TILLÆG TIL DATABEHANDLING HOS IVANTI

Dette Ivanti Data Processing Addendum ("DPA") udgør en del af Slutbrugerlicens- og Serviceaftale for Ivanti ("Aftale") og er lavet og indgået fra og med den sidste underskriftsdato nedenfor ("Ikrafttrædelsesdatoen") af og mellem kunden, der er identificeret nedenfor eller i Aftalen ("Dataansvarlig") og den relevante Ivanti-enhed, der er identificeret i denne DPA ("Ivanti" eller "Databehandler") (individuelt "Parten"; samlet "Parterne"). Alle udtryk skrevet med stort begyndelsesbogstav, der ikke er defineret heri, skal have de respektive betydninger, der gives dem i aftalen.

BETRAGTNINGER

EFTERSOM parterne har indgået Aftalen.

DERIMOD i forbindelse med leveringen af tjenesterne til den Dataansvarlige i henhold til Aftalen, kan Databehandleren behandle personoplysninger på vegne af den Dataansvarlige;

DERIMOD, for at sikre tilstrækkelige sikkerhedsforanstaltninger med hensyn til behandlingen af Personoplysninger, som den Dataansvarlige har leveret til Databehandleren, er parterne enige om at overholde følgende bestemmelser med hensyn til enhver Personoplysninger, idet hver af dem handler rimeligt og i god tro.

NU, DERFOR, i betragtning af de foregående præmisser og af de gensidige løfter og forpligtelser, der er angivet nedenfor, er den Registeransvarlige og Databehandleren enige om følgende:

AFTALE

1. DEFINITIONER

Alle udtryk skrevet med stort begyndelsesbogstav, der ikke er defineret heri, skal have de betydninger, der er afgivet i aftalen.

"Affilieret" betyder enhver enhed, der direkte eller indirekte kontrollerer, kontrolleres af eller er under fælles kontrol med den pågældende enhed. "Kontrol" betyder i denne definition direkte eller indirekte ejerskab eller kontrol over mere end 50 % af stemmeinteresserne i den pågældende enhed.

"Gældende databeskyttelseslove" betyder alle gældende love, regulativer, lovgivningsmæssige vejledninger eller krav i enhver jurisdiktion vedrørende databeskyttelse, privatliv eller fortrolighed af personlige oplysninger, herunder men ikke begrænset til (a) GDPR sammen med enhver transponering, implementering eller supplerende lovgivning og (b) CCPA.

"Autoriseret tilknyttet selskab" betyder enhver af den Registeransvarliges tilknyttede selskaber, som (a) er underlagt databeskyttelseslovene og reglerne i Det Europæiske Økonomiske Samarbejdsområde og/eller dets medlemslande, Det Forenede Kongerige og Schweiz, (b) er underlagt databeskyttelseslovene og regler uden for Det Europæiske Økonomiske Samarbejdsområde og/eller dets medlemsstater, Schweiz og Storbritannien (hvis det er relevant), og (c) har tilladelse til at bruge Databehandleren til behandling i henhold til aftalen.

"CCPA" står for California Consumer Privacy Act, Cal. Civ. code § 1798.100 *ff.*, og dens gennemførelsesforordninger.

"Dataansvarlig" betyder den enhed, der bestemmer formålene med og midlerne til Behandlingen af personoplysninger. For at undgå tvivl er den Part, der er identificeret ovenfor som "Dataansvarlig", en registeransvarlig i henhold til denne databeskyttelsesmyndighed.

"Brud på datasikkerheden" betyder et brud på sikkerheden, der fører til utilsigtet, uautoriseret eller ulovlig ødelæggelse, tab, ændring, videregivelse af, adgang til eller anden behandling af personlige oplysninger, der overføres, opbevares eller på anden måde behandles.

"Databeskyttelsesmyndighed" betyder enhver repræsentant eller agent for en statslig enhed eller et agentur, der har beføjelse til at håndhæve gældende databeskyttelseslove.

"Den registrerede" betyder en fysisk person, som personoplysninger vedrører.

"GDPR" betyder Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne data og om ophævelse af direktivet 95/46/EF (Generel databeskyttelsesforordning).

