vidare, för nya ändamål, utan lagstöd.

3.10 Ofullständig och komplex information till de registrerade från Microsoft som personuppgiftsansvarig

Den information som görs tillgänglig för de registrerade av Microsoft på Microsofts olika hemsidor är ytterst omfattande och kan inte anses särskilt lättillgänglig. Information som är relevant ur ett integritetsskyddsperspektiv blandas med information om bland annat informationssäkerhet. I regel uppmanas de registrerade att ta kontakt med den egna organisationen för mer information. I det fall det finns information om hur en registrerad kan kontakta Microsoft direkt för begäran om tillgång, rättelse eller radering, har sådana försök resulterat i ungefär samma information som redan finns tillgänglig på Microsofts hemsida. Bland annat har de registrerade fått följande svar:

- Uppmaning att kontakta organisationens administratör, trots att förfrågan tydligt ställts till Microsoft i egenskap av personuppgiftsansvarig och regionen för den utpekade behandlingen inte är personuppgiftsansvarig.
- Uppmaning att själv enligt given instruktion konfigurera sina sekretessinställningar, trots att förfrågan från de registrerade rörde information och inte hjälp med olika inställningar i lösningen.
- Exempel på säkerhetsåtgärder som Microsoft kan vidta, utan förtydligande om för vilka risker eventuella säkerhetsåtgärder faktiskt vidtagits och vilka bedömningar som ligger till grund.
- Information om datakategorier utan konkreta omnämnanden av specifika kategorier eller behandlingar av personuppgifter. Informationen är densamma som i standardvillkoren, och det går inte att förstå om datakategorier kan eller ska likställas med en behandling eller på annat sätt förhåller sig till behandlingar av personuppgifter.

Trots att förfrågan om tillgång ställts på svenska till Microsoft skickas svar tillbaka på engelska av Microsofts sekretessteam, vilket kan försvåra för de registrerade att ta till sig informationen om hur deras personuppgifter behandlas.

Risk

Då de registrerade inom ramen för regionens Teams inte på ett enkelt sätt kan ta del av någon utförlig dokumentation om i vilken omfattning Microsoft behandlar personuppgifter i egenskap av personuppgiftsansvarig, saknar de registrerade möjlighet att bedöma rimligheten i dessa behandlingar och möjlighet att framföra eventuella specifika klagomål.

Microsoft försvårar också för de registrerade att utöva sina rättigheter genom att hänvisa de registrerade till annan part (regionen), även i lägen då förfrågan från de registrerade uttryckligen efterfrågar tillgång till information från Microsoft i egenskap av personuppgiftsansvarig.

4. Sammanfattande slutsatser

4.1 Grundfrågorna

Denna rapport har tagit avstamp i risker som följer av frågeställningen ”vilka personuppgifter hanteras av vem, hur och varför inom ramen för respektive lösning som regionen nyttjar eller kan komma att nyttja?. Det är nödvändigt att båda parter har en förståelse för dessa grundfrågor för att kunna ha en effektiv och konkret dialog avseende de integritetsskyddsfrågor som följer av regionens användning av Teams och den har därför utgjort den centrala frågeställningen i de dialoger som förts med Microsoft sedan 2019. Regionen anser att det med ett svar på den övergripande frågan finns goda förutsättningar att bedriva ett fortsatt systematiskt riskbaserat integritetsskyddsarbete, medan avsaknad av svar, vaga eller svårtolkade svar skulle peka på sämre förutsättningar att arbeta effektivt med integritetsskydd kopplat till Teams.

Dialogen med Microsoft har visat på ett antal riskområden kopplade till dessa frågor, som redogjorts för ovan. Som en återkoppling till grundfrågeställningen, redogörs nedan för de slutsatser som kunnat dras kopplad till denna.

1) Vilka personuppgifter behandlas i Teams?

Regionens användning av Teams innebär alltid att personuppgifter behandlas i någon utsträckning, bl.a. som ett resultat av att användarbaserad inloggning och autentisering ingår i Teams grundinförande. Dessa personuppgifter utgörs av förnamn, efternamn, e-postadress, telefonnummer (om uppgiften finns tillgänglig), medarbetarens/användarens organisationstillhörighet, kostnadsställe samt vissa uppgifter om användarens enhet. Utöver dessa kategorier av personuppgifter, behandlas personuppgifter som regionen själv för in i Teams, och som därför beror på regionens instruktioner till användarna.

