Microsoft AB
Box 27, 164 93 KISTA
Org.nr: 556233-4804
Säte: Stockholm

Växel +46 (0)8 752 56 00
Kundservice + 46 (8)0 55 99 00 00
Fax + 46 (0)8 750 51 58
www.microsoft.se

Microsoft

Att. Sara Ahmed
sara.ahmed@regeringskansliet.se

Kista den 18 november 2016

Remissvar till delbetänkandet Hur står det till med den personliga integriteten? (SOU 2016:41)

Ju2016/04398/L6

Microsoft har beretts möjlighet att yttra sig över Integritetskommitténs delbetänkande Hur står det till med den personliga integriteten? (SOU 2016:41). Microsoft lämnar följande kommentarer med anledning av Integritetskommitténs delbetänkande.

Sammanfattning

Integritetskommittén konstaterar i delbetänkandet att publika molntjänster innebär en allvarlig risk för den personliga integriteten. Microsofts uppfattning är att molntjänster snarare kan användas som ett verktyg för att förbättra säkerheten och minska risker för intrång i den personliga integriteten.

Integritetskommittén menar även att kunden förlorar kontroll och insyn i hanteringen av sin kunddata vid användningen av molntjänster. Avseende de molntjänster som Microsoft erbjuder idag finns tekniska lösningar som gör att kunden enkelt kan styra över vem som har tillgång till kunddata, både internt och externt. Kunden har full äganderätt till sin kunddata och styr således över hanteringens ändamål. Microsoft är fullt transparent med var och hur data lagras och informerar kunden om vilka underleverantörer som används.

Utredningen konstaterar även att bristande kompentens hos myndigheter gällande IT och hantering av personuppgifter utgör en risk vid köp av molntjänster. För att minska denna risk och förenkla förståelsen för de krav som behöver uppfyllas, finns integritetsstandarder enligt vilka molntjänstleverantörer kan certifieras och som molntjänstkunder kan använda som vägledning. På så sätt kan myndigheter säkerställa att skyddsnivån hos molntjänstleverantörer upprätthålls. Den internationella standardiseringsorganisationen (ISO) har i september 2016 publicerat en standard för molntjänstavtal, ISO/IEC 19086. Standarden är vägledande och utformad för att kunder ska kunna göra en utförlig utvärdering av molntjänstavtalen. Som svar på den nya standarden har Microsoft skapat en checklista som hjälper kunder att göra en sådan utvärdering. Microsoft vill peka på standarder och checklistor som bra verktyg till myndigheter för att förbättra integritetsskyddet.

Nedan följer en mer detaljerad redogörelse av Microsofts resonemang med hänvisningar till relevanta avsnitt i delbetänkandet.

Microsoft AB
Box 27, 164 93 KISTA
Org.nr: 556233-4804
Säte: Stockholm

Växel +46 (0)8 752 56 00
Kundservice + 46 (8)0 55 99 00 00
Fax + 46 (0)8 750 51 58
www.microsoft.se

Microsoft

21.1 Molntjänster

Med hänvisning till avsnitt 21.1 i delbetänkandet om molntjänster önskar Microsoft förtydliga följande avseende de globala molntjänster Microsoft erbjuder.

21.1.1 Företeelsen

Integritetskommittén konstaterar i avsnitt 21.1.1 på sida 563 att det sällan är klart hur och var informationen lagras. Microsoft vill i sammanhanget förtydliga att Microsofts molntjänstkunder kan ta reda på var deras data lagras och hur den hanteras genom Microsoft Trust Center via följande länk: https://www.microsoft.com/en-us/trustcenter/Privacy/default.aspx.

I avsnitt 21.1.1 på sida 563 konstaterar Integritetskommittén även att de globala molntjänstleverantörerna oftast *lagrar* data i länder utanför EES-området. Microsoft vill förtydliga att avseende Microsofts europeiska kunder används europeiska datacenter för publika molntjänster. Microsoft är transparent med hur och var data lagras. Kraven för att tillhandahålla tjänsterna kan emellertid innebära att viss data överförs, lagras eller behandlas av Microsofts personal eller underleverantörer utanför det primära lagringsområdet. På Microsofts Trust Center beskrivs de specifika och begränsade situationer där överföring kan ske för respektive tjänst. Det kan exempelvis inträffa då Microsoft erbjuder kundsupport dygnet runt och supportpersonal är placerad i ett land utanför kundens geografiska zon.

