CHISA Standard Databehandleraftale

Definitioner of fortolkning

De betegnelser og definitioner, der er angivet i denne Aftale, har følgende betydning:

Ved "**Persondatalovgivningen**" forstås den til enhver tid gældende persondatalovgivning i Danmark, for nuværende særligt persondataloven (lov nr. 421 af 31. maj 2000 med senere ændringer), sikkerhedsbekendtgørelsen (bekendtgørelse 528/2000 med senere ændringer), fra den 25. maj 2018 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 oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), databeskyttelsesloven og andre nationale særregler, herunder men ikke begrænset til love, regler eller bindende vejledninger fra myndigheder, der finder anvendelse på behandlingen af Personoplysninger.

Definitionen af Personoplysninger, Særlige Kategorier af Personoplysninger (herefter "Følsomme Personoplysninger"), Behandling, den Registrerede, Dataansvarlig og Databehandler er den samme som i GDPR.

Baggrund

Ved brug af CHISA Project & CHISA Tender (herefter kaldet "Applikationerne") vil den Dataansvarlige være ansvarlig for sin behandling af Personoplysninger i Applikationerne. Databehandleren vil behandle Personoplysninger på vegne af den Dataansvarlige. For at sikre, at parterne lever op til sine forpligtelser under Persondatalovgivningen, indgår parterne denne databehandleraftale (herefter "Aftale"), som udgør instruksen fra den Dataansvarlige til Databehandleren og dermed regulerer Databehandlerens behandling af Personoplysninger på vegne af den Dataansvarlige.

Begge parter bekræfter, at det har fuldmagt til at underskrive Aftalen.

Parterne indgår denne Aftale med henblik på at regulere Databehandlerens behandling af Personoplysningerne og sikre, at behandlingen sker i overensstemmelse med Persondatalovgivningen.

Aftalen er et tillæg de eksisterende abonnementsvilkår.

Databehandlerens ansvar

Databehandleren skal udelukkende behandle Personoplysninger på vegne af og som følge af den Dataansvarliges instruktioner, medmindre Behandlingen kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt; i så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden Behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.

Ved at indgå denne Aftale, instruerer den Dataansvarlige Databehandleren i at behandle Personoplysninger på følgende måder:

i) i overensstemmelse med gældende lovgivning

ii) for at opfylde sine forpligtelser i henhold til abonnementsvilkår for applikationerne

iii) som yderligere specificeret ved den Dataansvarliges normale brug af applikationerne

iv) som i øvrigt er beskrevet i denne Aftale.

Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter Databehandlerens mening er i strid med Persondatalovgivningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Som en del af at kunne levere applikationerne er Databehandleren forpligtet til enhver tid at give den Dataansvarlige gode og konkurrencedygtige løsninger der følger med udviklingen. Databehandleren kan tilbyde bedre løsninger, som er tilpasset den enkelte Dataansvarliges behov, ved at registrere hvordan Dataansvarlig og dennes repræsentanter bruger applikationerne. Dette gør Databehandler for at kunne lave en bedre version af applikationerne, og generelt yde bedre tjenester og give mere relevant kommunikation til den Dataansvarlige og dennes repræsentanter. Målet er at Dataansvarlig skal løse så mange udfordringer som muligt på ét sted. I det omfang at Personoplysninger fra applikationerne indgår i dette arbejde, og Behandlingen sker til disse formål, er CHISA A/S dataansvarlig for Behandlingen af disse Personoplysninger.

Kategorierne af Registrerede og Personoplysninger som behandles i henhold til denne Aftale er beskrevet i bilag A.

Under hensyntagen til den teknologi, der er tilgængelig, og omkostningerne ved implementeringen, samt omfanget, konteksten og formålet med Behandlingen, er Databehandleren forpligtet til at foretage alle rimelige foranstaltninger, herunder tekniske og organisatoriske, for at sikre et tilstrækkeligt sikkerhedsniveau i forhold til den risiko og kategorien af Personoplysninger, der skal beskyttes.

