

Volymlicensiering

Dataskyddstillägg för Microsoft Onlinetjänster Januari 2020

Innehållsförteckning

INLEDNING	3	Behållande och radering av data.....	9
Tillämpligt DPA och uppdateringar.....	3	Personuppgiftsbiträdes konfidentialitetsåtagande	9
Elektroniska meddelanden.....	3	Meddelande om och kontroll över användning av underordnade	
Tidigare versioner	3	personuppgiftsbiträden	9
FÖRTYDLIGANDEN OCH SAMMANFATTNING AV ÄNDRINGAR	3	Utbildningsinstitutioner	10
DEFINITIONER	4	CJIS-kundavtal	10
ALLMÄNNA VILLKOR	5	HIPAA Business Associate	10
Efterlevnad av lagar	5	California Consumer Privacy Act (CCPA)	10
DATASKYDDSVILLKOR	5	Så här kontaktar du Microsoft	10
Omfattning.....	5	TILLÄGG A – SÄKERHETSÅTGÄRDER.....	11
Typ av databehandling, ägarskap.....	5	BILAGA 1 – MEDDELANDEN	14
Utlämnande av behandlade data	6	PROFESSIONELLA TJÄNSTER	14
Behandling av personuppgifter, GDPR	6	California Consumer Privacy Act (CCPA)	16
Datasäkerhet.....	7	BILAGA 2 – STANDARDAVTALSCLAUSULER	
Meddelande om säkerhetsincidenter	8	(PERSONUPPGIFTSBITRÄDEN)	17
Dataöverföringar och plats.....	8	BILAGA 3 – VILLKOR I EU:S ALLMÄNNA DATASKYDDSFÖRORDNING	
		23

[Innehållsförteckning](#)

[Inledning](#)

[Allmänna villkor](#)

[Dataskyddsvillkor](#)

[Bilaga](#)

Inledning

Parterna avtalar att detta villkor för Dataskyddstillägg för Microsoft Onlinetjänster (DPA) anger deras skyldigheter beträffande behandling av och säkerhet för kunddata och personuppgifter i samband med onlinetjänsterna. Parterna avtalar även att detta DPA, såvida inte ett separat avtal om professionella tjänster föreligger, reglerar behandling av och säkerhet för data i professionella tjänster. Separata villkor, däribland olika integritets- och säkerhetsvillkor, reglerar Kundens användning av produkter som inte härrör från Microsoft.

I händelse av konflikt eller bristande överensstämmelse mellan detta DPA och andra villkor i Kundens volymlicensieringsavtal (inbegripet produktvillkor eller villkor för onlinetjänster) ska detta DPA gälla. Bestämmelserna i detta DPA ersätter eventuella motstridiga bestämmelser i Microsofts sekretesspolicy som annars skulle gälla för behandling av kunddata, personuppgifter eller data i professionella tjänster enligt vad som anges häri. För tydlighets skull: i enlighet med klausul 10 i standardavtalsklausulerna i [Bilaga 2](#) ska dessa ha företräde före annat eventuellt villkor i DPA.

Microsoft åtar sig skyldigheterna i detta DPA gentemot alla kunder med volymlicensieringsavtal. Dessa åtaganden är bindande för Microsoft vad kunden beträffar, oavsett (1) vilken version av OST som i övrigt är tillämplig på en viss onlinetjänstprenumeration, (2) eventuellt annat avtal som hänvisar till OST.

Tillämpligt DPA och uppdateringar

När Kunden förnyar eller köper ett nytt abonnemang för en Onlinetjänst, kommer den då aktuella DPA tillämpas. Den ändras inte under Kundens abonnemang för denna Onlinetjänst. När Microsoft introducerar nya funktioner, tillägg eller tillhörande programvara (det vill säga, som inte tidigare har ingått i abonnemanget), får Microsoft tillhandahålla villkor eller göra uppdateringar av DPA som gäller för Kundens användning av dessa nya funktioner, tillägg eller tillhörande programvara.

Elektroniska meddelanden

Microsoft får tillhandahålla kunden information och meddelanden om onlinetjänster elektroniskt, inklusive via e-post, genom portalen för onlinetjänsten eller via en webbsida som Microsoft anger. Meddelande är lämnat det datum meddelandet görs tillgängligt av Microsoft.

Tidigare versioner

DPA och OST innehåller villkor för onlinetjänster som är tillgängliga för tillfället. För tidigare versioner av DPA och OST kan Kunden se <https://aka.ms/licensingdocs> eller kontakta återförsäljaren eller Microsofts kundansvariga.

Förtydliganden och sammanfattning av ändringar

Inga

[Innehållsförteckning/Allmänna villkor](#)

[Innehållsförteckning](#)



Inledning



[Allmänna villkor](#)



[Dataskyddsvillkor](#)



[Bilaga](#)

Definitioner

Termer med versal som används men inte definieras i detta DPA ska ha de betydelser som anges i volymlicensieringsavtalet. Följande definierade termer används i detta DPA:

Med "kunddata" avses alla data, inklusive alla text-, ljud-, video- eller bildfiler och programvara, som Microsoft tillhandahålls av Kunden eller för Kundens räkning genom Kundens användning av onlinetjänsten. Kunddata innefattar inte data i professionella tjänster.

Med "diagnostikdata" avses data som samlas in eller inhämtas av Microsoft från programvara som installeras lokalt av Kunden i samband med onlinetjänsten. Diagnostikdata kan också kallas telemetri. Diagnostikdata innefattar inte kunddata, tjänstgenererade data eller data i professionella tjänster.

Med "dataskyddskrav" avses den allmänna dataskyddsförordningen GDPR, lokala dataskyddslagar inom EU/EES samt andra tillämpliga lagar, förordningar eller andra krav enligt lag avseende (a) sekretess och datasäkerhet (b) användning, insamling, behållande, lagring, säkerhet, utlämnande, överföring, kassering och annan behandling av personuppgifter.

Med "GDPR" avses Europaparlamentets och rådets förordning (EU) av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Med "lokala dataskyddslagar inom EU/EES" avses all underordnad lagstiftning och reglering som genomför GDPR.

Med "GDPR-villkor" avses villkoren i [Bilaga 3](#), enligt vilka Microsoft gör bindande åtaganden angående sin behandling av personuppgifter enligt kraven i Artikel 28 i GDPR.

Med "personuppgifter" avses eventuell information om en identifierad eller identifierbar fysisk person. En identifierbar fysisk person är en som kan identifieras, direkt eller indirekt, i synnerhet genom referens till en identifikation såsom ett namn, id-nummer, platsdata, ett online-id eller till en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Med "data i professionella tjänster" avses alla data, inklusive alla text-, ljud-, video- och bildfiler eller programvara, som Microsoft tillhandahålls av Kunden eller för Kundens räkning (eller som Kunden ger Microsoft behörighet att inhämta från en Onlinetjänst), eller som i övrigt inhämtas eller behandlas av eller åt Microsoft genom en kontakt med Microsoft för att få professionella tjänster. Data i professionella tjänster innefattar supportdata.

Med "tjänstgenererade data" avses data som genererats eller erhållits av Microsoft genom användning av en onlinetjänst. Tjänstgenererade data innefattar inte kunddata, diagnostikdata eller data i professionella tjänster.

Med "standardavtalsklausuler" avses standarddataskyddsklausuler för överföring av personuppgifter till personuppgiftsbiträden som är etablerade i tredje land och som inte säkerställer adekvat dataskyddsnivå enligt vad som anges i Artikel 46 i GDPR, och som godkänts i Europeiska kommissionens beslut 2010/87/EG, av den 5 februari 2010. Standardavtalsklausulerna finns i [Bilaga 2](#).

Med "underordnat personuppgiftsbiträde" avses andra personuppgiftsbiträden som Microsoft anlitar för behandling av kunddata och personuppgifter, inbegripet eventuell underleverantör som behandlar kunddata och personuppgifter.

Med "supportdata" avses alla data, inklusive alla text-, ljud-, video- och bildfiler eller programvara, som Microsoft tillhandahålls av kunden eller för kundens räkning (eller som kunden ger Microsoft behörighet att inhämta från en onlinetjänst) genom en kontakt med Microsoft för att få teknisk support för de onlinetjänster som omfattas av detta avtal. Supportdata utgör en underordnad del av data i professionella tjänster.

Termer som används men inte definieras i detta DPA, exempelvis "personuppgiftsincident", "behandling", "personuppgiftsansvarig", "personuppgiftsbiträde", "profilering", "personuppgifter" och "registrerad" har samma betydelse som anges i artikel 4 i GDPR, oavsett om GDPR är tillämplig. Termerna "dataimportör" och "dataexportör" har samma betydelse som anges i standardavtalsklausulerna.

[Innehållsförteckning/Allmänna villkor](#)

[Innehållsförteckning](#)



[Inledning](#)



[Allmänna villkor](#)



[Dataskyddsvillkor](#)



[Bilaga](#)

Allmänna villkor

Efterlevnad av lagar

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.

Dataskyddsvillkor

I detta avsnitt av DPA ingår följande underavsnitt:

- Omfattning
- Typ av databehandling, ägarskap
- Utlämnande av behandlade data
- Behandling av personuppgifter, GDPR
- Datasäkerhet
- Meddelande om säkerhetsincidenter
- Dataöverföringar och plats
- Behållande och radering av data
- Personuppgiftsbiträdes konfidentialitetsåtagande
- Meddelande om och kontroll över användning av underordnade personuppgiftsbiträden
- Utbildningsinstitutioner
- CJIS-kundavtal
- HIPAA Business Associate
- Villkor enligt California Consumer Privacy Act (CCPA)
- Så här kontaktar du Microsoft
- Tillägg A – Säkerhetsåtgärder

Omfattning

Villkoren i detta DPA gäller för alla onlinetjänster utom sådana som i Bilaga 1 till OST anges specifikt som undantagna, vilka styrs av de villkor för integritet och säkerhet i tillämpliga specifika villkor för onlinetjänsten.

För förhandsversioner kan mindre omfattande eller andra integritets- och säkerhetsåtgärder gälla än de som normalt förekommer i onlinetjänsterna. Såvida inget annat anges ska kunden inte använda förhandsversioner i behandling av personuppgifter eller andra data som är underkastade krav på efterlevnad enligt lag eller reglering. Följande villkor i detta DPA gäller inte för förhandsversioner: Behandling av personuppgifter: GDPR, Datasäkerhet och HIPAA Business Associate.

[Bilaga 1](#) till DPA innehåller villkoren för integritet och säkerhet för data i professionella tjänster, inbegripet eventuella personuppgifter däri, i samband med tillhandahållandet av professionella tjänster. Därför är villkoren i detta DPA inte tillämpliga på tillhandahållandet av professionella tjänster, såvida inget annat uttryckligen görs tillämpligt i [Bilaga 1](#).

Typ av databehandling, ägarskap

Microsoft ska endast använda och i övrigt behandla kunddata och personuppgifter (a) för att tillhandahålla Kunden onlinetjänsterna enligt Kundens dokumenterade instruktioner (b) för Microsofts berättigade verksamhetsutövning, enligt detaljer och begränsningar nedan. Parterna emellan behåller kunden alla rättigheter, äganderätt och intressen i och till kunddata. Microsoft förvärvar inga rättigheter till kunddata annat än de rättigheter Kunden beviljar Microsoft i detta avsnitt. Denna punkt påverkar inte Microsofts rättigheter avseende programvara eller tjänster som Microsoft licensierar till Kunden.

Behandling för att tillhandahålla Kunden onlinetjänsterna

I detta DPA inbegriper ”att tillhandahålla” en onlinetjänst följande:

- 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).

[Innehållsförteckning](#)[Inledning](#)[Allmänna villkor](#)[Dataskyddsvillkor](#)[Bilaga](#)

I tillhandahållandet av onlinetjänster ska Microsoft inte använda eller på annat sätt behandla kunddata eller personuppgifter för följande: (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.

Behandling för Microsofts berättigade verksamhetsutövning

I detta DPA inbegriper "Microsofts berättigade verksamhetsutövning" följande, som vardera hör till leveransen av onlinetjänsterna till Kunden: (1) Fakturering och kontohantering. (2) Ersättning (t.ex. beräkning av personalens provision eller partnerincitament). (3) Intern rapportering och modellering (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).