"**Ivanti**" betyder den enhed, der er identificeret nedenfor i samme geografiske område som Kunden:

- Ivanti, Inc., et Delaware-selskab i Amerika, undtagen Brasilien.

- Ivanti Comércio de Software Brasil Ltda, en brasiliansk virksomhed i Brasilien.
- Ivanti Software K.K., en japansk virksomhed i Japan.
- Ivanti Software Technology (Beijing) Co., Ltd., en kinesisk virksomhed i Kina.
- Ivanti International Limited, et irsk selskab, for Wavelink- og Naurtech-mærkevarer og tjenester i Europa, Mellemøsten, Afrika og Asien og Stillehavsområdet.
- Ivanti UK Limited, et aktieselskab registreret i England og Wales samt alle andre steder.

"Personoplysninger" betyder enhver information, der identificerer, relaterer til, beskriver, kan associeres med eller med rimelighed kan kædes direkte eller indirekte til en identificeret eller identificerbar fysisk person eller bestemt husstand. En identificerbar fysisk person er en person, der kan identificeres, direkte eller indirekte, især ved henvisning til en identifikator såsom et navn, et identifikationsnummer, lokaliseringsdata, en online identifikator eller til en eller flere faktorer, der er specifikke for den fysiske, fysiologiske, den fysiske persons genetiske, mentale, økonomiske, kulturelle eller sociale identitet.

"Proces" skal betyde enhver operation eller et sæt af operationer, der udføres på Personoplysninger af eller i forbindelse med og med henblik på leveringen af Tjenesterne, uanset om de udføres automatisk eller ej, såsom indsamling, registrering, organisering, opbevaring, tilpasning eller ændring, genfinding, konsultation, brug, offentliggørelse ved transmission, formidling eller på anden måde tilgængeliggørelse, justering eller kombination, blokering, sletning eller ødelæggelse; og som defineret af Gældende databeskyttelseslove.

"Databehandler" betyder den enhed, der behandler Personoplysninger på vegne af den Dataansvarlige. For at undgå tvivl er den part, der er identificeret som "Databehandler" ovenfor, en Databehandler for denne DPA.

"Tjenester" betyder Databehandlerens Behandling af Personoplysninger i forbindelse med og med henblik på leveringen af de tjenester, der skal leveres af Databehandleren i henhold til Aftalen.

"Tjenesteudbyder" betyder en enkeltmandsvirksomhed, et partnerskab, aktieselskab, selskab, forening eller anden juridisk enhed, der er organiseret eller drevet til profit eller økonomisk fordel for sine aktionærer eller andre ejere, som behandler oplysninger på vegne af en Dataansvarlig og hvortil den Dataansvarlige videregiver en Registreret persons personoplysninger til et forretningsformål i henhold til en skriftlig kontrakt, forudsat at kontrakten forbyder Tjenesteudbyderen at opbevare, bruge eller videregive personoplysningerne til andre formål end til det specifikke formål udføre de tjenester, der er specificeret i kontrakten, eller som på anden måde er tilladt af CCPA, herunder at beholde, bruge eller videregive personoplysningerne til et kommercielt formål, bortset fra at levere de tjenester, der er specificeret i kontrakten med den Dataansvarlige. Udtrykkene "Erhvervsmæssigt formål" og "Kommercielt formål" har samme betydning, som disse udtryk bruges i CCPA. For at undgå tvivl er Databehandleren en Tjenesteudbyder.

"Underdatabehandler" betyder enhver enhed, som behandler personoplysninger på vegne af Databehandleren.

2. BEHANDLING AF PERSONOPLYSNINGER

2.1 Parternes roller. Parterne anerkender og er enige om, at den Dataansvarlige er dataansvarlig, Databehandleren er databehandleren eller tjenesteyderen vedrørende behandlingen af personoplysninger. Emnet, varigheden, formålet med behandlingen og typerne af personoplysninger og kategorier af registrerede, der behandles i henhold til denne DPA, er yderligere specificeret i skema 1.

2.2 Den Dataansvarliges forpligtelser. Den dataansvarliges instruktioner for behandling af Personoplysninger skal overholde databeskyttelseslove og -forskrifter. Den dataansvarlige har eneansvaret for nøjagtigheden, kvaliteten og lovligheden af Personoplysninger og den måde, hvorpå den Dataansvarlige erhverver personoplysninger og leverer dem til Databehandleren.

