

DATEBEHANDLERAFTALE

Kunde:

INVENTIO.IT A/S(CVR: 26112001)
(herefter benævnt "Dataansvarlig")

og

Leverandør:

INVENTIO.IT A/S (CVR: 26112001)

(herefter benævnt "Databehandler")

har indgået følgende databehandleraftale ("Aftalen") om Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige:

1. Baggrund, formål og omfang

1.1 Som led I den Dataansvarliges indgåelse af aftale om levering af ydelser, ERP-hosting ("Hostingaftalen") som beskrevet i Aftalens bilag 1, behandler Databehandleren personoplysninger, som den Dataansvarlige er ansvarlig for.

1.2 Databehandleren skal overholde det til enhver tid gældende lovkrav til databehandlere, herunder den Generelle Databeskyttelsesforordning (Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. April 2016 om beskyttelse af fysiske personer med hensyn til behandling af personoplysninger og om fri udveksling af sådanne data) med relaterede retsakter og sekundær national lovgivning.

1.3 Det er et krav i persondatalovgivningen, at den Dataansvarlige og Databehandleren indgår en skriftlig aftale om den behandling der skal udføres, en såkaldt "databehandleraftale". Aftalen udgør en sådan databehandleraftale.

2. Definitioner

2.1 "Gældende databeskyttelseslovgivning" betyder, medmindre andet er skriftligt aftalt mellem parterne; (i) den Generelle Databeskyttelsesforordning, (ii) den nationale databeskyttelseslovgivning i Danmark, som er gældende for Tjenesterne; og (iii) Datatilsynets regler og beslutninger gældende for behandling af personoplysninger i henhold til denne databeskyttelsesmyndighed i Sverige, Danmark, Norge og/eller Finland, alt efter hvad der er relevant.

2.2 "Tjenesterne" betyder, tjenester som er ydet under Hostingaftalen.

2.3 "SCC" betyder (i) EU's standardkontraktklausuler som vedtaget ved Europa-Kommisionens beslutning 2021/914 af 4. Juni 2021; (ii) I det omfang det er relevant, enhver fremtidig beslutning fra Europa-Kommisionen, der ændrer eller erstatter denne beslutning; eller (iii) under enhver henstandsperiode givet i henhold til en sådan gældende beslutning, den tidligere version heraf.

2.4 "Tredjeland" betyder et land uden for EU/EØS.

3. Personoplysninger omfattet af aftalen

3.1 Aftalen og tilhørende instruktion dækker alle typer af personoplysninger som beskrevet i bilag 1 til Aftalen.

4. Underdatabehandlere og geografiske krav

4.1 Databehandleren kan benytte en anden databehandler ("Underdatabehandler") til at behandle personoplysningerne i henhold til Aftalen, både inden for og uden for EU/EØS, forudsat at (i) et sådant engagement vil være underlagt en skriftlig kontrakt, og (ii) en sådan kontrakt vil kræve, at underdatabehandleren overholder i det væsentlige de samme forpligtelser, som gælder for Databehandleren i henhold til Aftalen. Aktuell liste over underdatabehandlere og lande, hvor personoplysninger kan behandles findes i bilag 1. Databehandleren forbliver fuldt ud ansvarlig over for den Dataansvarlige for udførelsen af denne underdatabehandlers forpligtelser. Men med hensyn til Microsoft, Atlassian Pty Ltd og Zendesk Inc., hvor det er relevant, anerkender og accepterer den Dataansvarlige, at Databehandleren ikke er ansvarlig for eller forpligtet til at tvinge disse tjenesteudbydere til at overholde andre forpligtelser vedrørende behandling af personoplysninger end som angivet i den respektive tjenesteudbyders egne vilkår og betingelser, som tilbydes ved brug af deres tjenester. Efter anmodning og i det omfang det er muligt under hensyn til fortrolighedsforpligtelsen, skal Databehandleren holde den Dataansvarlige orienteret om indholdet af sådanne aftaler.