Vid behandling för Microsofts berättigade verksamhetsutövning ska Microsoft inte använda eller på annat sätt behandla kunddata eller personuppgifter för följande: (a) Användarprofilering. (b) Annonsering eller liknande kommersiella ändamål. Vid behandling av sådana data för Microsofts berättigade verksamhetsutövning ska Microsoft dessutom endast behandla dessa för de ändamål som anges i detta avsnitt.

Utlämnande av behandlade data

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. I detta avsnitt avses med "Behandlade data" följande: (a) Kunddata. (b) Personuppgifter. (c) Andra data som behandlas av Microsoft i samband med den onlinetjänst som är Kundens konfidentiella information enligt volymlicensieringsavtalet. All behandling av behandlade data är underkastad Microsofts konfidentialitetsskyldighet enligt volymlicensieringsavtalet.

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.

Microsoft ska inte tillhandahålla tredje man något av följande: (a) Direkt, indirekt, allmän eller fri tillgång till behandlade data. (b) Plattforms-krypteringsnycklar som används för att säkra behandlade data eller förmågan att knäcka en sådan kryptering. (c) Tillgång till behandlade data om Microsoft känner till att sådana uppgifter ska användas för andra ändamål än de som anges i tredje mans begäran.

Till stöd för ovanstående får Microsoft tillhandahålla tredje man Kundens grundläggande kontaktuppgifter.

Behandling av personuppgifter, GDPR

Alla personuppgifter som behandlas av Microsoft i samband med onlinetjänsterna inhämtas som antingen kunddata, diagnostikdata eller tjänstgenererade data. Personuppgifter som tillhandahålls Microsoft av Kunden eller för Kundens räkning genom dennas användning av onlinetjänsterna är också kunddata. Pseudonymiserade identifierare kan ingå i diagnostikdata eller tjänstgenererade data, och är också personuppgifter. Personuppgifter som är pseudonymiserade, eller avidentifierade men inte anonymiserade, eller personuppgifter som härrör från personuppgifter är också personuppgifter

I den mån Microsoft är personuppgiftsbiträde eller underordnat personuppgiftsbiträde underkastat GDPR reglerar GDPR-villkoren i [Bilaga 3](#) den behandlingen, och parterna godkänner också följande villkor i detta underavsnitt (Behandling av personuppgifter, GDPR):

Roller och ansvar för personuppgiftsbiträden och personuppgiftsansvariga

Kunden och Microsoft avtalar att Kunden är personuppgiftsansvarig och Microsoft är personuppgiftsbiträde för dessa uppgifter, utom i följande fall: (a) När Kunden agerar personuppgiftsbiträde, då Microsoft är ett underordnat personuppgiftsbiträde. (b) När annat anges i de specifika villkoren för onlinetjänsten eller detta DPA. När Microsoft är personuppgiftsbiträde eller underordnat personuppgiftsbiträde för personuppgifter ska de endast behandla personuppgifter enligt dokumenterade instruktioner från Kunden. Kunden samtycker till att dennas volymlicensieringsavtal (inbegripet detta DPA och OST) tillsammans med produktdokumentationen och Kundens användning och konfiguration av funktioner i onlinetjänsterna är Kundens fullständiga och slutliga dokumenterade instruktioner till Microsoft för behandling av personuppgifter. Information om användning och konfiguration av onlinetjänsterna finns på <https://docs.microsoft.com/sv-se/> eller på en efterträdande plats. Eventuella ytterligare eller alternativa instruktioner måste godkännas i enlighet med processen för ändring av Kundens volymlicensieringsavtal. I annat fall där GDPR är tillämplig och Kunden är personuppgiftsbiträde intygar Kunden för Microsoft att dennas instruktioner, inbegripet att ge Microsoft uppdraget som personuppgiftsbiträde eller underordnat personuppgiftsbiträde, har godkänts av relevant personuppgiftsansvarig.

I den mån Microsoft använder eller i övrigt behandlar personuppgifter som är underkastade GDPR eller andra dataskyddskrav i samband med Microsofts berättigade verksamhetsutövning är Microsoft en oberoende personuppgiftsansvarig för sådan användning, och ansvarar för att

[Innehållsförteckning](#)[Inledning](#)[Allmänna villkor](#)[Dataskyddsvillkor](#)[Bilaga](#)

efterleva alla tillämpliga lagar och skyldigheter som gäller för personuppgiftsansvariga. Microsoft vidtar säkerhetsåtgärder för att skydda kunddata och personuppgifter vid behandling, inbegripet de som anges i detta DPA och de som avses i Artikel 6(4) i GDPR.

Detaljer om behandling

Parterna bekräftar och avtalar följande:

- **Föremål.** Föremålet för behandlingen begränsas till personuppgifter inom ramen för avsnittet ovan i detta DPA med rubriken "Typ av behandling, ägarskap" samt GDPR.
- **Behandlingens varaktighet.** Behandlingens varaktighet ska överensstämma med Kundens instruktioner och villkoren i DPA.
- **Typ av och syfte med behandlingen.** Typen av och syftet med behandlingen ska vara att tillhandahålla onlinetjänsten enligt kundens volymlicensieringsavtal (vilket beskrivs utförligare i avsnittet "Typ av behandling, ägarskap" ovan i detta DPA).
- **Datakategorier.** Personuppgifter som behandlas av onlinetjänsten innefattar följande typer: (i) Personuppgifter som Kunden väljer att inkludera i kunddata. (ii) De som uttryckligen anges i Artikel 4 i GDPR som kan ingå i diagnostikdata eller tjänstgenererade data. Typer av personuppgifter som Kunden väljer att inkludera i kunddata kan vara vilken kategori som helst av personuppgifter som finns i register som förs av Kunden som personuppgiftsansvarig enligt Artikel 30 i GDPR, inbegripet de kategorier av personuppgifter som anges i [Tillägg 1 till Bilaga 2](#) – Standardavtalsklausulerna (personuppgiftsbiträden) i DPA.
- **Registrerade.** Kategorierna av registrerade är Kundens representanter och slutanvändare, såsom anställda, uppdragstagare, samarbetspartner och kunder, och kan innefatta andra kategorier av registrerade som finns i register som förs av Kunden som personuppgiftsansvarig enligt Artikel 30 i GDPR, inbegripet de kategorier av registrerade som anges i [Tillägg 1 till Bilaga 2](#) – Standardavtalsklausulerna (personuppgiftsbiträden) i DPA.

Registrerades rättigheter: assistans med begäran

Microsoft ska på ett sätt som är förenligt med onlinetjänstens funktionalitet och Microsofts roll som personuppgiftsbiträde ge Kunden tillgång till registrerades personuppgifter och möjlighet att fullgöra registrerades begäran om att utöva sina rättigheter enligt GDPR. Om Microsoft får en begäran från kundens registrerade om att utöva sina rättigheter enligt GDPR, i samband med en onlinetjänst som Microsoft är personuppgiftsbiträde eller underordnat personuppgiftsbiträde för, ska Microsoft hänvisa den registrerade till att ställa sin begäran direkt till kunden. Kunden ansvarar för att besvara sådan begäran, i förekommande fall med hjälp av onlinetjänstens funktioner. Microsoft ska fullgöra rimlig begäran från Kunden om hjälp med att besvara sådan begäran från registrerad.

Register över behandling

I den mån GDPR kräver att Microsoft samlar in och bibehåller register med viss information avseende Kunden ska denna, om det begärs, tillhandahålla Microsoft sådan information och hålla den korrekt och uppdaterad. Microsoft får göra sådan information tillgänglig för tillsynsmyndigheten om detta krävs enligt GDPR.

Datasäkerhet

Säkerhetsrutiner och säkerhetspolicier

Microsoft ska implementera och upprätthålla lämpliga tekniska och organisatoriska åtgärder avsedda att skydda kunddata och personuppgifter mot oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt utlämnande av eller åtkomst till personuppgifter som överförs, lagras eller i övrigt behandlas. Dessa åtgärder ska anges i en Microsoft-säkerhetspolicy. Microsoft ska göra den policyn tillgänglig för kunden, tillsammans med beskrivningar av införda säkerhetskontroller för onlinetjänsten och annan information som kunden skäligen begär angående Microsofts säkerhetsrutiner och säkerhetspolicier.

Dessa åtgärder ska också efterleva de krav som anges i ISO 27001, ISO 27002 och ISO 27018. Varje central onlinetjänst efterlever också de kontrollstandarder och ramverk som visas i tabellen i Bilaga 1 till OST, och implementerar och upprätthåller de säkerhetsåtgärder som anges i Tillägg A till skydd av kunddata.

Microsoft får när som helst lägga till bransch- eller myndighetsstandarder. Microsoft ska inte utesluta ISO 27001, ISO 27002, ISO 27018 eller standarder eller ramverk i tabellen i Bilaga 1 till OST, såvida de inte längre används inom branschen och har ersatts av nya (om tillämpligt).

Kundens ansvar

Kunden är ensam ansvarig för att självständigt fastställa huruvida tekniska och organisatoriska åtgärder för en onlinetjänst uppfyller Kundens krav, däribland eventuella säkerhetsskyldigheter enligt tillämpliga dataskyddskrav. Kunden bekräftar och samtycker (med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens typ, omfattning, sammanhang och syften vad gäller dennas personuppgifter samt riskerna för enskilda) till att de säkerhetsrutiner och säkerhetspolicier som införs och upprätthålls av Microsoft ger en säkerhetsnivå som är lämplig i förhållande till risken vad gäller deras personuppgifter. Kunden är ansvarig för att implementera och underhålla integritetsskydd och säkerhetsåtgärder för komponenter som kunden tillhandahåller eller råder över (såsom enheter som är registrerade i Microsoft Intune eller inom en Microsoft Azure-kunds virtuella maskin eller program).

[Innehållsförteckning](#)[Inledning](#)[Allmänna villkor](#)[Dataskyddsvillkor](#)[Bilaga](#)

Granskning av efterlevnad

Microsoft ska utföra granskningar av säkerheten för datorerna, datamiljön och de fysiska datacenter som används för att behandla kunddata och personuppgifter enligt följande:

- Om en standard eller ett ramverk föreskriver granskningar ska en granskning av kontrollstandarderna eller ramverket i fråga initieras minst årligen.
- Varje granskning ska utföras enligt standarder och regler för tillsyns- eller ackrediteringsorganet för tillämpliga kontrollstandarder eller ramverk.
- Varje granskning ska utföras av kvalificerade, oberoende säkerhetsgranskare från tredje man som Microsoft väljer och bekostar.

Varje granskning ska leda till att en granskningsrapport skapas (Microsofts granskningsrapport) som Microsoft ska göra tillgänglig på <https://servicetrust.microsoft.com/> eller annan plats som Microsoft tillkännager. Microsofts granskningsrapport ska vara Microsofts konfidentiella information och tydligt visa granskarens väsentliga fynd. Microsoft ska omgående åtgärda problem som tas upp i Microsofts granskningsrapport enligt granskarens önskemål. På kundens begäran ska Microsoft tillhandahålla Kunden varje Microsoft-granskningsrapport. Microsofts granskningsrapport ska vara underkastad Microsofts och granskarens sekretess- och distributionsbegränsningar.

I den mån Kundens granskningskrav enligt standardavtalsklausuler eller dataskyddskrav inte rimligen kan tillgodoses genom granskningsrapporter, dokumentation eller efterlevnadsinformation som Microsoft gör allmänt tillgängliga för sina kunder, ska Microsoft omgående svara på Kundens ytterligare granskningsinstruktioner. Innan en granskning påbörjas ska Kunden och Microsoft gemensamt avtala om omfattning, tidpunkt, varaktighet, kontroll och beviskrav samt avgifter för granskningen, förutsatt att detta krav på att avtala inte tillåter att Microsoft oskäligt fördröjer granskningens genomförande. I den utsträckning som är nödvändig för genomförandet av granskningen ska Microsoft tillgängliggöra behandlingssystem, resurser och stöddokumentation som är relevanta för Microsofts, deras koncernbolags och underordnade personuppgiftsbiträdens behandling av kunddata och personuppgifter. Sådan granskning ska genomföras av en oberoende, behörig revisionsfirma tillhörande tredje man under ordinarie kontorstid, med rimligt varsel till Microsoft, och underkastat rimliga konfidentialitetsförfaranden. Vare sig Kunden eller granskaren ska ha tillgång till data från Microsofts andra kunder, eller till Microsofts system eller resurser som inte ingår i onlinetjänsterna. Kunden ska svara för alla kostnader och avgifter för sådan granskning, inbegripet alla rimliga kostnader och avgifter för all den tid Microsoft ägnar åt sådan granskning, i tillägg till avgifter för de tjänster som utförs av Microsoft. Om granskningsrapporten som genereras genom Kundens granskning visar på väsentligt bristande efterlevnad ska Kunden dela granskningsrapporten med Microsoft, som omgående ska avhjälpa sådana brister.

