IVANTI DATABEHANDLERAVTALE

Ivanti Databehandleravtale (DPA) utgjør en del av Ivanti sluttbrukerlisens- og tjenesteavtale (Avtalen) og er laget og inngått fra den siste signaturdatoen nedenfor (Ikrafttredelsesdatoen), av og mellom kunden, som er identifisert nedenfor eller i avtalen (som Kontrollør) og gjeldende Ivanti-enheten identifisert i denne DPA (som Ivanti eller Behandler) (individuelt som en Part eller samlet som Partene). Alle termer med stor forbokstav som ikke er definert her, skal ha de respektive betydningene gitt til dem i Avtalen.

INNLEDNINGSAVSNITT

Partene som har inngått avtalen.

Under levering av Tjenestene til Kontrolløren, i henhold til avtalen, kan Behandleren behandle personopplysninger på vegne av Kontrolløren,

For å sørge for tilstrekkelige sikkerhetstiltak med hensyn til Behandling av personopplysninger, som er gitt av Kontrolløren til Behandleren, er partene enige om å overholde følgende bestemmelser med hensyn til personopplysninger, begge parter i innenfor rimeligheten og i god tro.

I betraktning av de foregående premissene og de gjensidige løftene og paktene som er angitt nedenfor, samtykker Kontrolløren og Behandleren i følgende:

AVTALE

1. DEFINISJONER

Alle termer med stor forbokstav som ikke er definert her, skal ha betydningen som framgår i Avtalen.

"Tilknyttet selskap" vil si alle enheter som direkte eller indirekte kontrollerer, er kontrollert av eller er under felles kontroll av den aktuelle enheten. "Kontroll" betyr i denne definisjonen direkte eller indirekte eierskap eller kontroll over mer enn 50 % av stemmeinteressene til den aktuelle enheten.

"**Gjeldende databeskyttelseslover**" vil si alle gjeldende lover, forskrifter, regulatoriske veiledninger eller krav i alle jurisdiksjoner tilknyttet databeskyttelse, personvern eller konfidensialitet av personopplysninger, inkludert men ikke begrenset til (a) GDPR sammen med eventuell transponering, implementerings- eller tilleggslovgivning og (b) CCPA.

"**Autoriserte tilknyttede selskaper**" vil si alle Kontrollørers tilknyttede selskaper som (a) er underlagt databeskyttelseslover og -forskrifter i Det europeiske økonomiske samarbeidsområde (EØS) og/eller dets medlemsland, Storbritannia og Sveits, (b) er underlagt databeskyttelseslover og -forskrifter utenfor EØS og/eller dets medlemsland, Sveits og Storbritannia (der det er aktuelt) og (c) tillatelse til å bruke Behandleren for behandling i henhold til Avtalen.

"CCPA" betyr California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* og dets implementerende forskrifter.

"Kontrollør" vil si enheten som bestemmer formålene og midlene for behandlingen av personopplysninger. For å unngå tvil er parten identifisert ovenfor som Kontrollør, en Kontrollør i samsvar med denne DPA.

"Databrudd" vil si et sikkerhetsbrudd som fører til utilsiktet, uautorisert eller ulovlig ødeleggelse, tap, endring, utlevering, tilgang eller annen behandling av personopplysninger som overføres, lagres eller på annen måte behandles.

"Datatilsyn" vil si alle representanter eller agenter som representerer en statlig enhet eller etat som har myndighet til å håndheve gjeldende databeskyttelseslover.

"Den registrerte" vil si en fysisk person som personopplysningene omhandler.

"GDPR" vil si EUs personvernforordning 2016/679 av 27. april 2016 om beskyttelse av fysiske personer med hensyn til behandling av personopplysninger og om fri flyt av slike data, og opphever direktiv 95/46/EF (GDPR).

