Volumlisens

Tillegg om databeskyttelse for produkter og tjenester fra Microsoft

Sist oppdatert 2. januar 2024

Microsoft

Innholdsfortegnelse

Introduksjon

Partene er enige om at Microsoft produkter og tjenester og tilleggskontrakt for databeskyttelse ("DPA") angir sine forpliktelser med hensyn til behandling og sikkerhet av kundedata, faglig tjenestedata og personopplysninger i forbindelse med produktene og tjenestene. DPA-en er innarbeidet ved henvisning i produktvilkårene og andre Microsoft-avtaler. Partene er også enige om at med mindre det eksisterer en egen avtale om Faglige Tjenester, skal denne DPA-en regulere behandlingen av og sikkerheten til Data for Faglige Tjenester. Separate vilkår, inkludert ulike personvern- og sikkerhetsvilkår, regulerer Kundens bruk av Ikke-Microsoft-produkter.

I tilfelle konflikt eller inkonsekvens mellom DPA-vilkårene og andre vilkår i Kundens volumlisensavtale eller andre gjeldende avtaler i forbindelse med Produktene og Tjenestene ("Kundens avtale"), skal DPA-vilkårene ha forrang. Bestemmelsene i DPA-vilkårene har forrang for alle motstridende bestemmelser i Microsofts Personvernerklæring som ellers kan gjelde for behandling av Kundedata, Data for Faglige Tjenester eller personopplysninger, som definert her.

Microsoft tar på seg forpliktelsene i denne DPA-en overfor alle kunder med en eksisterende volumlisensavtale. Forpliktelsene er bindende for Microsoft overfor Kunden uavhengig av (1) produktvilkårene som ellers gjelder for et gitt produktabonnement eller lisens, eller (2) enhver annen avtale som refererer til produktvilkårene.

Gjeldende DPA-vilkår og -oppdateringer

Begrensninger på Oppdateringer

Når kunden fornyer eller kjøper et nytt abonnement på et produkt eller inngår en arbeidsbestilling for en faglig tjeneste, vil de gjeldende DPA-vilkårene gjelde og vil ikke endres under kundens abonnement på det produktet eller begrepet for den faglige tjenesten. Når kunden får en permanent lisens til programvare, vil de gjeldende DPA-vilkårene gjelde (etter samme bestemmelse for å bestemme de gjeldende produktvilkårene for den programvaren i kundens avtale) og vil ikke endres under kundens lisens for den programvaren.

Nye Funksjoner, Tillegg eller Relatert programvare

Uavhengig av de foregående grensene for oppdateringer, gjelder følgende: Når Microsoft introduserer funksjoner, tilbud, tillegg eller relatert programvare som er ny (dvs. som ikke tidligere var inkludert i produktene eller tjenestene), kan Microsoft gi vilkår eller foreta oppdateringer av DPA-en som skal gjelder for kundens bruk av de nye funksjonene, tilbudene, tilleggene eller relaterte programvaren. Hvis disse vilkårene inkluderer vesentlige endringer i DPA-vilkårene, skal Microsoft gi kunden et valg om å bruke de nye funksjonene, tilbudene, tilleggene eller den relaterte programvaren, uten å miste eksisterende funksjonalitet ved et generelt tilgjengelig produkt eller faglig tjeneste. Hvis kunden ikke installerer eller bruker de nye funksjonene, tilbudene, tilleggene eller den relaterte programvaren, skal de tilsvarende nye vilkårene ikke gjelde.

Offentlige forskrifter og krav

Uavhengig av de foregående grensene for oppdateringer gjelder følgende: Microsoft kan endre eller avslutte produkter eller faglige tjenester i ethvert land eller enhver jurisdiksjon der det finnes nåværende eller fremtidige offentlige krav eller forpliktelser som (1) utsetter Microsoft for reguleringer eller krav som ikke allment gjelder for selskaper som driver virksomhet der, (2) gjør det vanskelig for Microsoft å fortsette driften av produktet eller den faglige tjenesten uten endringer, og/eller (3) gir Microsoft grunn til å tro at DPA-vilkårene eller produktet eller den faglige tjenesten kan være i konflikt med slike krav eller forpliktelser.

Elektroniske meddelelser

Microsoft kan formidle informasjon og meldinger til kunden om produkter og tjenester elektronisk, inkludert per e-post, gjennom portalen for den Elektroniske Tjenesten eller et nettsted som Microsoft angir. En melding anses for å være gitt på datoen den gjøres tilgjengelig av Microsoft.

Tidligere versjoner

DPA-vilkårene gir vilkår for produkter og tjenester som for øyeblikket er tilgjengelige. Kunden kan finne tidligere versjoner av DPA-vilkårene på https://aka.ms/licensingdocs eller ved å kontakte sin forhandler eller Microsoft Account Manager.

Innholdsfortegnelse / Generelle vilkår

Definisjoner

Begreper med store forbokstaver som er brukt, men ikke definert i denne DPA-en, skal ha den betydningen som er gitt i Kundens avtale. Følgende definerte begrep brukes i denne DPA-en:

Med "Kundedata" menes alle data, inkludert alle tekst-, lyd-, video- og bildefiler samt programvare, som overføres til Microsoft av, eller på vegne av, Kunden gjennom bruk av den Elektroniske Tjenesten. Kundedata omfatter ikke Data for Faglige Tjenester.

Med "Personvernkrav" menes GDPR, lokal personvernlovgivning i EU/EØS og eventuelle gjeldende lover, regler og andre juridiske krav knyttet til (a) personvern og datasikkerhet; og (b) bruk, innsamling, oppbevaring, lagring, sikkerhet, fremlegging, overføring, avhending og annen behandling av personopplysninger.

"DPA-vilkår" betyr vilkår i DPA-en og eventuelle produktspesifikke vilkår i produktvilkårene som spesifikt supplerer eller modifiserer personvern og sikkerhetsvilkår i DPA-en for et spesifikk produkt (eller funksjonen i et produkt). I tilfelle konflikt eller manglende overensstemmelse mellom DPA-en og slike produktspesifikke vilkår, skal de produktspesifikke vilkårene ha forrang for det gjeldende produktet (eller funksjonen til dette produktet).

Med "GDPR" menes Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning).

Med "Lokal personvernlovgivning i EU/EØS" menes alle underordnede lover og regler som implementerer GDPR.

Med "GDPR-vilkår" menes vilkårene i vedlegg 1, der Microsoft tar på seg bindende forpliktelser knyttet til sin behandling av Personopplysninger i samsvar med artikkel 28 i GDPR.

Med "Personopplysninger" menes enhver opplysning om en identifisert eller identifiserbar fysisk person. En identifiserbar fysisk person er én som kan identifiseres, direkte eller indirekte, spesielt ved henvisning til en identifikator som et navn, et identifikasjonsnummer, stedsdata, en online identifikator eller til én eller flere faktorer som er spesifikke for den fysiske, fysiologiske, genetiske, mentale, økonomiske, kulturelle eller sosiale identiteten til den fysiske personen.

Med "Produkt" menes betydningen som er gitt i volumlisensavtalen. For enkel referanse inkluderes "Produkt" i Elektroniske Tjenester og programvare, hver som definert i volumlisensavtalen.

Med "Produkt og Tjenester" menes produkter og faglige tjenester. Tilgjengeligheten av produkter og faglige tjenester kan variere etter region og anvendelighet av denne DPA-en, og om spesifikke produkter og faglige tjenester er underlagt begrensningene i omfanget i denne DPA-en.

Med "Faglige tjenester" menes de følgende tjenestene: (a) Microsofts konsulenttjenester, bestående av planlegging, råd, veiledning, datamigrering, distribusjon og løsning-/ programvareutviklingstjenester levert under en Microsoft Enterprise Services arbeidsbestilling, eller når det er avtalt i prosjektbeskrivelsen under en Cloud Workload Acceleration-avtale som inneholder denne DPA-en som referanse; og (b) tekniske støttetjenester levert av Microsoft som hjelper kunder med å identifisere og løse problemer som påvirker produkter, inkludert teknisk støtte som en del av Microsoft Unified Support eller Premier Support Services (som henholdsvis beskrevet i Services Consulting and Support Description eller Description of Services) og andre kommersielle tekniske støttetjenester. Faglige tjenester inkluderer ikke produktene eller, kun for formålene med DPA-en, supplerende faglige tjenester.

Med "Faglig Tjenestedata" menes alle data, herunder tekst-, lyd-, video, bildefiler eller programvare som gjøres tilgjengelig for Microsoft av eller på vegne av kunden (eller som kunden gir Microsoft fullmakt til å hente fra et produkt), eller som på annet vis innhentes eller behandles av eller på vegne av Microsoft i forbindelse med et Microsoft-oppdrag for å få faglige tjenester.

Med "2021 standardkontraktsvilkår" menes standard databeskyttelsesklausuler (databehandler-til-databehandler modul) mellom Microsoft Ireland Operations Limited og Microsoft Corporation for overføring av personopplysninger fra databehandlere i EØS til behandlere etablert i tredjeland som ikke sikrer tilstrekkelig databeskyttelse, som beskrevet i artikkel 46 i GDPR og godkjent av EU-kommisjonen i vedtak 2021/914/EC, datert 4. juni 2021.

Med "Underbehandler" menes andre behandlere som brukes av Microsoft til å behandle kundedata, faglig tjenestedata og personopplysninger, som beskrevet i Artikkel 28 i GDPR.

Med "Supplerende Faglige Tjenester" menes støtteforespørsler som eskaleres fra support til et produktingeniørteam for løsning og annen rådgivning og støtte fra Microsoft levert i forbindelse med produkter eller en volumlisensavtale som ikke er inkludert i definisjonen av faglige tjenester.

Begreper med små bokstaver som blir brukt, men ikke definert i denne DPA-en, for eksempel "brudd på personopplysningssikkerheten", "behandling", "behandlingsansvarlig", "databehandler", "profilering", "personopplysninger" og "registrerte" skal ha samme betydning som angitt i artikkel 4 i GDPR, uavhengig av om GDPR gjelder.