Utöver de personuppgifter som aktivt läggs in i Teams av regionens användare, och som regionen därigenom har kontroll över, skapas enligt regionens förståelse också nya personuppgifter genom regionens användning av Teams. Dessa kan bestå av t.ex. information kopplad till säkerställande av Teams säkerhet, prestanda och kundupplevelse, och behandlas i form av t.ex. loggdata. Dessa personuppgifter definieras enligt Microsoft som datakategorierna ”Diagnostiska data”, ”Tjänstegenererade data” och ”Data från Professionella

tjänster”. Regionen saknar insikt i mer exakt vilka kategorier av personuppgifter som behandlas i dessa datakategorier.

Regionen bedömer med hänvisning till ovan att den saknar den insikt avseende vilka personuppgifter som uppkommer som ett resultat av regionens användning av Team, som skulle krävas för att bedöma lagligheten och lämpligheten i behandlingen av dem.

2) Av vem behandlas personuppgifter i Teams?

Att förstå hur personuppgiftsansvaret är fördelat mellan parterna är helt avgörande för att kunna säkerställa ett tillräckligt skydd för enskildas integritet. Enbart då en tydlighet kring dessa frågor föreligger, kan relevanta diskussioner föras avseende hur skyddet för enskildas integritet bör upprätthållas vid regionens användning av Teams.

Enligt Personuppgiftsbiträdesavtalet fördelas personuppgiftsansvaret för behandlingarna i Teams utifrån behandlingarnas ändamål. För de behandlingar som utförs av Microsoft för ändamålet att tillhandahålla Teams, utgör regionen personuppgiftsansvarig medan Microsoft är personuppgiftsbiträde. För de behandlingar som utförs av Microsoft för ändamålet Microsofts berättigade verksamhetsutövning, utgör Microsoft självständig personuppgiftsansvarig.

Vid granskning av Personuppgiftsbiträdesavtalet och genom dialogen med Microsoft, har det framkommit att behandling av ”Diagnostiska data”, ”Tjänstegenererade data” och ”Data från Professionella tjänster” sker t.ex. för ändamålet att *säkerställa att skalning och andra tjänster som påverkar kundupplevelsen fungerar på den nivå som våra kunder kräver*. Eftersom detta är ett ändamål som inte uttryckligen återfinns i varken den uttömmande lista Microsoft tillhandahållit över vilka underändamål som ska anses falla under Microsofts berättigade verksamhetsutövning, eller listan över de underändamål som ska anses falla under tillhandahållande av Teams, är det inte tydligt för regionen vem av parterna som enligt Personuppgiftsbiträdesavtalet utgör personuppgiftsansvarig. Det i sin tur försvårar för regionen att avgöra dess lämplighet och laglighet.

Utformningen av de behandlingar som sker av Microsoft för ändamålet att tillhandahålla Teams är i hög grad standardiserad, och bestäms i första hand av Microsoft. Regionen menar därför att det kan ifrågasättas om regionen har tillräcklig insikt i och inflytande över sådana behandlingar, i de fall de går utöver ren teknisk lagring och bearbetning av regionens personuppgifter, för att kunna anses utgöra personuppgiftsansvarig. Med hänsyn till att personuppgiftsansvar ska bedömas utifrån de faktiska omständigheterna vid varje behandling av personuppgifter, och inte kan regleras genom avtal, ser regionen en risk att den fördelning av personuppgiftsansvar som följer av Personuppgiftsbiträdesavtalet därför inte återspeglar den faktiska rättsliga fördelningen.

Regionen bedömer med hänvisning till ovan att ansvarsrollerna för de olika behandlingarna av personuppgifter som förekommer i Teams behöver utredas

närmare för att möjliggöra för regionen att säkerställa efterlevnad av GDPR och annan lagstiftning på integritetsskyddsområdet.

3) Hur behandlas personuppgifter i Teams?

Genom Personuppgiftsbiträdesavtalet åtar sig Microsoft att vidta ett antal säkerhetsåtgärder för det som definieras som kunddata. Regionen har inte tagit del av någon information om hur övriga datakategorier skyddas. Regionen har förvisso möjlighet att ta ställning till de säkerhetsåtgärder som Microsoft vidtar som standard för kunddata, men ges i nuläget inte möjlighet att vare sig påverka eller följa upp de implementerade säkerhetsåtgärdernas effektivitet. Den standardiserade karaktären på säkerhetsåtgärder försvårar vidare för regionen att utvärdera hur väl behandlingarnas art, ändamål, sammanhang och omfattning beaktats vid implementering av dem.