"Ivanti" vil si enheten identifisert nedenfor i samme geografiske region som kunden:

- Ivanti, Inc., et Delaware-selskap, i Amerika, unntatt Brasil.
- Ivanti Comércio de Software Brasil Ltda, et brasiliansk selskap, i Brasil.
- Ivanti Software K.K., et japansk selskap, i Japan.
- Ivanti Software Technology (Beijing) Co., Ltd., et kinesisk selskap, i Kina.
- Ivanti International Limited, et irsk selskap, for Wavelink- og Naurtech-merkede produkter og tjenester i Europa, Midtøsten, Afrika og Asia-Stillehavsregionen.
- Ivanti UK Limited, et aksjeselskap registrert i England og Wales, for alle andre steder.

"Personopplysninger" vil si all informasjon som identifiserer, er relaterer til, beskriver, er tilknyttet til eller med rimelighet kan knyttes direkte eller indirekte til en identifisert eller identifiserbar fysisk person eller bestemt husholdning. En identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved henvisning til en identifikasjon som et navn, identifikasjonsnummer, stedsdata, en nettbasert identifikasjon eller med én eller flere faktorer som er spesifikke for den fysiske personens fysiske, fysiologiske, genetiske, mentale, økonomiske, kulturelle eller sosiale identitet.

"Behandling" vil si alle handlinger som utføres vedrørende personopplysningene eller i forbindelse med og med det formål å levere tjenester, enten de utføres med automatiske midler, for eksempel innsamling, registrering, organisering, lagring, tilpasning eller endring, henting, konsultasjon, bruk, utlevering ved overføring, formidling eller på annen måte tilgjengeliggjøring, justering, blokkering, sletting eller ødeleggelse, og som definert av gjeldende databeskyttelseslover.

"Behandler" vil si enheten som behandler personopplysninger på vegne av Kontrolløren. For å unngå tvil er den parten som er identifisert som "behandler" ovenfor, en behandler for denne DPA.

"Tjenester" vil si behandling av personopplysninger av Behandleren i forbindelse med og med det formål å levere Behandlerens tjenester i henhold til Avtalen.

"Tjenesteleverandør" vil si et enkeltpersonforetak, partnerskap, aksjeselskap, organisasjon eller annen juridisk enhet som er organisert eller driftes for profitt eller økonomisk omsetning for sine aksjonærer eller andre eiere som behandler informasjon på vegne av en Datakontrollør og der Datakontrolløren avslører en registrerts personopplysninger for et forretningsformål i henhold til en skriftlig kontrakt, forutsatt at kontrakten forbyr tjenesteleverandøren å beholde, bruke eller utlevere personopplysningene til andre formål enn det som er spesifisert i kontrakten, eller som på annen måte er tillatt av CCPA. Dette inkluderer å beholde, bruke eller avsløre personopplysninger for et kommersielt formål, annet enn å tilby tjenestene spesifisert i kontrakten med Datakontrolløren. Begrepene "forretningsformål" og "kommersielt formål" har samme betydning som disse begrepene i CCPA. For å unngå tvil er Behandleren en tjenesteleverandør.

“Underbehandler” vil si enheten som behandler personopplysninger på vegne av behandleren.

2. BEHANDLING AV PERSONOPPLYSNINGER

2.1 Partenes roller. Partene erkjenner og samtykker i at behandlingsansvarlig er behandlingsansvarlig for behandling av personopplysninger, behandler er behandler eller tjenesteleverandør. Emnet, varigheten, behandlingsformålet, og hva slags personopplysninger og datasubjektkategorier som behandles i henhold til denne DPA er nærmere spesifisert i vedlegg 1.

2.2 Kontrollørens forpliktelser. Kontrollørens instrukser for behandling av personopplysninger skal være i samsvar med personvernlover og -forskrifter. Kontrolløren skal ha eneansvar for personopplysningenes nøyaktighet, kvalitet og lovlighet samt måten Kontrolløren innhenter personopplysninger på og gir dem videre til Behandleren.

