This translation is provided for convenience only, in the event of any dispute or claim the English language version will take precedence.
Denne oversættelse er kun beregnet som en hjælp. I tilfælde af tvister eller krav finder den engelske version anvendelse.

BILAG F.
DATABEHANDLINGSAFTALE

mellem

[indsæt kundens navn]
[Indsæt CVR nr. eller Virksomhedsregistreringsnummer]
[Indsæt adresse]
("Dataansvarlig" eller "Kunde")

og

Planday A/S
CVR nr. 2766 6248
Kuglegårdsvej 7-9-11, Bygning 181
1434 Copenhagen K
Denmark
("Databehandler" eller "Planday")

(hver for sig "Parten" og samlet "Parterne")

vedrørende Databehandlerens behandling af personoplysninger oplysninger på vegne af den Dataansvarlige.

1 FORMÅL OG BAGGRUND

1.1 Den Dataansvarlige har accepteret at udpege Databehandleren til at levere software og serviceydelser til den Dataansvarlige i henhold til aftalevilkårene.

1.2 Som en del af leveringen af software og serviceydelser skal Databehandleren behandle Personoplysninger, der kan henføres til specifikke fysiske personer som beskrevet i Bilag A.

1.3 Databehandlingsaftalen fastsætter de vilkår, der skal gælde for Databehandlerens behandling af Personoplysninger.

2 DEFINITIONER OG FORTOLKNING

2.1 Følgende ord og udtryk har den betydning, der er anført nedenfor i Databehandlingsaftalen, medmindre andet følger af omstændighederne.

Bilag	betyder bilag til denne Databehandlingsaftale.
Hverdag	alle dage ud over lørdag, søn- og helligdage
Åbningstid	9:00 til 17:00 på hverdage
Aftale	betyder kundeaftalen mellem Databehandleren og Kunden vedrørende levering af serviceydelser og

	Databehandlerens generelle vilkår, herunder alle dokumenter, bilag og ændringer hertil.
Dataansvarlig	Kunden som defineret i Aftalen og i overensstemmelse med definitionen i den gældende Databeskyttelseslov.
Databehandlingsaftale	denne aftale med Bilag.
Databehandlingsydelser	serviceydelser beskrevet i Bilag A
Databeskyttelseslov	lovgivningen, med ændringer, til beskyttelse af fysiske personers grundlæggende rettigheder og friheder og ikke mindst deres ret til beskyttelse af privatlivet for så vidt angår Behandling af Personoplysninger, der gælder for en Dataansvarlig i EØS-landet, hvor den Dataansvarlige har hjemsted, herunder GDPR, den engelske databeskyttelseslov fra 2018, Direktiv om Behandling af Personoplysninger og Beskyttelse af Privatlivets Fred i den Elektroniske Kommunikationssektor (2002/58/EC) (som opdateret af Direktiv 2009/136/EC) samt den engelske bekendtgørelse fra 2003 om behandling af personoplysninger og beskyttelse af privatlivets i elektroniske kommunikationssektor (*SI 2003/2426*). Reference til Databeskyttelseslov er en henvisning til loven som til enhver tid ændret, udvidet eller atter vedtaget.
Den Registrerede	en identificeret eller identificerbar fysisk person (en identificerbar person er en, der kan identificeres direkte eller indirekte, især ved reference til en identifikator, såsom et navn, identifikationsnummer, lokaliseringsdata eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet).
Tilintetgøre/Tilintetgørelse	betyder, at Personoplysninger slettes uigenkaldeligt fra alle lagermedier, hvorpå de har været lagret, og at Personoplysningerne ikke på nogen måde kan genskabes, herunder af Underdatabehandlere. Dette gælder for alle lagringsmedier anvendt i forbindelse med Behandlingen og omfatter alle eksisterende kopier.
Distributør	betyder [indsæt navn, CVR-nummer og adresse for den relevante distributør].

