Volym-
licensiering

Dataskyddstillägg för Microsofts produkter och tjänster

Senast uppdaterat 2 januari 2024

Microsoft

Innehållsförteckning

Inledning

Parterna avtalar att detta Dataskyddstillägg för Microsofts produkter och tjänster (DPA) anger deras skyldigheter beträffande behandling av och säkerhet för kunddata, data i Professionella tjänster och personuppgifter i samband med produkterna och tjänsterna. DPA införlivas genom referens i produktvillkoren och andra Microsoft-avtal. 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 DPA-villkoren och andra villkor i Kundens volymlicensieringsavtal eller andra tillämpliga avtal i anknytning till produkterna och tjänsterna (Kundens avtal) ska DPA-villkoren gälla. Bestämmelserna i DPA-villkoren ersätter eventuella motstridiga bestämmelser i Microsofts sekretesspolicy som annars skulle gälla för behandling av Kunddata, Data i professionella tjänster eller Personuppgifter enligt vad som anges häri.

Microsoft gör åtagandena i detta DPA gentemot alla kunder med ett befintligt kundavtal (Kundens avtal). Dessa åtaganden är bindande för Microsoft gentemot Kunden, oavsett (1) vilka Produktvillkor som i övrigt är tillämpliga på en viss produktprenumeration eller -licens, (2) eventuellt annat avtal som refererar till Produktvillkoren.

Tillämpliga DPA-villkor och uppdateringar

Uppdateringsbegränsningar

När Kunden förnyar eller köper en ny prenumeration på en produkt eller inleder en arbetsorder för en professionell tjänst ska då aktuella DPA-villkor gälla, och ska inte ändras under Kundens prenumeration på den produkten eller avtalstid för den professionella tjänsten. När Kunden anskaffar en evig licens för programvara ska då aktuella DPA-villkor gälla (enligt samma villkor för fastställande av tillämpliga då aktuella Produktvillkor för programvaran i Kundens avtal), och ska inte ändras under Kundens licenstid för den programvaran.

Nya funktioner, tillägg eller tillhörande programvara

Oaktat de förutnämnda uppdateringsbegränsningarna gäller att när Microsoft introducerar nya funktioner, erbjudanden, tillägg eller relaterad programvara (dvs. som inte tidigare har ingått i produkterna eller tjänsterna) får Microsoft föreskriva villkor eller göra uppdateringar av DPA som är tillämpliga på Kundens användning av dessa nya funktioner, erbjudanden, tillägg eller tillhörande programvara. Om dessa villkor innefattar några väsentliga negativa ändringar av DPA-villkoren ska Microsoft ge Kunden valet att använda de nya funktionerna, erbjudandena, tilläggen eller relaterad programvara utan förlust av befintlig funktionalitet i en allmänt tillgänglig produkt eller professionell tjänst. Om Kunden inte installerar eller använder de nya funktionerna, erbjudandena, tilläggen eller relaterad programvara ska motsvarande nya villkor inte gälla.

Myndighetsförordningar och krav

Oaktat uppdateringsbegränsningarna ovan kan Microsoft ändra eller avsluta en produkt eller professionell tjänst i ett land eller en jurisdiktion där nuvarande eller framtida myndighetskrav eller skyldigheter som (1) omfattas av bestämmelser eller krav som inte är allmänt tillämpliga på företag som är verksamma där (2) innebär svårigheter för Microsoft att fortsätta driva produkten eller erbjuda den professionella tjänsten utan att ändra dem (3) får Microsoft att anse att DPA-villkoren eller produkten eller den professionella tjänsten kan stå i konflikt med sådana krav eller skyldigheter.

Elektroniska meddelanden

Microsoft får tillhandahålla Kunden information och meddelanden om produkter och tjänster elektroniskt, inklusive via e-post, genom portalen för en Onlinetjänst eller via en webbsida som Microsoft anger. Meddelande är lämnat det datum detta görs tillgängligt av Microsoft.

Tidigare versioner

DPA-villkoren innehåller villkor för produkter och tjänster som är tillgängliga vid tillfället. För tidigare versioner av DPA-villkoren kan Kunden se https://aka.ms/licensingdocs eller kontakta återförsäljaren eller Microsofts kundansvariga.

Innehållsförteckning/Allmänna villkor

Innehållsförteckning → Introduktion → Allmänna villkor → Dataskyddsvillkor → Bilagor

Definitioner

Termer med versal som används men inte definieras i detta DPA ska ha de betydelser som anges i Kundens avtal. 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 ”Dataskyddskrav” avses den allmänna dataskyddsförordningen GDPR, lokala dataskyddslagar i EU/EES samt andra tillämpliga lagar 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 ”DPA-villkor” avser villkoren i DPA och eventuella produktspecifika villkor i produktvillkoren som specifikt utgör tillägg till eller ändring av sekretess- och säkerhetsvillkoren i DPA för en viss produkt (eller funktion i en produkt). I händelse av konflikt eller bristande överensstämmelse mellan DPA och sådana produktspecifika villkor ska de produktspecifika villkoren gälla för den tillämpliga produkten (eller funktion i den produkten).

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 1, 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 ”Produkt” avses den betydelse som anges i volymlicensieringsavtalet. För underlättande av referens innefattar ”produkt” Onlinetjänster och programvara så som dessa definieras i volymlicensieringsavtalet.

”Produkter och tjänster” avser produkter och Professionella tjänster. Produkters och Professionella tjänsters tillgänglighet kan variera efter region, och tillämpligheten av detta DPA på specifika produkter och Professionella tjänster är underkastad begränsningarna i avsnittet Omfattning i detta DPA.

Med ”professionella tjänster” avses följande tjänster: (a) Microsofts konsulttjänster, bestående av planering, rådgivning, vägledning, datamigrering, distributions- och lösnings-/programutvecklingstjänster som tillhandahålls enligt en Microsoft Enterprise Services-arbetsorder eller, om detta medges i Projektbeskrivningen, enligt ett Cloud Workload Acceleration-avtal som införlivar detta DPA genom referens, (b) tekniska supporttjänster från Microsoft som hjälper kunder att identifiera och lösa problem som påverkar Produkter, däribland teknisk support som tillhandahålls som en del av Microsoft Unified Support- eller Premier Support-tjänster, samt andra eventuella kommersiella tekniska supporttjänster. Professionella tjänster innefattar inte Produkterna eller, endast vad beträffar DPA, professionella tilläggstjänster.

rMed ”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 Produkt) eller som i övrigt inhämtas eller bearbetas av eller åt Microsoft genom ett avtal med Microsoft för att erhålla Professionella tjänster.