Om standardavtalsklausulerna tillämpas är detta avsnitt ett tillägg till klausul 5 punkt f och klausul 12 punkt 2 i standardavtalsklausulerna. Inget i detta avsnitt av DPA ändrar standardavtalsklausulerna eller GDPR-villkoren, eller påverkar någon tillsynsmyndighets eller registrerads rättigheter enligt standardavtalsklausulerna eller dataskyddskrav. Microsoft Corporation är en avsedd tredjemansförmanstagare i detta avsnitt.

Meddelande om säkerhetsincidenter

Om Microsoft får kännedom om en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt utlämnande av eller åtkomst till kunddata eller personuppgifter under Microsofts behandling (vardera en säkerhetsincident), ska Microsoft omgående och utan oskäligt dröjsmål (1) meddela kunden om säkerhetsincidenten, (2) undersöka säkerhetsincidenten och ge kunden utförlig information om denna, (3) vidta rimliga åtgärder för att mildra effekterna och minimera eventuell skada till följd av säkerhetsincidenten.

Meddelanden om säkerhetsincidenter ska levereras till en eller flera av kundens administratörer på ett sätt som Microsoft väljer, inklusive via e-post. Kunden är ensam ansvarig för att se till att kundens administratörer upprätthåller korrekta kontaktuppgifter på varje tillämplig portal för onlinetjänster. Kunden är ensam ansvarig för att fullgöra sina skyldigheter enligt lagar om incidentmeddelande som är tillämpliga på kunden samt eventuella meddelandeskyldigheter gentemot tredje man avseende eventuell säkerhetsincident.

Microsoft ska göra rimliga insatser för att hjälpa kunden att fullgöra sina skyldigheter enligt Artikel 33 i GDPR eller annan tillämplig lag eller förordning att meddela relevant tillsynsmyndighet och registrerade om sådan säkerhetsincident.

Microsofts meddelande om eller svar på en säkerhetsincident enligt detta avsnitt är inte en bekräftelse från Microsoft av något fel eller ansvar beträffande säkerhetsincidenten.

Kunden måste omgående meddela Microsoft om varje eventuellt missbruk av dennas konton eller autentiseringsuppgifter och varje form av säkerhetsincident gällande en onlinetjänst.

Dataöverföringar och plats

Dataöverföringar

Med undantag för vad som beskrivs på andra ställen i DPA får kunddata och personuppgifter som Microsoft behandlar för Kundens räkning överföras till, lagras och behandlas i USA eller något annat land där Microsoft eller dess underordnade personuppgiftsbiträden är verksamma. Kunden uppdrar åt Microsoft att utföra sådan överföring av kunddata och personuppgifter till varje sådant land och att lagra och behandla kunddata och personuppgifter för att tillhandahålla onlinetjänsterna.

[Innehållsförteckning](#)[Inledning](#)[Allmänna villkor](#)[Dataskyddsvillkor](#)[Bilaga](#)

All överföring av kunddata ut ur Europeiska unionen, Europeiska Ekonomiska Samarbetsområdet och Schweiz som görs med centrala onlinetjänster regleras av standardavtalsklausulerna i Bilaga 3, såvida inte Kunden har valt bort dessa klausuler.

Microsoft ska följa kraven enligt dataskyddslagar i EES och Schweiz avseende insamling, användning, överföring, behållande och annan behandling av personuppgifter från EES och Schweiz. Alla överföringar av personuppgifter till tredje man eller internationell organisation ska underkastas tillämpliga säkerhetsåtgärder enligt beskrivningen i Artikel 46 i GDPR, och sådana överföringar och säkerhetsåtgärder ska dokumenteras i enlighet med Artikel 30(2) i GDPR.

Microsoft är därutöver certifierat för EU:s–USA:s och Schweiz–USA:s Privacy Shield Framework-standarder och de åtaganden dessa innebär. Microsoft samtycker till att underrätta Kunden om man fastställer att man inte längre kan fullgöra sin skyldighet att tillhandahålla skydd på samma nivå som krävs enligt Privacy Shield-standarderna.

Plats för vilande kunddata

Vad gäller centrala onlinetjänster ska Microsoft lagra vilande kunddata inom vissa större geografiska områden (vardera ett geo-område) enligt vad som anges i Bilaga 1 till OST.

Microsoft har inte kontroll över och begränsar inte de regioner från vilka Kunden eller Kundens slutanvändare har åtkomst till eller kan flytta kunddata.

Behållande och radering av data

Kunden har när som helst under sin prenumerations giltighetstid möjlighet att komma åt, extrahera och radera kunddata som har lagrats i vardera onlinetjänst.

Med undantag för kostnadsfria utvärderingsversioner och LinkedIn-tjänster ska Microsoft behålla kvarvarande kunddata i onlinetjänster i ett konto med begränsad funktionalitet i 90 dagar efter att kundens prenumeration har upphört eller sagts upp så att kunden kan hämta sina data. När denna 90-dagars behållandeperiod upphör inaktiverar Microsoft Kundens konto och tar bort kunddata och personuppgifter inom ytterligare 90 dagar, såvida inte Microsoft enligt tillämplig lag eller enligt detta DPA har rätt att behålla sådana data.

Onlinetjänsten stöder eventuellt inte behållande eller hämtning av programvara som tillhandahålls av Kunden. Microsoft har inget ansvar för borttagning av kunddata eller personuppgifter enligt beskrivning i det här avsnittet.

Personuppgiftsbiträdes konfidentialitetsåtagande

Microsoft ska säkerställa att dess personal som deltar i behandlingen av kunddata och personuppgifter (i) endast behandlar sådana data på Kundens instruktioner eller så som beskrivs i detta DPA (ii) åläggs att upprätthålla konfidentialitet och säkerhet för sådana data, även efter att deras deltagande har upphört. Microsoft ska tillhandahålla anställda med åtkomst till kunddata och personuppgifter regelbunden och obligatorisk integritets- och säkerhetsutbildning och medvetandegörande enligt tillämpliga dataskyddskrav samt enligt branschstandarder.

Meddelande om och kontroll över användning av underordnade personuppgiftsbiträden

Microsoft har rätt att anlita tredje man för att tillhandahålla vissa begränsade eller tillhörande tjänster för sin räkning. Kunden samtycker till anlitan av sådan tredje man och Microsofts koncernbolag som underordnade personuppgiftsbiträden. Ovanstående godkännanden utgör Kundens föregående skriftliga medgivande till att Microsoft lägger ut behandling av kunddata och personuppgifter på underentreprenad, om sådant medgivande krävs enligt standardavtalsklausulerna eller GDPR-villkoren.

Microsoft ansvarar för sina underordnade personuppgiftsbiträdes fullgörande av Microsofts skyldigheter enligt detta DPA. Microsoft tillgängliggör information om underordnade personuppgiftsbiträden på en Microsoft-webbplats. När ett underordnat personuppgiftsbiträde anlitas ska Microsoft säkerställa genom skriftligt avtal att det underordnade personuppgiftsbiträdet får tillgå och använda kunddata eller personuppgifter endast för att leverera de tjänster Microsoft har anlitat dem för, och att de förbjuds att använda kunddata eller personuppgifter för något annat syfte. Microsoft ska säkerställa att underordnade personuppgiftsbiträden är bundna av skriftliga avtal som ålägger dem att tillhandahålla minst den nivå av dataskydd som Microsoft avkrävs enligt DPA. Microsoft förbinder sig till att ha överinseende över underordnade personuppgiftsbiträden för att säkerställa att deras skyldigheter enligt avtal fullgörs.

Microsoft får från tid till annan anlita nya underordnade personuppgiftsbiträden. Microsoft ska meddela Kunden (genom att uppdatera webbplatsen och förse Kunden med en metod för att ta emot meddelande om uppdateringen) om ett eventuellt nytt underordnat personuppgiftsbiträde minst sex månader innan det underordnade personuppgiftsbiträdet ges åtkomst till kunddata. Vidare ska Microsoft meddela Kunden (genom att uppdatera webbplatsen och förse kunden med en metod för att ta emot meddelande om uppdateringen) om ett eventuellt nytt underordnat personuppgiftsbiträde minst 14 dagar innan det underordnade personuppgiftsbiträdet ges åtkomst till personuppgifter utöver sådana som finns i kunddata.

Om Kunden inte godkänner det nya underordnade personuppgiftsbiträdet får Kunden säga upp eventuell prenumeration på den berörda onlinetjänsten utan påföljd genom att före uppsägningstidens slut tillhandahålla ett skriftligt meddelande om uppsägning. Kunden kan också i meddelandet om uppsägning lämna en förklaring om anledningen till att detta inte godkänns, så att Microsoft kan omvärdera sådant nytt underordnat personuppgiftsbiträde utifrån de aktuella invändningarna. Om den berörda onlinetjänsten ingår i en svit (eller liknande enskilt köp av

[Innehållsförteckning](#)[Inledning](#)[Allmänna villkor](#)[Dataskyddsvillkor](#)[Bilaga](#)

tjänster) är uppsägningen tillämplig på hela sviten. Efter uppsägningen ska Microsoft avlägsna betalningsskyldigheter avseende eventuella prenumerationer på den uppsagda onlinetjänsten från kundens eller dennas återförsäljares efterföljande fakturor.

Utbildningsinstitutioner

Om Kunden är en skolförvaltning eller institution som lyder under den amerikanska lagen om familjens rätt till utbildning och integritet (FERPA), 20 U.S.C. § 1232g, godkänner Microsoft att, vad gäller DPA, betecknas som "utbildningsrepresentant" med "ett rättmätigt utbildningsintresse" i kunddata, såsom dessa termer har definierats enligt FERPA och bestämmelserna för dess tillämpning, och Microsoft samtycker till att följa begränsningar och krav som åläggs utbildningsrepresentanter i enlighet med 34 CFR 99.33(a).

Kunden är införstådd med att Microsoft kan ha begränsad eller ingen kontaktinformation till kundens elever och elevernas föräldrar. Följaktligen ska Kunden ansvara för att inhämta eventuellt medgivande från föräldrar för slutanvändares användning av onlinetjänsten som kan krävas enligt tillämplig lag, och för att förmedla meddelande på uppdrag av Microsoft till studenter (eller, i fråga om studenter under 18 år som inte studerar vid en eftergymnasial institution, till elevens förälder) om ett domstolsbeslut eller lagligen utfärdat åläggande om utlämnande av kunddata i Microsofts ägo som kan krävas enligt tillämplig lag.

CJIS-kundavtal

Microsoft tillhandahåller vissa molntjänster för myndigheter ("tjänster som omfattas") enligt FBI Criminal Justice Information Services (CJIS) säkerhetspolicy ("CJIS-policy"). CJIS-policyn reglerar användning och överföring av straffrättslig information. Alla Microsoft CJIS-tjänster som omfattas regleras av de allmänna villkor i CJIS-kundvillkoren som finns här: <http://aka.ms/CJISCustomerAgreement>.

HIPAA Business Associate

Om Kunden är en "omfattad enhet" eller en "affärskontakt" och omfattas av "skyddad hälsoinformation" i Kunddata såsom dessa termer är definierade i 45 CFR § 160.103 omfattar utförandet av Kundens volymlicensieringsavtal utförandet av HIPAA Business Associate-avtalet ("BAA"). Den fullständiga texten för detta, som anger de onlinetjänster det avser, finns på <http://aka.ms/BAA>. Kunden kan välja bort BAA genom att skicka följande information till Microsoft i ett skriftligt meddelande (inom ramen för villkoren för Kundens volymlicensieringsavtal):

- Kundens fullständiga namn som juridisk person och eventuella koncernbolag som väljer bort.
- om Kunden har flera volymlicensieringsavtal, det volymlicensieringsavtal som ärendet gäller.