Generelle Vilkår

Samsvar med lovgivning

Microsoft skal overholde alle lover og regler som gjelder for levering av produktene og tjenestene, inkludert lover og regler om varsling ved sikkerhetsbrudd og personvernkrav. Microsoft er imidlertid ikke ansvarlig for overholdelse av lover eller retningslinjer som gjelder for Kunden eller Kundens bransje, men ikke generelt for leverandører av IT-tjenester. Microsoft bestemmer ikke om kundedata omfatter informasjon som er underlagt spesifikke lover eller regler. Alle Sikkerhetsbrudd er underlagt vilkårene for Varsling om Sikkerhetsbrudd nedenfor.

Kunden skal overholde alle lover og regler som gjelder for bruken av produkter og tjenester, inkludert lover og regler om biometriske data, taushetsplikt og personvernkrav. Kunden er ansvarlig for å avgjøre om de produktene og tjenestene er formålstjenlige for lagring og behandling av informasjon underlagt spesiell lov eller forskrift og for bruk av produktene og tjenestene på en måte som er i samsvar med kundens juridiske og lovmessige forpliktelser. Kunden står ansvarlig for å svare på forespørsler fra tredjeparter knyttet til kundens bruk av produkter og tjenester, som for eksempel forespørsler om å fjerne innhold i henhold til den amerikanske loven om opphavsrettigheter knyttet til digitale medier, Digital Millennium Copyright Act, og annen gjeldende lovgivning.

Vilkår for personvern

Denne delen av DPA har følgende underpunkt:

- Omfang
- Art av Databehandling; Eierskap
- Utlevering av behandlede opplysninger
- Behandling av Personopplysninger; GDPR
- Datasikkerhet
- Varsling om sikkerhetsbrudd
- Overføring og lokalisering av opplysninger
- Oppbevaring av data og sletting
- Databehandlers taushetsplikt
- Varsel og kontroller ved bruk av underdatabehandlere
- Utdanningsinstitusjoner
- CJIS-kundeavtale
- HIPAA Business Associate
- Telekommunikasjonsdata
- California Consumer Privacy Act (CCPA)
- Biometriske Data
- Supplerende faglige tjenester.
- Hvordan kontakte Microsoft
- Tillegg A – Sikkerhetstiltak
- Tillegg B – datasubjekter og kategorier av personopplysninger
- Tillegg C – tillegg om ekstra sikkerhetstiltak.

Omfang

Vilkårene i denne DPA-en gjelder alle produkter og tjenester bortsett fra de som er beskrevet i denne delen.

Vilkårene i denne DPA-en gjelder ikke for produkter eller profesjonelle tjenester som er spesifikt identifisert som ekskludert, eller i den grad det er identifisert som ekskludert, i produktvilkårene eller den gjeldende arbeidsordren, som er underlagt personvern- og sikkerhetsvilkårene i de gjeldende produktspesifikke eller arbeidsordrespesifikke vilkårene.

For klarhet gjelder DPA-vilkårene bare for behandling av data i miljøer som kontrolleres av Microsoft og Microsofts underbehandlere. Dette inkluderer data som sendes til Microsoft av produkter og tjenester, men inkluderer ikke data som forblir i kundens lokaler eller i noen kundemessige tredjepartsmiljøer.

For supplerende faglige tjenester, forplikter Microsoft seg bare til delen om tilleggstjenester for faglige tjenester nedenfor.

Forhåndsvisninger kan bruke mindre eller forskjellige personvern- og sikkerhetstiltak enn de som vanligvis finnes i produkter og tjenester. Med mindre annet er angitt, skal Kunden ikke bruke Forhåndsvisninger til å behandle Personopplysninger eller andre opplysninger som er underlagt lov- eller forskriftskrav. For produkter vil følgende vilkår i denne DPA-en ikke gjelde for forhåndsvisninger: Behandling av personopplysninger; GDPR, Datasikkerhet og HIPAA-forretningspartner. For faglige tjenester oppfyller tilbud som er forhåndsvisninger eller begrenset utgivelse bare vilkårene i de supplerende faglige tjenestene.

Art av databehandling; eierskap

Microsoft vil bruke og på annen måte behandle kundedata, faglig tjenestedata og personopplysninger bare i samsvar med kundens dokumenterte instruks og som beskrevet og underlagt begrensningene nedenfor (a) for å levere produkter og tjenester til kunden, og (b) for forretningsvirksomhet som skyldes levering av produktene og tjenestene til kunden. Kunden beholder alle rettigheter, eierrettigheter og interesser knyttet til kundedata og faglig tjenestedata. Microsoft tilegner seg ingen rettigheter i Kundedata eller faglig tjenestedata, annet enn rettighetene kunden gir Microsoft i denne delen. Dette avsnittet påvirker ikke Microsofts rettigheter til programvare eller tjenester som Microsoft lisensierer til Kunden.

Databehandling for å kunne levere produktene og tjenestene til kunden

I denne DPA-en skal "å levere" en faglig tjeneste omfatte følgende:

- Levering av funksjonsegenskaper slik de lisensieres, konfigureres og brukes av Kunden og dennes brukere, inkludert ytelse av personlig tilpassede brukeropplevelser;
- Feilsøking (forhindring, oppdaging og reparasjon av problemer); og
- Holde produktene oppdatert og ytelsesdyktige, og forbedring av brukerproduktivitet, pålitelighet, effektivitet, kvalitet og sikkerhet.

For formålene med denne DPA-en består "å tilby" faglige tjenester av:

- Levering av Faglige Tjenester, inkludert levering av teknisk støtte, profesjonell planlegging, rådgivning, veiledning, migrering av data, distribusjon, og tjenester for løsnings-/programvareutvikling.
- Feilsøking (forebygging, avdekking, undersøking, reduksjon av skadevirkningene til og reparasjon av problemer, inkludert sikkerhetsbrudd og problemer som avdekkes i faglige tjenester eller relevante produkt(er) under levering av faglige tjenester); og
- Forbedring av levering, effektivitet, kvalitet og sikkerhet for faglige tjenester og de underliggende produktene basert på problemer som ble identifisert under levering av faglige tjenester, inkludert å fikse programvarefeil, og ellers holde produkter og tjenester oppdatert og ytelsesdyktige.

I hvert tilfelle utføres levering av produktene og tjenestene med tanke på sikkerhetsforpliktelser i henhold til databeskyttelseskrav.

Når Microsoft leverer produkter og tjenester, skal ikke Microsoft bruke eller på annen måte behandle kundedata, faglig tjenestedata eller personopplysninger til: (a) brukerprofilering, (b) annonsering eller lignende kommersielle formål, eller (c) markedsundersøkelser rettet mot å skape nye funksjoner, tjenester eller produkter eller andre formål, med mindre slik bruk eller behandling er i samsvar med kundens dokumenterte instrukser.

Behandling for forretningsvirksomhet til levering av produkter og tjenester til kunden:

I denne DPA-en skal "forretningsvirksomhet" omfatte behandlingsoperasjonene som er autorisert av kunden i denne delen.

Kunden gir tillatelse til Microsoft:

(i.) til å lage aggregerte statistiske, ikke-personlige data fra data som inneholder pseudonymiserte identifikatorer (som brukslogger som inneholder unike, pseudonymiserte identifikatorer); og

(ii.) til å beregne statistikker relatert til Kundedata eller Data for Faglige Tjenester

i hvert tilfelle uten å ha tilgang til eller analysere innholdet i kundedata eller data om faglige tjenester, og begrenset til å oppnå formålene nedenfor, hver som en hendelse for å levere produktene og tjenestene til kunden.

Disse formålene er:

- fakturering og kontoadministrasjon;
- kompensasjon som beregning av ansattes provisjoner og partnerinsentiver;
- intern rapportering og forretningsmodellering, slik som prognoser, inntekter, kapasitetsplanlegging og produktstrategi; og
- finansiell rapportering.

Ved behandling av denne forretningsvirksomheten vil Microsoft anvende prinsipper for dataminimering og vil ikke bruke eller på annen måte behandle kundedata, faglig tjenestedata eller personopplysninger til: (a) brukerprofilering, (b) reklame eller lignende kommersielle formål eller (c) andre formål, annet enn for de formålene som er beskrevet i dette punktet. I tillegg, som med all behandling under denne DPA-en, forblir behandling for forretningsvirksomhet underlagt Microsofts taushetsplikt og forpliktelser under Avsløring av behandlede data.

Utlevering av behandlede opplysninger

Microsoft skal ikke utlevere eller gi tilgang til Behandlede Data bortsett fra: (1) som instruert av Kunden; (2) som beskrevet i denne DPA-en; eller (3) som lovpålagt. I dette punktet skal "Behandlede Opplysninger" bety: (a) Kundedata; (b) Faglige Tjenestedata; (c) Personopplysninger; og (d) alle andre data som Microsoft behandler i forbindelse med produktene og tjenestene som er Kundens konfidensielle opplysninger i henhold til Kundens avtale. All behandling av Behandlede Opplysninger er underlagt Microsoft sin taushetsplikt i henhold til Kundens avtale.

Microsoft skal ikke utlevere eller gi tilgang til Behandlede Data til rettshåndhevende organer med mindre lover og regler krever det. Hvis rettshåndhevende organer kontakter Microsoft med et krav om Behandlede Opplysninger, skal Microsoft anmode det rettshåndhevende organet om å be om disse opplysningene direkte fra Kunden. Hvis de blir tvunget til å fremlegge Behandlede Opplysninger til lovhåndhevere eller gi dem tilgang til slike Data, vil Microsoft omgående varsle Kunden og levere en kopi av kravet, med mindre lover og regler hindrer dem i å gjøre det.

Når Microsoft mottar forespørsler om Behandlede Opplysninger fra andre tredjeparter, skal Microsoft omgående varsle Kunden med mindre lover og regler hindrer dem i å gjøre det. Microsoft avslår forespørselen med mindre lovverket krever at Microsoft etterkommer forespørselen. Hvis forespørselen er gyldig, prøver Microsoft å få tredjeparten til å rette forespørselen om disse dataene direkte til Kunden.

Microsoft vil bare avsløre eller gi tilgang til behandlede data som kreves av loven, forutsatt at lovene og praksisene respekterer essensen av de grunnleggende rettighetene og frihetene, og ikke går utover det som er nødvendig og forholdsmessig i et demokratisk samfunn og, der det er aktuelt, for å beskytte et av målene oppført i artikkel 23(1) i GDPR.