2.3 Databehandlerens forpligtelser. Alle personoplysninger, der behandles af Databehandleren i henhold til Aftalen, er fortrolige oplysninger, og Databehandleren vil kun behandle Personoplysninger i overensstemmelse med den Dataansvarliges dokumenterede instruktioner angivet i skema 1 eller som på anden måde angivet skriftligt af den Dataansvarlige. Databehandleren vil ikke sælge de personoplysninger, der behandles i henhold til denne databeskyttelsesmyndighed, og vil ikke beholde, bruge eller videregive personoplysninger uden for det direkte forretningsforhold mellem Databehandler og Dataansvarlig. Databehandleren skal overholde alle Gældende databeskyttelseslove med hensyn til behandling af Personoplysninger. Hvis Databehandleren mener, at overholdelse af instruktionerne fra den Dataansvarlige vil resultere i en overtrædelse af enhver Gældende databeskyttelseslov, skal Databehandleren underrette den Dataansvarlige skriftligt herom uden forsinkelse. Databehandleren skal stille alle

nødvendige oplysninger til rådighed for den Dataansvarlige for at påvise Databehandlerens overholdelse af sine forpligtelser i henhold til denne DPA.

2.3.1. Bistandskrav. Databehandleren skal bistå den Dataansvarlige med: overholdelse af Gældende databeskyttelseslove; mistænkte og relevante brud på datasikkerheden; meddelelser til eller henvendelser fra en Databeskyttelsesmyndighed; meddelelser til og forespørgsler fra Registrerede; og den Dataansvarliges forpligtelse til at udføre databeskyttelseskonsekvensvurderinger og forudgående konsultationer med en Databeskyttelsesmyndighed.

3. UNDERRETNINGSPLIGT

3.1 Databehandlerens underretningspligt. Databehandler skal straks skriftligt underrette den Dataansvarlige om følgende:

3.1.1 En Registreret anmodning om at udøve sine privatlivsrettigheder såsom adgang til, berigtigelse, sletning, overførsel, indsigelse mod eller begrænsning af dennes Personoplysninger;

3.1.2 Enhver anmodning eller klage modtaget fra den Dataansvarliges kunder eller medarbejdere;

3.1.3 Ethvert spørgsmål, en klage, undersøgelse eller anden forespørgsel fra en Databeskyttelsesmyndighed;

3.1.4 Enhver anmodning om videregivelse af personoplysninger, der på nogen måde er relateret til Databehandlerens behandling af personoplysninger i henhold til denne Databeskyttelsesmyndighed;

3.1.5 Et Brud på datasikkerheden i henhold til underretningsforpligtelserne angivet i afsnit 7.1; og

3.1.6 Hvor personoplysningerne bliver genstand for ransagning og beslaglæggelse, en udlægskendelse, konfiskation under konkurs- eller insolvensbehandling eller lignende begivenheder eller foranstaltninger fra tredjemands side, mens de behandles.

Databehandleren vil bistå den Dataansvarlige med at opfylde den Dataansvarliges forpligtelser til at reagere på anmodninger vedrørende afsnit (3.1.1) - (3.1.6) ovenfor og vil ikke svare på sådanne anmodninger uden den Dataansvarliges forudgående skriftlige samtykke, medmindre Databehandleren er forpligtet til at svare ved lov.

4. FORTROLIGHED

4.1 Fortrolige oplysninger. Alle oplysninger givet til Databehandleren i henhold til aftalen er fortrolige oplysninger.

4.2 Databehandlerens medarbejdere. Databehandleren skal sikre, at dennes personale, der er involveret i behandlingen af Personoplysninger, er informeret om den fortrolige karakter af Personoplysningerne, har modtaget passende uddannelse i deres ansvar og har indgået skriftlige aftaler om fortrolighed. Databehandleren skal sikre, at sådanne fortrolighedsforpligtelser overlever ophøret af det respektive ansættelsesforhold med sådanne personer.

4.3 Begrænsning af adgang. Databehandleren skal sikre, at Databehandlerens adgang til Personoplysninger er begrænset til det personale, der udfører tjenester i overensstemmelse med aftalen.