Med ”2021 års standardavtalsklausuler” avses standardmässiga dataskyddsklausuler (processor till processor-modul) Microsoft Ireland Operations Limited och Microsoft Corporation för överföring av personuppgifter från personuppgiftsbiträden inom EES 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 2021/914/EG av den 4 juni 2021.

Med ”Underordnat personuppgiftsbiträde” avses andra personuppgiftsbiträden som används av Microsoft för att behandla kunddata, data från Professionella tjänster samt personuppgifter enligt beskrivningen i artikel 28 i GDPR.

Med ”Professionella tilläggstjänster” avses begäran om support som eskaleras till ett produktteknikerteam för lösning och annan konsultation och support från Microsoft som tillhandahålls i anknytning till produkter eller ett volymlicensieringsavtal som inte omfattas av definitionen av Professionella tjänster.

Termer med inledande gemen 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.

Allmänna villkor

Efterlevnad av lagar

Microsoft ska efterleva alla tillämpliga lagar och andra föreskrifter som är tillämpliga på deras tillhandahållande av produkterna och tjänsterna, inbegripet lagar om meddelande om säkerhetsincident och dataskyddskrav. Microsoft är dock inte skyldiga att efterleva lagar och andra föreskrifter som är tillämpliga på Kunden eller dennas bransch som inte också är allmänt tillämpliga på IT-tjänstleverantörer. Microsoft avgör inte huruvida Kundens data innefattar information som är underkastad någon särskild lag eller föreskrift. Alla säkerhetsincidenter regleras av nedanstående villkor för Meddelande om säkerhetsincidenter.

Kunden måste efterleva alla lagar och andra föreskrifter som gäller för dennas användning av produkter och tjänster, inbegripet lagar som rör biometriska data, konfidentialitet för kommunikation och dataskyddskrav. Kunden ansvarar för att avgöra om Produkter och Tjänster är lämpliga för lagring och behandling av information underkastat särskilda lagar eller förordningar, och för att använda Produkter och Tjänster på ett sätt som överensstämmer med Kundens skyldigheter enligt lagar och förordningar. Kunden är ansvarig för att svara på alla begäranden från tredje man angående Kundens användning av Produkter och Tjänster, som t ex en begäran om att ta ner 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
- Telekommunikationsdata
- California Consumer Privacy Act (CCPA)
- Biometriska data
- Professionella tilläggstjänster
- Så här kontaktar du Microsoft
- Bilaga A – Säkerhetsåtgärder
- Bilaga B – Registrerade och kategorier av personuppgifter
- Bilaga C – Bilaga om ytterligare säkerhetsåtgärder.

Omfattning

DPA-villkoren är tillämpliga på alla produkter och tjänster med undantag för vad som beskrivs i detta avsnitt.

DPA-villkoren är inte tillämpliga på produkter eller professionella tjänster som anges specifikt som undantagna, eller i den utsträckning de identifieras som undantagna, i produktvillkoren eller en tillämplig arbetsorder som regleras av villkoren för integritet och säkerhet i de tillämpliga produktspecifika villkoren eller villkoren i arbetsordern.

För tydlighets skull: DPA-villkoren är endast tillämpliga på behandling av data i miljöer som Microsoft och dess underordnade personuppgiftsbiträden råder över. Detta innefattar data som skickas till Microsoft av produkter och tjänster, men innefattar inte data som förblir i Kundens lokaler eller i driftmiljöer tillhörande tredje man som Kunden valt.

För professionella tilläggstjänster förbinder sig Microsoft endast till åtagandena i avsnittet Professionella tilläggstjänster nedan.

För förhandsversioner kan mindre omfattande eller andra integritets- och säkerhetsåtgärder gälla än de som normalt förekommer i produkter och tjänster. 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. För produkter är följande villkor i detta DPA inte tillämpliga på förhandsversioner: Behandling av personuppgifter: GDPR, Datasäkerhet och HIPAA Business Associate. För Professionella tjänster uppfyller erbjudanden med benämningen Förhandsversioner eller Begränsad utgåva endast villkoren för professionella tilläggstjänster.

Typ av databehandling, ägarskap

Microsoft ska endast använda och i övrigt behandla Kunddata, data i Professionella tjänster och Personuppgifter så som beskrivs och enligt nedanstående begränsningar (a) för att tillhandahålla Kunden Produkterna och Tjänsterna enligt Kundens dokumenterade instruktioner och (b) för verksamhetsutövning i samband med att Kunden tillhandahålls Produkterna och Tjänsterna. Parterna emellan behåller Kunden alla rättigheter, äganderätt och intresse i och till kunddata och data i Professionella tjänster. Microsoft förvärvar inga rättigheter till kunddata eller data i Professionella tjänster annat än de rättigheter Kunden beviljar Microsoft i detta avsnitt. Detta stycke påverkar inte Microsofts rättigheter gällande programvara eller tjänster som Microsoft licensierar till Kunden.

Behandling för att tillhandahålla Kunden produkterna och tjänsterna

I detta DPA inbegriper ”att tillhandahålla” en produkt 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).
- Hålla Produkter uppdaterade och välfungerande, och förbättra användarproduktivitet, tillförlitlighet, effektivitet, kvalitet och säkerhet.

I detta DPA inbegriper ”att tillhandahålla” Professionella tjänster följande:

- Leverans av Professionella tjänster, inklusive tillhandahållande av teknisk support, professionell planering, rådgivning, vägledning, datamigrering, distribution och lösnings-/programvaruutveckling.
- Felsökning (förebyggande, detektering, utredning, avhjälpande och åtgärdande av problem, inklusive Säkerhetsincidenter och problem som identifieras i Professionella tjänster eller relevanta Produkter under leveransen av Professionella tjänster).
- Förbättring av leverans, effektivitet, kvalitet och säkerhet för Professionella tjänster och underliggande Produkter baserat på problem som identifieras under tillhandahållandet av Professionella tjänster, däribland åtgärda defekter i programvara och i övrigt hålla Produkter och Tjänster uppdaterade och välfungerande.