Databehandleren skal bistå den Dataansvarlige med passende tekniske og organisatoriske foranstaltninger, som dette er muligt og under hensyntagen til Behandlingens art og kategorien af Personoplysninger, der er tilgængelige for Databehandleren, for at sikre overholdelse af den Dataansvarliges forpligtelser i henhold til gældende Databeskyttelseslovgivning, herunder for så vidt angår bistand i forhold til opfyldelse af anmodninger fra Registrerede samt generel overholdelse af bestemmelserne under GDPR artikel 32-36.

Databehandleren skal underrette den Dataansvarlige uden unødig forsinkelse via kontaktperson oplyst i Databehandleraftalen, hvis Databehandleren bliver bekendt med sikkerhedsbrist. Endvidere skal Databehandleren så vidt muligt og lovligt underrette den Dataansvarlige, hvis;

i) En anmodning om indsigt i Personoplysninger modtages direkte fra den Registrerede

ii) En anmodning om indsigt i Personoplysninger modtages direkte fra statslige myndigheder, herunder politiet.

Databehandleren må ikke besvare sådanne anmodninger fra Registrerede, medmindre denne er autoriseret af den Dataansvarlige til at gøre det. Databehandleren vil endvidere ikke videregive information om denne Aftale til statslige myndigheder såsom politiet, herunder Personoplysninger, medmindre Databehandleren er forpligtet til det i medfør af lovgivningen, såsom ved en retskendelse eller lignende.

Hvis den Dataansvarlige kræver information eller assistance omkring sikkerhedsforanstaltninger, dokumentation eller information om, hvordan Databehandleren behandler Personoplysninger generelt, og en sådan anmodning indeholder information, som går ud over, hvad der er nødvendigt ifølge gældende Databeskyttelseslovgivning, må Databehandleren kræve betaling for sådanne yderligere services. Databehandleren og dennes ansatte skal sikre fortrolighed i forhold til Personoplysninger, som behandles i henhold til Aftalen. Denne bestemmelse skal ligeledes gælde efter ophør af Aftalen.

Den Dataansvarliges forpligtelser

Den Dataansvarlige bekræfter ved indgåelse af denne aftale, at:

- Den Dataansvarlige skal ved brug af applikationerne stillet til rådighed af Databehandleren, udelukkende behandle Personoplysninger i overensstemmelse med kravene i den gældende Databeskyttelseslovgivning.
- Den Dataansvarlige har et lovligt grundlag for at behandle og videregive Personoplysninger til Databehandleren (herunder til underdatabehandlere som Databehandleren anvender).
- Den Dataansvarlige har ansvaret for nøjagtigheden, integriteten, indholdet af pålideligheden og lovligheden af de Personoplysninger som behandles af Databehandleren.
- Den Dataansvarlige har opfyldt alle obligatoriske krav og pligter i forhold til anmeldelse hos eller opnåelse af tilladelse fra de relevante offentlige myndigheder for så vidt angår Behandlingen af Personoplysninger.
- Den Dataansvarlige har opfyldt sin oplysningsforpligtelser over for de Registrerede vedrørende Behandlingen af Personoplysninger i henhold til Persondatalovgivningen.
- Den Dataansvarlige er enig i, at Databehandleren har givet de relevante garantier for så vidt, angår implementeringen af tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre de Registreredes rettigheder og deres Personoplysninger.
- Den Dataansvarlige skal ved brug af applikationerne ikke registrere og behandle følsomme Personoplysninger i applikationerne.
- Den Dataansvarlige skal have en opdateret liste over de kategorier af Personoplysninger, som denne behandler, dette gælder særligt i det omfang sådan Behandling afviger fra de kategorier af Personoplysninger, som fremgår af bilag A.