5. UNDERDATABEHANDLERE

5.1 Udpegning af underdatabehandlere. Den Dataansvarlige anerkender og accepterer, at Databehandleren og Databehandlerens tilknyttede virksomheder kan engagere tredjeparts Underdatabehandlere i forbindelse med leveringen af Tjenesterne. Databehandleren eller Databehandlerens tilknyttede virksomhed skal indgå en skriftlig aftale med hver Underdatabehandler, der indeholder databeskyttelsesforpligtelser, der ikke er mindre beskyttende end dem i denne databeskyttelsesmyndighed i det omfang, det er relevant for arten af de Tjenester, der leveres af en sådan Underdatabehandler. Den Dataansvarlige bemyndiger hermed Databehandleren til at engagere sin aktuelle liste over Underdatabehandlere som anført på https://www.ivanti.com/company/legal/ivanti-subprocessors til at behandle personoplysninger i overensstemmelse med denne DPA. Den dataansvarlige vil ikke kommunikere direkte med Databehandlerens Underdatabehandlere om Tjenesterne, medmindre det er godkendt af Databehandleren efter Databehandlerens eget skøn.

5.2 Meddelelse om ændringer til Underdatabehandlere. Databehandleren vil informere den Dataansvarlige om eventuelle påtænkte ændringer vedrørende tilføjelse eller udskiftning af Underdatabehandlere ved at give Dataansvarlige en mekanisme til at abonnere på meddelelser om nye Underdatabehandlere på https://www.ivanti.com/company/legal/ivanti-subprocessors. Databehandleren vil underrette den Dataansvarlige om eventuelle påtænkte ændringer vedrørende tilføjelse eller udskiftning af Underdatabehandlere forud for sin brug af Underdatabehandleren.

5.3 Indsigelsesret overfor nye Underbehandlere. Den Dataansvarlige kan med rimelighed gøre indsigelse mod Databehandlerens brug af en ny Underdatabehandler ved at underrette Databehandleren omgående skriftligt inden for femten (15) hverdage efter modtagelsen af Databehandlerens meddelelse. I tilfælde af at den Dataansvarlige gør indsigelse mod en ny Underdatabehandler, vil Databehandleren gøre en rimelig indsats for at stille en ændring i Tjenesterne til rådighed for den Dataansvarlige for at undgå behandling af Personoplysninger af den nye Underdatabehandler, der er gjort indsigelse mod. Hvis Databehandleren ikke er i stand til at stille en sådan ændring til rådighed, kan den Dataansvarlige opsige den gældende Aftale med hensyn til de Tjenester, som ikke kan leveres af Databehandleren uden brug af den nye Underdatabehandler, der er gjort indsigelse mod.

5.4 Ansvar for Underbehandlers handlinger. Databehandleren er ansvarlig for sine Underdatabehandleres handlinger og undladelser i samme omfang som Databehandleren ville være ansvarlig, hvis denne udfører hver enkelt Underdatabehandlers tjenester direkte i henhold til vilkårene i denne Databeskyttelsesmyndighed.

6. SIKKERHED

6.1 Beskyttelse af personoplysninger. Databehandleren skal opretholde passende tekniske og organisatoriske foranstaltninger til beskyttelse af sikkerheden (herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændelig eller ulovlig ødelæggelse, tab eller ændring eller beskadigelse, uautoriseret videregivelse af eller adgang til Personoplysninger), fortrolighed og integritet af Personoplysninger.