California Consumer Privacy Act (CCPA)

Om Microsoft behandlar personuppgifter inom CCPA:s omfattning gör Microsoft följande ytterligare utfästelser till Kunden. Microsoft ska behandla kunddata och personuppgifter för Kundens räkning och inte behålla, använda eller lämna ut data i något annat syfte än de som anges i detta DPA och som tillåts enligt CCPA, inbegripet enligt något "försäljningsundantag". Microsoft ska under inga omständigheter sälja sådana data. Dessa CCPA-villkor begränsar eller minskar inga dataskyddsåtaganden som Microsoft gör gentemot Kunden i DPA, villkoren för onlinetjänster eller annat avtal dem mellan.

Så här kontaktar du Microsoft

Om Kunden anser att Microsoft inte följer sina åtaganden för integritet eller säkerhet kan kunden kontakta kundtjänst eller använda Microsofts webbformulär för integritetsfrågor som finns på <http://go.microsoft.com/?linkid=9846224>. Microsofts postadress är:

Microsoft Enterprise Service Privacy

Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited är Microsofts dataskyddsrepresentant för det europeiska ekonomiska samarbetsområdet och Schweiz. Representanten för integritetsskydd på Microsoft Ireland Operations Limited kan nås på följande adress:

Microsoft Ireland Operations, Ltd.

Att.: Data Protection
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18, D18 P521, Ireland

[Innehållsförteckning](#)/[Allmänna villkor](#)

[Innehållsförteckning](#)



[Inledning](#)



[Allmänna villkor](#)



[Dataskyddsvillkor](#)



[Bilaga](#)

Tillägg A – Säkerhetsåtgärder

Microsoft har implementerat och ska för kunddata i de centrala onlinetjänsterna upprätthålla följande säkerhetsåtgärder som, tillsammans med säkerhetsåtgärderna i detta DPA (inbegripet GDPR-villkoren), är Microsofts enda ansvar vad gäller säkerheten för dessa data.

Domän	Praxis
Organisation av informationssäkerhet	<p>Säkerhetsägarskap. Microsoft har utsett en eller flera säkerhetsansvariga som ansvarar för att samordna och övervaka regler och förfaranden kring säkerhet.</p> <p>Säkerhetsroller och ansvar. Microsofts personal med åtkomst till Kunddata är underkastade sekretesskyldigheter.</p> <p>Program för riskhantering. Microsoft gjorde en riskbedömning innan Kunddata behandlades eller Onlinetjänsten lanserades.</p> <p>Microsoft behåller sina säkerhetsdokument i enlighet med sina krav på behållande när de inte längre gäller.</p>
Tillgångshantering	<p>Förteckning över tillgångar. Microsoft upprätthåller en förteckning över alla medier på vilka Kunddata lagras. Åtkomst till förteckningen över sådana medier är begränsad till Microsofts personal som skriftligen getts behörighet till sådan åtkomst.</p> <p>Hantering av tillgångar</p> <ul style="list-style-type: none"> - Microsoft klassificerar kunddata för att kunna identifiera dessa och för att se till att åtkomsten till dem är tillfredsställande begränsad. - Microsoft inför begränsningar vad gäller utskrift av kunddata och har rutiner för kassering av utskrivet material som innehåller kunddata. - Microsofts personal måste få behörighet från Microsoft innan de får lagra Kunddata på bärbara enheter, bereda sig fjärråtkomst till Kunddata eller behandla Kunddata utanför Microsofts anläggningar.
HR-säkerhet	<p>Säkerhetsutbildning. Microsoft informerar sin personal om relevanta säkerhetsförfaranden och personalens respektive roller. Microsoft informerar även personalen om möjliga konsekvenser av överträdelse mot säkerhetsregler och förfaranden. Microsoft använder endast anonyma data i utbildningen.</p>
Fysisk säkerhet och miljösäkerhet	<p>Fysisk åtkomst till anläggningar. Microsoft begränsar tillträdet till lokaler med informationssystem som behandlar Kunddata till identifierade behöriga personer.</p> <p>Fysisk åtkomst till komponenter. Microsoft för register över inkommande och utgående medier som innehåller Kunddata, inklusive typ av medier, behörig avsändare/mottagare, datum och tid, antalet medier och typer av Kunddata dessa innehåller.</p> <p>Skydd mot störningar. Microsoft använder en mängd olika branschstandardsystem för att skydda mot förlust av data på grund av elavbrott eller kommunikationsstörningar.</p> <p>Kassering av komponenter. Microsoft använder branschstandardprocesser för att radera Kunddata när de inte längre behövs.</p>
Kommunikations- och verksamhetshantering	<p>Verksamhetspolicy. Microsoft upprätthåller säkerhetsdokument som beskriver säkerhetsåtgärder och relevanta förfaranden samt ansvarsområden för personalen som har åtkomst till Kunddata.</p> <p>Dataåterställningsförfaranden</p> <ul style="list-style-type: none"> - Microsoft gör flera kopior av Kunddata regelbundet, men i inget fall mer sällan än en gång i veckan (förutom då inga Kunddata har uppdaterats under den perioden), från vilka Kunddata kan återställas. - Microsoft lagrar kopior av Kunddata och dataåterställningsrutinerna på ett annat ställe än där den primära datorutrustningen som behandlar Kunddata finns. - Microsoft har specifika rutiner som reglerar vem som har åtkomst till kopiorna av Kunddata. - Microsoft granskar förfaranden för dataåterställning minst en gång var sjätte månad, utom förfaranden för dataåterställning avseende Azure-myndighetstjänster, som granskas en gång om året. - Microsoft loggar insatser för dataåterställning, bland annat ansvarig person, beskrivning av återställda data och i förekommande fall, den person som är ansvarig och vilka data (om några) som måste matas in manuellt i dataåterställningsprocessen. <p>Skadlig programvara. Microsoft har kontroller med skydd mot skadlig programvara som bidrar till att undvika att skadlig programvara får obehörig åtkomst till Kunddata, inklusive skadlig programvara som kommer från offentliga nätverk.</p>

[Innehållsförteckning](#)

[Inledning](#)

[Allmänna villkor](#)

[Dataskyddsvillkor](#)

[Bilaga](#)

Domän	Praxis
	<p>Data utanför Microsofts gränser</p> <ul style="list-style-type: none"> - Microsoft krypterar, eller gör det möjligt för Kunden att kryptera, Kunddata som skickas via offentliga nätverk. - Microsoft begränsar åtkomst till Kunddata i medier som lämnar Microsofts anläggningar. <p>Händelseloggning. Microsoft loggar, eller gör det möjligt för Kunden att logga, åtkomst till och användning av informationssystem som innehåller Kunddata och registrerar åtkomst-ID, tid, beviljad eller avvisad behörighet och relevant aktivitet.</p>
Åtkomstkontroll	<p>Åtkomstpolicy. Microsoft för register över säkerhetsrättigheter för personer som har åtkomst till Kunddata.</p> <p>Beviljande av åtkomst</p> <ul style="list-style-type: none"> - Microsoft för och uppdaterar ett register över personal som är behöriga att få åtkomst till Microsofts system som innehåller Kunddata. - Microsoft inaktiverar behörighetsuppgifter som inte har använts under en period på minst sex månader. - Microsoft identifierar den personal som får bevilja, ändra eller avbryta behörig åtkomst till data och resurser. - Microsoft ser till att i de fall där fler än en person har åtkomst till system som innehåller Kunddata har dessa personer separata ID-nummer/inloggningar. <p>Minsta behörighet</p> <ul style="list-style-type: none"> - Teknisk supportpersonal har endast behörighet att bereda sig åtkomst till kunddata vid behov. - Microsoft begränsar åtkomst till Kunddata till endast de personer som behöver sådan åtkomst för att kunna utföra sina arbetsuppgifter. <p>Integritet och sekretess</p> <ul style="list-style-type: none"> - Microsoft anvisar sin personal att inaktivera administrativa sessioner när de lämnar lokaler som Microsoft kontrollerar eller i situationer då datorer lämnas utan uppsikt. - Microsoft lagrar lösenord på ett sätt som gör dem obegripliga medan de gäller. <p>Autentisering</p> <ul style="list-style-type: none"> - Microsoft använder branschstandardrutiner för att identifiera och autentisera användare som försöker bereda sig åtkomst till informationssystem. - Om autentiseringsmekanismen baseras på lösenord kräver Microsoft att lösenorden förnyas regelbundet. - Om autentiseringsmekanismen baseras på lösenord kräver Microsoft att lösenordet är minst åtta tecken långt. - Microsoft ser till att identifierare som har inaktiverats eller upphört att gälla inte beviljas andra personer. - Microsoft övervakar, eller gör det möjligt för Kunden att övervaka, upprepade försök att bereda sig åtkomst till informationssystemet med användning av ett ogiltigt lösenord. - Microsoft följer branschstandardrutiner för att inaktivera lösenord som har blivit korrupta eller röjda av misstag. - Microsoft använder branschstandardrutiner för lösenordsskydd, inklusive rutiner avsedda för att upprätthålla lösenordens sekretess och integritet när de tilldelas och distribueras, och under lagring. <p>Nätverksutformning. Microsoft har kontroller för att undvika att personer som tror att de har åtkomstbehörigheter som de inte har blivit tilldelade bereder sig åtkomst till Kunddata som de inte har behörighet till.</p>
Incidenthantering avseende informationssäkerhet	<p>Process för incidentrespons</p> <ul style="list-style-type: none"> - Microsoft för register över säkerhetsbrott med en beskrivning av brottet, tidsperioden, brottets konsekvenser, namn på den person som rapporterade och till vem brottet rapporterades samt rutinen för dataåterställning. - Microsoft ska meddela varje säkerhetsöverträdelse som är en säkerhetsincident (enligt beskrivning i avsnittet "Meddelande om säkerhetsincidenter" ovan) utan oskäligt dröjsmål och, under alla omständigheter, inom 72 timmar. - Microsoft spårar, eller gör det möjligt för Kunden att spåra, utlämnanden av kunddata, inklusive vilka data som har lämnats ut, till vem och vid vilken tidpunkt. <p>Tjänstövervakning. Microsofts säkerhetspersonal verifierar loggar minst var sjätte månad för att ge förslag på åtgärder för avhjälpande vid behov.</p>

[Innehållsförteckning](#)

[Inledning](#)

[Allmänna villkor](#)

[Dataskyddsvillkor](#)

[Bilaga](#)

Domän	Praxis
Hantering av affärskontinuitet	<ul style="list-style-type: none">- Microsoft upprätthåller kris- och beredskapsplaner för anläggningar där Microsofts informationssystem som behandlar Kunddata finns.- Microsofts redundanslagring och dess rutiner för dataåterställning är utformade för att försöka omskapa kunddata till ursprungligt skick eller senast kopierade skick från tiden innan de gick förlorade eller förstördes.

[Innehållsförteckning](#)/[Allmänna villkor](#)

[Innehållsförteckning](#)



[Inledning](#)



[Allmänna villkor](#)



[Dataskyddsvillkor](#)



[Bilaga](#)

Bilaga 1 – Meddelanden

Professionella tjänster

Professionella tjänster tillhandahålls underkastat nedanstående villkor för professionella tjänster. Om professionella tjänster tillhandahålls enligt ett separat avtal gäller dock villkoren i det separata avtalet för de professionella tjänsterna.

De Professionella tjänster som detta meddelande gäller är inte onlinetjänster, och resten av villkoren för onlinetjänster och DPA gäller inte såvida inte detta uttryckligen framgår av nedanstående villkoren för professionella tjänster.