EØS	Det Europæiske Økonomiske Samarbejdsområde.
Slutbrugerlicens	aftalen mellem Planday og en Registreret, der tilgår personalets turnussoftware kaldet “Planday“ og/eller relateret software.
GDPR	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 (Persondataforordningen).
Personoplysninger	oplysninger, uanset form, vedrørende den Registrerede samt som defineret i databeskyttelseslovgivningen.
Brud på persondatasikkerheden	et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til Personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
Behandle/behandling	enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som Personoplysninger eller en samling af Personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.
Behandlingsaktiviteter	Som defineret i Bilag A
Databehandler	betyder Planday som defineret i Databehandlingsaftalen og i overensstemmelse med definitionen i den gældende Databeskyttelseslov.
Tilbagelevering	betyder, at alle Personoplysninger tilbageleveres fysisk eller elektronisk til den Dataansvarlige, og at alle kopier deraf, som måtte være i Databehandlerens besiddelse, eller som Databehandleren måtte have til sin disposition, herunder Personoplysninger overgivet til Underdatabehandlere, gøres til genstand for Tilintetgørelse.

Underdatabehandler	betyder en anden behandler, der er engageret af Databehandleren med det formål at udføre særlige behandlingsaktiviteter på vegne af den Dataansvarlige.
Planday-system	et IT-system eller systemer, hvori Databehandlingsydelserne udføres i overensstemmelse med denne Databehandlingsaftale.

2.2 Medmindre konteksten i øvrigt kræver det, omfatter ord i ental flertal, og ord i flertal omfatter ental.

2.3 Alle ord efter begreberne "herunder", "omfatte", "især" eller "for eksempel" eller en anden lignende frase skal fortolkes som illustrativ og begrænser ikke almindeligheden i de relaterede generelle ord.

2.4 En undtagelse eller øvre grænse for ansvar i Aftalen gælder også for Databehandlerens ansvar i henhold til denne Databehandlingsaftale.

3 OMFANG

3.1 Databehandlingsaftalen gælder for al Behandling af Personoplysninger udført af Databehandleren i forbindelse med udførelsen af Databehandlingsydelser til den Dataansvarlige som defineret i Bilag A (sagsgenstanden).

3.2 Kunden og Planday anerkender, at Kunden er den Dataansvarlige, og at Planday er Databehandleren hvad angår Personoplysninger leveret til Planday af eller på vegne af Kunden, herunder Personoplysninger beskrevet i bilag A, som led i leveringen af Databehandlingsydelserne.

3.3 Arten af og formålet med Databehandlingen, typer af Personoplysninger og kategorier af Registrerede er anført i Bilag A.

3.4 Intet i denne Databehandlingsaftale må være til præjudice for Plandays rettigheder og forpligtelser anført i Slutbrugerlicensen.

4 DATABEHANDLERENS FORPLIGTELSER

4.1 Databehandleren skal:

a) Kun behandle Personoplysninger efter dokumenterede instrukser fra den Dataansvarlige som anført i denne Databehandlingsaftale og til de formål, der er anført i Bilag A,

b) udføre sit arbejde i henhold til denne Databehandlingsaftale med al passende dygtighed og omhu,

c) føre en fortegnelse som beskrevet i artikel 30 i GDPR på dets sædvanlige forretningssted for eventuel Databehandling af Personoplysninger udført som led i Databehandlingsydelserne og overholdelsen af sine forpligtelser som anført i Databehandlingsaftalen ("Fortegnelser"),

d) sikre, at personer bemyndiget til at behandle Personoplysninger har forpligtet sig til fortrolighed eller er genstand for en passende lovfæstet fortrolighedsforpligtelse,

e) indføre passende tekniske og organisatoriske foranstaltninger for at beskytte Personoplysninger mod hændelig eller ulovlig tilintetgørelse eller hændeligt tab, ændring, uautoriseret videregivelse eller adgang og mod alle andre ulovlige former for behandling, herunder kravet angående disse foranstaltninger i henhold til Databeskyttelseslov som anført i klausul 6,

f) kun tage kopier af Personoplysningerne i det omfang, det med rimelighed er nødvendigt, hvilket blandt andet kan omfatte backup, spejling, sikkerhed, IT-katastrofeberedskab og test af Personoplysningerne,

g) kun give i underentreprise med Underdatabehandlere i overensstemmelse med kravene i klausul 7.