4.2 Databehandleren vil informere den Dataansvarlige om eventuelle påtænkte ændringer af enhver underdatabehandler ved at give den Dataansvarlige forudgående skriftlig meddelelse herom. Meddelelsen vil indeholde (i) navnet på underdatabehandleren, (ii) det formål, som den vil blive ansat til, (iii) placeringen af underdatabehandleren, og hvor personoplysningerne kan behandles og, hvor det er relevant (iv) overførselsmekanisme, der er relevant for tredjelandsoverførslen. Den dataansvarlige har ret til at fremsætte en skriftlig indsigelse mod ændringen inden for fjorten dage efter modtagelsen af meddelelsen. Såfremt Databehandleren trods den Dataansvarliges indsigelse alligevel ønsker at foretage ændringen, er den Dataansvarlige berettiget til at opsiges Aftalen med tre måneders varsel

4.3 Den Dataansvarlige skal sikre, at der er en gyldig overførselsmekanisme på plads for overførsel af personoplysninger til et Tredjeland. En sådan overførselsmekanisme kan være SCC eller andre tilsvarende bestemmelser i Kapitel V i GDPR, som er gældende fra tid til anden.

4.4 I tilfælde af overførsler af personoplysninger til et Tredjeland og i det omfang SCC anvendes som retsgrundlag for overførsel af personoplysninger til et Tredjeland, kan Databehandleren eller underdatabehandleren, alt efter hvad der er relevant, efter eget skøn bestemme, hvilken version og hvilke moduler af SCC, der er relevante og skal anvendes i hvert enkelt tilfælde, typisk modulet til behandler-til-behandler overførsler.

4.5 I det omfang at det er lovpligtigt, vil Databehandleren foretage en risikovurdering i forhold til en overførsel af data til et Tredjeland. Skulle kravet om at udføre en

sådan vurdering i stedet ligge hos en underdatabehandler udpeget af Databehandleren, vil Databehandleren anmode om, at underdatabehandleren udfører en sådan vurdering. Nogle underdatabehandlere kan offentliggøre oplysninger i denne forbindelse, såsom risikovurderinger, på deres respektive websteder, som ligger uden for Databehandlerens kontrol. Den Dataansvarlige anerkender hermed, at sådanne oplysninger, herunder eventuelle vurderinger, ligger uden for databehandlerens kontrol, og for brug af tjenesterne accepteres de.

4.6 Den Dataansvarlige er ansvarlig for at sikre, at den udførte risikovurdering og eventuelle supplerende foranstaltninger er på plads og opfylder den Dataansvarliges krav vedrørende tilstrækkelig sikkerhed for de personoplysninger, der behandles i henhold til Gældende databeskyttelseslovgivning. På den Dataansvarliges rimelige anmodning forpligter Databehandleren sig til at give tilstrækkelig information til den Dataansvarlige til at vurdere enhver udført risikovurdering. Såfremt Databehandleren foretager ændringer i vurderinger foretaget efter aftalens indgåelse eller udvælger en ny underdatabehandler, og den Dataansvarlige finder at denne ændring eller nye vurdering ikke kan opfylde forpligtelserne i henhold til gældende databeskyttelseslovgivning, skal den Dataansvarlige straks gøre indsigelse. En sådan indsigelse bør indeholde oplysninger om årsagerne til hvorfor og hvordan ændringen ikke opfylder den Dataansvarliges forpligtelser. Databehandleren vil herefter tage en sådan indsigelse i betragtning og, i det omfang Databehandleren skønner det muligt og nødvendigt, opdatere vurderingen og indføre eventuelle foranstaltninger, der er truffet på baggrund af indsigelsen. Såfremt Databehandleren efter eget skøn vurderer, at det ikke er muligt eller ikke rimeligt nødvendigt at foretage sådanne ændringer, og indsigelserne fra den Dataansvarlige indeholder gyldige grunde, er den Dataansvarlige berettiget til at opsiges Aftalen i overensstemmelse med generelle betingelser for tjenesten. "Gyldig grund" betyder, i dette afsnit, forhold fra underdatabehandlerens side, der væsentligt påvirker eller kan forventes at påvirke beskyttelsen af registreredes personoplysninger, såsom en ny underdatabehandler, der ikke overholder de forpligtelser der er pålagt databehandlere i henhold til Gældende databeskyttelseslovgivning.