Microsoft vil ikke gi noen Tredjepart: (a) direkte, indirekte, generell eller ubegrenset tilgang til Behandlede Opplysninger; (b) krypteringsnøkler for plattformer som brukes til å sikre Behandlede Opplysninger eller evne til å bryte slik kryptering; eller (c) tilgang til Behandlede Opplysninger hvis Microsoft er klar over at opplysningene skal brukes til andre formål enn de som er angitt i Tredjepartens forespørsel.

Til støtte for ovennevnte kan Microsoft gi Kundens grunnleggende kontaktinformasjon til Tredjepart.

Behandling av personopplysninger; GDPR

Alle personopplysninger som behandles av Microsoft i forbindelse med leveringen av produktene og tjenestene, er innhentet som en del av enten (a) kundedata, (b) faglig tjenestedata, eller (c) data generert, avledet eller innsamlet av Microsoft, inkludert data sendt til Microsoft som et resultat av en kundes bruk av tjenestebaserte funksjoner eller hentet av Microsoft fra lokalt installert programvare. Personopplysninger som leveres til Microsoft av eller på vegne av kunder gjennom bruk av den Elektroniske Tjenesten, er også kundedata. Personopplysninger som leveres til Microsoft av eller på vegne av kunder gjennom bruk av den Elektroniske Tjenesten, er også faglig tjenestedata. Pseudonymiserte identifikatorer kan være inkludert i Diagnostiske data som behandles av Microsoft i forbindelse med levering av produktene, og er også personopplysninger. Alle Personopplysninger som er pseudonymisert eller avidentifisert, men ikke anonymisert, eller Personopplysninger som er utledet av Personopplysninger, er også Personopplysninger.

I den grad Microsoft er databehandler eller underdatabehandler av Personopplysninger som omfattes av GDPR, skal GDPR-vilkårene i vedlegg 1 regulere slik behandling, og språket i underseksjonen ("Behandling av personopplysninger; GDPR") skal anses som et tillegg:

Databehandler og behandlingsansvarlig, roller og ansvar

Kunden og Microsoft er enige om at kunden er behandlingsansvarlig for personopplysninger, og at Microsoft er databehandler for slike opplysninger, bortsett fra (a) når kunden fungerer som databehandler for personopplysninger, hvor Microsoft blir å anse som underdatabehandler; eller (b) som angitt på annen måte i de produktspesifikke vilkårene for den Elektroniske Tjenesten eller i denne DPA-en. Når Microsoft fungerer som databehandler eller underdatabehandler av Personopplysninger, skal Microsoft behandle Personopplysninger bare etter dokumenterte instrukser fra Kunden. Kunden samtykker i at Kundens avtale (inkludert DPA-vilkårene og gjeldende oppdateringer), sammen med produktdokumentasjonen og kundens bruk og konfigurasjon av funksjoner i produktene, er kundens fullstendige og dokumenterte instrukser til Microsoft for behandling av personopplysninger, eller dokumentasjonen for Faglige Tjenester og kundens bruk av de faglige tjenestene. Informasjon om bruk og konfigurasjon av produktene finner du på https://docs.microsoft.com (eller et etterfølgende sted) eller en annen avtale som inneholder denne DPA-en. Eventuelle tilleggs- eller alternative instruksjoner må avtales i henhold til prosessen for å endre kundens avtale. I alle tilfeller der GDPR gjelder og Kunden er databehandler, garanterer Kunden overfor Microsoft at Kundens instrukser, inkludert utnevnelse av Microsoft som databehandler eller underdatabehandler, har blitt godkjent av den aktuelle behandlingsansvarlige.

I den grad Microsoft bruker eller på annen måte behandler personopplysninger som omfattes av GDPR, for Microsofts legitime forretningsvirksomhet knyttet til levering av produkter og tjenester til kunden, skal Microsoft overholde forpliktelsene til en uavhengig behandlingsansvarlig under GDPR for slik bruk. Microsoft godtar det ekstra ansvaret som "behandlingsansvarlig" i henhold til GDPR for slik behandling for å: (a) handle i samsvar med forskriftskrav, i den grad det kreves under GDPR; og (b) gi økt åpenhet for Kundene og bekrefte Microsofts ansvarlighet for slik behandling. Microsoft anvender sikkerhetstiltak for å beskytte kundedata, faglig tjenestedata og personopplysninger under slik behandling, inkludert sikkerhetstiltakene som er nevnt i denne DPA-en, og sikkerhetstiltakene som er beskrevet i artikkel 6 nr. 4 i GDPR. Med hensyn til behandling av personopplysninger i henhold til dette avsnittet, forplikter Microsoft seg som angitt i delen tillegg om ekstra sikkerhetstiltak; for disse formålene, (i) enhver Microsoft-fremlegging av personopplysninger, som beskrevet i tillegg om ekstra sikkerhetstiltak-delen, som er overført i forbindelse med forretningsvirksomhet, anses som en "relevant fremlegging" og (ii) forpliktelsene i tillegg om ekstra sikkerhetstiltak-delen gjelder for slike personopplysninger.

Behandling av detaljer

Partene bekrefter og er enige om at:

- **Innhold.** Innholdet i behandlingen er begrenset til Personopplysninger innenfor rammen av punktet med tittelen «Art av databehandling; eierskap» ovenfor i denne DPA-en og av GDPR.
- **Varigheten av behandlingen.** Varigheten av behandlingen skal være i samsvar med Kundens instrukser og vilkårene i DPA-en.
- **Behandlingens art og formål.** Behandlingens art og formål skal være å tilby Produktene og Tjenestene i henhold til Kundens avtale og for Microsofts forretningsvirksomhet knyttet til levering av produktene og tjenestene til kunden (som nærmere beskrevet i punktet med tittelen "Art av databehandling; eierskap" ovenfor).

- **Datakategorier.** Typene av personopplysninger som behandles av Microsoft ved levering av produktene og tjenestene inkluderer: (i) Personopplysninger som kunden velger å inkludere i kundedata og faglig tjenestedata; og (ii) de uttrykkelig identifisert i artikkel 4 i GDPR som kan genereres, hentes eller samles inn av Microsoft, inkludert data som sendes til Microsoft som følge av en kundes bruk av tjenestebaserte funksjoner eller hentet av Microsoft fra lokalt installert programvare. De typene av personopplysninger som kunden velger å inkludere i kundedata og faglig tjenestedata, kan være alle kategorier av personopplysninger som er identifisert i poster som oppbevares av kunden som fungerer som kontroller i henhold til artikkel 30 i GDPR, inkludert kategoriene av personopplysninger som er angitt i tillegg B.
- **Registrerte.** Kategoriene av registrerte subjekter er kundens representanter og sluttbrukere, for eksempel ansatte, entreprenører, samarbeidspartnere og kunder, og kan omfatte andre kategorier av registrerte som identifisert i poster som oppbevares av kunden som opptrer som kontrollør i henhold til artikkel 30 i GDPR, inkludert kategoriene av registrerte angitt i tillegg B.

Datasubjektets rettigheter; Hjelp med forespørsler

Microsoft vil gjøre tilgjengelige for kunden, på en måte som er i samsvar med funksjonaliteten til produktene og tjenestene og Microsofts rolle som behandler av personopplysninger om datasubjekter, muligheten til å oppfylle datasubjektenes forespørsler om å utøve sine rettigheter under GDPR. Hvis Microsoft mottar en forespørsel fra kundens datasubjekt om å utøve én eller flere av sine rettigheter under GDPR i forbindelse med produktene og tjenestene som Microsoft er en databehandler eller underbehandler for, vil Microsoft omdirigere datasubjektet til å rette forespørselen direkte til kunden. Kunden skal være ansvarlig for å svare på en slik forespørsel, også, hvis nødvendig, ved å bruke funksjonaliteten i produktene og tjenestene. Microsoft skal etterkomme rimelige forespørsler fra kunden om å få hjelp til å håndtere svar på slike dataforespørsler.

Protokoller over behandlingsaktiviteter

I den grad GDPR krever at Microsoft fører protokoll over visse opplysninger knyttet til Kunden, skal Kunden ved forespørsel levere slike opplysninger til Microsoft og holde dem nøyaktige og oppdatert. Microsoft kan gjøre alle slike opplysninger tilgjengelige for tilsynsmyndigheten hvis det kreves av GDPR.

Datasikkerhet

Sikkerhetspraksis og -retningslinjer

Microsoft vil gjennomføre og opprettholde egnede tekniske og organisatoriske tiltak for å beskytte kundedata, faglig tjenestedata og personopplysninger mot utilsiktet eller ulovlig ødeleggelse, tap, endring, uautorisert fremlegging av, eller tilgang til, personopplysninger som overføres, lagres eller på annen måte behandles. Tiltakene skal fastsettes i Microsoft sikkerhetsretningslinjer. Microsoft skal gjøre disse retningslinjene tilgjengelige for Kunden i tillegg til annen informasjon om Microsofts rutiner og retningslinjer for sikkerhet som Kunden rimelig kan be om.

I tillegg skal disse tiltakene oppfylle kravene som er angitt i ISO 27001, ISO 27002 og ISO 27018. En beskrivelse av sikkerhetskontrollene for disse kravene er tilgjengelig for kundene.

Hver Elektroniske Kjernetjeneste overholder også kontrollstandardene og rammene vist i tabellen i produktvilkårene. Hver Elektroniske Kjernetjeneste og Faglige tjeneste implementerer og opprettholder sikkerhetstiltakene som er angitt i tillegg A for beskyttelse av kundedata og faglig tjenestedata.

Microsoft implementerer og opprettholder også sikkerhetstiltakene som er angitt i Vedlegg II til 2021-standardkontraktsklausulene for beskyttelse av personopplysninger innenfor omfanget av GDPR.

Microsoft kan legge til bransje- eller myndighetsstandarder når som helst. Microsoft vil ikke fjerne ISO 27001, ISO 27002, ISO 27018 eller noen standarder eller et rammeverk i tabellen for Elektroniske Kjernetjenester i produktvilkårene, med mindre disse ikke lenger brukes i bransjen og er erstattet av nye (hvis slike finnes).

Datakryptering

Kundedata og Faglig tjenestedata (hver inkludert eventuelle inkluderte personopplysninger) som overføres over offentlige nettverk mellom kunden og Microsoft eller mellom Microsofts datasentre, krypteres som standard.