Behandling av data i professionella tjänster, ägarskap

Microsoft ska endast använda och i övrigt behandla data i professionella tjänster (a) för att tillhandahålla Kunden de professionella tjänsterna enligt Kundens dokumenterade instruktioner (b) för Microsofts berättigade verksamhetsutövning, enligt detaljer och begränsningar nedan. Parterna emellan behåller Kunden alla rättigheter, äganderätter och intressen i och till data i professionella tjänster. Microsoft förvärvar inga rättigheter till data i professionella tjänster annat än de rättigheter Kunden beviljar Microsoft för att tillhandahålla Kunden de professionella tjänsterna. Denna punkt påverkar inte Microsofts rättigheter avseende programvara eller tjänster som Microsoft licensierar till Kunden.

Behandling för att tillhandahålla Kunden de professionella tjänsterna

I detta DPA inbegriper "att tillhandahålla" professionella tjänster följande:

- Leverans av de professionella tjänsterna, inbegripet att tillhandahålla teknisk support, professionell planering, rådgivning, vägledning, datamigrering, distribution och lösnings-/programvaruutveckling.
- Felsökning (förebyggande, detektion, undersökning, avhjälpande och åtgärdande av problem, inbegripet säkerhetsincidenter).
- Fortlöpande förbättring (underhålla de professionella tjänsterna inklusive installera de senaste uppdateringarna och göra förbättringar för tillförlitlighet, effektivitet, kvalitet och säkerhet).

I tillhandahållandet av professionella tjänster ska Microsoft inte använda eller på annat sätt behandla data i professionella tjänster för följande: (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.

Behandling för Microsofts berättigade verksamhetsutövning

I detta DPA består Microsofts berättigade verksamhetsutövning av följande: (1) Fakturering och kontohantering. (2) Ersättning (t.ex. beräkning av personalens provision). (3) Intern rapportering och modellering (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), vardera en följd av leverans av de professionella tjänsterna till Kunden.

Vid behandling för Microsofts berättigade verksamhetsutövning ska Microsoft inte använda eller på annat sätt behandla data i professionella tjänster för följande: (a) Användarprofilering. (b) Annonsering eller liknande kommersiella ändamål.

Utlämnande av data i professionella tjänster

Villkoret "Utlämnande av behandlade data" i avsnittet Dataskyddsvillkor i OST är tillämpligt på Kundens delaktighet i professionella tjänster vad gäller data i dessa.

Behandling av personuppgifter, GDPR

Personuppgifter som tillhandahålls Microsoft av Kunden eller för Kundens räkning genom en kontakt med Microsoft för att få professionella tjänster utgör också data i professionella tjänster.

I den mån Microsoft är personuppgiftsbiträde eller underordnat personuppgiftsbiträde underkastat GDPR reglerar GDPR-villkoren i [Bilaga 3](#) den behandlingen, och parterna godkänner också följande villkor i detta underavsnitt (Behandling av personuppgifter, GDPR):

Roller och ansvar för personuppgiftsbiträden och personuppgiftsansvariga

Kunden och Microsoft avtalar att Kunden är personuppgiftsansvarig för data som ingår i professionella tjänster, och att Microsoft är personuppgiftsbiträde för dessa uppgifter, utom när (a) Kunden agerar personuppgiftsbiträde, då Microsoft är ett underordnat personuppgiftsbiträde (b) om annat anges i dessa villkor för professionella tjänster. När Microsoft är personuppgiftsbiträde eller underordnat personuppgiftsbiträde för personuppgifter ska de endast behandla personuppgifter enligt dokumenterade instruktioner från Kunden. Kunden samtycker till att dennas volymlicensieringsavtal (inklusive detta DPA och OST) med eventuellt utlåtande om tjänster som avtalats mellan parterna är Kundens fullständiga och slutliga dokumenterade instruktioner till Microsoft för behandling av personuppgifter som ingår i data i professionella tjänster. Eventuella ytterligare eller alternativa instruktioner måste godkännas i enlighet med processen för ändring av Kundens

[Innehållsförteckning](#)[Inledning](#)[Allmänna villkor](#)[Dataskyddsvillkor](#)[Bilaga](#)

volymlicensieringsavtal eller utlåtan om tjänster. I annat fall där GDPR är tillämplig och Kunden är personuppgiftsbiträde intygar Kunden för Microsoft att dennas instruktioner, inbegripet att ge Microsoft uppdraget som personuppgiftsbiträde eller underordnat personuppgiftsbiträde, har godkänts av relevant personuppgiftsansvarig.

I den mån Microsoft använder eller i övrigt behandlar data i professionella tjänster som är underkastade GDPR eller andra dataskyddskrav i samband med Microsofts berättigade verksamhetsutövning är Microsoft en oberoende personuppgiftsansvarig för sådan användning, och ansvarar för att efterleva alla tillämpliga lagar och skyldigheter som gäller för personuppgiftsansvariga. Microsoft vidtar säkerhetsåtgärder för att skydda data i professionella tjänster vid behandling, inbegripet de som anges i detta DPA och de som avses i Artikel 6(4) i GDPR.

Detaljer om behandling

Parterna bekräftar och avtalar följande:

- **Föremål.** Föremålet för behandlingen begränsas till personuppgifter inom ramen för avsnittet ovan i dessa villkor för professionella tjänster med rubriken "Behandling av data i professionella tjänster, ägarskap" samt GDPR.
- **Behandlingens varaktighet.** Behandlingens varaktighet ska överensstämma med Kundens instruktioner och dessa villkor för professionella tjänster.
- **Typ av och syfte med behandlingen.** Behandlingens typ och syfte ska vara att tillhandahålla professionella tjänster enligt Kundens volymlicensieringsavtal och eventuellt utlåtande om tjänster (enligt vidare beskrivning i avsnittet "Behandling av data i professionella tjänster, ägarskap" ovan i dessa villkor för professionella tjänster).
- **Datakategorier.** Typer av personuppgifter som behandlas i samband med tillhandahållandet av professionella tjänster innefattar (i) personuppgifter som Kunden väljer att inkludera i data i professionella tjänster. (ii) Sådana som uttryckligen anges i artikel 4 i GDPR. Typer av personuppgifter som Kunden väljer att inkludera i data i professionella tjänster kan vara vilken kategori som helst av personuppgifter som finns i register som förs av Kunden som personuppgiftsansvarig enligt Artikel 30 i GDPR, inbegripet de kategorier av personuppgifter som anges i [Tillägg 1 till Bilaga 2](#) – Standardavtalsklausulerna (personuppgiftsbiträden) i DPA.
- **Registrerade.** Kategorierna av registrerade är Kundens representanter och slutanvändare, såsom anställda, uppdragstagare, samarbetspartner och kunder, och kan innefatta andra kategorier av registrerade som finns i register som förs av Kunden som personuppgiftsansvarig enligt Artikel 30 i GDPR, inbegripet de kategorier av registrerade som anges i [Tillägg 1 till Bilaga 2](#) – Standardavtalsklausulerna (personuppgiftsbiträden) i DPA.

Registrerades rättigheter: assistans med begäran

Vad gäller data i professionella tjänster som Kunden lagrar i en Onlinetjänst ska Microsoft följa de skyldigheter som anges i villkoret "Registrerades rättigheter: assistans med begäran" och "Register över behandling" i avsnittet Dataskyddsvillkor i DPA. För övriga professionella tjänster ska Microsoft radera alla exemplar av data i professionella tjänster enligt avsnittet "Radering eller retur av data" nedan.

Register över behandling

I den mån GDPR kräver att Microsoft samlar in och bibehåller register med viss information avseende Kunden ska denna, om det begärs, tillhandahålla Microsoft sådan information och hålla den korrekt och uppdaterad. Microsoft får göra sådan information tillgänglig för tillsynsmyndigheten om detta krävs enligt GDPR.

Datasäkerhet

Säkerhetsrutiner och säkerhetspolicyer

Microsoft ska implementera och upprätthålla lämpliga tekniska och organisatoriska åtgärder avsedda att skydda data i professionella uppgifter mot oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt utlämnande av eller åtkomst till personuppgifter som överförs, lagras eller i övrigt behandlas. Dessa åtgärder ska anges i Microsofts säkerhetspolicy. Microsoft ska göra den policyn tillgänglig för Kunden, tillsammans med annan information som Kunden skäligen begär angående Microsofts säkerhetsrutiner och säkerhetspolicyer.

Kundens ansvar

Villkoret "Kundens ansvar" i avsnittet Dataskyddsvillkor i DPA är tillämpligt på Kundens delaktighet i professionella tjänster vad gäller data i dessa. Kunden samtycker också till, vad gäller Kundens delaktighet i professionella tjänster, att inte lämna ut data i professionella tjänster annat än supportdata till Microsoft som är underkastade bestämmelser enligt Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA) eller Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191) (HIPAA).

Meddelande om säkerhetsincidenter

Villkoret "Meddelande om säkerhetsincidenter" i avsnittet Dataskyddsvillkor i DPA är tillämpligt på kundens delaktighet i professionella tjänster vad gäller data i dessa.

[Innehållsförteckning](#)[Inledning](#)[Allmänna villkor](#)[Dataskyddsvillkor](#)[Bilaga](#)

Dataöverföringar

Vad gäller data i professionella tjänster åtar sig Microsoft de skyldigheter som är tillämpliga på personuppgifter enligt villkoret Dataöverföringar i avsnittet Dataskyddsvillkor i DPA.

Radering eller retur av data

Microsoft ska radera eller returnera alla exemplar av data i professionella tjänster efter att affärssyftet som låg till grund för att dessa samlades in eller överfördes har fullgjorts, eller tidigare på Kundens begäran, såvida inte Microsoft har rätt eller skyldighet att behålla sådana data enligt tillämplig lag eller detta DPA.

Personuppgiftsbiträdes konfidentialitetsåtagande

Microsoft ska säkerställa att dess personal som deltar i behandlingen av data i Professionella tjänster (i) endast behandlar sådana data efter instruktion från Kunden eller enligt beskrivningen i dessa villkor för professionella uppgifter (ii) åläggs att upprätthålla konfidentialitet och säkerhet för sådana data, även efter att deras deltagande har upphört. Microsoft ska tillhandahålla anställda med åtkomst till data i professionella uppgifter regelbunden och obligatorisk dataintegritets- och säkerhetsutbildning och medvetandegörande enligt tillämpliga dataskyddskrav och branschstandarder.

Meddelande om och kontroll över användning av underordnade personuppgiftsbiträden

Microsoft har rätt att anlita tredje man för att tillhandahålla vissa begränsade eller tillhörande tjänster för sin räkning. Kunden samtycker till anlitan av sådan tredje man och Microsofts koncernbolag som underordnade personuppgiftsbiträden. Ovanstående godkännanden utgör Kundens föregående skriftliga medgivande till att Microsoft lägger ut behandling av data i professionella tjänster på underentreprenad, om sådant medgivande krävs enligt standardavtalsklausulerna eller GDPR-villkoren.

Microsoft ansvarar för att deras underordnade personuppgiftsbiträden som behandlar data i professionella tjänster uppfyller Microsofts skyldigheter enligt [Bilaga 1](#) i DPA. Microsoft ska säkerställa genom skriftligt avtal att det underordnade personuppgiftsbiträdet får tillgång och använda data i professionella tjänster endast för att leverera de tjänster Microsoft har anlitat dem för, och att de förbjuds att använda data i professionella tjänster för något annat syfte. Microsoft ska säkerställa att dessa andra personuppgiftsbiträden är bundna av skriftliga avtal som ålägger dem att tillhandahålla minst den nivå av dataskydd som Microsoft avkrävs enligt dessa villkor för professionella tjänster. Microsoft förbinder sig till att ha överinseende över underordnade personuppgiftsbiträden för att säkerställa att deras skyldigheter enligt avtal fullgörs.

Vad gäller andra data i professionella tjänster än supportdata är en förteckning över Microsofts underordnade personuppgiftsbiträden tillgänglig på begäran. Om en sådan förteckning begärs minst 30 dagar innan ett eventuellt nytt underordnat personuppgiftsbiträde ges behörighet och åtkomst till Personuppgifter ska Microsoft uppdatera förteckningen och förse Kunden med ett sätt att meddelas om denna uppdatering.