6.2 Revisionsrettigheder. Den Dataansvarlige accepterer sin ret til at revidere Databehandleren kan være opfyldt ved at Databehandleren præsenterer opdaterede attester, rapporter eller uddrag fra uafhængige organer, herunder, ikke begrænset til eksterne eller interne revisorer, Databehandlerens databeskyttelsesansvarlige, IT-sikkerhedsafdelingen, databeskyttelses- eller kvalitetsrevisorer eller anden gensidigt aftalt med tredjeparter eller certificering i form af en it-sikkerheds- eller databeskyttelsesrevision. I det omfang det ikke er muligt at opfylde en revisionsforpligtelse påbudt af gældende Databeskyttelseslove og -forordninger gennem sådanne attester, rapporter eller uddrag, har den Dataansvarlige eller den Dataansvarliges udpegede ret til at revidere og inspicere – på den Dataansvarliges regning – databehandlerens lokaler, politikker, procedurer og computeriserede systemer for at sikre, at Databehandleren overholder kravene i denne DPA. Den Registeransvarlige, eller den Registeransvarliges udpegede, vil give mindst tredive (30) dages varsel, før der udføres en revision, medmindre en sådan revision er påkrævet på grund af et brud på datasikkerheden, der involverer Databehandleren. Revisioner foretaget af den Dataansvarlige eller den Dataansvarliges udpegede vil ikke overtræde Databehandlerens fortrolighedsforpligtelser over for Databehandlerens andre kunder. Alle revisioner vil blive udført inden for normal arbejdstid på Databehandlerens primære forretningssted eller andre af Databehandler lokationer, hvor der tilgås, behandles eller administreres Personoplysninger, og vil ikke urimeligt forstyrre Databehandlerens daglige drift. Før en sådan revision påbegyndes, skal Databehandleren og den Dataansvarlige gensidigt aftale tidspunktet, omfanget og varigheden af revisionen. Den Dataansvarlige kan anmode om en sammenfattende revisionsrapport eller en Revisionsbehandler én gang årligt.

7. BRUD PÅ DATASIKKERHEDEN

7.1 Underretning om brud på datasikkerheden. Databehandleren skal underrette den dataansvarlige skriftligt uden unødig forsinkelse, efter at denne er blevet opmærksom på et formodet brud på datasikkerheden. Under ingen omstændigheder skal en sådan underretning gives senere end 72 timer efter Databehandlerens opdagelse af bruddet på datasikkerheden.

7.2 Håndtering af brud på datasikkerheden. Databehandleren skal gøre en rimelig indsats for at identificere årsagen til et sådant brud på datasikkerheden og tage de skridt, som Databehandleren anser for nødvendige og rimelige for at afhjælpe årsagen til et sådant brud på datasikkerheden, i det omfang afhjælpningen er inden for Databehandlerens rimelige kontrol.

8. OPHØR

8.1 Ophør. Denne DPA ophører automatisk efter (a) opsigelse eller udløb af Aftalen eller (b) Databehandlerens sletning eller returnering af Personoplysninger. Den Dataansvarlige er endvidere berettiget til at opsige denne DPA med en begrundelse, hvis Databehandleren efter den Dataansvarliges efter eget skøn er i et væsentligt eller vedvarende brud på denne DPA, som i tilfælde af et brud, der kan afhjælpes, ikke er blevet afhjulpet inden for ti (10) dage fra datoen for Databehandlerens modtagelse af en underretning fra den Dataansvarlige, der identificerer bruddet og anmoder om afhjælpning heraf.

8.2 Returnering eller sletning af data. Ved ophør af denne DPA vil Databehandleren slette eller returnere alle eksisterende kopier af Personoplysninger, medmindre gældende lov kræver fortsat opbevaring af Personoplysninger. På anmodning fra den Dataansvarlige skal Databehandleren skriftligt bekræfte overholdelsen af sådanne forpligtelser

og slette alle eksisterende kopier. I tilfælde, hvor lokal lovgivning kræver, at Databehandleren opbevarer personoplysninger, vil Databehandleren beskytte fortroligheden, integriteten og tilgængeligheden af personoplysningerne; vil ikke aktivt behandle personoplysningerne; og vil fortsætte med at overholde betingelserne i denne DPA.

9. MEKANISMER TIL INTERNATIONAL OVERFØRSEL

9.1 Overførsler uden for EU. I forbindelse med leveringen af Tjenester under DPA'en kan det være nødvendigt for den Dataansvarlige at overføre personoplysninger fra Den Europæiske Union, Det Europæiske Økonomiske Samarbejdsområde og/eller deres medlemslande, Schweiz eller Det Forenede Kongerige, til Databehandleren i et land der ikke har en afgørelse om tilstrækkeligheden af beskyttelsesniveauet fra Europa-Kommissionen eller ikke er beliggende i Det Europæiske Økonomiske Samarbejdsområde.