I samtliga fall tillhandahålls Produkterna och Tjänsterna med hänsyn till säkerhetsskyldigheter enligt Dataskyddskrav.

I tillhandahållandet av Produkter och Tjänster ska Microsoft inte använda eller på annat sätt behandla Kunddata, data i Professionella tjänster 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 verksamhetsutövning för att tillhandahålla Produkterna och Tjänsterna till Kunden

I detta DPA avser ”verksamhetsutövning” behandlingen av uppgifter som godkänns av Kunden i detta avsnitt.

Kunden ger Microsoft tillåtelse

(i.) att skapa sammanställda, icke-personliga uppgifter från data som innehåller pseudonymiserade identifierare (såsom användningsloggar som innehåller unika, pseudonymiserade identifierare)
(ii.) att beräkna statistik som avser Kunddata eller data i Professionella tjänster

alltid utan att få åtkomst till eller analysera innehållet i Kunddata eller data i Professionella tjänster och begränsat till att uppnå de syften som anges nedan, och alltid för att tillhandahålla Kunden Produkterna och Tjänsterna.

Dessa syften är:

- fakturering och kontorhantering
- ersättning, till exempel beräkning av personalens provision eller partnerincitament
- intern rapportering och företagsmodellering, till exempel prognostisering, intäkter, kapacitetsplanering, produktstrategi
- ekonomisk rapportering.

Vid behandling för denna verksamhetsutövning ska Microsoft tillämpa principer om dataminimering och inte använda eller på annat sätt behandla Kunddata, data i Professionella tjänster eller Personuppgifter för följande: (a) användarprofilering, (b) marknadsföring eller liknande kommersiella syften eller (c) något annat syfte än de syften som anges i detta avsnitt. Därutöver, som med all behandling enligt detta DPA, styrs behandlingen för verksamhetsutövning alltjämt av Microsofts sekretesskyldigheter och åtaganden enligt Utlämnande av behandlade data.

Utlämnande av behandlade data

Microsoft lämnar inte ut eller ger åtkomst till 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) Data i professionella tjänster, (c) Personuppgifter, (d) andra data som Microsoft behandlar i samband med de produkter och tjänster som är Kundens konfidentiella information enligt Kundens avtal. All behandling av Behandlade data omfattas av Microsofts sekretesskyldighet enligt Kundens avtal.

Microsoft ska inte lämna ut eller ge åtkomst till 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 eller ge åtkomst till Behandlade data till rättsvårdande myndighet ska Microsoft omgående meddela Kunden och tillhandahålla en kopia av begäran, såvida inte Microsoft är förhindrande 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 lämnar endast ut eller ger åtkomst till Behandlade data när detta krävs enligt lag under förutsättningen att lagar och praxis respekterar andemeningen i de grundläggande rättigheterna och friheterna och inte överskrider vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle och, som tillämpligt, för att skydda ett av målen som listas i artikel 23(1) i GDPR.

Microsoft ska inte tillhandahålla tredje man något av följande: (a) Direkt, indirekt, allmän eller fri tillgång till behandlade data. (b) Plattformskrypteringsnycklar 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 tillhandahållandet av produkterna och tjänsterna inhämtas som en del av (a) kunddata, (b) data i Professionella tjänster eller (c) data genererade, härledda eller insamlade av Microsoft, däribland data som skickas till Microsoft i samband med en kunds användning av tjänstbaserade funktioner eller inhämtade av Microsoft från lokalt installerad programvara. Personuppgifter som tillhandahålls Microsoft av Kunden eller för Kundens räkning genom dennas användning av Onlinetjänsterna är också kunddata. Personuppgifter som tillhandahålls Microsoft av Kunden eller för Kundens räkning genom användning av Professionella tjänster är också data i Professionella tjänster. Pseudonymiserade identifierare kan ingå i data som behandlas av Microsoft i sambandet med tillhandahållandet av produkterna, och de 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 är GDPR-villkoren i Bilaga 1 reglerande, och språket i underavsnittet (Behandling av Personuppgifter, GDPR) ska betraktas som kompletterande:

Roller och ansvar för personuppgiftsbiträden och personuppgiftsansvariga

Kunden och Microsoft överenskommer att Kunden är personuppgiftsansvarig och Microsoft är personuppgiftsbiträde för sådana uppgifter, utom i följande fall: (a) När Kunden agerar personuppgiftsbiträde, i vilket fall Microsoft är underordnat personuppgiftsbiträde, (b) När annat anges i de produktspecifika villkoren 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 Kundens avtal (inbegripet DPA-villkoren och eventuella tillämpliga uppdateringar) tillsammans med produktdokumentationen och Kundens användning och konfigurering av funktioner i produkterna är Kundens fullständiga dokumenterade instruktioner till Microsoft för behandling av Personuppgifter, eller Dokumentation i professionella tjänster och Kundens användning av de professionella tjänsterna. Information om användning och konfiguration av Produkterna finns på https://docs.microsoft.com (eller på en efterträdande plats) eller i annat avtal som införlivar detta DPA. Eventuella ytterligare eller alternativa instruktioner måste godkännas i enlighet med processen för ändring av Kundens avtal. 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 för verksamhetsutövning i samband med att Kunden tillhandahålls produkterna och tjänsterna ska Microsoft ha samma skyldigheter som en oberoende personuppgiftsansvarig enligt GDPR för sådan användning. Microsoft accepterar det extra ansvaret som ”personuppgiftsansvarig” enligt GDPR för sådan behandling för att (a) agera enligt lagkrav i den omfattning som krävs enligt GDPR och (b) ge Kunden ökad insyn och bekräfta Microsofts ansvar för sådan behandling. Microsoft vidtar säkerhetsåtgärder för att skydda Kunddata, data i Professionella tjänster och Personuppgifter vid sådan behandling, inbegripet de som anges i detta DPA och de som avses i Artikel 6(4) i GDPR. Vad gäller behandling av Personuppgifter enligt detta stycke gör Microsoft de åtaganden som anges i avsnittet Ytterligare säkerhetsåtgärder för dessa syften (i) Microsofts utlämnande av Personuppgifter, enligt beskrivningen i avsnittet Ytterligare säkerhetsåtgärder, som har överförts i samband med verksamhetsutövning betraktas som relevant utlämnande och (ii) åtaganden i avsnittet Ytterligare säkerhetsåtgärder är tillämpliga på sådana Personuppgifter.