2.3 Behandlerens forpliktelser. Alle personopplysninger som behandles av Behandleren i samsvar med Avtalen er konfidensiell informasjon og Behandleren vil behandle personopplysninger kun i henhold til Kontrollørens dokumenterte instruksjoner, angitt i vedlegg 1 eller på annen måte gitt skriftlig av Kontrolløren. Behandler skal ikke selge personopplysningene som er underlagt denne DPA og skal ikke oppbevare, bruke eller utlevere personopplysninger utenfor det direkte forretningsforholdet mellom Behandleren og Kontrolløren. Behandleren skal overholde alle gjeldende databeskyttelseslover under behandling av personopplysninger. Behandleren vil ikke kombinere personopplysninger fra Kontrolløren med personopplysninger som mottas fra andre kilder. I de tilfeller der Behandleren mener at Kontrollørens instruksjonsoverholdelse vil føre til brudd på gjeldende databeskyttelseslover, skal Behandleren varsle Kontrolløren skriftlig om dette, uten forsinkelse. Behandleren skal gjøre tilgjengelig all informasjon som er nødvendig for å vise Behandlerens overholdelse av sine forpliktelser overfor Kontrolløren, i henhold til denne DPA.

2.3.1. Krav til assistanse. Behandleren skal bistå Kontrolløren med dette: overholdelse av gjeldende databeskyttelseslover, mistenkte og relevante databrudd, henvendelser til eller fra et datatilsyn, henvendelser til og fra de registrerte, og Kontrollørens plikt til å gjennomføre konsekvensvurderinger av databeskyttelse og forutgående konsultasjoner med et datatilsyn.

3. VARSLINGSPLIKT

3.1 Behandlerens varslingsplikter. Behandleren skal umiddelbart varsle Kontrolløren skriftlig om følgende:

3.1.1 Den registrertes forespørsel om å utøve sine personvernrettigheter, som å få tilgang til, korrigere, slette, transportere, protestere mot eller begrense egne personopplysninger,

3.1.2 Alle forespørsler eller klager mottatt fra Kontrollørens kunder eller ansatte,

3.1.3 Eventuelle spørsmål, klager, etterforskning eller andre henvendelser fra et datatilsyn,

3.1.4 Alle forespørsler om utlevering av personopplysninger som på noen måte er relatert til Behandlerens behandling av personopplysninger under denne DPA,

3.1.5 Et databrudd i henhold til varslingspliktene angitt i avsnitt 7.1, og

3.1.6 I de tilfeller der personopplysningene blir gjenstand for ransakelse, beslagleggelse, inndragning som følge av konkurs- eller insolvensbehandling eller lignende hendelser eller tiltak fra tredjeparter mens de behandles.

Behandleren vil bistå Kontrolløren med å oppfylle Kontrollørens forpliktelser til å svare på forespørsler knyttet til paragrafene (3.1.1) - (3.1.6) ovenfor og skal ikke svare på slike forespørsler uten Kontrollørens skriftlige forhåndssamtykke, med mindre Behandleren er lovpålagt til å svare.

4. KONFIDENSIALITET

4.1 Konfidensiell informasjon. All informasjon som er gitt til Kontrolløren, i samsvar med avtalen, er konfidensiell informasjon.

4.2 Behandlerens ansatte. Behandler skal sørge for at de ansatte, som er involvert i behandlingen av personopplysninger, er informert om personopplysningens konfidensielle karakter og har fått passende opplæring om relevant ansvar og har inngått skriftlige konfidensialitetsavtaler. Behandleren skal sørge for at slike konfidensialitetsforpliktelser fortsetter etter oppsigelsen av de respektive arbeidsforholdene.

4.3 Tilgangsbegrensning. Behandleren skal sørge for at Behandlerens tilgang til personopplysningene er begrenset til de ansatte som utfører Tjenestene, i henhold til Avtalen.

5. UNDERBEHANDLERE

5.1 Utnevnelse av Underbehandlere. Kontrolløren erkjenner og godtar at Behandleren og Behandlerens tilknyttede selskaper kan engasjere tredjeparts Underbehandlere i forbindelse med levering av Tjenestene. Behandleren eller Behandlerens Tilknyttede selskaper skal inngå en skriftlig avtale med hver Underbehandler som inneholder databeskyttelsesforpliktelser, som ikke gir mindre beskyttelse enn det som er nevnt i denne DPA, i den grad det er relevant den type Tjenester som leveres av Underbehandleren. Kontrolløren autoriserer herved Behandleren til å involvere den nåværende listen over underbehandlere, som er oppført på https://www.ivanti.com/company/legal/ivanti-subprocessors, for å behandle personopplysningene i samsvar med denne DPA. Kontrolløren skal ikke kommunisere direkte med Behandlerens Underbehandlere om Tjenestene, med mindre Behandleren samtykker i dette, etter Behandlerens eget skjønn.