Regionen bedömer med hänvisning till ovan att den saknar möjlighet att utvärdera, påverka och följa upp de säkerhetsåtgärder som implementeras för att skydda regionens personuppgifter, på ett sätt som är nödvändigt för att säkerställa att personuppgifterna skyddas på det sätt som GDPR kräver.

4) Varför behandlas personuppgifter i Teams?

Teams används för behandling av personuppgifter för en stor mängd ändamål; både ändamål som bestäms av regionen och av Microsoft. Utöver de ändamål för vilka regionen använder Teams, behandlar Microsoft personuppgifter dels i egenskap av personuppgiftsbiträde för att tillhandahålla Teams, och dels i egenskap av personuppgiftsansvarig för sin berättigade verksamhetsutövning. Regionen har tagit del av uttömmande sammanställningar av de underandamål som Microsoft behandlar personuppgifter för under de två huvudändamålen. Regionen är dock av uppfattningen att varken underändamålen till tillhandahållandet av Teams eller till Microsofts berättigade verksamhetsutövning, är konkreta och specifika på ett sätt som möjliggör för regionen att ta ställning till lagligheten och lämpligheten av dem. Regionen konstaterar också att en följd av att ändamålen är vagt och allmänt beskrivna, är att det är svårt att bedöma vem av parterna som kan anses ha en sådan kontroll och inflytande över dem på ett sätt som föranleder personuppgiftsansvar enligt GDPR.

Regionen bedömer med hänvisning till ovan att det finns ett behov av att ytterligare förtydliga för vilka konkreta ändamål personuppgifter behandlas i Teams, på ett sätt som ger regionen möjlighet att utvärdera lagligheten och lämpligheten i behandling av personuppgifter för att uppnå ändamålen, samt kunna bedöma för vilka ändamål regionen är personuppgiftsansvarig för behandlingarna som utförs.

4.2 Framtida integritetsskyddsarbete

En av de främsta konsekvenserna av att ovan grundfrågor ännu inte är klarlagda, är svårigheter med att på ett konkret och systematiskt plan diskutera

och utvärdera de säkerhetsåtgärder som vidtas för att skydda de personuppgifter som behandlas, och således möjligheterna att på ett realiserbart sätt utforma lösningen utifrån behoven på ett lämpligt och lagligt sätt. För att kunna vidta tillräckliga säkerhetsåtgärder är det nödvändigt att ta hänsyn till varje behandlings natur, däribland vilka personuppgifter som behandlas och varför. I nuläget är regionen förpassad till att på ett generellt plan bedöma de säkerhetsåtgärder som vidtas för datakategorin ”kunddata”, vilken utgörs av alla personuppgifter som regionen för in i Teams, samt för övriga datakategorier, vars närmare innehåll är okänt för regionen. Regionen är vidare inte helt införstådd med kopplingen mellan ändamål och säkerhetsåtgärder i Teams, eftersom säkerhetsåtgärderna i första hand tycks vara kopplade till datakategori snarare än till ändamål. Det gör det svårt att utvärdera lämpligheten i de säkerhetsåtgärder som vidtas då de inte kan kopplas direkt till behandlingar.

Avsaknaden av insikt i de ändamål för vilka personuppgifter behandlas, skapar också svårigheter att bedöma lagligheten och lämpligheten av behandlingarna. Detta försvåras ytterligare av den otydlighet som ännu råder kring i vilka fall Microsofts anser sig behandla personuppgifter i egenskap av personuppgiftsbiträde respektive som självständig personuppgiftsansvarig.

Om ovanstående frågor tydliggöras kan regionen på ett tydligare sätt bedöma vilken typ av personuppgifter som kan behandlas på vilket sätt och i vilket syfte, i olika delar av lösningen. Regionen kan då begränsa användningen av Teams till sådana behandlingar där regionen bedömer att standardnivån för behandlingen av personuppgifter är tillräcklig. Regionen har för avsikt att fortsätta dialogen med Microsoft samt fortsatt utreda vilka av de identifierade riskerna som är möjliga att hantera med hjälp av säkerhetsåtgärder. Avseende detta arbete ska särskilt nämnas att Microsoft sedan denna rapport upprättades har uppdaterat Personuppgiftsbiträdesavtalet, vilket kan komma att få påverkan på de risker som beskrivs. Inledningsvis kommer därför regionen att analysera dessa uppdateringar och dess eventuella påverkan på riskerna.