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 produkterna och tjänsterna enligt Kundens avtal och för verksamhetsutövning som följer med att tillhandahålla Kunden produkterna och tjänsterna (vilket beskrivs utförligare i avsnittet ”Typ av behandling, ägarskap” ovan i detta DPA).
- **Datakategorier.** De typer av personuppgifter som behandlas av Microsoft när produkterna och tjänsterna tillhandahålls innefattar: (i) Personuppgifter som Kunden frivilligt anger i kunddata och data i Professionella tjänster, (ii) de som uttryckligen anges i Artikel 4 i GDPR som kan genereras, härledas eller samlas in av Microsoft, däribland data som skickas till Microsoft i samband med en kunds användning av tjänstbaserade funktioner eller inhämtade av Microsoft från lokalt installerad programvara. Typer av personuppgifter som Kunden väljer att

inkludera i kunddata och 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 Bilaga B.

- **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 Bilaga B.

Registrerades rättigheter: assistans med begäran

Microsoft ska på ett sätt som är förenligt med produkters och tjänsters 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 de produkter och tjänster 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 produkters och tjänsters 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 säkerhetspolicyer

Microsoft ska implementera och upprätthålla lämpliga tekniska och organisatoriska åtgärder avsedda att skydda kunddata, data i Professionella tjänster 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 annan information som Kunden skäligen begär angående Microsofts säkerhetsrutiner och säkerhetspolicyer.

Dessa åtgärder ska därutöver uppfylla de krav som anges i ISO 27001, ISO 27002 och ISO 27018. Kunder har tillgång till en beskrivning av säkerhetskontrollerna för dessa krav.

Varje central Onlinetjänst uppfyller också de kontrollstandarder och ramverk som visas i tabellen i produktvillkoren. Alla centrala Onlinetjänster och Professionella tjänster inför och upprätthåller också de säkerhetsåtgärder som anges i Bilaga A för skydd av kunddata och data i Professionella tjänster.

Microsoft inför och upprätthåller också de säkerhetsåtgärder som anges i Tillägg II i 2021 års standardavtalsklausuler för skydd av Personuppgifter inom ramen för GDPR.

Microsoft får när som helst lägga till bransch- eller myndighetsstandarder. Microsoft ska inte utesluta ISO 27001, ISO 27002, ISO 27018 eller någon standard eller ramverk i tabellen för centrala Onlinetjänster i produktvillkoren såvida de inte längre används inom branschen och har ersatts av nya (om tillämpligt).

Datakryptering

Kunddata och data i Professionella tjänster (vardera inklusive eventuella personuppgifter) som skickas via offentliga nätverk mellan Kund och Microsoft eller mellan Microsofts datacenter krypteras som standard.

Microsoft krypterar också kunddata som lagras vilande i Onlinetjänster och data i Professionella tjänster. I händelse av att Onlinetjänster på vilka Kunden eller en tredje man agerat å Kundens vägnar kan skapa applikationer (t.ex. vissa Azure-tjänster), kan kryptering av data lagrade i sådana applikationer distribueras efter Kundens eget godtycke, med hjälp av funktioner som antingen tillhandahålls av Microsoft eller som erhålls av Kunden från tredje man.

Dataåtkomst

Microsoft använder åtkomstmekanismer med lägsta behörighet för att kontrollera åtkomst till kunddata och data i Professionella tjänster (inklusive eventuella personuppgifter). Rollbaserad åtkomstkontroll används för att säkerställa att åtkomst till kunddata och data i Professionella tjänster som är nödvändiga för serviceåtgärder är för ett lämpligt ändamål och godkänd med överordnads överinseende. För centrala Onlinetjänster och Professionella tjänster upprätthåller Microsoft mekanismer för åtkomstkontroll som beskrivs i tabellen ”Säkerhetsåtgärder” i Bilaga A. Det finns ingen stående åtkomst för Microsofts personal till Kunddata, och nödvändig åtkomst är tidsbegränsad.

Kundens ansvar

Kunden är ensam ansvarig för att självständigt fastställa huruvida tekniska och organisatoriska åtgärder för Produkter och Tjänster uppfyller Kundens krav, inklusive 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 säkerhetspolicyer 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).

Granskning av efterlevnad

Microsoft ska utföra granskningar av säkerheten för datorerna, datormiljön och de fysiska datacenter som används för att behandla kunddata, data i Professionella tjänster och personuppgifter enligt följande:

- Om en standard eller ett ramverk föreskriver granskningar ska en granskning av kontrollstandarden 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 Dataskyddskraven 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, data i Professionella tjänster 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 tillhandahållandet av produkter och tjänster. 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.

Inget i detta avsnitt av denna DPA ändrar GDPR-villkoren eller påverkar rättigheterna för en tillsynsmyndighet eller registrerad enligt Dataskyddskraven. Microsoft Corporation är en avsedd tredjemansförmånstagare i detta avsnitt.

rMeddelande 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, data i Professionella tjänster 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 Kunden på ett sätt som Microsoft väljer, inklusive via e-post. Kunden är ensam ansvarig för att se till att upprätthålla korrekta kontaktuppgifter med Microsoft för varje tillämplig produkt och professionell tjänst. 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 eventuellt missbruk av dennas konton eller autentiseringsuppgifter och varje form av säkerhetsincident gällande produkter och tjänster.

Dataöverföringar och plats

Dataöverföringar

Kunddata, data i Professionella tjänster och personuppgifter som Microsoft behandlar å Kundens vägnar får inte överföras till, eller lagras och behandlas på en geografisk plats förutom enligt DPA-villkoren och de säkerhetsåtgärder som tillhandahålls nedan i detta avsnitt. Med beaktande av sådana säkerhetsåtgärder ger Kunden Microsoft i uppdrag att överföra kunddata, data i Professionella tjänster och personuppgifter till USA eller något annat land där Microsoft eller dess underordnade personuppgiftsbiträden är verksamma, samt att lagra och behandla kunddata och personuppgifter för att tillhandahålla produkterna med undantag för vad som beskrivs på andra ställen i DPA-villkoren.