Brug af underdatabehandlere og videregivelse af Personoplysninger

Som en del af driften af applikationerne anvender Databehandleren underleverandører ("Underdatabehandlere"). Dette er tredjepartsleverandører i og uden for EU/EØS. Disse fremgår af bilag B.

Databehandleren skal sikre sig, at dennes Underdatabehandlere skal overholde tilsvarende forpligtelser og krav, som er beskrevet i Aftalen. Hvis Underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver Databehandleren fuldt ansvarlig over for den Dataansvarlige for opfyldelsen af Underdatabehandlerens forpligtelser.

Denne Aftale udgør den Dataansvarliges forudgående generelle skriftlige godkendelse af Databehandlerens brug af Underdatabehandlere. Hvis en Underdatabehandler er etableret uden for eller Personoplysninger opbevares uden for EU/EØS giver den Dataansvarlige Databehandleren autorisation til at sikre et tilstrækkeligt grundlag for overførsel af Personoplysninger til tredjeland på vegne af den Dataansvarlige, herunder ved anvendelse af EU Kommissionens Standardkontrakter eller i overensstemmelse med Privacy Shield.

Den Dataansvarlige skal orienteres, inden Databehandler udskifter sine Underdatabehandlere. Den Dataansvarlige har dog kun ret til at protestere imod en ny Underdatabehandler, som behandler Personoplysninger på vegne af den Dataansvarlige, hvis denne ikke behandler Personoplysninger i overensstemmelse med Persondatalovgivningen. I en sådan situation skal Databehandleren demonstrere overensstemmelse ved at give den Dataansvarlige adgang til Databehandlerens databeskyttelsesvurdering af Underdatabehandleren. Hvis der stadig er uenighed om anvendelsen af Underdatabehandleren kan den Dataansvarlige opsige sit abonnement på applikationerne, herunder med et kortere varsel end normalt for at sikre, at den Dataansvarliges Personoplysninger ikke behandles af den pågældende Underdatabehandler.

Sikkerhed

Databehandleren er forpligtet til at sikre et højt sikkerhedsniveau i sine produkter og services, hvilket sikres ved relevante organisatoriske, tekniske og fysiske sikkerhedsforanstaltninger, som er påkrævede i henhold til information om sikkerhedsforanstaltninger som beskrevet i GDPR artikel 32.

De følgende foranstaltninger er særligt væsentlige:

- Klassificering af Personoplysninger for at sikre implementering af sikkerhedsforanstaltninger relevante i forhold til risikovurderinger.
- Vurdering af kryptering og pseudonymisering som risikoreducerende faktorer.
- Begrænse adgangen til Personoplysninger til de relevante personer, der skal til for at overholde krav og forpligtelser i Aftalen eller i henhold til Parternes aftale om anvendelse af applikationerne.
- Drift og implementering af systemer der kan opdage, genoprette, imødegå og rapportere hændelser i forhold til Personoplysninger.
- Kortlægge sikkerhedsstrukturen samt hvordan Personoplysninger overføres imellem Parterne.
- Foretage vurdering af eget sikkerhedsniveau for at sikre, at nuværende tekniske og organisatoriske foranstaltninger er tilstrækkelige til beskyttelse af Personoplysninger, herunder i henhold til GDPR artikel 32 om behandlingssikkerhed samt artikel 25 om privacy by design og default.

Adgang til revision

Databehandleren stiller alle oplysninger, der er nødvendige for at påvise Databehandlerens overholdelse af artikel 28 GDPR og denne aftale, til rådighed for den Dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den Dataansvarlige eller en anden revisor, som er bemyndiget af den Dataansvarlige.