9.1.1. I forhold til Personoplysninger, der er underlagt GDPR (i) vil Databehandleren blive anset for at være "dataimportøren", og den Dataansvarlige er "dataeksportøren"; (ii) Modul to-vilkårene skal gælde, hvor den Dataansvarlige er en Dataansvarlig, og hvor Databehandleren er en Databehandler; (iii) i paragraf 7 skal den valgfri docking-klausul slettes; (iv) i paragraf 9 i modul 2 gælder mulighed 2, og listen over underbehandlere og tidsperioden for meddelelse om ændringer skal være som aftalt i afsnit 5 i denne DPA; (v) i paragraf 11 skal det valgfrie sprog slettes; (vi) i paragraf 17 finder mulighed 1 anvendelse, og standardkontraktbestemmelserne skal være underlagt den medlemsstat, hvor den registeransvarlige er hjemmehørende; (vii) i paragraf 18(b) skal tvister løses ved domstolene i den medlemsstat, hvor den registeransvarlige har bopæl; (viii) Bilag I og Bilag II anses for at være udfyldt med de oplysninger, der er angivet i henholdsvis skema 1 i denne DPA; og (ix) hvis og i det omfang standardkontraktklausulerne er i konflikt med nogen bestemmelse i aftalen (inklusive denne DPA), skal standardkontraktklausulerne have forrang i omfanget af en sådan konflikt. For dette afsnit er standardkontraktbestemmelserne fra Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet (EU) 2021/914 indarbejdet ved reference og er tilgængelig 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.

9.1.2. I relation til personoplysninger, der er underlagt britisk Databeskyttelseslovgivning, gælder den internationale Dataoverførselsaftale ("IDTA") med følgende ændringer: (i) kontaktoplysningerne om parterne i aftalen er kontaktoplysningerne til IDTA; (ii) den Dataansvarlige er dataeksportøren og Databehandleren er dataimportøren; (iii) lovene, der regulerer IDTA, og det sted, hvor juridiske krav kan fremsættes, er England og Wales; (iv) UK GDPR gælder ikke for dataimportørens behandling af overførte data; (v) Parterne bruger ikke de yderligere sikkerheds- eller kommercielle klausuler fra IDTA; og (vi) oplysningerne i denne DPA og skema 1 kan bruges til tabel 1-4. For dette afsnit er Standardkontraktbestemmelserne fra Oplysningskommissærens kontor indarbejdet ved reference og tilgængelige 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/.

9.1.3. I relation til Personoplysninger, der er underlagt den schweiziske Databeskyttelsesmyndighed, gælder de standardkontraktbestemmelser, der henvises til i afsnit 9.1.1 med følgende ændringer (i) henvisninger til "Forordning (EU) 2016/679" skal fortolkes som referencer til schweizisk databeskyttelsesmyndighed; (ii) henvisninger til "EU", "unionen" og "medlemsstatslovgivningen" skal fortolkes som henvisninger til schweizisk lovgivning; og (iii) henvisninger til "den kompetente tilsynsmyndighed" og "kompetente domstole" skal erstattes med "den schweiziske føderale databeskyttelses- og informationskommissær" og de "relevante domstole i Schweiz".

9.2. Alternative dataoverførselsmekanismer. Parterne anerkender, at love, regler og bestemmelser vedrørende internationale dataoverførsler er under hastig udvikling. I tilfælde af at den Dataansvarlige går over til en anden mekanisme, der er autoriseret af gældende love, regler eller bestemmelser til at overføre Personoplysninger (hver en "Alternativ dataoverførselsmekanisme"), er Parterne enige om at arbejde sammen i god tro for at implementere eventuelle ændringer til denne Aftale, der er nødvendige for at implementere den alternative Dataoverførselsmekanisme.

10. DIVERSE BESTEMMELSER

10.1. Ændringer. Denne DPA må ikke ændres eller suppleres, og ingen af dens bestemmelser må anses for at være frafaldet eller på anden måde ændret, undtagen gennem en skriftlig behørig udførelse af autoriserede repræsentanter for begge parter.