Om Kunden inte godkänner ett nytt underordnat personuppgiftsbiträde får Kunden säga upp delaktigheten vad gäller de berörda professionella tjänsterna genom att, inom den aktuella uppsägningstiden, tillhandahålla ett skriftligt uppsägningsmeddelande. Kunden kan också i meddelandet om uppsägning lämna en förklaring om anledningen till att detta inte godkänns, så att Microsoft kan omvärdera sådant nytt underordnat personuppgiftsbiträde utifrån de aktuella invändningarna.

Vad gäller supportdata regleras Microsofts användning av underordnade personuppgiftsbiträden i samband med tillhandahållande av teknisk support för onlinetjänster av samma begränsningar och förfaranden som reglerar deras användande av underordnade personuppgiftsbiträden i samband med de onlinetjänster som anges i bestämmelsen "Meddelande om och kontroll över användning av underordnade personuppgiftsbiträden" i DPA.

Tilläggs villkor för supportdata

Säkerhet för supportdata

Microsoft ska införa och upprätthålla tillämpliga tekniska och organisatoriska åtgärder för att skydda supportdata. Dessa åtgärder ska uppfylla kraven enligt ISO 27001, ISO 27002 och ISO 27018

Utbildningsinstitutioner

Microsofts bekräftelser och samtycke till och Kundens skyldighet att inhämta förälders samtycke och framföra meddelande enligt vad som anges i bestämmelsen "Utbildningsinstitutioner" i avsnittet Dataskyddsvillkor i DPA är också tillämpliga beträffande supportdata.

California Consumer Privacy Act (CCPA)

Om Microsoft behandlar personuppgifter inom CCPA:s omfattning gör Microsoft följande ytterligare utfästelser till Kunden. Microsoft ska behandla data i professionella tjänster för Kundens räkning och inte behålla, använda eller lämna ut data i något annat syfte än de som anges i detta DPA och som tillåts enligt CCPA, inbegripet enligt något "försäljningsundantag". Microsoft ska under inga omständigheter sälja sådana data. Dessa CCPA-villkor begränsar eller minskar inga dataskyddsåtaganden som Microsoft gör gentemot Kunden i DPA, villkoren för onlinetjänster eller annat avtal dem mellan.

[Innehållsförteckning/Allmänna villkor](#)

[Innehållsförteckning](#)



[Inledning](#)



[Allmänna villkor](#)



[Dataskyddsvillkor](#)



[Bilaga](#)

Bilaga 2 – Standardavtalsklausuler (personuppgiftsbiträden)

Kundens verkställande av volymlicensieringsavtalet omfattar verkställande av denna Bilaga 2, vilken är kontrast signerad av Microsoft Corporation. För att välja bort standardavtalsklausuler måste Kunden skicka följande information i ett skriftligt meddelande till Microsoft (enligt villkoren i Kundens volymlicensieringsavtal):

- Kundens fullständiga namn som juridisk person och eventuella koncernbolag som väljer bort.
- Om kunden har flera volymlicensieringsavtal, vilket volymlicensieringsavtal det gäller.
- Ett uttalande om att kunden (eller dess koncernbolag) väljer bort standardavtalsklausulerna.

I länder där det krävs myndighetsgodkännande för användning av standardavtalsklausulerna kan dessa inte åberopas enligt Europeiska kommissionen 2010/87/EU (från februari 2010) för att legitimera export av data från landet, såvida inte kunden har erhållit erforderligt myndighetsgodkännande.

Med början den 25 maj 2018 och därefter behandlas referenser till diverse artiklar i direktivet 95/46/EG i nedanstående standardavtalsklausuler som referenser till relevanta och tillämpliga artiklar i GDPR.

För artikel 26(2) i direktiv 95/46/EG beträffande överföring av personuppgifter till personuppgiftsbiträden i tredje land med otillräckligt dataskydd, har Kunden (som dataexportör) och Microsoft Corporation (som dataimportör, vars signatur visas nedan), vardera en "part", sammantaget "parterna", enats om följande avtalsklausuler ("Klausulerna" eller "Standardavtalsklausulerna") för att säkerställa ett tillräckligt skydd för integritet och grundläggande fri- och rättigheter för enskilda individer i samband med dataexportörens överföring till dataimportören av sådana personuppgifter som anges i Tillägg 1.

Klausul 1: Definitioner

(a) "Personuppgifter", "särskilda kategorier av uppgifter", "behandling", "personuppgiftsansvarig", "personuppgiftsbiträde", "registrerad" och "tillsynsmyndighet" ska ha samma innebörd som i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

(b) Med "dataexportör" avses den personuppgiftsansvariga som överför personuppgifterna.

(c) Med "dataimportör" avses det personuppgiftsbiträde som samtycker till att ta emot personuppgifter från dataexportören för vidare behandling i enlighet med dennas instruktioner och villkoren i klausulerna, och som inte är underkastad ett system i tredje land som garanterar ett adekvat skydd i den mening som avses i artikel 25(1) i direktivet 95/46/EG.

(d) Med "underordnat personuppgiftsbiträde" avses det personuppgiftsbiträde som anlitas av dataimportören eller av en annan av dataimportörens underordnade personuppgiftsbiträden och som samtycker till att från dataimportören eller en dennas underordnade personuppgiftsbiträde ta emot personuppgifter i den enda avsikten att efter överföringen behandla personuppgifter för dennas räkning i enlighet med dennas instruktioner, villkoren i klausulerna samt villkoren i det skriftliga avtalet om underordnade personuppgiftsbiträden.

(e) Med "tillämplig dataskyddslagstiftning" avses sådan lagstiftning som skyddar personers grundläggande fri- och rättigheter, särskilt deras integritet i samband med behandling av personuppgifter som är tillämplig på personuppgiftsansvariga i den medlemsstat där dataexportören är etablerad.

(f) Med "tekniska och organisatoriska säkerhetsåtgärder" avses åtgärder avsedda att skydda personuppgifter mot oavsiktlig eller olaglig förstöring, oavsiktlig förlust, ändring, obehörigt utlämnande eller åtkomst, i synnerhet när behandlingen inbegriper överföring av data i ett nätverk, och mot varje annan form av olaglig behandling.

Klausul 2: Information om överföringen

Information om överföringen, och i förekommande fall om särskilda kategorier av personuppgifter, anges i Tillägg 1 nedan, vilket utgör en integrerad del av Klausulerna.

Klausul 3: Tredjemansförmånstagare

1. Den registrerade kan i egenskap av tredjemansförmånstagare åberopa denna klausul och klausulerna 4(b) till (i), klausul 5(a) till (e) och (g) till (j), klausul 6(1) och (2), klausul 7, klausul 8(2) och klausulerna 9 till 12 gentemot dataexportören.

2. Den registrerade kan gentemot dataimportören åberopa denna klausul, klausulerna 5(a) till (e) och (g), klausul 6, klausul 7, klausul 8(2) och klausulerna 9 till 12, i sådana fall där dataexportören har upphört att existera i faktisk eller rättslig mening, såvida inte en annan enhet enligt avtal eller lag till fullo har övertagit dataexportörens rättsliga skyldigheter, och som en följd av detta påtar sig dataexportörens rättigheter och skyldigheter, i vilket fall den registrerade kan åberopa de ovannämnda klausulerna gentemot denna.

3. Den registrerade kan gentemot det underordnade personuppgiftsbiträdet åberopa denna klausul, klausulerna 5(a) till (e) och (g), klausul 6, klausul 7, klausul 8(2) och klausulerna 9 till 12, i de fall där dataexportören har upphört att existera i faktisk eller rättslig mening eller har hamnat på

[Innehållsförteckning](#)[Inledning](#)[Allmänna villkor](#)[Dataskyddsvillkor](#)[Bilaga](#)

obestånd, såvida inte en annan enhet enligt avtal eller lag till fullo har övertagit dennas rättsliga skyldigheter, och som en följd av detta övertar dataexportörens rättigheter och skyldigheter, i vilket fall den registrerade kan åberopa de ovan nämnda klausulerna gentemot denna enhet. Skadeståndsansvaret ska i sådana fall vara begränsat till det underordnade personuppgiftsbitrådets egna behandling enligt klausulerna.

4. Parterna har inget att invända mot att en registrerad företräds av sammanslutningar eller andra organ om denne uttryckligen så önskar och i den mån det är tillåtet enligt nationell rätt.

Klausul 4: Dataexportörens skyldigheter

Dataexportören godtar och garanterar följande:

- (a) Att behandlingen, inbegripet själva överföringen, av personuppgifterna har skett och även i fortsättningen kommer att ske i enlighet med tillämplig dataskyddslagstiftning (och i förekommande fall anmäls till behöriga myndigheter i den medlemsstat där dataexportören är etablerad) och inte strider mot gällande lagar eller andra författningar i den medlemsstaten.
- (b) Att denna har instruerat och under behandlingen av personuppgifter kommer att instruera dataimportören att behandla de överförda personuppgifterna endast för dataexportörens räkning och i enlighet med tillämplig dataskyddslagstiftning och klausulerna.
- (c) Att dataimportören kommer att ge tillräckliga garantier vad gäller de tekniska och organisatoriska säkerhetsåtgärder som anges i Bilaga 2 nedan.
- (d) Att denna, mot bakgrund av tillämplig dataskyddslagstiftning, har funnit säkerhetsåtgärderna lämpliga för att skydda personuppgifter mot oavsiktlig eller olaglig förstöring, oavsiktlig förlust, ändring, otillåtet utlämnande eller otillåten åtkomst, i synnerhet när behandlingen inbegriper överföring av uppgifter i ett nätverk, och mot varje annan form av olaglig behandling, med hänsyn tagen till teknikens standpunkt, kostnaden för vidtagande av åtgärderna och de risker behandlingen innebär och den typ av uppgifter som ska behandlas.
- (e) Att denna kommer att se till att säkerhetsåtgärderna efterlevs.
- (f) Att, om överföringen avser särskilda kategorier av uppgifter, de registrerade har informerats eller informeras senast när överföringen sker eller så snart som möjligt därefter om att deras uppgifter kan komma att överföras till ett tredje land som inte tillhandahåller adekvat skydd i den mening som avses i direktiv 95/46/EG.
- (g) Att vidarebefordra anmälningar från dataimportören eller eventuellt underordnat personuppgiftsbiträde i enlighet med klausul 5(b) och klausul 8(3) till tillsynsmyndigheten om dataexportören beslutar att fortsätta överföringen eller häva avbrottet.
- (h) Att på begäran tillhandahålla de registrerade en kopia av klausulerna, med undantag för bilaga 2, och en sammanfattande beskrivning av säkerhetsåtgärderna, samt en kopia av eventuella avtal om underordnat personuppgiftsbiträde som måste ingås i enlighet med klausulerna, såvida inte dessa eller avtalet innehåller affärsinformation, som dataexportören i så fall får ta bort.
- (i) Att behandlingen vid en eventuell utläggning på entreprenad utförs i enlighet med klausul 11 av en ett underordnat personuppgiftsbiträde som tillhandahåller åtminstone samma skydds nivå för personuppgifter och den registrerades rättigheter som dataimportören ska göra enligt klausulerna.
- (j) Att denna kommer att se till att klausul 4(a) till (i) efterlevs.

Klausul 5: Dataimportörens skyldigheter

Dataimportören godtar och garanterar följande:

- (a) Att behandla personuppgifter för dataexportörens räkning och enlighet med dennas instruktioner samt dessa klausuler. Om denna av något skäl inte kan fullgöra detta krav går denna med på att omedelbart informera dataexportören om detta, varvid denna har rätt att avbryta överföringen av uppgifter och/eller häva avtalet.
- (b) Att denna inte har anledning att förmoda att den lagstiftning som är tillämplig hindrar dataimportören från att fullfölja dataexportörens instruktioner och sina skyldigheter enligt detta avtal. Om lagstiftningen ändras på ett sätt som sannolikt har en avsevärt skadlig inverkan på de garantier som klausulerna innebär, ska dataimportören meddela ändringen till dataexportören, varvid denna har rätt att avbryta överföringen av uppgifter och/eller häva avtalet.
- (c) Att denna har vidtagit de tekniska och organisatoriska säkerhetsåtgärder som anges i bilaga 2 innan de överförda personuppgifterna behandlas.
- (d) Att denna utan dröjsmål kommer att underrätta dataexportören om följande:
 - (i) Varje rättsligt bindande begäran från rättsliga myndigheter om utlämnande av personuppgifterna, om inte detta är förbjudet på grund av exempelvis ett straffrättsligt förbud som syftar till att bevara sekretessen vid brottsutredningar.
 - (ii) Varje oavsiktlig eller otillåten åtkomst.
 - (iii) Varje begäran direkt från registrerade, utan att svara på dem om denna inte getts tillstånd till det.