All överföring av kunddata, data i professionella tjänster och personuppgifter från EU, EES, Storbritannien och Schweiz som görs för att tillhandahålla produkterna och tjänsterna lyder under villkoren från 2021 års standardavtalsklausuler implementerade av Microsoft. Överföringar från Storbritannien lyder också under det IDTA som har implementerats av Microsoft. I detta DPA avser ”IDTA” tillägget om Internationell dataöverföring i Europeiska Kommissionens standardavtalsklausuler för internationella dataöverföringar som har utfärdats av Information Commissioner’s Office i Storbritannien enligt S119A(1) i UK Data Protection Act 2018. Microsoft följer kraven i dataskyddslagstiftning för EES, Storbritannien och Schweiz avseende insamling, användning, överföring, lagring och annan behandling av Personuppgifter från EES, Storbritannien och Schweiz. Alla överföringar av personuppgifter till tredjeland 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.

Därutöver är Microsoft certifierat för EU:s–USA:s och Schweiz–USA:s dataskyddsramverk, tillägg för Storbritannien i EU:s-USA:s dataskyddsramverk och de åtaganden dessa innebär. Microsoft samtycker till att underrätta Kunden om de fastställer att de inte längre kan uppfylla sin skyldighet att tillhandahålla skydd på samma nivå som krävs enligt dataskyddsramverkens principer.

Plats för Kunddata

Vid centrala onlinetjänster kommer Microsoft att lagra vilande kunddata inom vissa större geografiska områden (vardera ett geo-område) i enlighet med produktvillkoren.

Vid onlinetjänster som omfattas av EU-datagräns kommer Microsoft att lagra och behandla kunddata och personuppgifter inom EU i enlighet med produktvillkoren.

Microsoft har inte kontroll över och begränsar inte regioner där kunden eller kundens slutanvändare har åtkomst till eller kan flytta kunddata.

Behållande och radering av data

Kunden har när som helst under sin prenumeration eller avtal om tillämplig professionell tjänst möjlighet att komma åt, extrahera och radera kunddata som har lagrats i vardera Onlinetjänst och data i Professionella tjänster.

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 som lagrats i Onlinetjänster inom ytterligare 90 dagar, såvida inte Microsoft enligt detta DPA har rätt att behålla sådana data.

För personuppgifter i samband med programvara och för data i Professionella tjänster ska Microsoft radera alla exemplar av dessa efter att affärssyftet som låg till grund för att dessa data samlades in eller överfördes har fullgjorts, eller tidigare på Kundens begäran, såvida inte Microsoft har rätt att behålla sådana data enligt detta DPA.

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

Personuppgiftsbiträdes konfidentialitetsåtagande

Microsoft ska säkerställa att dess personal som deltar i behandlingen av kunddata, data i Professionella tjänster 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, data i Professionella tjänster 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 underordnade personuppgiftsbiträden för att tillhandahålla vissa begränsade eller relaterade tjänster för sin räkning. Kunden samtycker till detta anlitande och till Microsofts koncernbolag som underordnade personuppgiftsbiträden. Ovanstående godkännanden utgör Kundens föregående skriftliga medgivande till att Microsoft lägger ut behandling av kunddata, data i Professionella tjänster och personuppgifter på underentreprenad, om sådant medgivande krävs enligt Standardavtalsklausulerna eller GDPR-villkoren.

Microsoft ansvarar för sina underordnade personuppgiftsbiträdens 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, data i Professionella tjänster eller personuppgifter endast för att leverera de tjänster Microsoft har anlitat dem för, och att de förbjuds att använda kunddata, data i Professionella tjänster eller personuppgifter i 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, inklusive begränsningarna om utlämnande av Behandlade data. Microsoft förbinder sig till att ha överinseende över underordnade personuppgiftsbiträden för att säkerställa att deras skyldigheter enligt avtal fullgörs.

Microsoft kan från tid till annan anlita nya underordnade Personuppgiftsbiträden. Microsoft ska meddela Kunden och, som tillämpligt, 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 och, som tillämpligt, uppdatera webbplatsen och förse Kunden med en metod för att ta emot meddelande om uppdateringen om ett eventuellt nytt underordnat Personuppgiftsbiträde minst 30 dagar innan det underordnade Personuppgiftsbiträdet ges åtkomst till data i Professionella tjänster eller Personuppgifter utöver sådana som finns i Kunddata. Om Microsoft anlitar ett nytt underordnat personuppgiftsbiträde för en ny produkt eller professionell tjänst som behandlar kunddata, data i Professionella tjänster eller personuppgifter ska Microsoft meddela Kunden innan den produkten eller professionella tjänsten blir tillgänglig.

Om Kunden inte godkänner ett nytt underordnat personuppgiftsbiträde för en Onlinetjänst eller Professionella tjänster har Kunden rätt att säga upp prenumeration på berörd Onlinetjänst eller tillämpliga beskrivningar av den professionella tjänsten i fråga utan straff- eller uppsägningsavgift genom att före utgången av aktuell period tillhandahålla ett skriftligt meddelande om uppsägning. Om Kunden inte godkänner ett nytt underordnat personuppgiftsbiträde för programvara, och Kunden inte rimligen kan undvika användning av det underordnade personuppgiftsbiträdet genom att begränsa Microsoft från att behandla data såsom anges i dokumentationen eller detta DPA, har Kunden rätt att säga upp licensen för berörd programvaruprodukt utan straffavgift genom att före utgången av aktuell period 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 produkten ingår i en svit (eller liknande enskilt köp av tjänster) är uppsägningen tillämplig på hela sviten. Efter uppsägningen ska Microsoft avlägsna betalningsskyldigheter avseende eventuella prenumerationer eller annat tillämpligt obetalt arbete för de uppsagda produkterna eller tjänsterna från Kundens eller dennas återförsäljares efterföljande fakturor.