Microsoft krypterer også lagrede kundedata i Elektroniske Tjenester og faglig tjenestedata blir lagret i hvile. I tilfelle av Elektroniske Tjenester der Kunden eller en tredjepart som handler på Kundens vegne, kan bygge applikasjoner (f.eks. visse Azure-tjenester), kan kryptering av data som er lagret i slike applikasjoner, benyttes etter Kundens skjønn, ved å bruke begge funksjonene som gis av Microsoft eller innhentes av Kunden fra tredjeparter.

Tilgang til Data

Microsoft benytter tilgangsmekanismer med minste privilegium for å styre tilgangen til kundedata og faglig tjenestedata (inkludert personopplysningene de inneholder). Rollebaserte tilgangskontroller benyttes for å sikre at tilgang til kundedata og faglig tjenestedata som kreves for serviceoperasjoner, er for et passende formål og godkjent med ledelsestilsyn. For Elektroniske Kjernetjenester og Faglige Tjenester

opprettholder Microsoft tilgangskontrollmekanismer beskrevet i tabellen "Sikkerhetstiltak" i tillegg A. For Elektroniske Tjenester er det ingen permanent tilgang for Microsoft-personell til kundedata, og all nødvendig tilgang har tidsbegrensning.

Kundens ansvar

Kunden er alene ansvarlig for å foreta en uavhengig avgjørelse av om tekniske og organisatoriske tiltak for om produkter og tjenester oppfyller kundens krav, inkludert noen av sikkerhetsforpliktelsene i henhold til gjeldende databeskyttelseskrav. Kunden bekrefter og samtykker i at (tatt i betraktning den tekniske utviklingen, kostnadene ved implementering og behandlingens natur, omfang, kontekst og formål for å behandle Personopplysninger samt risikoer for individer) rutinene og retningslinjene for sikkerhet som er implementert og opprettholdt av Microsoft gir et sikkerhetsnivå som er tilstrekkelig for risiko med hensyn til Personopplysninger. Kunden er ansvarlig for å implementere og videreføre personvernbeskyttelse og sikkerhetstiltak for komponenter som Kunden leverer og kontrollerer (for eksempel enheter som er registrert i Microsoft Intune, eller i Microsoft Azure-kunders virtuelle maskiner eller programmer).

Revisjon av etterlevelse

Microsoft vil utføre revisjoner av sikkerheten til datamaskinene, databehandlingsmiljøet og fysiske datasentre som den bruker til behandling av kundedata, faglig tjenestedata og personopplysninger, som følger:

- Når kontroller fastsettes i en standard eller et rammeverk, skal en kontroll i henhold til standarden eller rammeverket gjennomføres minst én gang i året.
- Hver enkelt kontroll gjennomføres i henhold til standardene og reglene til myndighets- eller akkrediteringsorganet for hver gjeldende kontrollstandard eller -rammeverk.
- Hver kontroll skal gjennomføres av kvalifiserte, uavhengige tredjepartskontrollører som velges og betales av Microsoft.

Hver kontroll skal resultere i utforming av en kontrollrapport («Microsoft Audit Report»), som Microsoft skal gjøre tilgjengelig på https://servicetrust.microsoft.com/ eller et annet sted angitt av Microsoft. Kontrollrapporten skal være Microsofts Konfidensielle Opplysninger og skal tydelig angi vesentlige funn revisoren har gjort. Microsoft skal omgående rette opp problemer som tas opp i revisjonsrapporter (Microsoft Audit Report) på en måte som tilfredsstiller revisoren. Hvis Kunden ber om det, skal Microsoft gjøre hver revisjonsrapport (Microsoft Audit Report) tilgjengelig for kunden. Revisjonsrapporten (Microsoft Audit Report) skal være underlagt taushets- og distribusjonsbegrensninger angitt av Microsoft og revisoren.

I den grad Kundens revisjonskrav i henhold til Standardkontraktsvilkårene eller Personvernkrav ikke med rimelighet kan oppfylles gjennom revisjonsrapporter, dokumentasjon eller samsvarsinformasjon Microsoft gjør generelt tilgjengelig for kundene sine, skal Microsoft omgående svare på kundens ytterligere revisjonsinstrukser. Før en revisjon starter, skal Kunden og Microsoft bli enige om omfanget, tidspunktet, varigheten, kontroll- og beviskravene og gebyrene for revisjonen, forutsatt at dette kravet om enighet ikke gir Microsoft mulighet til å utsette revisjonen på urimelig måte. I den grad det er nødvendig for å utføre revisjonen, skal Microsoft gjøre tilgjengelig behandlingssystemer, -anlegg og støttedokumentasjon som er relevant for Microsoft, dets tilknyttede selskaper og dets underdatabehandlere sin behandling av kundedata, faglig tjenestedata og personopplysninger. En slik revisjon skal utføres av et uavhengig, akkreditert tredjeparts revisjonsselskap i løpet av ordinær arbeidstid, med rimelig forhåndsvarsel til Microsoft og underlagt rimelige konfidensialitetsprosedyrer. Verken kunden eller revisor skal ha tilgang til data fra Microsofts andre kunder eller til Microsoft-systemer eller -fasiliteter som ikke er involvert levering av gjeldende produkter og tjenester. Kunden er ansvarlig for alle kostnader og avgifter knyttet til slik revisjon, inkludert alle rimelige kostnader og gebyrer for all tid Microsoft bruker på en slik revisjon, i tillegg til prisene for tjenester utført av Microsoft. Hvis revisjonsrapporten som utarbeides på grunnlag av Kundens revisjon, inkluderer funn av vesentlig manglende overholdelse, skal Kunden dele revisjonsrapporten med Microsoft, og Microsoft skal omgående rette opp all vesentlig manglende overholdelse.

Ingenting i denne delen av DPA-en varierer eller modifiserer GDPR-vilkårene eller påvirker noen tilsynsmyndighets eller datasubjekts rettigheter under databeskyttelseskravene. Microsoft Corporation er en begunstiget tredjepart i dette punktet.

Varsling om sikkerhetsbrudd

Hvis Microsoft blir klar over et sikkerhetsbrudd som fører til tilfeldig eller ulovlig ødeleggelse, tap, endringer, uautorisert fremlegging eller tilgang til kundedata, faglig tjenestedata eller personopplysninger mens de behandles av Microsoft (hver enkelt et "Sikkerhetsbrudd"), vil Microsoft umiddelbart og uten ugrunnet opphold (1) varsle kunden om sikkerhetsbruddet, (2) granske sikkerhetsbruddet og gi kunden detaljert informasjon om sikkerhetsbruddet og (3) iverksette rimelige tiltak for å begrense konsekvenser av og skader som skyldes sikkerhetsbruddet.

Varsler om sikkerhetsbrudd leveres til kunden gjennom en metode som Microsoft selv velger, inkludert e-post. Det er kundens eget ansvar å sikre at kunden opprettholder nøyaktig kontaktinformasjon med Microsoft for hvert gjeldende produkt og faglige tjeneste. Kunden er ansvarlig for å oppfylle sine forpliktelser i henhold til lover om hendelsesvarsler som gjelder for kunden, og oppfylle tredjeparts varslingsforpliktelser relatert til sikkerhetshendelser.

Microsoft skal gjøre en rimelig innsats for å hjelpe Kunden med å oppfylle Kundens forpliktelser i henhold til artikkel 33 i GDPR eller annen gjeldende lov eller forskrift om å varsle relevante tilsynsmyndigheter og registrerte om Sikkerhetsbruddet.

Microsofts varsling eller håndtering av en sikkerhetshendelse i henhold til dette punktet utgjør ikke noen erkjennelse av feil eller ansvar fra Microsofts side med hensyn til sikkerhetshendelsen.

Kunden må varsle Microsoft omgående om mulig misbruk av kontoer eller autentiseringsinformasjon eller sikkerhetshendelser relatert til produktene og tjenestene.

Overføring og lokalisering av opplysninger

Dataoverføringer

Kundedata, faglig tjenestedata og personopplysninger som Microsoft behandler på kundens vegne, kan ikke overføres til, eller lagres og behandles på et geografisk sted, bortsett fra i samsvar med DPA-vilkårene og sikkerhetstiltakene nedenfor i denne delen. Med hensyn til slike garantier, gir kunden Microsoft tillatelse til å overføre kundedata, faglig tjenestedata og personopplysninger til USA eller ethvert annet land der Microsoft eller dets underdatabehandlere driver virksomhet, og til å lagre og behandle kundedata og personopplysninger for å levere produktene, bortsett fra som beskrevet andre steder i DPA-vilkårene.

Alle overføringer av kundedata, faglig tjenestedata og personopplysninger fra EU, Det europeiske økonomiske området, Storbritannia og Sveits for å levere produkter og tjenester skal være underlagt 2021 standardkontraktsvilkårene implementert av Microsoft. I tillegg skal overføringer fra Storbritannia være underlagt IDTA-vilkårene implementert av Microsoft. For formålet med denne DPA-en betyr "IDTA" tillegget for internasjonal dataoverføring til EU-kommisjonens standard kontraktuelle klausuler for internasjonale dataoverføringer utstedt av UK Information Commissioner's Office under S119A(1) i UK Data Protection Act 2018. Microsoft vil overholde i henhold til kravene i Det europeiske økonomiske samarbeidsområdet, Storbritannia og sveitsisk databeskyttelseslov angående innsamling, bruk, overføring, oppbevaring og annen behandling av personopplysninger fra Det europeiske økonomiske samarbeidsområdet, Storbritannia og Sveits. All overføring av personopplysninger til et tredjeland eller en internasjonal organisasjon vil være underlagt passende sikkerhetstiltak som beskrevet i artikkel 46 i GDPR, og slike overføringer og sikkerhetstiltak vil bli dokumentert i henhold til artikkel 30 nr. 2 i GDPR.

I tillegg er Microsoft sertifisert i henhold til EU-U.S. og Swiss-U.S. Data Privacy Frameworks, Storbritannias utvidelse til EU-U.S. Data Privacy Framework og alle forpliktelser dette innebærer. Microsoft forplikter seg til å varsle Kunden hvis Microsoft kommer frem til at Microsoft ikke lenger kan oppfylle forpliktelsene sine med hensyn til beskyttelsesnivået som kreves av prinsippene i Data Privacy Frameworks.