Den Dataansvarlige er berettiget til at igangsætte en revision af Databehandlerens forpligtelser i henhold til Aftalen én gang årligt. Hvis den Dataansvarlige er forpligtet hertil efter gældende lovgivning, kan der foretages revision oftere end én gang årligt. Den Dataansvarlige skal i forbindelse med anmodning om en revision medsende en detaljeret revisionsplan med en beskrivelse af omfang, varighed og startdato minimum fire uger forud for den foreslåede startdato. Det skal besluttes i fællesskab mellem Parterne, hvis en tredjepart skal foretage revisionen. Imidlertid kan den Dataansvarlige lade Databehandleren bestemme, at revisionen af sikkerhedsårsager skal foretages af en neutral tredjepart efter Databehandlerens valg, såfremt der er tale om et behandlingsmiljø hvor den Dataansvarliges data er anvendt.

Under alle omstændigheder skal revision finde sted i normal kontortid på den relevante facilitet i overensstemmelse med Databehandlerens politikker og må ikke på urimelig vis forstyrre Databehandlerens sædvanlige kommercielle aktiviteter.

Den Dataansvarlige er ansvarlig for alle omkostninger i forbindelse med anmodningen om revision. Databehandlerens assistance i forbindelse hermed, som overskrider den almindelige service som Databehandleren skal stille til rådighed som følge af Persondatalovgivningen, afregnes særskilt.

Varighed og ophør

Aftalen er gældende, så længe Databehandleren behandler Personoplysninger på vegne af den Dataansvarlige i forbindelse med den Dataansvarliges brug af applikationerne. Denne Aftale vil automatisk ophøre ved udgangen af den Dataansvarliges opsigelsesperiode i forhold til abonnement på applikationerne.

Foreligger der ikke senest én (1) måned efter ophør af abonnementet instruks fra den Dataansvarlige angående tilbagelevering eller sletning af Personoplysningerne, er Databehandleren berettiget til at slette Personoplysningerne. Databehandleren vil dog fortsat opbevare Personoplysninger, hvis EU-retten eller national ret foreskriver en sådan opbevaring.

Såfremt den Dataansvarlige ønsker bistand til returnering af Personoplysninger, fastsættes omkostninger forbundet hermed i fællesskab af Parterne og skal baseres på i) timetakster for Databehandlerens anvendte tid, ii) kompleksiteten af den anmodede proces og iii) det valgte format.

Ændringer

Ændringer til Aftalen skal vedlægges i et særskilt bilag til Aftalen. Hvis nogen af bestemmelserne i Aftalen er ugyldige, får dette ikke indvirkning på de resterende bestemmelser. Parterne skal erstatte ugyldige bestemmelser med en lovlig bestemmelse, som afspejler formålet med den ugyldige bestemmelse.

Ansvar

Ansvar for handlinger i strid med bestemmelserne i denne Aftale reguleres af ansvars- og erstatningsbestemmelser i abonnementsvilkårene for applikationerne. Dette gælder ligeledes for enhver overtrædelse, som foretages af Databehandlerens Underdatabehandlere.

For CHISA A/S

Claus Navntoft, CEO

Bilag A – Kategorier af Personoplysninger og Registrerede

Kategorier af Registrerede:

- Den Dataansvarliges medarbejdere og slutbrugere
- Den Dataansvarliges kunder medarbejdere og slutbrugere
- Den Dataansvarliges kunders rådgiveres medarbejdere og slutbrugere
- Den Dataansvarliges leverandører og dennes medarbejdere og slutbrugere
- Andre, som den Dataansvarlige beslutter, skal have adgang til applikationerne.

Kategorier af Personoplysninger:

- Navn
- Titel
- Telefonnummer
- E-mail
- Adresse
- IP-adresse
- Billede

Der registreres og behandles ikke Følsomme Personoplysninger, herunder informationer om:

- Politisk, filosofisk eller religiøs overbevisning
- Fagforeningsmæssige tilhørsforhold
- Race eller etnisk oprindelse
- Oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering
- Genetiske eller biometriske data med det formål entydigt at identificere en fysisk person.

