Microsoft AB
Regeringsgatan 25
Box 33
103 68 Stockholm
Org.nr: 556233-4804
Säte: Stockholm

Växel +46 (0)8 752 56 00

Kundservice + 46 (8)0 55 99 00 00

www.microsoft.se

Microsoft

YTTRANDE

2021-05-07 I2021/00342

Infrastrukturdepartementet

103 33 Stockholm

MICROSOFTS REMISSVAR PÅ IT-DRIFTSUTREDNINGENS DELBETÄNKANDE SÄKER OCH KOSTNADSEFFEKTIV IT-DRIFT – RÄTTSLIGA FÖRUTSÄTTNINGAR FÖR UTKONTRAKTERING (SOU 2021:1)

SAMMANFATTNING

Microsoft AB inkommer i detta dokument med synpunkter rörande IT-driftsutredningens delbetänkande ”Säker och kostnadseffektiv IT-drift – rättsliga förutsättningar för utkontraktering” (SOU 2021:1) (”**Utredningen**”).

Microsoft ser positivt på den genomförda utredningen. I följande ger vi både några allmänna tankar om Utredningen samt förslag på förtydliganden.

Att lagra data i molntjänster är inte bara tidsbesparande utan även betydligt mer säkert, miljövänligt och kostnadseffektivt än motsvarande lokala lösningar. Microsofts ambition är att från ett leverantörsperspektiv beskriva vilka förtydliganden som önskas av nedan begrepp och även vilka säkerhetsåtgärder som är relevanta vid utkontraktering av IT-drift.

De fyra teman vi önskar lyfta är (i) tredjelandsöverföringar, (ii) röjandebegreppet, (iii) tolkningen av ”teknisk bearbetning och teknisk lagring”, och (iv) kryptering som skyddsåtgärd. Yttrandet följer betänkandets struktur.

7.4 TREDJELANDSÖVERFÖRING ENLIGT DATASKYDDSFÖRORDNINGEN

När EU-domstolen i Schrems II-domen underkände överföringsmekanismen Privacy Schield medförde det en rättslig osäkerhet kring vilka mekanismer som kan användas vid överföring av data mellan EU och USA.

Flera molntjänstleverantörer arbetar idag aktivt med att kontraktuellt finna en väg framåt på området i samråd med kunderna. Microsoft har bland annat lanserat ”*Defending Your Data*”, ett initiativ som ger ett ökat integritetsskydd för kunder i EU. Initiativet innebär att Microsoft åtar sig att (i) bestrida varje enskild begäran om utlämnande av kunddata oavsett vilken stat som begär ut informationen under förutsättning att det finns laglig grund att bestrida sådan begäran och (ii) utge ersättning till den registrerade vid eventuellt utlämnande av data i strid med EU:s dataskyddlagstiftning (GDPR).

Vidare anser Microsoft att Utredningens påståenden om tredjelandsöverföringar i förhållande till amerikansk övervakningslagstiftning framstår som alltför kategorisk då det under vissa förutsättningar går att hitta kompletterande skyddsåtgärder till standardavtalsklausulerna som möjliggör tredjelandsöverföringar.

8.9 RÖJANDEBEGREPPET

Utredningen framhåller att begreppet ”röjande” ska tolkas på så sätt att ett röjande alltid ska anses ske vid utkontraktering. Microsoft uppfattar Utredningens ståndpunkt som att uppgifter som lagras hos leverantören måste anses ”utlämnade” och därmed röjda eftersom utlämnande, enligt t.ex. 3 kap. 1 § OSL i definitionen av ”sekretess” anförs som ett exempel på röjande.

För en fortsatt hållbar digitaliseringsutveckling och för att möjliggöra utkontraktering av IT-tjänster krävs att tolkningen av röjandebegreppet utgår från en sannolikhetsbedömning. Denna bedömning bör beakta: (i) de klassificeringar av data som beskrivs nedan, (ii) hur data används i tjänsten ifråga, och (iii) vilka säkerhetsåtgärder som vidtagits (t.ex. kryptering och administrativa säkerhetsåtgärder) hos relevant leverantör. En sådan bedömning bör göras utifrån omständigheterna i det enskilda fallet.

9.8.2 TEKNISK BEARBETNING OCH TEKNISK LAGRING

Microsoft anser att begreppet ”teknisk lagring och teknisk bearbetning” bör förtydligas alternativt att den föreslagna bestämmelsen utvidgas till att även innefatta nödvändiga dataklassificeringar för drift av en IT-tjänst.

Från ett leverantörsperspektiv används flera olika klassificeringar av data inom IT-drift. För att kunna navigera i dagens digitaliserade samhälle, krävs förtydligande av vilka klassificeringar av data som omfattas av begreppet.

Klassificering av datatyper vanligt förekommenade inom IT-drift och som bör övervägas som del i begreppets omfång är följande: (i) kunddata, data inkl. text, ljud, video, bildfiler och programvara, som kunden tillhandahåller vid användandet av en IT-tjänst, (ii) diagnostisk data, avser data som "samlats in" från programvara en kund installerar lokalt för användning i samband med molntjänster (används för att hjälpa till att säkerställa att programvaran är säker och fungerar på korrekt sätt), (iii) tjänstegenererad data, som omfattar all data som "genereras" eller "härleds" via en molntjänst (används för att säkerställa att prestanda, säkerhet), och (iv) data från professionella tjänster inkl. supportdata som tillhandahålls till leverantören under teknisk support för en onlinetjänst.

10.1.4 AVTALSREGLERAD TYSTNADSPLIKT, KRYPTERING OCH PSEUDONYMISERING

Utredningen för ett generellt resonemang kopplat till kryptering som skulle kunna tolkas på så sätt att kryptering inte är en tillräcklig teknisk skyddsåtgärd.

I avsnitt 10.1.4 framhåller Utredningen att det inte finns några ”*nu kända säkerhetsåtgärder som gör det helt, både i teori och praktik, omöjligt för tjänsteleverantören att ta del av uppgifterna*”.

Vidare hänvisar Utredningen till sitt resonemang ovan och framhåller tolkningen att ”*en utkontraktering innebär att uppgifterna som omfattas av utkontrakteringen lämnas ut och därmed röjs i den mening som avses i OSL oavsett om de krypterats eller pseudonymiserats*.”

Microsofts uppfattning är att kryptering kan anses som en tillräcklig säkerhetsåtgärd. Det finns idag tekniker som möjliggör komplex kryptering för verksamhetskritisk information. Kryptering anses idag utgöra en industristandard för att skydda information mot röjande och hindra åtkomst för en obehörig att ta del av uppgifter. Kryptering kan ske av datan i sig, då den är i vilande form, eller vid överföringen av data. Kryptering av vilande data skyddar bland annat vid intrång och stöld, medan kryptering vid överföring av data skyddar mot avlyssning eller manipulationer. Kryptering utgör även en s.k. teknisk säkerhetsåtgärd och kan anpassas efter situation beroende på syfte, nödvändigt skydd och kontext.

Microsoft menar därför att information som krypterats ej ska anses vara röjd trots att informationen fysiskt befinner sig utanför organisationens datanätverk. Vidare anser Microsoft att Utredningen i sitt slutbetänkande bör förtydliga att kryptering kan vara en effektiv skyddsåtgärd för att göra information oläsbar och således att kontrollen för densamma förblir hos myndigheten.