Plassering for Kundedata

Når det gjelder Elektroniske Kjernetjenester, vil Microsoft lagre inaktive kundedata innenfor visse geografiske områder (hvert av disse et Geo) som angitt i produktvilkårene.

Når det gjelder EUs datagrense for Elektroniske Tjenester, vil Microsoft lagre og behandle kundedata og personopplysninger innenfor EU, som angitt i produktvilkårene.

Microsoft verken styrer eller begrenser områdene der Kunden eller Kundens sluttbrukere kan få tilgang til eller flytte Kundedata.

Oppbevaring av data og sletting

Til enhver tid i løpet av abonnementstiden eller det gjeldende engasjementet for faglige tjenester, vil kunden ha tilgang til, trekke ut og slette kundedata som er lagret i hver Elektroniske Tjeneste og Faglige tjenestedata.

Unntatt for gratis prøveversjoner og LinkedIn-tjenester lagrer Microsoft kundedata i en Elektronisk Tjeneste i en konto med begrenset funksjonalitet i 90 dager etter utløp eller oppsigelse av kundens abonnement, slik at kunden kan hente ut dataene. Når oppbevaringsperioden på 90 dager utløper, vil Microsoft deaktivere kundens konto og slette kundedataene og personopplysningene som er lagret i den Elektroniske Tjenesten innen ytterligere 90 dager, med mindre denne DPA-en gir tillatelse til å lagre slike opplysninger.

For personopplysninger i forbindelse med programvaren og for faglig tjenestedata, vil Microsoft slette alle kopier etter at forretningsformålene som dataene ble samlet inn eller overført til er oppfylt, eller tidligere på kundens forespørsel, med mindre det er autorisert i henhold til denne DPA-en å beholde slike data.

Den Elektroniske Tjenesten støtter kanskje ikke lagring eller uthenting ved hjelp av programvare levert av kunden. Microsoft kan ikke holdes erstatningsansvarlig for sletting av kundedata, faglig tjenestedata eller personopplysninger, slik dette er beskrevet i denne delen.

Databehandlers taushetsplikt

Microsoft vil sørge for at dets personell som er involvert i behandlingen av kundedata, faglig tjenestedata og personopplysninger, (i) bare skal behandle slike opplysninger etter instruks fra kunden eller som beskrevet i denne DPA-en, og (ii) skal være forpliktet til å opprettholde konfidensialiteten og sikkerheten til slike opplysninger selv etter at oppdraget deres er avsluttet. Microsoft skal gi regelmessig og obligatorisk opplæring og bevisstgjøring om personvern og sikkerhet til ansatte som har tilgang til kundedata, faglig tjenestedata og personopplysninger i samsvar med gjeldende personvernkrav og bransjestandarder.

Varsel og kontroller ved bruk av Underdatabehandlere

Microsoft kan leie inn Underbehandlere til å levere visse begrensede tjenester eller andre tjenester på sine vegne. Kunden samtykker til dette engasjementet og til Microsoft-tilknyttede selskaper som Underbehandlere. Ovennevnte godkjenning skal utgjøre kundens forutgående skriftlige tillatelse til at Microsoft kan bruke underleverandører til behandlingen av kundedata, faglig tjenestedata og personopplysninger dersom slikt samtykke er påkrevd ifølge standardkontraktsvilkårene eller GDPR-vilkårene.

Microsoft er ansvarlig for at Underdatabehandlerne de benytter, overholder Microsofts forpliktelser etter denne DPA-en. Microsoft gjør informasjon om Underdatabehandlere tilgjengelig på Microsofts nettsted. Når de bruker underdatabehandlere, skal Microsoft gjennom en skriftlig avtale sørge for at underdatabehandleren får tilgang til og kan bruke kundedata, faglig tjenestedata eller personopplysninger bare for å levere tjenestene Microsoft har engasjert dem for å levere, og at underdatabehandleren forbys å bruke kundedata, faglig tjenestedata eller personopplysninger til andre formål. Microsoft vil sørge for at underbehandlere er bundet av skriftlige avtaler som krever at de skal gi minst det nivået av databeskyttelse som kreves av Microsoft av DPA-en, inkludert begrensningene for avsløring av Behandlede Data. Microsoft samtykker i å føre tilsyn med Underdatabehandlerne for å sikre at disse avtaleforpliktelsene blir oppfylt.

Fra tid til annen kan Microsoft engasjere nye underbehandlere. Microsoft vil gi kunden varsel og eventuelt oppdatere nettsiden, og gi kunden tilgang til en mekanisme som gir varsel om oppdateringen om enhver ny underbehandler minst 6 måneder før underleverandøren får tilgang til Kundedata eller Personopplysninger. I tillegg skal Microsoft gi kunden varsel og eventuelt oppdatere nettsiden, og sørge for at kunden blir varslet om oppdateringen om enhver ny underdatabehandler minst 30 dager før denne underdatabehandleren får tilgang til andre faglige tjenestedata eller personopplysninger enn de som kundedataene inneholder. Hvis Microsoft engasjerer en ny underdatabehandler for et nytt produkt eller en faglig tjeneste som behandler kundedata, faglig tjenestedata eller personopplysninger, vil Microsoft gi kunden beskjed før dette produktet eller den faglige tjenesten er tilgjengelig.

Hvis kunden ikke godkjenner en ny underprosessor for en Elektronisk Tjeneste eller Faglige tjenester, kan kunden avslutte ethvert abonnement på den berørte Elektroniske Tjenesten eller gjeldende tjenestevilkår for den gjeldende faglige tjenesten, henholdsvis uten straff eller oppsigelsesgebyr ved å gi skriftlig varsel om oppsigelse før den aktuelle oppsigelsestiden er over. Hvis kunden ikke godkjenner en ny underprosessor for programvare, og kunden ikke med rimelighet kan unngå bruk av underprosessoren ved å begrense Microsoft fra å behandle data som beskrevet i dokumentasjonen eller denne DPA-en, kan kunden avslutte enhver lisens for det berørte programvareproduktet uten straff ved å gi skriftlig varsel om oppsigelse før slutten av den aktuelle oppsigelsestiden. Kunden kan også legge en forklaring av grunnene til den manglende godkjenningen ved oppsigelsesvarselet, for å gi Microsoft mulighet til å revurdere en slik ny Underdatabehandler basert på de aktuelle bekymringene. Hvis det berørte produktet inngår i en serie (eller et tilsvarende samlet kjøp av flere tjenester), gjelder oppsigelser hele serien. Etter oppsigelsen skal Microsoft fjerne betalingsforpliktelser knyttet til eventuelle abonnementer eller annet gjeldende ulønnet arbeid for de avsluttede produktene eller tjenestene fra påfølgende fakturaer til kunden eller forhandleren.

Utdanningsinstitusjoner

Hvis kunden er et utdanningsorgan eller -institusjon som omfattes av regelverket i henhold til Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), erkjenner Microsoft at Microsoft innenfor rammene av DPA-en er en “school official” med “legitimate educational interests” i kundedataene og de faglige tjenestedataene, slik disse vilkårene har blitt definert i FERPA og dens gjennomføringsforskrifter, og Microsoft samtykker i å overholde de begrensningene og kravene som stilles av 34 CFR 99.33(a) til skoleansatte.

Kunden forstår at Microsoft har begrensede eller ingen kontaktopplysninger for elever/studenter hos Kunden og foreldrene deres. Følgelig skal kunden være ansvarlig for å innhente slikt foreldresamtykke for enhver sluttbrukers bruk av den produktene og tjenestene som kan være påkrevd i henhold til gjeldende lov, og for å gi slikt varsel til studenter (eller når det gjelder studenter under 18 år som ikke studerer ved høyskole eller universitet: studentens foreldre) om eventuelle rettslige pålegg eller rettsgyldige vitnestevninger som krever fremlegging av kundedata og faglige tjenestedata i Microsofts besittelse, som kan være påkrevd i henhold til gjeldende lov.

CJIS-kundeavtale

Microsoft leverer visse offentlige skytjenester (“Omfattede Tjenester”) i samsvar med Sikkerhetsretningslinjene (“CJIS-retningslinjer”) til FBIs Criminal Justice Information Services. CJIS-retningslinjene styrer bruk og overføring av strafferettslige opplysninger. Alle Microsoft CJIS-dekkede tjenester skal reguleres av vilkårene og betingelsene i CJIS-forvaltningsavtale.

HIPAA Business Associate

Hvis kunden er en “dekket enhet” eller en “forretningsforbindelse” og inkluderer “beskyttet helseinformasjon” i kundedata eller faglige tjenestedata, slik disse vilkårene er definert i henhold til loven om helseforsikring, portabilitet og ansvarlighet fra 1996, med endringer, og forskrifter som er kunngjort derunder (samlet, “HIPAA”), omfatter gjennomføring av Kundens avtale utførelse av HIPAA Business Associate Agreement (“BAA”). Fullteksten i BAA identifiserer de Elektroniske Tjenestene eller Faglige Tjenestene den gjelder for og er tilgjengelig i http://aka.ms/BAA. Kunden kan velge bort BAA ved å sende følgende informasjon til Microsoft i en skriftlig melding (i henhold til vilkårene i Kundens avtale):

- det fullstendige juridiske navnet på Kunden og ethvert Tilknyttet Selskap som reserverer seg; og
- hvis Kunden har flere avtaler, vil Kundens avtale som avmeldingen gjelder.

Telekommunikasjonsdata

I den grad Microsoft behandler trafikk, innhold og andre personopplysninger i leveringen av produkter og tjenester som kvalifiserer som telekommunikasjonstjenester i henhold til gjeldende lov, kan spesifikke lovpålagte forpliktelser gjelde. Microsoft vil overholde alle telekommunikasjonsspesifikke lover og forskrifter som gjelder for å levere produktene og tjenestene, inkludert varsling om sikkerhetsbrudd, databeskyttelseskrav og telekommunikasjonshemmeligheter.