Utbildningsinstitutioner

Om Kunden är en utbildningsorganisation eller institution som lyder under det amerikanska utbildningsdepartementets bestämmelser (FERPA) i 20 U.S.C. § 1232g, bekräftar Microsoft vad gäller denna DPA anbelangar att Microsoft betecknas som ”utbildningsrepresentant” med ”ett rättmätigt utbildningsintresse” i kunddata och data i Professionella tjänster, såsom dessa termer har definierats enligt FERPA och dess implementeringsbestämmelser, 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 produkterna och tjänsterna 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 och data i Professionella tjänster 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 Microsofts CJIS-tjänster som omfattas regleras av de allmänna villkoren i avtalet om CJIS-information, ”CJIS Information Agreement”.

HIPAA Business Associate

Om Kunden är en omfattad enhet eller en affärsförbindelse och omfattas av skyddad hälsoinformation i kunddata eller Data i professionella tjänster, så som dessa termer definieras i Health Insurance Portability and Accountability Act of 1996, med ändringar, och förordningar som utfärdats därunder (benämns gemensamt HIPAA), omfattar verkställandet av Kundens avtal verkställandet av HIPAA Business Associate-avtalet (BAA). Den fullständiga texten för BAA anger de Onlinetjänster eller professionella tjänster det avser och finns på http://aka.ms/BAA. Kunden kan välja bort BAA genom att skicka följande information till Microsoft i ett skriftligt meddelande (enligt villkoren för Kundens avtal):

- Kundens fullständiga namn som juridisk person och eventuella koncernbolag som väljer bort.
- Om Kunden har flera avtal gäller detta Kundens avtal som bortvalet avser.

Telekommunikationsdata

I den mån Microsoft behandlar trafik, innehåll och andra Personuppgifter i tillhandahållandet av Produkter och tjänster som är att betrakta som telekommunikationstjänster enligt tillämplig lag kan specifika lagstadgade skyldigheter föreligga. Microsoft ska efterleva alla telekommunikationsspecifika lagar och andra föreskrifter som är tillämpliga på deras tillhandahållande av Produkter och tjänster, inbegripet meddelande om säkerhetsöverträdelse, Dataskyddskrav och telekommunikationssekretess.

California Consumer Privacy Act (CCPA)

Om Microsoft behandlar personuppgifter inom CCPA:s omfattning gör Microsoft följande ytterligare utfästelser till Kunden: Microsoft ska behandla kunddata, data i Professionella tjänster och personuppgifter för Kundens räkning och inte behålla, använda eller lämna ut data i något annat syfte än de som anges i DPA-villkoren 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, produktvillkoren eller annat avtal dem mellan.

Biometriska data

Om Kunden använder produkter och tjänster för att behandla biometriska data ansvarar Kunden för följande: (i) Att underrätta registrerade personer, inklusive avseende lagringsperioder och förstöring, (ii) att erhålla samtycke från registrerade personer och (iii) att radera biometriska data, allt i den mån som krävs enligt tillämpliga dataskyddskrav. Microsoft ska behandla biometriska data enligt Kundens dokumenterade instruktioner (enligt beskrivningen i avsnittet ”Roller och ansvar för personuppgiftsbiträden och personuppgiftsansvarig” ovan) och skydda dessa biometriska data enligt datasäkerhets- och dataskyddsvillkoren i detta DPA. För ändamål som rör detta avsnitt ska ”biometriska data” ha den innebörd som anges i artikel 4 i GDPR och, i förekommande fall, motsvarande villkor i andra dataskyddskrav.

Professionella tilläggstjänster

När den används i de avsnitt som anges nedan inbegriper den definierade termen ”Professionella tjänster” professionella tilläggstjänster, och termen ”data i Professionella tjänster” inbegriper data som inhämtas för professionella tilläggstjänster.

För professionella tilläggstjänster gäller följande avsnitt i DPA på samma sätt som de gäller för Professionella tjänster: Inledning, Efterlevnad av lagar, Typ av behandling: ansvar, Utlämnande av behandlade data, Behandling av personuppgifter: GDPR, första stycket i Säkerhetsförfaranden och säkerhetspolicyer, Kundens ansvar, Meddelande om säkerhetsincident, Dataöverföring (inbegripet villkor avseende 2021 års standardavtalsklausuler), tredje stycket i Lagring och radering av data, Personuppgiftsbiträdets konfidentialitetsåtagande, Meddelande om och kontroll över användning av underordnade Personuppgiftsbiträden, HIPAA Business Associate (i tillämplig utsträckning i BAA), California Consumer Privacy Act (CCPA), Biometriska data, Så här kontaktar du Microsoft, Bilaga B – Registrerade och kategorier av Personuppgifter samt Bilaga C – Bilaga om ytterligare säkerhetsåtgärder.