Sedan 2016 erbjuder Microsoft även kunder som befinner sig inom EES-området möjligheten att lagra kunddata i tyska datacenter. Enligt denna modell lagras kunddata i datacenter inom Tyskland och tillgången till kunddata styrs av tredje part i Tyskland, av en så kallad dataförvaltare.

21.1.2 Det skyddade regelverket

Integritetskommittén konstaterar i avsnitt 21.1.1 på sida 563 att det finns risker med att molntjänstleverantörer *överför* uppgifter till länder utanför EES-området, som vanligen har en lagstiftning som ger sämre skydd än EU:s dataskyddsdirektiv. De anför vidare i avsnitt 21.1.2 på sida 570 att överföring med stöd av Safe Harbor-principen inte längre gäller samt att det nya avtalet för transatlantiska överföringar Privacy Shield inte ännu är färdigställt.

Som global molntjänstleverantör åtar sig Microsoft, i kontrakt med kunder, att följa kraven enligt dataskyddslagstiftningen i EES-området avseende insamling, användning, överlåtelse och lagring och annan behandling av personlig information från EES-området. För den begränsade överföringen av personuppgifter som sker till tredje land använder sig Microsoft för närvarande av EU:s standardkontraktsklausuler och Privacy Shield som stöd för överföringen.

Det finns även integritetsstandarder inom EU enligt vilka molntjänstleverantörer kan certifieras. På så sätt kan kunden säkerställa att skyddsnivån upprätthålls fortlöpande. ISO har utfärdat flera standarder avseende skydd för personuppgifter. Avseende sina molntjänster är Microsoft certifierade enligt bland annat ISO 27018, en standard med riktlinjer för skydd av personuppgifter i publika molntjänster. Microsoft har även publicerat en

Microsoft AB
Box 27, 164 93 KISTA
Org.nr: 556233-4804
Säte: Stockholm

Växel +46 (0)8 752 56 00
Kundservice + 46 (8)0 55 99 00 00
Fax + 46 (0)8 750 51 58
www.microsoft.se

Microsoft

checklista avseende den nya standarden ISO/IEC 19086 gällande molntjänstavtal, se bilaga 1. ISO/IEC 19086 publicerades i september 2016 och är vägledande för kunder som vill göra en utförlig utvärdering av molntjänstavtalen. Checklistan ger privata och statliga organisationer en möjlighet att identifiera sina egna krav på datahantering samt efterlevnad av sådana krav. Microsoft anser att standarder och checklistor kan användas som goda verktyg i myndigheters integritetsskyddsarbete. För mer information om Microsofts certifieringar hänvisas till Microsoft Trust Center: https://www.microsoft.com/en-us/trustcenter/Compliance/default.aspx

21.1.3 Kommitténs samlande bedömning av området

I avsnitt 21.1.3 på sida 572 konstaterar Integritetskommittén att det finns risk att uppgifter kan komma att behandlas för biträdets eller underbiträdets egna ändamål. Här önskar vi förtydliga att avseende Microsofts globala molntjänster används kunddata endast för att tillhandahålla tjänsten. Microsoft använder inte kunddata för att härleda information från kunden i reklamsyfte eller för något annat liknande kommersiellt syfte. Kunden behåller alla rättigheter, äganderätter och intressen i och till kunddata. Kunden kan när som helst ta bort data från molntjänsten utan att behöva underrätta Microsoft i förväg.

Integritetskommittén konstaterar vidare i avsnitt 21.1.2 sida 572 att användningen av underleverantörer innebär en förlust av insyn med risk för obehörig åtkomst. Avseende Microsofts globala molntjänster finns ett kontraktuellt skydd mellan personuppgiftsansvarige och personuppgiftsbiträdet. I sådant skydd ingår en skyldighet för Microsoft att teckna avtal med underleverantörer, meddela vilka underleverantörer som används samt meddela förändringar av sådana. Underleverantörer som hanterar kunddata måste ingå avtal som är minst lika långtgående som Microsofts egna villkor för dataskydd.