5. Instruktion

5.1 Omfanget af de opgaver som Databehandleren skal varetage og understøtte, betyder, at der i henhold til Parternes aftale, Hostingaftalen, vil blive udført forskellige former for behandling af personoplysninger. De forskellige former for databehandling af personoplysninger er beskrevet i Bilag 1 til Aftalen. Den Dataansvarlige er ansvarlig for, at behandlingen af personoplysninger udføres i overensstemmelse med Gældende Databeskyttelseslovgivning i sin rolle som værende Dataansvarlig. Den Dataansvarlige skal sikre, at Databehandleren ikke behandler andre kategorier af personoplysninger på vegne af den Dataansvarlige end de kategorier af personoplysninger, der er anført i Bilag 1.

5.2 Databehandleren handler kun efter dokumenteret instruks fra den Dataansvarlige. Databehandleren skal sikre, at de betroede personoplysninger ikke anvendes til andre formål eller behandles på andre måder, end hvad der fremgår af den Dataansvarliges anvisning. Alle de beskrevne handlinger, der er nødvendige for behandlingen af Hostingaftalen, anses for at være dokumenteret. Anden behandling kan dog finde sted, hvis det kræves i henhold til EU-lovgivningen eller den nationale lovgivning i de medlemslande, som Databehandleren er underlagt; i så fald informerer Databehandleren den Dataansvarlige om dette lovlige krav inden behandlingen, medmindre nævnte lov forbyder en sådan meddelelse med henblik på vigtige offentlige interesser.

5.3 Såfremt en instruks efter Databehandlerens opfattelse er i strid med Gældende databeskyttelseslovgivning, skal Databehandleren informere den Dataansvarlige herom.

5.4 Denne aftale og tilhørende instruktion dækker kategorierne af de registrerede, der er specificeret i Bilag 1.

5.5 Såfremt behandlingen af personoplysninger hos Databehandleren helt eller delvist udføres ved brug af fjernforbindelse, herunder hjemmekontorer, skal Databehandleren opstille retningslinjer for medarbejdernes behandling af personoplysninger ved brug af fjernforbindelse, som også skal overholde kravene i Aftalen.

5.6 Databehandleren skal i det omfang det er muligt bistå den Dataansvarlige med at overholde den Dataansvarliges forpligtelser til at besvare anmodninger om udøvelse af den registreredes rettigheder, herunder om adgang, berigtigelse, begrænsning eller sletning, hvis de relevante personoplysninger behandles af Databehandleren. Hvis Databehandleren modtager sådan anmodning fra den registrerede, skal Databehandleren underrette den Dataansvarlige herom.

5.7 Den Dataansvarlige hæfter for alle Databehandlerens omkostninger til sådan bistand, se punkt 5.6, herunder for underdatabehandleren. Databehandlerens assistance faktureres efter den til enhver tid gældende databehandler timepris for sådant arbejde.

5.8 Hver af parterne skal sikre, at den anden part har ret til at behandle kontaktoplysninger og andre typer personoplysninger om den anden Parts medarbejdere, hvis og i det omfang en sådan behandling er nødvendig for at levere Tjenesterne.

6. Behandling og videregivelse af personoplysninger

6.1 Den Dataansvarlige garanterer at have den nødvendige bemyndigelse til at behandle de personoplysninger, der er omfattet af denne aftale.

6.2 Databehandleren må ikke uden skriftligt samtykke fra den Dataansvarlige videregive oplysninger til tredjemand, medmindre en sådan videregivelse følger af Gældende databeskyttelseslovgivning eller af en bindende anmodning fra en domstol eller anden databeskyttelsesmyndighed eller fremgår af denne aftale.

7. Sikkerhed

7.1 Databehandleren skal træffe passende tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger hændeligt eller uretmæssigt tilintetgøres, går tabt, forringes, eller kommer til tredjemands kendskab, misbruges eller på anden måde behandles i strid med lovgivningen, se punkt 1.2 ovenfor.

7.2 Databehandleren er gennem sit medlemskab af Danish Cloud Community (Brancheforeningen af IT-hostingvirksomheder i Danmark) ("DCC") certificeret i IT-hosting ("Hostingcertifikatet") og skal således overholde de angivne krav til sikkerhed, i certificeringsvejledningen. Databehandleren skal endvidere i henhold til punkt 7.1 implementere og bibeholde sikkerhedsforanstaltningerne beskrevet i Bilag 2 og i øvrigt overholde de krav, der stilles i Hostingaftalen. De sikkerhedskrav, der stilles i bilag 2, udgør den Dataansvarliges krav i forhold til sikkerhedsforhold hos Databehandleren, og den Dataansvarlige er således ansvarlig for, at disse sikkerhedsforanstaltninger opfylder sine forpligtelser til tilstrækkelig sikkerhed for, at personoplysninger behandles i henhold til Gældende databeskyttelseslovgivning.