5.2 Varsling om endringer vedrørende Underbehandlere. Behandleren skal informere Kontrolløren om eventuelle tiltenkte endringer angående tillegg eller erstatning av Underbehandlere ved å gi Kontrolløren en mulighet til å abonnere på varsler fra nye Underbehandlere her: https://www.ivanti.com/company/legal/ivanti-subprocessors. Behandleren skal varsle Kontrolløren om eventuelle tiltenkte endringer angående tillegg eller erstatning av Underbehandlere før Behandleren bruker Underbehandleren.

5.3 Innsigelsesrett for nye Underbehandlere. Kontrolløren kan med rimelighet protestere mot Behandlerens bruk av en ny Underbehandler ved å varsle Behandleren umiddelbart skriftlig innen femten (15) virkedager etter mottak av Behandlerens varsel. Hvis Kontrolløren protesterer mot en ny Underbehandler skal Behandleren anstrenge seg, på rimelig måte, for at Kontrolløren har tilgang til endringer i tjenestene, slik at man unngår at den nye Underbehandleren behandler personopplysninger. Hvis Behandleren ikke er i stand til å gjøre slik endring tilgjengelig, kan Kontrolløren si opp den gjeldende Avtalen med hensyn til de Tjenestene som ikke kan leveres av Behandleren uten bruk av den nye Underbehandleren som det er en innsigelse mot.

5.4 Ansvar for Underbehandlers handlinger. Behandler er ansvarlig for handlingene og unnlatelsene til Underbehandlerne, i samme grad som Behandleren ville være ansvarlig hvis de selv utfører tjenestene, i henhold til vilkårene i denne DPA.

6. SIKKERHET

6.1 Beskyttelse av personopplysninger. Behandler skal opprettholde passende tekniske og organisatoriske tiltak for sikkerhetsbeskyttelse (det omfatter også beskyttelse mot uautorisert eller ulovlig behandling og mot utilsiktet eller ulovlig ødeleggelse, tap eller endring eller skade, uautorisert utlevering av eller tilgang til personopplysninger), konfidensialitet og integritet av personopplysninger.

6.2 Kontrolleringsrettigheter. Kontrolløren aksepterer retten til å kontrollere Behandleren og kan be om at Behandleren viser frem oppdaterte attester, rapporter eller utdrag fra uavhengige organer, inkludert, uten begrensning, eksterne eller interne revisorer, Behandlerens databeskyttelsesansvarlig, IT-sikkerhetsavdelingen, databeskyttelses- eller kvalitetsrevisorer eller annen gjensidig avtalt tredjepart eller sertifisering i form av en IT-sikkerhets- eller databeskyttelsesrevisjon. I den grad det ikke er mulig å oppfylle en kontrolleringsplikt, som er pålagt av gjeldende databeskyttelseslover og -forskrifter, gjennom slike attester, rapporter eller utdrag, har Kontrolløren, eller den som er utpekt av Kontrolløren, rett til å kontrollere og inspisere – for Kontrollørens regning – Behandlerens lokaler , retningslinjer, prosedyrer og datastyrte systemer for å sørge for at Behandleren overholder kravene i denne DPA. Kontrolløren eller den som er utpekt av Kontrolløren, skal gi minst tretti (30) dagers varsel før en kontroll utføres, med mindre kontrollen er nødvendig grunnet et databrudd som involverer Behandleren. Kontroller utført av Kontrolløren eller den som er utnevnt av Kontrolløren, skal ikke bryte Behandlerens taushetsplikt i forhold til Kontrollørens andre kunder. Alle kontroller vil bli utført i løpet av normal arbeidstid, på Behandlerens hovedkontor eller andre steder der Behandleren befinner seg, der det er mulig å få tilgang til, behandle og administrere personopplysninger og skal ikke forstyrre Behandlerens daglige drift på en urimelig måte. Før en slik kontroll starter skal Behandleren og Kontrolløren bli enige om kontrollens tidspunkt, omfang og varighet. Kontrolløren kan be om oppsummerende revisjonsrapport(er) eller kontrollere Behandleren ikke mer enn én gang i året.