Microsoft vill tillägga att avseende Microsofts molntjänster implementeras och upprätthålls lämpliga tekniska och organisatoriska åtgärder som är avsedda att skydda kunddata mot otillåten åtkomst, avslöjande, förändring, förlust eller förstörelse. De processer som styr åtkomst till kunddata skyddas av starka kontroller och verifieringar. Åtkomsten till kunddata begränsas och loggas för Microsofts personal och underleverantörer och revision av tredje part görs regelbundet för att säkerställa att all åtkomst är korrekt.

Microsofts molntjänster erbjuder flera funktioner som på olika sätt ger kunden möjlighet att begränsa Microsofts åtkomst till dess kunddata. Ett exempel på en sådan funktion är Customer Lockbox som ger kunden full kontroll över vem som har åtkomst till kunddata. Med Customer Lockbox krävs kundens godkännande varje gång en tekniker begär åtkomst till kundens data. Det sker vanligen i supportärenden och då får teknikern endast åtkomst som är begränsad i tid och till ändamålet. Ett annat exempel på en funktion är Azure Key Vault där kunden enkelt kan bygga sin egen nyckel till krypterad information. Kunden hanterar då själv nyckeln till den information kunden väljer att kryptera.

Avseende utredningens konstaterande i avsnitt 21.1.3 sid 573 om ökade risker för utlämnande av personuppgifter till myndigheter eller organisationer i länder utanför EES-området vill Microsoft förtydliga att Microsoft inte lämnar ut data till myndigheter utan att det sker med stöd i lag.

Microsoft AB
Box 27, 164 93 KISTA
Org.nr: 556233-4804
Säte: Stockholm

Växel +46 (0)8 752 56 00
Kundservice + 46 (8)0 55 99 00 00
Fax + 46 (0)8 750 51 58
www.microsoft.se

Microsoft

Microsoft har tagit strid mot den amerikanska staten för att tillförsäkra att en korrekt legal process följs, bland annat i fall gällande husrannsakan. Enligt ett nyligen meddelat domslut från *United States Court of Appeals Second Circuit* kan inte amerikanska myndigheter tvinga Microsoft att lämna över kunders email som lagras i datacenter utanför USA. Beslutet är viktigt för hela industrin och understryker att samma regler som gäller husrannsakan för fysiska bevis även bör gälla för data lagrad i molntjänster. För mer information om fallet hänvisar vi till: https://digitalconstitution.com/.

I avsnitt 21.1.3 på sida 572-574 konstateras att det finns risker med att kompetensen hos statliga myndigheter är låg gällande IT och hantering av personuppgifter. Vid användandet av globala molntjänster så arbetar myndigheterna med partnerföretag som är specialiserade på dessa frågor och hjälper till med integritetsarbetet. Microsoft vill framhålla de möjligheter som finns för organisationer att genom digitala verktyg sätta upp regler för hantering av personuppgifter.

Microsoft har erfarit hur kunders övergång från klassisk mjukvara till molntjänster har inneburit en möjlighet för organisationer att skärpa kontrollen och förbättra hanteringen av personuppgifter, även gällande personuppgifter av känslig natur.

9 Hälsa och sjukvård och välfärdsteknik inom socialtjänst

Med hänvisning till avsnitt 9 i delbetänkandet om hälsa och sjukvård önskar Microsoft understryka de möjligheter som digitala verktyg medför.

9.7 Kommitténs samlade bedömning

I avsnitt 9.7 konstaterar Integritetskommittén att det finns stora risker inom hälsa och sjukvård gällande hantering av personuppgifter. I detta avseende vill Microsoft understryka de stora möjligheterna att hitta säkra verktyg som minskar riskerna inom sektorn. I Microsofts molntjänster finns det många verktyg som ger kunden en bättre översyn över hur uppgifter hanteras. För att hjälpa kunderna har Microsoft publicerat en checklista och ett whitepaper för vårdorganisationer att använda vid köp av molntjänster, se bilaga 2 och 3. Microsoft vill återigen understryka möjligheten att använda underlagen som stöd i de risk- och sårbarhetsanalyser och laglighetskontroller som krävs enligt svensk rätt.

Med vänliga hälsningar,

Mathias Strand
Microsoft