Bilag B

Bilag B1 – Systemunderleverandører

Navn	Adresse	Område
Heroku	Salesforce.com Inc 415 Mission Street, 3rd Floor San Francisco, CA 94105 United States of America	Application Hosting EU Datacenters
Microsoft Azure	Microsoft Ireland Operations, Ltd. One Microsoft Place Leopardstown Dublin 18 D18 P521 Ireland	Application Hosting EU Datacenters
Amazon Web Services	Amazon Web Services Inc. 410 Terry Avenue North Seattle, WA 98109 United States of America	Document Hosting EU Datacenters
Mandrill	The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Atlanta, GA 30308 United States of America	Transactional emails EU+US datacenters
Scrive	Scrive AB Grev Turegatan 11A 114 46 Stockholm Sweeden	Digital signing EU Datacenters
EEngine	EENGINE.pl Sp. z o.o. ul. Pabianicka 31 95-070 Aleksandrów Łódzki Poland	Test and Development EU Datacenters
AppSignal	AppSignal B.V. Rietwaard 4 5236 WC 's-Hertogenbosch Netherland	Tracing and error logging EU Datacenters
Microsoft Azure DevOps	Microsoft Ireland Operations, Ltd. One Microsoft Place Leopardstown Dublin 18 D18 P521 Ireland	Source code EU Datacenters

Bilag B2 – Back Office Underleverandører

Navn	Adresse	Område
GitHub	GitHub, Inc 88 Colin P. Kelly Jr. St. San Francisco, CA 94107 United States of America	Source code EU+US datacenters
WebCRM	WEBCRM A/S Lyngbyvej 2 2100 København Ø Denmark	CRM EU Datacenters
FreshDesk	Freshworks Inc 2950 S. Delaware Street San Mateo CA 94403 United States of America	Support EU Datacenters
Jira	Atlassian Plc 341 George Street Sydney, NSW 2000, Australia	Support and planning EU Datacenters
Backblaze	Backblaze 500 Ben Franklin Ct San Mateo, CA 94401 United States of America	Backup EU Datacenters
MailChimp	The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Atlanta, GA 30308 United States of America	Marketing and notification emails US datacenters
e-conomic	Visma e-conomic Gærtorvet 1 1799 København Denmark	Accounting system EU Datacenters
Danløn	Danske Lønsystemer A/S Engholm Parkvej 8 3450 Lillerød Denmark	Payroll system DK Datacenters
FarPay	FarPay ApS Applebys Plads 7 1411 København K Denmark	Payment Collection system EU Datacenters
HubSpot	1 Harbour Pl, Suite 175 Portsmouth, NH 03801 United States of America	CRM EU Datacenters

CodeTwo	Wolności 16 58-500 Jelenia Góra Poland	Email signatures EU Datacenters
1Password	4711 Yonge St, 10th Floor, Toronto, Ontario, M2N 6K8, Canada.	Passwords EU Datacenters
New Relic	New Relic, Inc., 188 Spear Street Suite 1000 San Francisco, CA 94105 United States of America	Tracing and error logging EU Datacenters
Twilio	*Twilio Ireland Limited.* *3 Dublin Landings, North Wall Quay, Dublin 1* *Ireland*	*SMS notification (2FA)* *EU Datacenters*
CloudFlare	CloudFlare Inc 101 Townsend Street San Francisco, CA 94107 United States of America	Website Hosting CDN, DDOS EU Datacenters
Google Analytics	Google LLC 1600 Amphitheatre Parkway Mountain View, California United States of America	Marketing tracking and statistics on website EU+US datacenters
LinkedIn	LinkedIn Corporation 1000 West Maude Avenue Sunnyvale, CA 94085 United States of America	Marketing tracking and statistics on website EU+US datacenters
Sentry	Functional Software, Inc. d/b/a Sentry, 45 Fremont Street, 8th Floor, San Francisco, CA 94105 United States of America	Tracing and usage logging US Datacenters
Microsoft Office 365	Microsoft Ireland Operations, Ltd. One Microsoft Place Leopardstown Dublin 18 D18 P521 Ireland	Office 365 EU Datacenters

Bilag B3 – Website Underleverandører

-//-