7. DATABRUDD

7.1 Varsling om databrudd. Behandleren skal varsle Kontrolløren skriftlig, uten unødig forsinkelse, etter å ha blitt oppmerksom på et antatt databrudd. Et slikt varsel skal ikke under noen omstendigheter gis senere enn 72 timer etter at Behandleren har oppdaget databruddet.

7.2 Håndtering av databrudd. Behandleren skal anstrenge seg, innenfor rimelige grenser, for å identifisere årsaken til et slikt databrudd og utføre de tiltakene som Kontrolløren anser som nødvendige og rimelige for å rette opp årsaken til et slikt databrudd, i den grad tiltakene er innenfor Kontrollørens rimelige kontroll.

8. OPPSIGELSE

8.1 Oppsigelse. Denne DPA skal avsluttes automatisk ved (a) oppsigelse eller utløp av Avtalen eller (b) Kontrollørens sletting eller retur av personopplysningene. Kontrolløren skal videre ha rett til å si opp denne DPA dersom Behandleren, etter Kontrollørens oppfatning, vesentlig bryter denne DPA. Hvis bruddet kan omgjøres, skal dette omgjøres innen ti (10) dager fra datoen Kontrolløren ble varslet av Behandleren og datoen Behandleren identifiserte bruddet og ber om å få rettet det opp.

8.2 Retur eller sletting av data. Ved oppsigelse av denne DPA, vil Behandleren slette eller returnere alle eksisterende kopier av personopplysninger, med mindre gjeldende lov fortsatt krever at personopplysningene oppbevares. På forespørsel fra Kontrolløren skal Behandleren bekrefte overholdelse av slike forpliktelser, skriftlig og slette alle eksisterende kopier. Hvis lokale lover krever at Behandleren skal oppbevare personopplysninger, skal Behandleren beskytte personopplysningenes konfidensialitet, integritet og tilgjengelighet og skal ikke lenger aktivt behandle personopplysningene samt fortsette å overholde vilkårene i denne DPA.

9. MEKANISMER FOR INTERNASJONALE OVERFØRINGER

9.1 Overføringer utenfor EU/Storbritannia/Sveits til et land med en adekvansbeslutning. Databehandler skal forholde seg til en adekvathetsbeslutning for å overføre personopplysninger når en slik adekvathetsbeslutning er gitt i henhold til gjeldende personvernlover For å unngå tvil, hvis databehandleren er sertifisert i henhold til Data Privacy Framework-programmet (rammeverk for overføring av personopplysninger), gitt av kommisjonens gjennomføringsbeslutning av 10.7.2023 med hensyn til et tilfredsstillende beskyttelsesnivå for personopplysninger under EU-US Data Privacy Framework («DPF»), skal DPF gjelde og erstatte gjeldende overføringsmekanismer angitt i avsnitt 9.2 i denne DPA som en gyldig overføringsmekanisme for personopplysninger overført til USA.

9.2 Overføringer utenfor EU/Storbritannia/Sveits til et land uten en adekvansbeslutning. Under leveringen av tjenester i henhold DPA, kan det være nødvendig for behandlingsansvarlig å overføre personopplysninger fra EU, EØS og/eller deres medlemsland, Sveits eller Storbritannia, til en databehandler i et land som ikke har en adekvathetsbeslutning eller som ikke er lokalisert i EØS.