7.3 Databehandleren er altid berettiget til at implementere alternative sikkerhedsforanstaltninger, forudsat at sådanne sikkerhedsforanstaltninger som minimum overholder eller tilbyder mere sikkerhed end de sikkerhedsforanstaltninger, der er beskrevet i Hostingcertifikatet og bilag 2, jf. punkt 7.2, og i øvrigt opfylder sikkerhedskravene i Hostingaftalen. Databehandleren kan ikke foretage forringelser af sikkerhedsforholdene uden den Dataansvarliges forudgående skriftlige godkendelse.

7.4 Databehandleren skal efter aftale med den Dataansvarlige i det omfang det er muligt og under hensyntagen til behandlingens art og de oplysninger, som Databehandleren har til rådighed, bistå den Dataansvarlige med at sikre overholdelse af forpligtelserne i § 32 i stk. forordningen (vedtagelse af passende tekniske og organisatoriske foranstaltninger), 34 (meddelelse til de registrerede om brud på persondatasikkerheden), 35 (gennemførelse af en konsekvensanalyse vedrørende databeskyttelse) og 36 (forudgående høring). Databehandleren er i den forbindelse berettiget til at fakturere den Dataansvarlige efter sædvanlig timepris for al Databehandlerens arbejdstid, som en sådan aftale måtte medføre for Databehandleren, og den Dataansvarlige hæfter for enhver betaling til dataunderbehandleren.

7.5 Såfremt specifikationerne i pkt. 7.4 medfører skærpede krav til sikkerhedsforanstaltninger i forhold til, hvad der allerede er aftalt mellem parterne i denne aftale, gennemfører Databehandleren, hvor det er muligt, sådanne foranstaltninger på betingelse af, at Databehandleren modtager betaling herfor, jf. punkt 7.6 nedenfor.

7.6 Omkostninger i forbindelse med gennemførelse af foranstaltninger, jf. punkt 7.5, betales af den Dataansvarlige og er således Databehandleren uvedkommende. Databehandleren er endvidere berettiget til at fakturere den Dataansvarlige efter sin sædvanlige timepris for al Databehandlerens arbejdstid, som en sådan implementering måtte medføre for Databehandleren, ligesom den Dataansvarlige hæfter for enhver betaling til dataunderbehandleren.

8. Ret til tilsyn

8.1 Efter anmodning fra den Dataansvarlige skal Databehandleren give den dataansvarlige tilstrækkelige oplysninger til, at den Dataansvarlige kan sikre, at databehandleren overholder artikel 28 i den Generelle databeskyttelsesforordning og denne aftale.

8.2 Hvis den Dataansvarlige ønsker at føre tilsyn som angivet i dette punkt 8, skal den Dataansvarlige altid give Databehandleren varsel på mindst 30 dage i sådan forbindelse.

8.3 Databehandleren skal én gang om året på anmodning fra den Dataansvarlige sørge for, at en generelt anerkendt og uafhængig tredjepart fremlægger en sikkerhedsrevisionsrapport udarbejdet i overensstemmelse med en anerkendt revisionsstandard (f.eks. ISAE 3402 med en referenceramme til ISO 27002: 2014 eller lignende), til den Dataansvarlige om overholdelse af kravene til sikkerhedsforanstaltninger i overensstemmelse med Databehandlerens certificering hos Danish Cloud Community, se pkt. 7.2 ovenfor og Bilag 2 til Aftalen. Som medlem af Danish Cloud Community bliver Databehandleren certificeret én gang årligt til at bruge Cloud Certifikatet, som bl.a. indeholder en ISAE 3402 med en referenceramme til ISO 27002. Ved Databehandlerens indsendelse af en kopi af det opdaterede hostingcertifikat og tilhørende ISAE 3402-erklæring med en referenceramme til ISO 27002, overholder Databehandleren kravet i denne bestemmelse.

8.4 Såfremt Databehandleren får udarbejdet en sikkerhedsrevisionsrapport, som beskriver sikkerhedsforholdene hos dataunderbehandleren i henhold til punkt 8.3, er den Dataansvarlige berettiget til efter anmodning at modtage en kopi heraf, forudsat at Databehandleren er berettiget at udlevere kopien.