California Consumer Privacy Act (CCPA)

Hvis Microsoft behandler personopplysninger innenfor rammen av CCPA, tar Microsoft på seg følgende tilleggsforpliktelser overfor kunden. Microsoft skal behandle kundedata, faglig tjenestedata og personopplysninger på vegne av kunden og skal ikke lagre, bruke eller fremlegge slike opplysninger for andre formål enn de som er angitt i DPA-vilkårene, og slik CCPA-en tillater, inkludert som del av et eventuelt "salgsfritak". Microsoft skal ikke under noen omstendigheter selge slike data. Disse CCPA-vilkårene verken begrenser eller reduserer noen personvernforpliktelser Microsoft tar på seg overfor kunden i DPA-vilkårene, produktvilkårene eller i andre avtaler mellom Microsoft og kunden.

Biometriske Data

Hvis kunden bruker produkter og tjenester til å behandle Biometriske Data, er kunden ansvarlig for å: (i) varsle datasubjekter, inkludert med hensyn til lagringsperioder og ødeleggelse; (ii) innhente samtykke fra datasubjekter; og (iii) slette de Biometriske Dataene, alt etter behov og det som kreves i henhold til gjeldende Personvernskrav. Microsoft skal behandle de Biometriske Dataene i henhold til Kundens dokumenterte instruksjoner (som beskrevet i punktet «Roller og ansvar for Databehandler og Behandlingsansvarlig» ovenfor) og beskytte de Biometriske Dataene i samsvar med vilkårene for datasikkerhet og -beskyttelse i henhold til denne DPA. I dette punktet skal «Biometriske data» ha betydningen angitt i Artikkel 4 i GDPR og, hvis relevant, tilsvarende vilkår i andre Personvernskrav.

Supplerende faglige tjenester

Når det brukes i delene nedenfor, inkluderer det definerte begrepet "Faglige tjenester" supplerende faglige tjenester, og det definerte begrepet "Faglig tjenestedata" inkluderer data innhentet for supplerende faglige tjenester.

For supplerende faglige tjenester gjelder følgende deler av DPA-en på samme måte som de gjelder for faglige tjenester: "Innledning", "Overholdelse av lover", "Behandlingens art; Eierskap"," Utlevering av behandlede data"," Behandling av personopplysninger; GDPR", første ledd i "Sikkerhetspraksis og retningslinjer", "Kundeansvar", "Sikkerhetshendelsemelding", "Dataoverføring" (inkludert vilkårene for 2021 standardkontraktsvilkår), tredje ledd i "Datalagring og sletting", "Underdatabehandlers taushetsplikt", "Merknad og kontroller om bruk av underprosessorer", "HIPAA Forretningsforbindelse" (i den utstrekning som er gjeldende i BAA), "California Consumer Privacy Act (CCPA)", "Biometriske Data", "Hvordan kontakte Microsoft", "Tillegg B – Datasubjekter og kategorier av personopplysninger" og "Tillegg C – Tillegg om tilleggsgarantier".

Hvordan kontakte Microsoft

Hvis Kunden mener at Microsoft ikke overholder sine personvern- eller sikkerhetsforpliktelser, kan Kunden kontakte kundestøtte eller bruke Microsofts nettskjema for personvern på http://go.microsoft.com/?linkid=9846224. Microsofts postadresse:

Microsoft Enterprise Service Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited er Microsofts personvernrepresentant for EØS og Sveits. Representanten vår for personvern kan kontaktes på følgende adresse:

Microsoft Ireland Operations, Ltd.
Attn: Personvern
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18, D18 P521, Ireland

Tillegg A – Sikkerhetstiltak

For kundedata i Elektroniske Kjernetjenester og Faglige Tjenester har Microsoft gjennomført og skal opprettholde følgende sikkerhetstiltak, som i forbindelse med sikkerhetsforpliktelsene i denne DPA-en (inkludert GDPR-vilkårene) utgjør Microsofts eneste ansvar knyttet til sikkerheten til slike opplysninger.

Domene	Praksis
Organisering av informasjonssikkerhet	**Eierskap til sikkerhet.** Microsoft har pekt ut én eller flere sikkerhetsansvarlige som har ansvar for koordinasjon og overvåkning av reglene og rutinene for sikkerhet. **Roller og ansvarsområder for sikkerhet.** Microsofts personell med tilgang til kundedata eller faglig tjenestedata er underlagt taushetsplikt. **Risikostyringsprogram.** Microsoft utførte en risikovurdering før behandling av kundedata eller lansering av Elektroniske Tjenester og før behandling av Faglige Tjenestedata eller lansering av faglige tjenester. Microsoft lagrer sikkerhetsdokumentene sine i henhold til oppbevaringskravene også etter at dokumentene ikke lenger er i bruk.
Verdiforvaltning	**Ressursbeholdning.** Microsoft opprettholder en oversikt over alle mediene som kundedata eller faglig tjenestedata er lagret på. Tilgang til listene til slike medier er begrenset til Microsoft-personell som er skriftlig autorisert til å ha slik tilgang. **Ressurshåndtering** - Microsoft klassifiserer kundedata og faglig tjenestedata for å identifisere dem og for å gi tilgang til å begrense dem på riktig måte. - Microsoft pålegger begrensninger for utskrift av kundedata og faglig tjenestedata og har prosedyrer for avhending av trykt materiale som inneholder slike opplysninger. - Microsoft-personell må innhente samtykke fra Microsoft før lagring av kundedata eller faglig tjenestedata på bærbare enheter, ekstern tilgang til slike opplysninger og behandling av kundedata utenfor Microsofts anlegg.
Sikkerhet for HR	**Sikkerhetsopplæring.** Microsoft informerer sitt personell om relevante sikkerhetsrutiner og personellets respektive roller. Microsoft informerer også personell om potensielle konsekvenser ved brudd på reglene og rutinene for sikkerhet. Microsoft bruker utelukkende anonyme data i opplæringen.
Fysisk sikkerhet og miljøsikkerhet	**Fysisk tilgang til anlegg.** Microsoft begrenser tilgangen til fasiliteter der informasjonssystemer som behandler kundedata eller faglig tjenestedata er lokalisert til identifiserte autoriserte personer. **Fysisk tilgang til komponenter.** Microsoft fører poster over innkommende og utgående medier som inneholder kundedata eller faglig tjenestedata, inkludert typen media, den autoriserte avsenderen / mottakerne, dato og klokkeslett, antall medier og hvilke typer av slike opplysninger de inneholder. **Beskyttelse mot forstyrrelser.** Microsoft bruker en rekke bransjestandardsystemer for å beskytte mot tap av data på grunn av strømforsyningssvikt eller linjeforstyrrelser. **Avhending av komponenter.** Microsoft bruker bransjestandardprosesser for å slette kundedata og faglig tjenestedata når det ikke lenger er behov for det.
Administrasjon av kommunikasjon og drift	**Retningslinjer for drift.** Microsoft opprettholder sikkerhetsdokumenter som beskriver sikkerhetstiltakene og de relevante prosedyrene og ansvarene til personalet som har tilgang til kundedata eller faglig tjenestedata. **Prosedyrer for datagjenoppretting** - Microsoft oppretter kontinuerlig, og aldri med lengre mellomrom enn én gang i uken (med mindre ingen oppdateringer er gjort i løpet av dette tidsrommet), Microsoft oppbevarer flere kopier av kundedata og faglig tjenestedata som slike data kan gjenopprettes fra. - Microsoft lagrer kopier av kundedata og faglig tjenestedata og prosedyrer for datagjenoppretting på et annet sted enn der det primære datautstyret som behandler kundedata og faglig tjenestedata ligger. - Microsoft har spesifikke prosedyrer på plass som regulerer tilgang til kopier av kundedata og faglig tjenestedata. - Microsoft gjennomgår prosedyrer for datagjenoppretting minst hvert halvår, bortsett fra prosedyrer for datagjenoppretting for Faglige Tjenester og Offentlige Azure-tjenester, som gjennomgås hvert år.

Domene	Praksis
	- Microsoft loggfører datagjenopprettingsoperasjoner, inkludert ansvarlig person, en beskrivelse av de gjenopprettede dataene og når det er aktuelt: den ansvarlige personen og hvilke data (om noen) som man har vært nødt til å legge inn manuelt i datagjenopprettingsprosessen. **Skadelig programvare.** Microsoft har kontroller mot skadelig programvare for å unngå at skadelig programvare får uautorisert tilgang til kundedata og faglig tjenestedata, inkludert skadelig programvare som stammer fra offentlige nettverk. **Data utenfor Microsofts lokaler** - Microsoft krypterer, eller gjør det mulig for kunden å kryptere, kundedata og faglig tjenestedata som overføres over offentlige nettverk. - Microsoft begrenser tilgangen til kundedata og faglig tjenestedata i media som forlater fasilitetene. **Loggføring av aktiviteter.** Microsoft logger, eller gjør det mulig for kunden å logge, få tilgang til og bruke informasjonssystemer som inneholder kundedata og faglig tjenestedata, registrere tilgangs-ID, tid, autorisasjon gitt eller avslått, og relevant aktivitet.
Tilgangskontroll	**Retningslinjer for tilgang.** Microsoft fører en oversikt over sikkerhetsrettigheter for personer som har tilgang til kundedata og faglig tjenestedata. **Godkjenning av tilgang** - Microsoft vedlikeholder og oppdaterer en oversikt over personell som er autorisert til å få tilgang til Microsoft-systemer som inneholder kundedata og faglig tjenestedata. - Microsoft deaktiverer autentiseringsinformasjon som ikke har blitt brukt i løpet av en periode for ikke å overstige seks måneder. - Microsoft identifiserer personell som har muligheten til å gi, endre eller trekke tilbake tilgang til data og ressurser. - Microsoft sikrer at der mer enn ett individ har tilgang til systemer som inneholder kundedata eller faglig tjenestedata, og at individene har separate identifikatorer / påloginger. **Minimale rettigheter** - Teknisk støttepersonell har bare tilgang til kundedata og faglig tjenestedata når det er nødvendig. - Microsoft begrenser tilgangen til kundedata og faglig tjenestedata bare til personer som trenger slik tilgang for å utføre sin jobbfunksjon. **Integritet og taushetsplikt** - Microsoft instruerer Microsoft-personell om å deaktivere administrative økter når de forlater Microsofts lokaler, eller når de ellers lar datamaskiner stå uten tilsyn. - Microsoft lagrer passord på en måte som gjør dem uforståelige mens de er i bruk. **Godkjenning** - Microsoft bruker metoder som er i samsvar med bransjestandarder, til å identifisere og godkjenne brukere som prøver å få tilgang til informasjonssystemer. - Der godkjenningsmekanismene er basert på passord, krever Microsoft at passordene fornyes regelmessig. - Der godkjenningsmekanismene er basert på passord, krever Microsoft at passordet skal inneholde minst åtte tegn. - Microsoft sørger for at deaktiverte eller utløpte ID-er ikke blir gitt til andre personer. - Microsoft overvåker, eller gir Kunden muligheten til å overvåke, gjentatte forsøk på å få tilgang til informasjonssystemer med et ugyldig passord. - Microsoft benytter prosedyrer som er i samsvar med bransjestandarder, til å deaktivere passord som har blitt ødelagt eller gjort kjent for andre. - Microsoft bruker metoder for passordbeskyttelse som er i samsvar med bransjestandarder, inkludert metoder som opprettholder passordenes konfidensialitet og integritet når de tildeles og distribueres, og under lagring. **Nettverkets utforming.** Microsoft har kontroller for å unngå at enkeltpersoner antar tilgangsrettigheter de ikke har fått tildelt for å få tilgang til kundedata og faglig tjenestedata de ikke er autorisert til å få tilgang til.