9.2.1. I forhold til personopplysninger som er underlagt GDPR (i) skal Behandleren bli ansett som "dataimportør" og Kontrolløren "dataeksportør", (ii) Modul to-vilkårene skal gjelde der Kontrolløren er en Datakontrollør og der Behandleren er en Databehandler, (iii) i klausul 7 skal den valgfrie inntredelsesklausulen slettes, (iv) i klausul 9 i modul to, skal alternativ 2 gjelde og listen over underbehandlere og tidsperiode for endringsvarsler skal være som avtalt i avsnitt 5 i denne DPA. (v) I klausul 11 skal det valgfrie språket slettes, (vi) i klausul 17 skal alternativ 1 gjelde og standardkontraktsklausulene skal styres av medlemsstaten der Kontrolløren er hjemmehørende, (vii) i klausul 18(b) skal tvister løses i domstolene i medlemsstaten der Kontrolløren er hjemmehørende, (viii) vedlegg I og vedlegg II skal anses som utfylt med informasjonen angitt i henholdsvis vedlegg 1 i denne DPA, og (ix) hvis standardkontraktsklausulene er i konflikt med bestemmelser i Avtalen (inkludert denne DPA), skal standardkontraktsklausulene ha forrang. For denne delen er standardkontraktsklausulene fra Kommisjonens implementeringsbeslutning (EU) 2021/914 innlemmet ved referanse og er tilgjengelig her: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

9.2.2. I forhold til personopplysninger som er underlagt britiske databeskyttelseslover, skal Den internasjonale dataoverføringsavtalen (IDTA) gjelde med følgende endringer: (i) kontaktinformasjonen for partene i avtalen er kontaktinformasjonen for IDTA, (ii) Kontrolløren er dataeksportøren og Behandleren er dataimportøren, (iii) lovene som styrer IDTA og stedet der juridiske krav kan fremsettes er England og Wales, (iv) Storbritannias GDPR gjelder ikke for dataimportørens behandling av overførte data, (v) Partene skal ikke ta i bruk tilleggssikkerhets- eller -kommersielle klausuler fra IDTA og (vi) informasjonen i denne DPA og vedlegg 1 kan brukes for tabellene 1-4. For denne delen er standardkontraktsklausulene fra Information Commissioner's Office innlemmet ved referanse og er tilgjengelig her: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

9.2.3. I forhold til personopplysninger som er underlagt den sveitsiske DPA, skal standardkontraktsklausulene som det er referert til i del 9.1.1 gjelde med følgende modifikasjoner (i) referanser til "Forordning (EU) 2016/679" skal tolkes som referanser til sveitsisk DPA, (ii) henvisninger til "EU", "union" og "medlemsstatslov" skal tolkes som henvisninger til sveitsisk lov, og (iii) referanser til "kompetent tilsynsmyndighet" og "kompetente domstoler" skal erstattes med "den sveitsiske føderale databeskyttelses- og informasjonskommissæren" og de "relevante domstolene i Sveits".

9.3. Alternative overføringsmekanismer. Partene erkjenner at lover, regler og forskrifter knyttet til internasjonale overføringer av personopplysninger utvikler seg raskt. Dersom behandlingsansvarlig tar i bruk en annen mekanisme autorisert av gjeldende lover, regler eller forskrifter til overføring av personopplysninger (hver en «alternativ overføringsmekanisme»), er partene enige om å samarbeide i god tro for å implementere eventuelle endringer i denne DPA nødvendig for å implementere den alternative overføringsmekanismen av personopplysninger.

10. DIVERSE BESTEMMELSER

10.1. Endringer. Denne DPA kan ikke endres og det kan ikke legges noe til, og ingen av bestemmelsene i DPA skal anses for å være fraveket eller på annen måte endret, unntatt gjennom et skriftlig dokument utarbeidet av autoriserte representanter for begge parter.

10.2 Gjeldende lov. Denne DPA skal styres av gjeldende lover angitt i Avtalen.

TIL BEVIS DERE har partene i denne Avtalen utført denne avtalen fra ikrafttredelsesdatoen.