[Innehållsförteckning](#)[Inledning](#)[Allmänna villkor](#)[Dataskyddsvillkor](#)[Bilaga](#)

- (e) Att utan dröjsmål och korrekt handlägga alla frågor från dataexportören om behandling av sådana personuppgifter som överförs och att rätta sig efter tillsynsmyndighetens rekommendationer med avseende på behandlingen av de uppgifter som överförs.
- (f) Att på dataexportörens begäran ställa sin databehandlingsutrustning till förfogande för granskning av den behandling som dessa klausuler avser. Granskningen ska genomföras av dataexportören eller av ett inspektionsorgan med oberoende och sakkunniga ledamöter. De av tystnadsplikt bundna ledamöterna utses av dataexportören, i förekommande fall enligt överenskommelse med tillsynsmyndigheten.
- (g) Att på begäran förse de registrerade med en kopia av klausulerna eller av eventuella befintliga avtal om underordnat personuppgiftsbiträde, såvida inte klausulerna eller kontraktet innehåller känslig affärsinformation. I så fall får dataexportören ta bort dessa uppgifter, med undantag för Tillägg 2, som ska ersättas av en sammanfattande beskrivning av säkerhetsåtgärderna i de fall där den registrerade inte kan erhålla en kopia från dataexportören.
- (h) Att denna, vid förekomst av underordnat personuppgiftsbiträde, i förväg har underrättat dataexportören och utverkat skriftligt medgivande från denna.
- (i) Att den behandling som utförs av det underordnade personuppgiftsbiträdet utförs i enlighet med klausul 11.
- (j) Att omedelbart översända till dataexportören en kopia av eventuella avtal om underordnat personuppgiftsbiträde som ingåtts enligt klausulerna.

Klausul 6: Ansvar

- Parterna avtalar att en registrerad som lidit skada till följd av att en part eller en parts underordnade personuppgiftsbiträde brutit mot de skyldigheter som avses i klausul 3 eller klausul 11 har rätt till ersättning för vållad skada från dataexportören.
- Om den registrerade, i situationer där dataimportören eller dennes underordnade personuppgiftsbiträde bryter mot någon av sina skyldigheter enligt klausulerna 3 eller 11, inte kan rikta skadeståndsanspråk mot dataexportören i enlighet med punkt 1 på grund av att dataexportören har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd, ska dataimportören godta att den registrerade kan rikta ett skadeståndsanspråk mot dataimportören som om denne var dataexportören, såvida inte en annan enhet enligt avtal eller lag till fullo har övertagit dataexportörens rättsliga skyldigheter, i vilket fall den registrerade kan göra sina rättigheter gällande gentemot denna enhet.
Dataimportören kan inte åberopa att ett underordnat personuppgiftsbiträde har brutit i sina skyldigheter för att undvika eget ansvar.
- Om en registrerad, i situationer där ett underordnat personuppgiftsbiträde har brutit mot någon av sina skyldigheter enligt klausulerna 3 eller 11, inte kan rikta ett skadeståndsanspråk mot dataexportören eller dataimportören i enlighet med punkt 1 och 2 på grund av att båda dessa har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd, ska det underordnade personuppgiftsbiträdet godta att den registrerade kan rikta ett skadeståndsanspråk mot denna, med avseende på dennas egna behandling av personuppgifter i enlighet med klausulerna, som om denne var dataexportör eller dataimportör, såvida inte en annan enhet enligt avtal eller lag till fullo har övertagit dataexportörens eller dataimportörens rättsliga skyldigheter, i vilket fall den registrerade kan göra sina rättigheter gällande gentemot denna enhet. Skadeståndsansvaret ska i sådana fall vara begränsat till det underordnade personuppgiftsbiträdets egna behandling av uppgifter enligt klausulerna.

Klausul 7: Medling och forum

- Dataimportören samtycker till att, om den registrerade åberopar sin rätt som tredjemansförmånstagare och/eller kräver ersättning för skador i enlighet med klausulerna, godta den registrerades beslut att
 - hänskjuta tvisten till medling av en oberoende person eller, i tillämpliga fall, av tillsynsmyndigheten
 - hänskjuta tvisten till domstol i den medlemsstat där dataexportören är etablerad.
- Parterna är överens om att den registrerades val inte påverkar dennes materiella eller processuella rätt att söka gottgörelse i enlighet med andra bestämmelser i nationell eller internationell lagstiftning.

Klausul 8: Samarbete med tillsynsmyndigheter

- Dataexportören åtar sig att deponera ett exemplar av detta avtal hos tillsynsmyndigheten, om så föreskrivs i tillämplig dataskyddslagstiftning eller om tillsynsmyndigheten begär det.
- Parterna avtalar att tillsynsmyndigheten har rätt att genomföra inspektioner hos dataimportören och dataimportörens eventuella underordnade personuppgiftsbiträden i samma omfattning och på samma villkor som skulle gälla för en revision hos dataexportören enligt tillämplig dataskyddslagstiftning.
- Dataimportören ska omedelbart underrätta dataexportören om dataimportören och dennes eventuella underordnade personuppgiftsbiträde omfattas av lagstiftning som förhindrar att de blir föremål för inspektion i enlighet med punkt 2. I sådant fall ska dataexportören ha rätt att vidta de åtgärder som anges i klausul 5 (b).

Klausul 9: Gällande lag.



Klausulerna regleras av lagen i den medlemsstat där dataexportören är etablerad.

Klausul 10: Ändring av avtalet

Parterna åtar sig att inte ändra klausulerna. Detta hindrar inte parterna från att om nödvändigt lägga till klausuler om affärsrelaterade frågor, så länge dessa inte står i strid med någon klausul.

Klausul 11: Användning av underordnat personuppgiftsbiträde

1. Dataimportören får inte utan dataexportörens föregående skriftliga medgivande använda underordnat personuppgiftsbiträde för någon del av den behandling som dataimportören utför för dataexportörens räkning i enlighet med klausulerna. Om dataimportören, med dataexportörens samtycke, använder ett underordnat personuppgiftsbiträde får detta endast ske genom ingående av ett skriftligt avtal med underentreprenören, varigenom detta åläggs samma skyldigheter som enligt klausulerna åligger dataimportören. Om det underordnade personuppgiftsbiträdet inte uppfyller sina skyldigheter i fråga om dataskydd enligt ett sådant avtal ska dataimportören förbli fullt ansvarig gentemot dataexportören för det underordnade personuppgiftsbiträdets fullgörande av sina skyldigheter enligt avtalet.
2. Det på förhand ingångna skriftliga avtalet mellan dataimportören och underordnat personuppgiftsbiträde ska även inbegripa en bestämmelse om tredjemansförmånstagare i enlighet med klausul 3 i sådana fall där den registrerade inte kan rikta skadeståndsanspråk i enlighet med klausul 6.1 mot dataimportören eller dataexportören, eftersom dessa har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd, och ingen annan enhet har till fullo övertagit deras rättsliga skyldigheter enligt avtal eller lag. Skadeståndsansvaret ska i sådana fall vara begränsat till det underordnade personuppgiftsbiträdets egna behandling enligt klausulerna.
3. Bestämmelserna om dataskyddsaspekter vid utläggning på entreprenad av det kontrakt som avses i punkt 1 till ett underordnat personuppgiftsbiträde ska omfattas av lagen i den medlemsstat där dataexportören är etablerad.
4. Dataexportören ska föra en förteckning över entreprenadavtal som ingåtts enligt klausulerna och anmälts av dataimportören i enlighet med klausul 5 (j). Förteckningen ska uppdateras minst en gång om året. Förteckningen ska vara tillgänglig för dataexportörens dataskyddsmyndighet.

Klausul 12: Skyldigheter efter att behandlingen av personuppgifter har upphört

1. Parterna avtalar att dataimportören och det underordnade personuppgiftsbiträdet efter behandlingens upphörande och beroende på vad dataexportören beslutar antingen ska återlämna alla överförda personuppgifter och kopior av dessa till dataexportören, eller förstöra alla personuppgifter och intyga för dataexportören att så skett, såvida inte den på dataimportören tillämpliga lagstiftningen helt eller delvis hindrar denna från att återlämna eller förstöra de överförda personuppgifterna. I så fall ska dataimportören garantera att denna kommer att garantera konfidentialiteten för de överförda personuppgifterna och inte aktivt behandla dessa ytterligare.
2. Dataimportören och det underordnade personuppgiftsbiträdet garanterar att de på dataexportörens och/eller tillsynsmyndighetens begäran kommer att ställa sin databehandlingsutrustning till förfogande för en granskning av de åtgärder som anges i punkt 1.

Tillägg 1 till standardavtalsklausulerna

Dataexportören: Kunden är datautföraren. Dataexportören är en användare av onlinetjänster enligt definitionen i DPA och OST.

Dataimportören: Dataimportören är MICROSOFT CORPORATION, en global producent av programvara och tjänster.

Registrerade: Registrerade omfattar dataexportörens representanter och slutanvändare inklusive dennas anställda, uppdragstagare, samarbetspartner och kunder. Registrerade kan även omfatta enskilda personer som försöker kommunicera eller överföra personuppgifter till användare av tjänster som tillhandahålls av dataimportören. Microsoft bekräftar att Kunden beroende på dennas användning av onlinetjänsterna kan välja att i kunddata inkludera personuppgifter avseende följande typer av registrerade:

- Dataexportörens anställda, uppdragstagare och tillfälliga personal (tidigare nuvarande, kommande).
- Ovanstående underordnade.
- Dataexportörens samarbetspartner/kontaktpersoner (fysiska personer) eller anställda, uppdragstagare eller tillfällig personal (tidigare nuvarande, kommande) hos samarbetspartner/kontaktpersoner som är juridiska personer.
- Användare (t.ex. kunder, klienter, patienter, besökare) och andra registrerade som använder dataexportörens tjänster.
- Partner, intressenter eller enskilda som aktivt samarbetar, kommunicerar eller i övrigt interagerar med dataexportörens anställda och/eller använder kommunikationsverktyg såsom appar och webbplatser som tillhandahålls av dataexportören.
- Intressenter eller enskilda som passivt interagerar med dataexportörens (t.ex. för att de är föremål för utredning, forskning eller omnämns i dokument eller korrespondens från eller till dataexportören).
- Underåriga
- Yrkesgrupper med yrkesrelaterade befogenheter (t.ex. läkare, jurister, notarier, religionsarbetare).