10.2 Lovvalg. Denne Databeskyttelsesmyndighed er underlagt den gældende lov, der er angivet i aftalen.

TIL BEKRÆFTELSE HERAF har parterne i denne Aftale udført denne aftale fra ikrafttrædelsesdatoen.

DATAANSVARLIG_____	**IVANTI**
Underskrift: _____	Underskrift: _____
Navn: _____	Navn: _____
Titel: _____	Titel: _____
Dato: _____	Dato: _____

Liste over skemaer:

Skema 1: Beskrivelse af Behandlingen

SKEMA 1:

Beskrivelse af Behandlingen

Kontaktoplysninger til Ivanti:

Ivanti

10377 South Jordan Gateway
Suite 110
South Jordan, Utah 84095

DPO Kontakt: privacy@ivanti.com

Emne
Emnet for Behandlingen
Levering af it-softwarelicenser, supporttjenester og implementering, hvad enten det er på stedet eller som en hostet SaaS-løsning, vedrørende administration og facilitering af væsentlige forretningsprocesser inden for områderne administration af samlet slutpunkt, administration af IT-tjenester, administration af IT-aktiver, sikkerhed, rapportering og analyser og forsyningskæde.

IT-tjenester omfatter brugen af software som en installation på stedet eller en SaaS-løsning inklusive installation af moduler (herunder, men ikke begrænset til, hændelse, ændring, aktiv, konfiguration og frigivelsesstyringsmoduler); selvbetjenings- og servicekataloger; support og vedligeholdelse, herunder, men ikke begrænset til, fjernadgang; og programrettelser, app-kontrol, slutpunkts-/mobilsikkerhed og privilegiestyring.

Behandlingsfrekvens:
Løbende.

Varighed
Behandlingens varighed:
Som anført i Aftalen.

Behandlingens omfang, type og formål
Behandlingens omfang, type og formål er som følger:
Som anført i Aftalen.

De registrerede
Behandling af personoplysninger kan relatere til følgende kategorier af registrerede:
Kunder, kundeemner; medarbejdere; leverandører; kommercielle repræsentanter; kontakter; entreprenører (herunder beredskabsarbejdere); frivillige; vikarer og løsarbejdere; freelancere, agenter, konsulenter og andre professionelle respondenter og deres respektive pårørende, begunstigede og nødkontakter; perspektiv ansatte og vikarer hos kunder; klagere, korrespondenter og forespørgere; rådgivere, konsulenter og andre professionelle eksperter; medarbejdere eller kontaktpersoner for dataeksportørens kundeemner, kunder, forretningspartnere og leverandører; forretningspartnere og leverandører af dataeksportører (som er fysiske personer); og dataeksportørens brugere godkendt af dataeksportøren til at bruge softwaren og relaterede tjenester.

Datakategorier
Behandlingen af personoplysninger kan relatere til følgende kategorier af oplysninger:
Kundedata uploadet til Tjenesterne under Kundens tjenester og konti.

Tekniske og organisatoriske foranstaltninger
Følgende beskriver de tekniske og organisatoriske sikkerhedsforanstaltninger implementeret af Databehandleren:

Træning i sikkerhedsbevidsthed
Databehandleren har træning i sikkerhedsbevidsthed, som omfatter obligatorisk sikkerhedstræning om håndtering og sikring af fortrolige oplysninger og følsomme oplysninger såsom personligt identificerbare oplysninger, finansielle kontooplysninger og helbredsoplysninger i overensstemmelse med gældende lovgivning, og periodisk sikkerhedsbevidsthedskommunikation og sikkerhedskurser, der fokuserer på slutbrugerbevidsthed.

Sikkerhedspolitikker og -procedurer
Databehandleren har informationssikkerhed, brug og administrationspolitikker, som dikterer medarbejderes og kontrahenters handlinger vedrørende passende brug, adgang til og opbevaring af fortrolige og følsomme oplysninger; begrænser adgangen til fortrolige og følsomme oplysninger for medlemmer af Databehandlerens arbejdsstyrke, som har et "behov for at vide" sådanne oplysninger; forhindrer opsagte medarbejdere i at få adgang til Databehandlerens oplysninger efter opsigelse; og pålægger disciplinære foranstaltninger for manglende overholdelse af sådanne politikker. Systemadgang til Databehandlerens ressourcer er nægtet, medmindre det er specifikt vurderet og adgang er givet. Databehandleren udfører baggrundstjek af sine medarbejdere på ansættelsestidspunktet, som tilladt ved lov.