KONTROLLØR:_____	**IVANTI**
Signatur: _____	Signatur: _____
Navn: _____	Navn: _____
Tittel: _____	Tittel: _____
Dato: _____	Dato: _____

Liste over tidsplaner:

Tidsplan 1: Beskrivelse av behandlingen

IVANTI DATABEHANDLERAVTALE

TIDSPLAN 1

Beskrivelse av behandlingen

Ivantis kontaktinformasjon:

Ivanti

10377 South Jordan Gateway
Suite 110
South Jordan, Utah 84095

DPO-kontakt: privacy@ivanti.com

Emne
Behandlingens emne:
Levering av IT-programvarelisenser, støttetjenester og implementering, enten på stedet eller som en vertsbasert SaaS-løsning, vedrørende administrering og tilrettelegging av viktige forretningsprosesser i feltet av enhetlig endepunktadministrering, IT-tjenesteadministrering, IT-administrering av eiendeler, sikkerhet, rapportering og analyser samt forsyningskjede.

IT-tjenester inkluderer bruk av programvare som en lokal installasjon eller en SaaS-løsning, inkludert installasjon av moduler (inkludert og uten begrensning, hendelser, endringer, eiendeler, konfigurasjon og utgivelse av administrasjonsmoduler); selvbetjenings- og servicekataloger, støtte og vedlikehold inkludert, uten begrensning, ekstern tilgang og oppdateringer, appkontroll, endepunkt/mobilsikkerhet og rettighetsadministrasjon.

Behandlingsfrekvens:
Kontinuerlig.

Varighet
Behandlingsvarighet:
Som angitt i Avtalen.

Omfang, type og formål med behandlingen
Omfang, type og formål med behandlingen er som følger:
Som angitt i Avtalen.

Datasubjekter
Behandling av personopplysninger kan knyttes til følgende datasubjektkategorier:
Kunder, prospekter, ansatte, leverandører, kommersielle representanter, kontakter, entreprenører (inkludert beredskapsarbeidere), frivillige, midlertidige og tilfeldige ansatte, frilansere, agenter, konsulenter og andre profesjonelle respondenter, og deres respektive pårørende, begunstigede og nødkontakter, kunders fremtidige og midlertidig ansatte, klagere, korrespondenter og etterforskere, rådgivere, konsulenter og andre profesjonelle eksperter, dataeksportørens ansatte eller kontaktpersoner samt prospekter, kunder, forretningspartnere og leverandører, forretningspartnere og leverandører av dataeksporter (som er fysiske personer), og dataeksportørens brukere som er autorisert av dataeksportøren til å bruke programvaren og relaterte tjenester.

Datakategorier
Personopplysningene som behandles kan gjelde følgende datakategorier:
Kundedata som er lastet opp til Tjenestene, under Kundens tjenester og kontoer.

Tekniske og organisatoriske tiltak
Følgende beskriver de tekniske og organisatoriske sikkerhetstiltakene som er implementert av Behandleren:

Sikkerhetsopplæring

Behandleren går gjennom sikkerhetsopplæring, dette inkluderer obligatorisk sikkerhetsopplæring om håndtering og sikring av konfidensiell og sensitiv informasjon, som personlig identifiserbar informasjon, finanskontoinformasjon og helseinformasjon, i samsvar med gjeldende lov og periodisk sikkerhetskommunikasjon samt sikkerhetskurs som fokuserer på sluttbrukerbevissthet.

Retningslinjer for sikkerhet og sikkerhetsprosedyrer
Behandleren har retningslinjer for informasjonssikkerhet, bruk og administrasjon som dikterer de ansattes og kontraktørers handlinger om hensiktsmessig bruk, tilgang og lagring av konfidensiell og sensitiv informasjon, begrensning av Behandlerens ansattes tilgang til konfidensiell og sensitiv informasjon som har kun har "behov-for-å-vite" slik informasjon, forhindre oppsagte ansatte fra å få tilgang til Behandlerens informasjon etter oppsigelse og pålegge disiplinære tiltak for manglende overholdelse av slike retningslinjer. Systemtilgang til Behandlerens ressurser er nektet med mindre det er spesifikt vurdert og tilgangen er gitt. Behandleren utfører bakgrunnssjekker av sine ansatte ved ansettelse, slik det er tillatt i loven.