[Innehållsförteckning](#)[Inledning](#)[Allmänna villkor](#)[Dataskyddsvillkor](#)[Bilaga](#)

Datakategorier: Personuppgifterna som överförs som ingår i e-post, dokument och andra data i elektronisk form i samband med onlinetjänsterna. Microsoft bekräftar att Kunden beroende på dennas användning av onlinetjänsterna kan välja att i kunddata inkludera personuppgifter från någon av följande kategorier:

- Grundläggande personuppgifter (t.ex. födelseort, gatunamn och husnummer (adress), postnummer, bostadsort, bosättningsland, mobiltelefonnummer, förnamn, efternamn, initialer, e-postadress, kön, födelsedatum), inbegripet grundläggande personuppgifter om familjemedlemmar och barn.
- Autentiseringsdata (t.ex. användarnamn, lösenord eller PIN-kod, säkerhetsfråga, redovisningsspårning).
- Kontaktuppgifter (t.ex. adresser, e-postadresser, telefonnummer, identifierare i sociala medier, kontaktuppgifter i nödfall).
- Unika identifieringsnummer och and signaturer (t.ex. personnummer, bankkontonummer, pass- och ID-kortnummer, körkortnummer och fordonsregistreringsuppgifter, IP-adresser, anställningsnummer, studentnummer, patientnummer, signatur, unik identifierare i spårningscookies eller liknande teknik).
- Pseudonyma identifierare.
- Ekonomi- och försäkringsuppgifter (t.ex. försäkringsnummer, bankkontonamn och -nummer, kreditkortsnamn och -nummer, fakturanummer, inkomst, typ av försäkring, betalningsbeteende, kreditvärdighet).
- Kommersiell information (t.ex. inköphistorik, specialerbjudanden, prenumerationsinformation, betalningshistorik).
- Biometrisk information (t.ex. DNA, fingeravtryck och irisskanningar).
- Platsdata (t.ex. mobil-ID, data från geoplatsnätverk, plats genom påbörjat/avslutat samtal. Platsdata härledda från användning av WiFi-åtkomstpunkter).
- Foton, video och ljud.
- Internet-aktivitet (t.ex. surfhistorik, sökhistorik, aktiviteter som läsning, tv-tittande, radiolyssnande).
- Enhetsidentifiering (t.ex. IMEI-nummer, SIM-kortnummer, MAC-adress).
- Profiler (t.ex. baserat på observerat kriminellt eller antisocialt beteende eller pseudonyma profiler baserade på besökta URL:er, klickströmmar, surfloggar, IP-adresser, domäner, installerade appar eller profiler baserade på marknadsföringspreferenser).
- HR- och rekryteringsdata (t.ex. uppgiven anställningsstatus, rekryteringsinformation (såsom CV, anställningshistorik, uppgifter om utbildningshistorik), arbets- och platsdata, inbegripet arbetade timmar, utvärderingar och lön, uppgifter om arbetstillstånd, tillgänglighet, anställningsvillkor, skatteuppgifter, betalningsuppgifter, försäkringsuppgifter samt plats och organisationer).
- Utbildningsuppgifter (t.ex. utbildningshistorik, nuvarande utbildning, betyg och resultat, högsta slutförda utbildning, inlärningssvårigheter).
- Medborgarskaps- och bosättningsinformation (t.ex. medborgarskap, naturaliseringsstatus, civilstånd, nationalitet, immigrationsstatus, passuppgifter, uppgifter om uppehålls- eller arbetstillstånd).
- Information som behandlas för utförande av en uppgift i allmänt intresse eller under myndighetsutövning.
- Särskilda kategorier av data (t.ex. ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk tro, fackföringsmedlemskap, genetiska data, biometriska data i syfte att unikt identifiera en fysisk person, data om hälsa, data om en fysisk persons sexualliv eller sexuella läggning, eller data angående straffdomar eller brott).
- Andra personuppgifter som anges i Artikel 4 i GDPR.

Behandling: De personuppgifter som överförs kommer att behandlas på följande sätt:

a. Databehandlingens varaktighet och målsättning. Varaktigheten för databehandling ska vara den period som anges i tillämpligt volymlicensieringsavtal mellan dataexportören och Microsoft-enheten till vilken dessa standardavtalsklausuler bifogas ("Microsoft"). Målet med databehandlingen är att onlinetjänsterna ska fungera.

b. Omfattning av och syfte med databehandlingen. Omfattningen av och syftet med behandlingen av personuppgifter beskrivs i avsnittet "Behandling av personuppgifter, GDPR" i DPA. Dataimportören driver ett globalt nätverk av datacenter och hanterings-/supportanläggningar, och behandlingen kan äga rum i vilken jurisdiktion som helst där dataimportören eller dennas underordnade personuppgiftsbiträden har sådana anläggningar i enlighet med avsnittet "Säkerhetsrutiner och säkerhetspolicier" i DPA.

c. Åtkomst till kunddata. Under den period som anges i tillämpligt volymlicensieringsavtal kommer dataimportören, efter eget val och när detta är nödvändigt enligt tillämplig lag, implementera artikel 12(b) i EU:s dataskyddsdirektiv och göra något av följande: (1) Ge

[Innehållsförteckning](#)[Inledning](#)[Allmänna villkor](#)[Dataskyddsvillkor](#)[Bilaga](#)

dataexportören möjlighet att korrigera, radera eller blockera kunddata eller (2) göra sådana korrigeringar, raderingar eller blockeringar å dennas vägnar.

d. Dataexportörens instruktioner. För onlinetjänster agerar dataimportören endast enligt dataexportörens instruktioner som förmedlas av Microsoft.

e. Radera eller returnera kunddata. När dataexportörens användning av onlinetjänsterna upphör eller sägs upp kan denna extrahera kunddata och dataimportören ska radera kunddata, allt i enlighet med OST och DPA som är tillämpliga på avtalet.

Underordnade personuppgiftsbiträden: Dataimportören kan i enlighet med DPA anlita andra företag för att tillhandahålla begränsade tjänster å dataimportörens vägnar, till exempel för att tillhandahålla kundsupport. Varje sådan underleverantör har rätt att få åtkomst till Kunddata endast för att leverera tjänsterna som dataimportören har anlitat dem att tillhandahålla och de är förbjudna att använda Kunddata för något annat ändamål.

Tillägg 2 till Standardavtalsklausulerna

Beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som implementeras av dataimportören i enlighet med klausul 4(d) och 5(c):

1. Personal. Dataimportörens personal ska inte behandla kunddata utan tillstånd. Personalen är skyldig att upprätthålla konfidentialiteten för alla kunddata och denna skyldighet fortsätter att gälla även efter att deras åtagande avslutas.

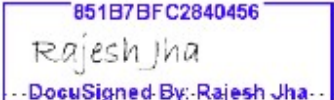
2. Dataskyddskontakt. Dataimportörens dataskyddsombud kan nås på följande adress:

Microsoft Corporation
Att.: Chief Privacy Officer
1 Microsoft Way
Redmond, WA 98052 USA

3. Tekniska och organisatoriska åtgärder. Dataimportören har infört och ska upprätthålla tillämpliga tekniska och organisatoriska åtgärder, interna kontroller och informationssäkerhetsrutiner som är avsedda att skydda kunddata, enligt definitionen i avsnittet "Säkerhetsrutiner och säkerhetspolicyer" i DPA, mot oavsiktlig förlust, förstöring eller ändring, otillåtet utlämnande eller åtkomst eller otillåten förstörelse enligt följande: De tekniska och organisatoriska åtgärder, interna kontroller och informationssäkerhetsrutiner som anges i avsnittet "Säkerhetsrutiner och säkerhetspolicyer" i DPA införlivas härmed i detta Tillägg 2 genom denna referens och är bindande för dataimportören som om de vore angivna i detta Tillägg 2 i sin helhet.

Microsoft Corporations underskrift finns på nästa sida.

Undertecknar standardklausulerna, Tillägg 1 och Tillägg 2 som representant för dataimportören:

Signature  851B7BFC2840456
Rajesh Jha

Rajesh Jha, Corporate Vice President

Microsoft Corporation

One Microsoft Way, Redmond WA, USA 98052

[Innehållsförteckning/Allmänna villkor](#)

[Innehållsförteckning](#)



[Inledning](#)



[Allmänna villkor](#)



[Dataskyddsvillkor](#)



[Bilaga](#)

Bilaga 3 – Villkor i EU:s allmänna dataskyddsförordning

Microsoft gör åtagandena i dessa GDPR-villkor gentemot alla kunder från och med den 25 maj 2018. Dessa åtaganden är bindande för Microsoft vad kunden beträffar, oavsett (1) vilken version av OST och DPA som i övrigt är tillämplig på en viss onlinetjänstprenumeration, (2) eventuellt annat avtal som hänvisar till denna bilaga.

För syftet med dessa GDPR-villkor avtalar kunden och Microsoft att kunden är personuppgiftsansvarig för kundens personuppgifter och Microsoft är personuppgiftsbiträde för dessa uppgifter, utom när kunden agerar personuppgiftsbiträde för personuppgifter, då Microsoft är ett underordnat personuppgiftsbiträde. Dessa GDPR-villkor är tillämpliga på Microsofts behandling av personuppgifter, inom ramen för GDPR, för kundens räkning. Dessa GDPR-villkor begränsar eller minskar inga dataskyddsåtaganden som Microsoft gör gentemot kunden enligt villkoren för onlinetjänster eller annat avtal dem mellan. Dessa GDPR-villkor är inte tillämpliga om Microsoft är personuppgiftsansvarig.

Relevanta skyldigheter enligt GDPR: Artikel 28, 32 och 33

1. Microsoft får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt medgivande har erhållits från Kunden. Om ett allmänt skriftligt tillstånd har erhållits, ska Microsoft informera Kunden om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att Kunden har möjlighet att göra invändningar mot sådana förändringar. (Artikel 28(2))
2. Microsofts databehandling regleras av dessa GDPR-villkor enligt Europeiska unionens (benämns härnåfter unionen) eller medlemsstats lagar och är bindande för Microsoft gentemot kunden. Föremålet för behandlingen, behandlingens varaktighet, art och syfte, typen av personuppgifter och kategorier av registrerade samt kundens skyldigheter och rättigheter anges i kundens licensavtal, inklusive dessa GDPR-villkor. Särskilt gäller att Microsoft ska göra följande:
 - (a) Endast behandla personuppgifter på dokumenterade instruktioner från Kunden, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som Microsoft omfattas av, och i så fall ska Microsoft informera Kunden om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt.
 - (b) Säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iakttä confidentiality eller omfattas av en lämplig lagstadgad sekretess.
 - (c) Vidta alla åtgärder som krävs enligt artikel 32 i GDPR.
 - (d) Respektera de villkor som avses i punkterna 1 och 3 för anlita ett annat personuppgiftsbiträde.
 - (e) Under beaktande av behandlingens art hjälpa Kunden genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att Kunden kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter enligt kapitel III i GDPR.
 - (f) Bistå Kunden med att se till att skyldigheterna enligt artiklarna 32–36 i GDPR fullgörs, med beaktande av typen av behandling och den information som Microsoft har tillgång till.
 - (g) Efter Kundens val radera eller returnera alla personuppgifter till Kunden efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstats nationella rätt.
 - (h) Ge Kunden tillgång till all information som krävs för att visa efterlevnad av de skyldigheter som fastställs i artikel 28 i GDPR och för att främja och bidra till granskningar, inbegripet inspektioner, som genomförs av Kunden eller av annan granskare på uppdrag av Kunden.

Microsoft ska omedelbart informera Kunden om man anser att en instruktion inkräktar på GDPR eller andra av Unionens eller medlemsstaternas dataskyddsbestämmelser. (Artikel 28(3))

3. I fall där Microsoft anlitar ett annat personuppgiftsbiträde för utförande av specifik behandling för Kundens räkning ska det andra personuppgiftsbiträdet, genom ett avtal eller en annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i dessa GDPR-villkor, och framförallt att ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven enligt GDPR. Om det andra personuppgiftsbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska Microsoft vara fullt ansvariga gentemot Kunden för utförandet av det andra personuppgiftsbiträdets skyldigheter. (Artikel 28(4))

4. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål, samt riskerna av varierande sannolikhetsgrad och allvar för fysiska personers rättigheter och friheter, ska Kunden och Microsoft genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken och, när det är lämpligt, inbegripet

[Innehållsförteckning](#)[Inledning](#)[Allmänna villkor](#)[Dataskyddsvillkor](#)[Bilaga](#)

- (a) pseudonymisering och kryptering av Personuppgifter
- (b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna
- (c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident
- (d) ett förfarande för att regelbundet testa, bedöma och utvärdera tekniska och organisatoriska åtgärders effektivitet för att säkerställa behandlingens säkerhet. (Artikel 32(1))

5. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt utlämnande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. (Artikel 32(2))

6. Kunden och Microsoft ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under Kundens eller Microsofts överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från Kunden, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det. (Artikel 32(4))

7. Microsoft ska utan oskäligt dröjsmål meddela Kunden efter att ha fått kännedom om en personuppgiftsincident. (Artikel 33(2)). Sådant meddelande ska innefatta den information som ett personuppgiftsbiträde måste tillhandahålla en personuppgiftsansvarig enligt Artikel 33(3), i den mån sådan information är skäligen tillgänglig för Microsoft.

[Innehållsförteckning/Allmänna villkor](#)

[Innehållsförteckning](#)



[Inledning](#)



[Allmänna villkor](#)



[Dataskyddsvillkor](#)



[Bilaga](#)