Domene	Praksis
Administrasjon av sikkerhetsbrudd	**Prosess for respons på hendelser** - Microsoft fører et oppdatert register over sikkerhetsbrudd med en beskrivelse av hendelsen, tidsrommet, konsekvensene ved hendelsen, navnet på personen som varslet om hendelsen, navnet på personen som mottok varslet, og metoden for datagjenoppretting. - For hver sikkerhetshendelse som utgjør et Sikkerhetsbrudd, skal Microsoft varsle (som beskrevet i punktet «Varsling om sikkerhetsbrudd» ovenfor) uten ugrunnet opphold og i alle fall innen 72 timer. - Microsoft tracks, eller muliggjør for kunden å spore, fremlegginger av kundedata og faglig tjenestedata, inkludert hvilke data som er blitt fremlagt, til hvem og på hvilket tidspunkt. **Overvåkning av tjenester.** Microsofts sikkerhetspersonell kontrollerer registre minst hver sjette måned og kommer med forbedringsforslag ved behov.
Administrasjon av driftskontinuitet	- Microsoft opprettholder beredskapsplaner og planer for uforutsette hendelser for fasilitetene der Microsoft informasjonssystemer som behandler kundedata eller faglig tjenestedata er lokalisert. - Microsofts overflødige lagring og prosedyrene for å gjenopprette data er designet for å forsøke å rekonstruere kundedata og faglig tjenestedata i sin opprinnelige eller sist kopierte tilstand fra før den gikk tapt eller ble ødelagt.

Innholdsfortegnelse / Generelle vilkår

Tillegg B – Datasubjekter og kategorier av personopplysninger

Datasubjekter: Datasubjekter omfatter kundens representanter og sluttbrukere, herunder kundens ansatte, leverandører samarbeidspartnere og kundens kunder. Datasubjekter kan også omfatte enkeltpersoner som forsøker å kommunisere eller overføre personlige data til brukere av tjenestene som Microsoft leverer. Microsoft erkjenner at, avhengig av kundens bruk av den produktene og tjenestene, kan kunden velge å inkludere personopplysninger fra en av følgende typer registrerte i personopplysninger:

- Ansatte, oppdragstakere og vikarer (nåværende, tidligere, fremtidige) hos kunden;
- Personer som de ovennevnte har omsorg for;
- Kundens samarbeidspartnere/kontaktpersoner (fysiske personer) eller ansatte, oppdragstakere eller vikarer hos samarbeidspartnere/kontaktpersoner (nåværende, fremtidige, tidligere) som er juridiske personer;
- Brukere (f.eks. kunder, klienter, pasienter, besøkende osv.) og andre registrerte som er brukere av kundens tjenester;
- Partnere, interessenter eller enkeltpersoner som aktivt samarbeider, kommuniserer eller på annen måte samhandler med ansatte hos kunden og/eller bruker kommunikasjonsverktøy som apper og nettsteder levert av kunden;
- Interessenter eller enkeltpersoner som passivt samhandler med kunden (f.eks. fordi de er gjenstand for en undersøkelse, forskning eller nevnt i dokumenter eller korrespondanse fra eller til kunden);
- Mindreårige; eller
- Fagpersoner med faglige privilegier (f.eks. leger, advokater, notarer, religiøse arbeidere osv.).

Datakategorier: Overførte personopplysninger som er inkludert i e-post, dokumenter og andre opplysninger i elektronisk form i tilknytning til produkter og tjenester. Microsoft erkjenner at, avhengig av kundens bruk av de produkter og tjenester, kan kunden velge å inkludere personopplysninger fra en av følgende kategorier i personopplysningene:

- Grunnleggende personopplysninger (for eksempel fødselssted, gatenavn og husnummer (adresse), postnummer, bosted, bostedsland, mobiltelefonnummer, fornavn, etternavn, initialer, e-postadresse, kjønn, fødselsdato), inkludert grunnleggende personopplysninger om familiemedlemmer og barn;
- Godkjenningsopplysninger (for eksempel brukernavn, passord eller PIN-kode, sikkerhetsspørsmål, revisjonsspor);
- Kontaktinformasjon (for eksempel adresser, e-postadresser, telefonnummer, identifikatorer for sosiale medier; kontaktinformasjon for nødstilfeller);
- Unike identifikasjonsnummer og signaturer (for eksempel personnummer, bankkontonummer, pass- og ID-kortnummer, førerkortnummer og kjøretøyregistreringsopplysninger, IP-adresser, ansattnummer, studentnummer, pasientnummer, signatur, unik identifikator i sporingskapsler eller lignende teknologi);
- Pseudonyme identifikatorer;
- Økonomiske opplysninger og forsikringsopplysninger (for eksempel forsikringsnummer, bankkontonavn og -nummer, kredittkortnavn og -nummer, fakturanummer, inntekt, type forsikring, betalingsatferd, kredittverdighet);
- Kommersielle opplysninger (for eksempel kjøpshistorikk, spesialtilbud, abonnementsopplysninger, betalingshistorikk);
- Biometriske opplysninger (for eksempel DNA, fingeravtrykk og irisskanninger);
- Posisjonsopplysninger (for eksempel celle-ID, opplysninger om geolokaliseringsnettverk, posisjon ved start av samtale / slutt på samtale. Posisjonsopplysninger utledet fra bruk av Wi-Fi-tilgangspunkter);
- Bilder, video og lyd;
- Internett-aktivitet (for eksempel surfehistorikk, søkehistorikk, lesing, TV-titting, radiolytting);
- Enhetsidentifikasjon (for eksempel IMEI-nummer, SIM-kortnummer, MAC-adresse);
- Profilering (for eksempel basert på observert kriminell eller krenkende atferd eller pseudonyme profiler basert på besøkte nettadresser, klikkstrømmer, surfelogger, IP-adresser, domener, installerte apper eller profiler basert på markedsføringspreferanser);

- Personal- og rekrutteringsopplysninger (for eksempel erklæring om ansettelsesstatus, rekrutteringsinformasjon (for eksempel CV, ansettelseshistorikk, utdanningshistorikk), jobb- og stillingsopplysninger, inkludert arbeidstid, vurderinger og lønn, opplysninger om arbeidstillatelse, tilgjengelighet, ansettelsesvilkår, skatteopplysninger, betalingsopplysninger, forsikringsopplysninger og bosted og organisasjoner);
- Utdanningsopplysninger (for eksempel utdanningshistorikk, nåværende utdanning, grader og resultater, oppnådd høyeste grad, lærevansker);
- Opplysninger om statsborgerskap og bosted (for eksempel statsborgerskap, naturaliseringsstatus, sivilstand, nasjonalitet, innvandringsstatus, passopplysninger, opplysninger om bosted eller arbeidstillatelse);
- Informasjon som behandles for å utføre en oppgave for fellesskapet eller under utøvelse av offisiell myndighet;
- Særlige kategorier opplysninger (for eksempel rasemessig eller etnisk opprinnelse, politiske oppfatninger, religiøs eller filosofisk tro, fagforeningsmedlemskap, genetiske opplysninger, biometriske opplysninger for å identifisere en fysisk person, opplysninger om helse, opplysninger om en fysisk persons sexliv eller seksuell legning eller opplysninger knyttet til straffedom eller lovbrudd); eller
- Andre personopplysninger angitt i artikkel 4 i GDPR.

Tillegg C – tillegg om ekstra sikkerhetstiltak

Med dette tillegget om ekstra sikkerhetstiltak til DPA-en (dette "Tillegget") gir Microsoft ekstra sikkerhetstiltak til kunden eller behandling av personopplysninger, innenfor rammen av GDPR, av Microsoft på vegne av kunden og ytterligere oppreisning til de registrerte som disse personopplysningene gjelder.

Dette tillegget supplerer og er en del av, men ikke en variasjon eller endring av DPA-en.

1. **Bestride pålegg.** I tilfelle av at Microsoft mottar en ordre fra en tredjepart om tvunget avsløring av personopplysninger som behandles i henhold til denne DPA-en, skal Microsoft:

   a. treffe alle rimelige tiltak for å få tredjeparten til å rette forespørselen om disse dataene direkte til Kunden;

   b. straks varsle Kunden, med mindre det er forbudt i henhold til loven som gjelder for den forespørrende tredjepart, og hvis forhindret av lov fra å varsle kunden, treffe alle lovlige tiltak for å oppnå retten til å gi avkall på forbudet for å kommunisere så mye informasjon til Kunden så snart som mulig og

   c. treffe alle lovlige tiltak for å bestride pålegg om fremlegging på bakgrunn av mangler i lovgivningen til den forespørrende parten eller relevante konflikter med lover i EU eller gjeldende lovgivning i medlemsstater.

Hvis, etter trinnene beskrevet i a. gjennom c. ovenfor, forblir Microsoft eller noen av dets tilknyttede selskaper tvunget til å offentliggjøre personopplysninger, Microsoft vil kun avsløre minimumsmengden av disse dataene som er nødvendig for å tilfredsstille bestillingen om tvunget fremlegging.