Fysiske og miljømessige tilgangskontroller
Behandleren begrenser fysisk tilgang til informasjonssystemer og fasiliteter ved hjelp av fysiske kontroller (f.eks. kodet passtilgang) som sørger for, på en rimelig måte, at tilgangen til datasentrene er begrenset til autoriserte personer og skal bruke kamera- eller videoovervåkingssystemer ved kritiske interne og eksterne inngangspunkter. Behandleren bruker lufttemperatur- og fuktighetskontroller for datasentrene sine og beskytter mot tap grunnet strømbrudd.

Logiske tilgangskontroller
Behandleren bruker logg- og overvåkingsteknologi for å oppdage samt forhindre uautoriserte tilgangsforsøk til nettverkene og produksjonssystemene. Behandlerens overvåking omfatter en gjennomgang av endringer som påvirker systemenes håndtering av autentisering, autorisasjon og kontroll, privilegert tilgang til Behandlerens produksjonssystemer.

Krypteringskontroller
Behandleren bruker forretningstilpassede krypteringskontroller på tvers av alle produktene våre. Behandleren evaluerer og bruker transitt- og inaktiv kryptering ved å bruke industriens beste praksis for chiffrering. Beste praksis brukes for livssyklusadministrasjon av krypteringsnøkler, inkludert generering, lagring, tilgangskontroll og rotasjon.

Sårbarhetsadministrasjon
Behandleren utfører regelmessig sårbarhetsskanninger og tar hånd om oppdagede sårbarheter, i samsvar med risikoen de utgjør. Behandlingsprodukter er også gjenstand for periodisk sårbarhetsvurdering og penetrasjonstesting.

Nødgjenoppretting og sikkerhetskopikontroller
Behandleren utfører periodiske sikkerhetskopier av produksjonsfilsystemene og databasene, i henhold til en definert tidsplan og opprettholder en formell nødgjenopprettingsplan for det skybaserte produksjonsdatasenteret, inkludert regelmessig testing.

Beredskapsplan for cyber-hendelser
Behandleren bruker en beredskapsplan for å håndtere og redusere effekten av uplanlagte cyber-hendelser som omfatter prosedyrer som skal følges hvis et faktisk eller potensielt sikkerhetsbrudd, inkludert: et internt beredskapsteam med en beredskapsleder, et etterforskningsteam som utfører en rotårsaksanalyse og identifiserer berørte parter, interne rapporterings- og varslingsprosesser, dokumentere beredskapshandlinger og utbedringsplaner samt en gjennomgang av hendelsene i ettertid.

Lagrings- og overføringssikkerhet
Behandleren benytter seg av tekniske sikkerhetstiltak for å beskytte mot uautorisert tilgang til Behandlerdata som overføres over et offentlig elektronisk kommunikasjonsnettverk eller lagres elektronisk.

Sikker avhending
Behandleren bruker retningslinjer og prosedyrer for avhending av materielle og immaterielle eiendeler som inneholder Behandlerdata, slik at Behandlerdata ikke kan leses eller rekonstrueres.

Risikoidentifisering og -vurdering

Behandleren bruker et risikovurderingsprogram for å identifisere, med rimelighet, forutsigbare interne og eksterne risikoer for Behandlers informasjonsressurser samt avgjøre om eksisterende kontroller, retningslinjer og prosedyrer er tilstrekkelige for å håndtere de identifiserte risikoene.

Leverandør og tjenesteleverandører

Tredjeparts tjenesteleverandører eller leverandører (samlet kalt "Leverandører") med tilgang til Behandlerens konfidensielle informasjon er underlagt risikovurderinger for å måle sårbarheten til Behandlerens informasjon, som deles. Leverandører forventes å overholde alle relevante kontraktsvilkår knyttet til sikkerheten til Behandlerdata samt Behandlers eventuelle gjeldende retningslinjer eller prosedyrer. Med jevne mellomrom kan Behandleren be en leverandør om å revurdere sikkerhetstiltakene, for å sørge for overholdelse.