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

Bilaga A – Säkerhetsåtgärder

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

Domän	Praxis
Organisation av informationssäkerhet	**Säkerhetsägarskap.** Microsoft har utsett en eller flera säkerhetsansvariga som ansvarar för att samordna och övervaka regler och förfaranden kring säkerhet. **Säkerhetsroller och ansvar.** Microsofts personal med åtkomst till kunddata eller data i Professionella tjänster är underkastade sekretesskyldigheter. **Program för riskhantering.** Microsoft gjorde en riskbedömning innan kunddata behandlades eller Onlinetjänsten startades, och innan data i Professionella tjänster behandlades eller Professionella tjänster startades. Microsoft behåller sina säkerhetsdokument i enlighet med sina krav på behållande när de inte längre gäller.
Tillgångshantering	**Förteckning över tillgångar.** Microsoft upprätthåller en förteckning över alla medier på vilka kunddata eller data i Professionella tjänster lagras. Åtkomst till förteckningen över sådana medier är begränsad till Microsofts personal som skriftligen getts behörighet till sådan åtkomst. **Hantering av tillgångar** - Microsoft klassificerar kunddata eller data i Professionella tjänster 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 data i Professionella tjänster och har förfaranden för kassering av utskrivet material som innehåller sådana data. - Microsofts personal måste få behörighet från Microsoft innan de får lagra kunddata eller data i Professionella tjänster på bärbara enheter, bereda sig fjärråtkomst till sådana data eller behandla sådana data utanför Microsofts anläggningar.
HR-säkerhet	**Säkerhetsutbildning.** Microsoft informerar sin personal om relevanta säkerhetsförfaranden och personalens respektive roller. Microsoft informerar även personalen om möjliga konsekvenser av överträdelser mot säkerhetsregler och förfaranden. Microsoft använder endast anonyma data i utbildningen.
Fysisk säkerhet och miljösäkerhet	**Fysisk åtkomst till anläggningar.** Microsoft begränsar tillträdet till lokaler med informationssystem som behandlar kunddata eller data i Professionella tjänster till identifierade behöriga personer. **Fysisk åtkomst till komponenter.** Microsoft för register över inkommande och utgående medier som innehåller kunddata eller data i Professionella tjänster, inklusive typ av medier, behörig avsändare/mottagare, datum och tid, antalet medier och typer av data i Professionella tjänster dessa innehåller. **Skydd mot störningar.** Microsoft använder en mängd olika branschstandardsystem för att skydda mot förlust av data på grund av elavbrott eller kommunikationsstörningar. **Kassering av komponenter.** Microsoft använder branschstandardprocesser för att radera kunddata och data i Professionella tjänster när de inte längre behövs.
Kommunikations- och verksamhetshantering	**Verksamhetspolicy.** Microsoft upprätthåller säkerhetsdokument som beskriver säkerhetsåtgärder och relevanta förfaranden samt ansvarsområden för personalen som har åtkomst till kunddata eller data i Professionella tjänster. **Dataåterställningsförfaranden** - Microsoft gör flera kopior av kunddata och data i Professionella tjänster regelbundet och aldrig mer sällan än en gång i veckan (förutom då inga uppdateringar har gjorts under den perioden), från vilka sådana data kan återställas. - Microsoft lagrar kopior av kunddata och data i Professionella tjänster och dataåterställningsrutinerna på ett annat ställe än där den primära datorutrustningen som behandlar kunddata och data i Professionella tjänster finns. - Microsoft har specifika rutiner som reglerar vem som har åtkomst till kopior av kunddata eller data i Professionella tjänster. - Microsoft granskar förfaranden för dataåterställning minst en gång var sjätte månad, utom förfaranden för dataåterställning för Professionella tjänster och Azure-myndighetstjänster, som granskas en gång om året.

Domän	Praxis
	- 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. **Skadlig programvara.** Microsoft har kontroller med skydd mot skadlig programvara som bidrar till att undvika att skadlig programvara får obehörig åtkomst till kunddata och data i Professionella tjänster, inklusive skadlig programvara som kommer från offentliga nätverk. **Data utanför Microsofts gränser** - Microsoft krypterar, eller gör det möjligt för Kunden att kryptera, kunddata och data i Professionella tjänster som skickas via offentliga nätverk. - Microsoft begränsar åtkomst till kunddata och data i Professionella tjänster i medier som lämnar Microsofts anläggningar. **Händelseloggning.** Microsoft loggar, eller gör det möjligt för Kunden att logga, åtkomst till och användning av informationssystem som innehåller kunddata och data i Professionella tjänster och registrerar åtkomst-ID, tid, beviljad eller avvisad behörighet och relevant aktivitet.
Åtkomstkontroll	**Åtkomstpolicy.** Microsoft för register över säkerhetsrättigheter för personer som har åtkomst till kunddata och data i Professionella tjänster. **Beviljande av åtkomst** - Microsoft för och uppdaterar ett register över personal som är behöriga att få åtkomst till Microsofts system som innehåller kunddata och data i Professionella tjänster. - 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 och data i Professionella tjänster har dessa personer separata ID-nummer/inloggningar. **Minsta behörighet** - Teknisk supportpersonal får endast bereda sig åtkomst till kunddata och data i Professionella tjänster vid behov. - Microsoft begränsar åtkomst till kunddata och data i Professionella tjänster till endast de personer som behöver sådan åtkomst för att kunna utföra sina arbetsuppgifter. **Integritet och sekretess** - 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. **Autentisering** - 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. **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 och data i Professionella tjänster som de inte har behörighet till.

Domän	Praxis
Incidenthantering avseende informationssäkerhet	**Process för incidentrespons** - 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 och data i Professionella tjänster, inklusive vilka data som har lämnats ut, till vem och vid vilken tidpunkt. **Tjänstövervakning.** Microsofts säkerhetspersonal verifierar loggar minst var sjätte månad för att ge förslag på åtgärder för avhjälpande vid behov.
Hantering av affärskontinuitet	- Microsoft upprätthåller kris- och beredskapsplaner för anläggningar där Microsofts informationssystem som behandlar kunddata och data i Professionella tjänster finns. - Microsofts redundanslagring och dess rutiner för dataåterställning är utformade för att försöka rekonstruera kunddata och data i Professionella tjänster i sitt ursprungliga skick eller senast kopierade skick från tiden innan de gick förlorade eller förstördes.

Innehållsförteckning/Allmänna villkor

Bilaga B – Registrerade och kategorier av personuppgifter

Registrerade: Registrerade omfattar Kundens 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 Microsoft. Microsoft bekräftar att Kunden beroende på Kundens användning av produkter och tjänster kan välja att i personuppgifterna inkludera personuppgifter avseende någon av följande typer av registrerade:

- Kundens anställda, uppdragstagare och tillfälliga personal (tidigare nuvarande, kommande).
- Ovanståendes underordnade.
- Kundens 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 Kundens tjänster.
- Partner, intressenter eller enskilda som aktivt samarbetar, kommunicerar eller i övrigt interagerar med Kundens anställda och/eller använder kommunikationsverktyg såsom appar och webbplatser som tillhandahålls av Kunden.
- Intressenter eller enskilda som passivt interagerar med Kunden (till exempel för att de är föremål för utredning, forskning eller omnämns i dokument eller korrespondens från eller till Kunden).
- Underåriga
- Yrkesgrupper med yrkesrelaterade befogenheter (t.ex. läkare, jurister, notarier, trossamfund osv.).

Datakategorier: Personuppgifterna som ingår i e-post, dokument och andra data i elektronisk form i samband med produkterna och tjänsterna. Microsoft bekräftar att Kunden beroende på Kundens användning av produkterna och tjänsterna kan välja att i personuppgifterna 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, körkortsnummer 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 försäkran, betalningsbeteende, kreditvärdighet).
- Kommersiell information (t.ex. inköpshistorik, 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).
- Profilering (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, fackföreningsmedlemskap, 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.