I dette avsnittet inkluderer ikke lovlige tiltak handlinger som kan føre til sivilrettslig eller strafferettslige sanksjoner, som forakt for retten i henhold til loven i den relevante jurisdiksjonen.

2. **Erstatning til registrerte.** Underlagt punkt 3 og 4 skal Microsoft holde en registrert skadesløs for materielle eller ikke-materielle skader påført den registrerte som følge av Microsofts fremlegging av personopplysninger tilhørende datasubjektet som har blitt overført i til en ordre fra et ikke-EU/EØS-statlig organ eller rettshåndhevelsesbyrå i strid med Microsofts forpliktelser i henhold til kapittel V i GDPR (en "Relevant fremlegging"). Uavhengig av det forestående har ikke Microsoft noen forpliktelse til å holde registrerte under dette punkt 2 skadesløse hvis den registrerte allerede har mottatt kompensasjon for den samme skaden, enten fra Microsoft eller på annen måte.

3. **Vilkår for erstatning.** Erstatning i henhold til punkt 2 er betinget av at den registrerte til Microsofts rimelige tilfredshet dokumenterer at:

   a. Microsoft gjennomførte en Relevant Fremlegging;

   b. den Relevante Fremleggingen var grunnlaget til en offisiell prosedyre av det ikke-EU/EØS statlige organet eller rettshåndhevende organet mot den registrerte; og

   c. den Relevante Fremleggingen forårsaket direkte at den registrerte ble påført materiell eller ikke-materiell skade.

Den registrerte har bevisbyrden med hensyn til vilkår a. til c.

Uavhengig av det forestående har ikke Microsoft noen forpliktelse til å holde registrerte under dette punkt 2 skadesløse hvis Microsoft dokumenterer at den Relevante Fremleggingen ikke var i strid med Microsofts forpliktelser i henhold til kapittel V i GDPR.

4. **Skadeomfang.** Erstatning i henhold til punkt 2 er begrenset til materielle og ikke-materielle skader som beskrevet i GDPR og utelukker følgesskader eller alle andre skader som ikke skyldes Microsofts krenkelse av GDPR.

5. **Utøvelser av rettigheter.** Rettigheter gitt registrerte i henhold dette Tillegget kan fremmes av den registrerte mot Microsoft uavhengig av eventuelle restriksjoner i punkt 3 eller 6 i Standardklausulene. Den registrerte kan bare fremme et krav i henhold til dette Tillegget på individuell basis, og ikke som del av et gruppesøksmål eller representativt søksmål. Rettigheter gitt til registrerte i henhold til dette Tillegget er personlige for de registrerte og kan ikke overdras.

6. **Varsling om endring.** I tillegg til punkt 2021(b) i Standardklausulene samtykker og garanterer Microsoft at Microsoft ikke har noen grunn til å tro at lovgivningen som gjelder for Microsoft eller Microsofts underbehandlere, inkludert i alle land som personopplysninger overføres til, enten av Microsoft selv eller en underbehandler, forhindrer Microsoft fra å oppfylle instruksjonene mottatt fra kunden og forpliktelsene i henhold til dette Tillegget eller 2021 Standardklausulene, og at hvis en endring i denne lovgivningen som med sannsynlighet vil ha en betydelig negativ påvirkning på garantiene og forpliktelsene gitt i dette Tillegget eller Standardklausulene, vil Microsoft straks varsle kunden om endringen så snart Microsoft blir oppmerksomme på den, i så tilfellet har kunden rett til å avbryte overføringen av data og/eller oppheve kontrakten.

Vedlegg 1 – Vilkår i EUs personvernforordning (GDPR)

Microsofts forpliktelser i disse GDPR-vilkårene til alle kunder trer i kraft 25. mai 2018. Disse forpliktelsene er bindende for Microsoft med hensyn til kunden uavhengig av (1) versjonen av produktvilkårene og DPA-en som på annen måte gjelder for et abonnement på enhver gitt produktbeskrivelse eller lisens, eller (2) andre avtaler som henviser til dette vedlegget.

I forbindelse med disse GDPR-vilkårene samtykker Kunden og Microsoft i at Kunden er behandlingsansvarlig for Personopplysninger, og at Microsoft er databehandler for slike opplysninger, unntatt når kunden fungerer som databehandler for Personopplysningene – i så tilfelle er Microsoft en underdatabehandler. Disse GDPR-Vilkårene gjelder behandling av Personlige Data innenfor rammene av GDPR, utført av Microsoft på vegne av Kunden. Disse GDPR-vilkårene begrenser ikke eller reduserer forpliktelser til databeskyttelse som Microsoft gjør overfor kunden i produktvilkårene, eller noen annen avtale mellom Microsoft og kunden. Disse GDPR-vilkårene gjelder ikke når Microsoft er en behandlingsansvarlig for Personopplysninger.

Relevante GDPR-forpliktelser: Artikkel 5, 28, 32 og 33

1. Microsoft støtter Kundens ansvarsforpliktelser via denne DPA-en og produktdokumentasjonen gitt til Kunden, og vil fortsette å gjøre det i løpet av perioden for kundens abonnement eller gjeldende engasjement for Faglige Tjenester i henhold til underpunkt 3(h) nedenfor. (Artikkel 5(2))

2. Microsoft skal ikke engasjere en annen databehandler uten spesifikk eller generell skriftlig tillatelse fra Kunden. I tilfeller med generelt skriftlig samtykke skal Microsoft informere Kunden om de planlagte endringene med hensyn til anskaffelse eller utskiftning av andre behandlere, slik at Kunden får anledning til å komme med innsigelser til de aktuelle endringene. (Artikkel 28 nr. 2)

3. Microsofts behandling skal være underlagt disse GDPR-vilkårene i henhold til EU-retten (heretter «Unionsretten») eller Medlemsstatenes nasjonale rett, og de er bindende for Microsoft overfor Kunden. Gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger, kategoriene av registrerte samt Kundens rettigheter og plikter er fastsatt i Kundens lisensavtale, inkludert disse GDPR-vilkårene. Nærmere bestemt skal Microsoft:

- **(a)** bare behandle de Personopplysningene etter dokumenterte instrukser fra Kunden, også med hensyn til overføring av Personopplysninger til et tredje land eller en internasjonal organisasjon, med mindre det kreves av lover i EU eller et Medlemsland som Microsoft er underlagt – i så tilfelle skal Microsoft informere Kunden om dette juridiske kravet før behandlingen, med mindre de aktuelle lovene forbyr slik informasjon på grunn av offentlig interesse,
- **(b)** sikre at personer som er autorisert til å behandle Personopplysninger, har godtatt å være underlagt taushetsplikt eller har lovmessig pålagt taushetsplikt,
- **(c)** iverksette alle tiltak som kreves i henhold til artikkel 32 i GDPR,
- **(d)** rette seg etter vilkårene for engasjering av andre databehandlere i avsnitt 1 og 3,
- **(e)** behandlingens natur tatt i betraktning, bistå Kunden med aktuelle tekniske og organisatoriske tiltak i den grad dette er mulig, for at Kunden skal kunne oppfylle sin forpliktelse til å svare på forespørsler der registrerte ønsker å benytte rettighetene de har i henhold til Kapittel III i GDPR,
- **(f)** bistå Kunden i å sikre overholdelse av forpliktelsene som følger av artikkel 32 til 36 i GDPR, tatt i betraktning behandlingens natur og informasjonen som er tilgjengelig for Microsoft,
- **(g)** etter kundens valg slette eller returnere alle Personopplysninger til Kunden etter å ha levert tjenestene knyttet til behandlingen, og slette eksisterende kopier med mindre lovene i EU eller et Medlemsland krever at de Personopplysningene lagres,
- **(h)** gjøre tilgjengelig for Kunden all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i artikkel 28 i GDPR er oppfylt, samt muliggjøre og bidra til revisjoner, inkludert inspeksjoner, som gjennomføres av Kunden eller en annen inspektør på fullmakt fra Kunden.

Microsoft skal øyeblikkelig informere Kunden hvis en instruks bryter med GDPR eller andre bestemmelser om vern av personopplysninger i Unionsretten eller Medlemsstatenes nasjonale rett. (Artikkel 28 nr. 3)

4. Dersom Microsoft engasjerer en annen databehandler for å utføre spesifikke behandlingsaktiviteter på vegne av Kunden, skal denne andre databehandleren pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i disse GDPR-vilkårene, ved hjelp av en avtale eller et annet rettslig dokument i henhold til Unionsretten eller Medlemsstatens nasjonale rett, der det særlig gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i GDPR. I tilfeller der den andre databehandleren ikke oppfyller personvernforpliktelsene sine, skal Microsoft fortsatt bære hele erstatningsansvaret overfor Kunden for oppfyllelsen av den andre databehandlerens forpliktelser. (Artikkel 28 nr. 4)

5. Tatt i betraktning den tekniske utviklingen, kostnadene ved implementering og behandlingens natur, omfang, kontekst og formål så vel som risiko av varierende sannsynlighet og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal Kunden og Microsoft treffe passende tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som står i forhold til risikoen, blant annet følgende:

(a) Personopplysninger må gjøres pseudonyme og krypteres,

(b) Systemers og tjenesters konfidensialitet, integritet, tilgjengelighet og motstandsdyktighet må være kontinuerlig sikret,

(c) evnen til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,

(d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er. (Artikkel 32 nr. 1)

6. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til Personopplysninger som er overført, lagret eller på annen måte behandlet. (Artikkel 32 nr. 2)

7. Kunden og Microsoft skal treffe tiltak for å sikre at enhver fysisk person som handler for Kunden eller Microsoft, og som har tilgang til Personopplysninger, behandler slike Personopplysninger bare etter instruks fra Kunden, med mindre Unionsretten eller Medlemsstatenes nasjonale rett krever at vedkommende gjør dette. (Artikkel 32 nr. 4)

8. Etter å ha fått kjennskap til et brudd på personopplysningssikkerheten skal Microsoft uten ugrunnet opphold underrette Kunden. (Artikkel 33 nr. 2). Slik varsling skal omfatte den informasjonen som en databehandler etter artikkel 33 nr. 3 har plikt til å oppgi, i den grad slik informasjon er rimelig tilgjengelig for Microsoft.

Innholdsfortegnelse / Generelle vilkår