8.5 Såfremt den Dataansvarlige ønsker at få udarbejdet anden eller yderligere sikkerhedsrevisionsrapport ud over de i pkt. 8.3 og 8.4 nævnte, eller i øvrigt ønskes tilsyn af Databehandlerens eller dataunderbehandlerens persondatabehandling, herunder hvis den Dataansvarlige ønsker en sikkerhedsrevisionsrapport udarbejdet på et bestemt tidspunkt, aftales dette nærmere med Databehandleren. Den Dataansvarlige eller dataunderbehandleren kan altid kræve, at en sådan sikkerhedsrevisionsrapport udarbejdes i overensstemmelse med en anerkendt revisionsstandard (f.eks. ISAE 3402 med referenceramme til ISO 27002:2014 eller lignende) af en alment kendt og uafhængig tredjepart som er engageret i sådanne sager.

8.6 Den Dataansvarlige betaler alle omkostninger i forbindelse med tilsynet af sikkerhedsforhold, jf. punkt 8, hos Databehandleren og i forhold til underdatabehandleren, herunder at Databehandleren er berettiget til at fakturere den Dataansvarlige efter sædvanlig timepris pr. al Databehandlerens arbejdstid, som et sådant tilsyn måtte medføre for Databehandleren, og den Dataansvarlige hæfter for enhver betaling til dataunderbehandleren.

9. Personoplysninger, sikkerhedsbrud

9.1 Hvis Databehandleren bliver opmærksom på et sådant brud på persondatasikkerheden, hvilket betyder et sikkerhedsbrud, der resulterer i hændelig eller ulovlig ødelæggelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, som er blevet videregivet, opbevaret eller på anden måde behandlet, er Databehandleren forpligtet til, uden unødigt forsinkelse, at forsøge at lokalisere et sådant brud og søge at mitigere opstået skade i det omfang det er muligt, og i det omfang det er muligt at genoprette eventuelle tabte data.

9.2 Databehandleren er endvidere forpligtet til, uden unødigt forsinkelse, at underrette den Dataansvarlige efter at have fået kendskab til, at der er sket brud på persondatasikkerheden. Efter anmodning fra den Dataansvarlige skal Databehandleren herefter, uden unødigt forsinkelse, i videst muligt omfang give en skriftlig meddelelse til den Dataansvarlige, som i videst muligt omfang skal indeholde:

- (a) En beskrivelse af arten af bruddet, herunder kategorieme og det omtrentlige antal af berørte registrerede og hvilke registreringer af personoplysninger.
- (b) Navn og kontaktoplysninger på DPO.
- (c) En beskrivelse af de sandsynlige konsekvenser af databruddet.
- (d) En beskrivelse af de foranstaltninger som er igangsat af Databehandleren eller underdatabehandleren eller vil blive igangsat for at håndtere sikkerhedsbruddet, herunder foranstaltninger for at undgå potentielle følger.

9.3 Hvis det ikke er muligt at give oplysningerne i pkt. 9.2 samlet, kan oplysningerne gives i trin uden unødigt yderligere forsinkelse.

10. Kompensation

10.1 Ud over det, der er anført i denne Aftale, er Databehandleren berettiget til rimelig kompensation for at efterkomme den Dataansvarliges skriftlige instrukser, medmindre den ønskede handling er specifikt angivet i Aftalen. Såfremt Databehandleren er berettiget til kompensation for udført arbejde, vil Databehandlerens til enhver tid gældende prisliste være gældende, medmindre andet fremgår af Aftalen.

11. Ansvarsbegrænsning

11.1 Medmindre parterne har aftalt anden ansvarsbegrænsning der medfører mindre ansvar fra Databehandlerens side, gælder dette punkt 11.

11.2 For handlinger og undladelser i forbindelse med den databehandling, som Databehandleren foretager for den Dataansvarlige, er Databehandleren ansvarlig over for den Dataansvarlige efter dansk rets almindelige regler med de begrænsninger, der følger af dette punkt 11.

11.3 Databehandleren er aldrig ansvarlig over for den Dataansvarlige for indirekte tab, herunder, men ikke begrænset til, tab for følgeskader, tabt arbejdsfortjeneste, driftsafbrydelse, tab af goodwill, tab af data, tredjepartstab eller andet indirekte tab fra Dataansvarlige eller en tredjepart.