Bilaga C – Bilaga om ytterligare säkerhetsåtgärder

Genom detta tillägg till DPA om ytterligare säkerhetsåtgärder (detta tillägg) tillhandahåller Microsoft Kunden ytterligare säkerhetsåtgärder för Microsofts behandling av personuppgifter för Kundens räkning, inom ramen för GDPR, och ytterligare avhjälpande för registrerade som dessa personuppgifter avser.

Detta tillägg kompletterar och införlivas i, men avses inte som avvikelse från eller ändring av, DPA.

1. **Bestridande av order** I händelse av att Microsoft får en order från tredje man om tvingat utlämnande av personuppgifter som behandlas enligt detta DPA ska Microsoft:

   a. göra alla rimliga ansträngningar för att hänvisa tredje man direkt till Kunden med sin begäran om data.

   b. omgående meddela Kunden, såvida det inte är förbjudet enligt lag som är tillämplig på begärande tredje man, och, om det är förbjudet att meddela Kunden, använda alla lagliga medel för att erhålla rätten att undanröja förbudet för att kunna lämna så mycket information som möjligt till Kunden så snart som möjligt

   c. använda alla lagliga medel för att bestrida ordern om utlämnande baserat på rättsliga brister enligt den begärande partens lagar eller eventuella relevanta lagkonflikter med tillämplig lag i EU eller tillämplig medlemsstat.

Om efter att ha vidtagit stegen a. till c. ovan, Microsoft eller något av deras koncernbolag fortfarande tvingas lämna ut personuppgifter ska Microsoft endast lämna ut den minsta mängd av dessa data som är nödvändig för att uppfylla ordern om tvingat utlämnande.

För vad som avses i detta stycke inbegriper lagliga medel inte åtgärder som skulle leda till civil- eller straffrättsliga följder, såsom domstolstrots, enligt den relevanta jurisdiktionens lagar.

2. **Skadeersättning till registrerade** Underkastat stycke 3 och 4 ska Microsoft ersätta en registrerad för eventuell materiell eller ideell skada som drabbar denna till följd av Microsofts utlämnande av den registrerades personuppgifter som har överförts enligt standardavtalsklausulerna som svar på en order från rättsvårdande eller annan myndighet i ett land utanför EU/EES i strid mot Microsofts skyldigheter enligt Kapitel V i GDPR (ett relevant utlämnande). Utan hinder av det förestående har Microsoft ingen skyldighet att ersätta den registrerade enligt detta stycke 2 i den mån den registrerade redan har kompenserats för samma skada, av Microsoft eller på annat sätt.

3. Villkor för skadeersättning Skadeersättning enligt stycke 2 förutsätter att den registrerade, till Microsofts rimliga tillfredsställelse, kan påvisa att

   a. Microsoft har gjort ett relevant utlämnande

   b. det relevanta utlämnandet utgjorde grunden för en rättslig process mot den registrerade inledd av rättsvårdande eller annan myndighet i ett land utanför EU/EES

   c. det relevanta utlämnandet har direkt orsakat den registrerade materiell eller ideell skada.

Den registrerade bär bevisbördan avseende omständigheterna i a till och med c.

Utan hinder av det förestående har Microsoft ingen skyldighet att ersätta den registrerade enligt detta stycke 2 om Microsoft påvisar att det relevanta utlämnandet inte kränkte deras skyldigheter enligt Kapitel V i GDPR.

4. **Skadornas omfattning** Skadeersättning enligt stycke 2 begränsas till materiella och ideella skador enligt vad som anges i GDPR och omfattar inte följdskador eller andra skador som inte härrör från Microsofts överträdelse av GDPR.

5. **Utövande av rättigheter** Rättigheter som beviljas registrerade enligt detta tillägg kan av den registrerade hävdas gentemot Microsoft oberoende av eventuell begränsning i klausul 3 eller 6 i standardavtalsklausulerna. Den registrerade får endast väcka enskild talan enligt detta tillägg, och inte ingå i någon grupptalan, kollektiv process eller representativ talan. Rättigheter som beviljas registrerade enligt detta tillägg avser den registrerade personligen och kan inte överlåtas.

6. **Meddelande om ändring** Microsoft samtycker till och försäkrar att de inte har någon anledning att tro att den lagstiftning som är tillämplig på dem eller deras underordnade personuppgiftsbiträden, i alla länder som personuppgifter överförs till av Microsoft eller ett underordnat personuppgiftsbiträde, förhindrar dem att fullgöra instruktioner från Kunden och sina skyldigheter enligt detta tillägg eller 2021 års standardavtalsklausuler, och att de i händelse av en ändring i denna lagstiftning som sannolikt har en betydande negativ effekt på försäkringar och skyldigheter i detta tillägg eller i standardavtalsklausulerna skyndsamt ska underrätta Kunden om ändringen så snart de får kännedom om den, i vilket fall Kunden har rätt att avbryta överföringen av data och/eller säga upp avtalet.

Bilaga 1 – 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 produktvillkoren och DPA som i övrigt är tillämpliga på en viss produktprenumeration eller -licens, (2) eventuellt annat avtal som hänvisar till denna bilaga.

För ändamål som rör dessa GDPR-villkor avtalar Kunden och Microsoft att Kunden är personuppgiftsansvarig för personuppgifter och Microsoft är personuppgiftsbiträde för dessa uppgifter, utom när Kunden agerar personuppgiftsbiträde för personuppgifter, då Microsoft är underbiträde. 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 produktvillkoren eller något annat avtal dem mellan. Dessa GDPR-villkor är inte tillämpliga om Microsoft är personuppgiftsansvarig.

Relevanta skyldigheter enligt GDPR: Artikel 5, 28, 32 och 33

1. Microsoft stöder Kundens ansvarsskyldigheter via detta DPA och den produktdokumentation som Kunden tillhandahålls, och ska så fortsatt göra under varaktigheten för Kundens prenumeration eller den tillämpliga överenskommelsen om professionelle tjänster i enlighet med underavsnitt 3(h) nedan. (Artikel 5(2))

2. 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))

3. Microsofts databehandling regleras av dessa GDPR-villkor enligt Europeiska unionens (benämns hädanefter 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 iaktta konfidentialitet 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 anlitandet av 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 att tillgå.

(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))

4. 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))

5. 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

(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))

6. 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))

7. 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))

8. 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