Fysisk og miljømæssig adgangskontrol
Databehandleren begrænser fysisk adgang til sine informationssystemer og faciliteter ved hjælp af fysiske kontroller (f.eks. kodet adgang), der giver rimelig sikkerhed for, at adgangen til datacentre er begrænset til autoriserede personer og anvender kamera- eller videoovervågningssystemer ved kritiske interne og eksterne indgangspunkter. Databehandleren anvender lufttemperatur- og fugtighedskontrol til sine datacentre og beskytter mod tab på grund af strømsvigt.

Logisk adgangskontrol
Databehandleren anvender lognings- og overvågningsteknologi til at hjælpe med at opdage og forhindre uautoriseret adgangsforsøg til sine netværk og produktionssystemer. Databehandlerens overvågning omfatter en gennemgang af ændringer, der påvirker systemernes håndtering af autentificering, autorisation og revision; privilegeret adgang til Databehandlerens produktionssystemer.

Krypteringskontrol
Databehandleren anvender forretningsegnede krypteringskontroller på tværs af vores produkter. Databehandleren evaluerer og anvender kryptering under transport og hvile ved at bruge industriens bedste praksis for koder. Bedste praksis bruges til livscyklusstyring af krypteringsnøgler, herunder generering, lagring, adgangskontrol og rotation.

Sårbarhedshåndtering
Databehandleren udfører regelmæssigt sårbarhedsscanninger og adresserer opdagede sårbarheder i overensstemmelse med risici. Databehandlerens produkter er også underlagt periodisk sårbarhedsvurdering og penetrationstest.

Katastrofeberedskab og backup-controller
Databehandleren udfører periodiske sikkerhedskopier af produktionsfilsystemer og databaser i henhold til en defineret tidsplan og vedligeholder en formel katastrofegenopretningsplan for produktionsskyens datacenter, inklusive regelmæssig test.

Plan for reaktion på cyberangreb
Databehandleren anvender en hændelsesresponsplan til at styre og minimere virkningerne af uplanlagte cyberangreb, som omfatter procedurer, der skal følges i tilfælde af et faktisk eller potentielt brud på sikkerheden, herunder: et internt hændelsesresponsteam med en indsatsleder; et efterforskningshold, der udfører en grundlæggende årsagsanalyse og identificerer berørte parter; interne rapporterings- og underretningsprocesser; dokumenterer responsive handlinger og afhjælpningsplaner; og en gennemgang af angrebet efter hændelsen.

Opbevaring og overførselssikkerhed
Databehandleren anvender tekniske sikkerhedsforanstaltninger for at beskytte mod uautoriseret adgang til Databehandlerens oplysninger, der transmitteres over et offentligt elektronisk kommunikationsnetværk eller opbevares elektronisk.

Sikker bortskaffelse
Databehandleren anvender politikker og procedurer vedrørende bortskaffelse af materielle og immaterielle ejendomme, der indeholder Databehandlerens oplysninger, således at Databehandlerens oplysninger ikke praktisk kan læses eller rekonstrueres.

Risikoidentifikation og -vurdering
Databehandleren anvender et risikovurderingsprogram til at hjælpe med rimelighed at identificere forudsigelige interne og eksterne risici for Databehandlerens informationsressourcer og afgøre, om eksisterende kontroller, politikker og procedurer er tilstrækkelige til at håndtere de identificerede risici.

Leverandører og serviceudbydere
Tredjepartstjenesteudbydere eller -leverandører (samlet kaldet "Leverandører") med adgang til Databehandlerens fortrolige oplysninger er underlagt risikovurderinger for at måle følsomheden af Databehandlerens oplysninger, der deles. Leverandører forventes at overholde alle relevante kontraktvilkår vedrørende sikkerheden af Databehandlerens oplysninger, såvel som Databehandlerens eventuelle gældende politikker eller procedurer. Databehandleren kan med jævne mellemrum bede en leverandør om at revurdere sin sikkerhedsposition for at sikre overholdelse.