11.4 Uanset årsagen til Databehandlerens eventuelle erstatningsansvar over for den Dataansvarlige, kan Databehandlerens samlede erstatningsansvar aldrig overstige et beløb svarende til det løbende vederlag, som den Dataansvarlige udbetaler til Databehandleren i henhold til Hostingaftalen. I løbet af 3 måneder forud for den skadevoldende handling eller undladelse. Hvis Hostingaftalen ikke har været i kraft i tre måneder på tidspunktet for den skadevoldende handling eller undladelse, opgøres beløbet som det beløb, der i henhold til aftalen løbende er blevet udbetalt som vederlag eller burde være udbetalt pr. løbende vederlag i henhold til Hostingaftalen i de første tre måneder af Hostingaftalen.

12. Tavshedspligt

12.1 Databehandleren skal holde de personoplysninger, der behandles i henhold til Aftalen, fortrolige, og er således kun berettiget til at bruge personoplysningerne som led i opfyldelse af sine forpligtelser og rettigheder i henhold til Aftalen. Databehandleren skal pålægge sine medarbejdere og eventuelle andre, herunder dataunderbehandlerne, der er bemyndiget til at behandle de personoplysninger, der er omfattet af Aftalen, at holde dem fortrolige. En sådan fortrolighed gælder også efter aftalens udløb.

13. Forrang

13.1 Medmindre andet fremgår af Aftalen, har bestemmelser i Aftalen forrang i forhold til tilsvarende bestemmelser i andre aftaler mellem parterne, herunder Hostingaftalen.

14. Databehandleraftalens løbetid og opsigelse

14.1 Aftalen træder i kraft efter godkendelse af den Dataansvarlige.

14.2 I tilfælde af at Hostingaftalen opsiges, uanset årsagen, ophører denne aftale også. Bortset fra at aftalen fortsat vil være gyldig i den periode, Databehandleren stadig behandler personoplysninger på vegne af den Dataansvarlige.

14.3 Aftalen kan ikke opsiges individuelt, men kan erstattes af en anden databehandleraftale om samme forhold. Hvis ikke, er Databehandleren bundet af denne Aftale, så længe Databehandleren behandler personoplysninger på vegne af den Dataansvarlige.

14.4 Den Dataansvarlige skal hurtigst muligt, og senest 14 dage efter Hostingaftalens udløb, skriftligt meddele Databehandleren, om Databehandleren skal returnere eller slette de behandlede personoplysninger. 30 dage efter opsigelse af Hostingaftalen er Databehandleren forpligtet til at slette alle personoplysninger, som er blevet behandlet under den opsagte Hostingaftale på vegne af den Dataansvarlige. Databehandleren kan dog altid opbevare de behandlede data, hvis det følger af EU-retten eller medlemslandenes nationale lovgivning.

15. Bilag

Bilag 1: Beskrivelse af baggrunden og formålet med aftalen mv.

Bilag 2: Beskrivelse af sikkerhedsforanstaltninger

*** En liste over de tredjelande, som Kommissionen vurderer som værende lande, der generelt, enten gennem gældende databeskyttelseslovgivning eller andre foranstaltninger, sikrer et tilstrækkeligt beskyttelsesniveau (sikre tredjelande), vises på Datatilsynets hjemmeside. 2. Disse er tilgængelige på Europa-Kommissionens websted

Bilag 1. Beskrivelse af baggrund og formålet med Aftalen osv.

1. Aftalens baggrund og formål

1.1 Denne aftale er indgået i forbindelse med Parternes indgåelse af en aftale om levering af Ydelserne (i aftalen benævnt "Hostingaftalen"), i hvilken forbindelse Databehandleren behandler personoplysninger på vegne af Dataansvarlig og for at opfylde formålet med Hostingaftalen.

1.2 Formålet med behandlingen af personoplysninger er generelt at hoste forretningsapplikations- og lagringsdata.

2. Typer af personoplysninger omfattet af Aftalen

2.1 Aftalen og tilhørende instruks omfatter alle typer personoplysninger der behandles af Databehandleren under der mellem Parterne indgåede Hostingaftale.

2.2 Den Dataansvarlige kan indsende personlige oplysninger til Tjenesten, hvis omfang bestemmes og kontrolleres af den Dataansvarlige efter eget skøn, og som kan omfatte, men er ikke begrænset til, følgende kategorier af personoplysninger: Loginoplysninger; navn; titel; position; arbejdsgiver; kontaktoplysninger (virksomhed, e-mail, telefon, adresse); ID data; forbindelsesdata; lokaliseringsdata; slutbrugeres adfærd; betalingsdata og uddannelse.

2.3 Den Dataansvarlige kan også indsende særlige kategorier af personoplysninger til Tjenesten, hvis omfang bestemmes og kontrolleres af den Dataansvarlige efter eget skøn, og som kan omfatte, men ikke er begrænset til, følgende kategorier af personoplysninger: etnisk oprindelse; politiske meninger; religiøse eller filosofiske overbevisninger; fagforeningsmedlemskab; data vedrørende sundhed eller seksuelle præferencer.

3. Kategorier af registrerede

3.1 Behandlede personoplysninger vedrører enhver individuel bruger af Tjenesten. Derudover kan den Dataansvarlige indsende personoplysninger til Tjenestene, i hvis omfang bestemmes og kontrolleres af den dataansvarlige efter eget skøn, og som kan omfatte, men ikke er begrænset til, personoplysninger vedrørende følgende kategorier af registrerede personer :

- (1) kundeemner, kunder, forretningspartnere og leverandører af den Dataansvarlige (som er fysiske personer);
- (2) Medarbejdere eller kontaktpersoner relateret til (1) ovenfor;
- (3) Ansatte, agenter, rådgivere, konsulenter for den dataansvarlige (som er fysiske personer);
- (4) Den Dataansvarliges brugere, der er autoriseret af den Dataansvarlige til at bruge tjenesten.

4. Behandlingsaktiviteter

4.1 Databehandleren opretter 2 forskellige brugertyper, der har adgang til kundens data. Disse brugere er defineret som en systembruger og en supportbruger. Systembruger bruges til automatiserede behandlingsaktiviteter såsom; afsendelse / start af opgave, tilsyn, scripting, fejlretning, opgradering, backup, gendannelse. Supportbruger bruges til manuelle handlinger såsom; support, fejlfinding, vedligeholdelse, test, opgradering, installationer, udvikling, fjernforbindelser og rettelser

Bilag 2. Beskrivelse af sikkerhedsforanstaltninger

1. Introduktion

1.1 Dette bilag er det bilag, der henvises til i Aftalens punkt 7.2.

1.2 Bilaget beskriver de sikkerhedsforanstaltninger, som Databehandleren anvender i forbindelse med den fysiske, tekniske og organisatoriske sikkerhed i forbindelse med Databehandlerens levering af Tjenestene.

1.3 Databehandleren er gennem sit medlemskab af Danish Cloud Community (Brancheforeningen af IT-hostingvirksomheder i Danmark) ("DCC") certificeret i IT-hosting ("Cloud-certifikat").

1.4 Følgende beskrivelse af sikkerhedsforanstaltningerne hos Databehandleren er beskrevet i Databehandlerens ISAE 3402 Type II-rapport. Rapporten kan findes her:

<https://www.inventio.it/om-inventio/it-revisorerklæring>

2. Fysisk sikkerhed

2.1 Den fysiske sikkerhed hos Databehandleren er beskrevet i ISAE 3402 Type II-rapporten kapitel 2.

3. Teknisk sikkerhed

3.1 Den tekniske sikkerhed hos Databehandleren er beskrevet i ISAE 3402 Type II-rapporten kapitel 2.

4. Organisatorisk sikkerhed

4.1 Den organisatoriske sikkerhed hos Databehandleren er beskrevet i ISAE 3402 Type II-rapporten kapitel 2.

5. Sletning og kassering

5.1 Den Dataansvarliges data slettes en måned efter Aftalens udløb.

6. Brug af underdatabehandlere

På tidspunktet for Aftalens indgåelse benyttes følgende underdatabehandlere som fremgår af nærværende liste:

<https://www.inventio.it/databehandleraftale/underleverandoerer> disse er udvalgt af Databehandleren og er godkendt af den Dataansvarlige, denne godkendelse indeholder også lokaliteten for behandlingen.

Godkendt af Kenneth Kornbeck
07-12-2022 11:25:06
IP: 83.140.16.52