h) straks informere den Dataansvarlige hvis, efter dennes mening, en instruks krænker Databeskyttelseslove,

i) assistere den Dataansvarlige med passende tekniske og organisatoriske foranstaltninger, i det omfang dette er muligt, til opfyldelse af den Dataansvarliges pligt til at svare på anmodninger om udøvelse af den Registreredes ikke-eksklusive rettigheder til adgang, korrektion, sletning og dataportabilitet, som disse er anført i Databeskyttelseslovgivningen,

j) efter den Dataansvarliges valg tilintetgøre eller tilbagelevere alle Personoplysninger til den Dataansvarlige enten under eller efter gyldighedsperioden for denne Databehandlingsaftale, jf. Klausul 11,

k) stille alle oplysninger, der er nødvendige for at bevise overholdelse af Databeskyttelseslovene, til rådighed for den Dataansvarlige, f.eks. et eventuelt årligt certifikat for overholdelse af ISO27001,

l) i forbindelse med klausul 4.1(k), hvis juridisk og teknisk muligt tillade og bidrage til revisioner, herunder inspektioner udført af den Dataansvarlige eller anden bemyndiget af den Dataansvarlige som anført i klausul 8,

m) overholde sine forpligtelser i henhold til Databeskyttelseslovgivning, herunder, hvor det er muligt, udpege en databeskyttelsesrådgiver.

4.2 Hvis Databehandleren modtager en klage, meddelelse eller kommunikation, der direkte eller indirekte vedrører behandlingen af Personoplysninger eller en af parternes overholdelse af Databeskyttelseslovgivning, skal denne straks meddele den Dataansvarlige og denne skal yde Databehandleren fuldt samarbejde og hjælp angående en sådan klage, meddelelse eller kommunikation.

4.3 Databehandlerens ansvar i henhold til Aftalen, herunder Databehandlingsaftalen, er maksimeret og fraskrevet i henhold til vilkårene i Aftalen.

4.4 Databehandleren skal uden ugrundet ophold informere den Dataansvarlige, hvis Databehandleren bliver klar over et brud på persondatasikkerheden.

4.5 Databehandleren er berettiget til at opkræve Dataansvarlige separat for omkostninger (herunder interne ressourcer til Databehandlerens standardsatser), der måtte påløbe i forbindelse med assistance som henvist til i klausul 4.1(a)-(m).

5 DEN DATAANSVARLIGES FORPLIGTELSER

5.1 Den Dataansvarlige er alene ansvarlig for sin overholdelse af gældende lov som Dataansvarlig. Den Dataansvarlige sikrer, før anvendelse af softwaren og modtagelse af tjenester i henhold til Aftalenpå en måde, der omfatter behandling af Personoplysninger,om at man overholder al Databeskyttelseslovgivning, f.eks. vedrørende levering af krævede oplysninger/meddeleser til/eller godkendelser fra Registrerede og/eller tilsynsmyndigheder i forbindelse med behandlingen.

5.2 Den Dataansvarlige skal straks meddele Databehandleren, hvis man bliver klar over, at behandlingen af den Dataansvarliges Personoplysninger kan være i strid med Databeskyttelseslovgivning.

5.3 Den Dataansvarlige garanterer, at Databehandlerens strenge overholdelse af instrukser fra den Dataansvarlige hvad angår behandling af Personoplysninger, ikke medfører en overtrædelse af gældende Databeskyttelseslovgivning.

5.4 Den Dataansvarlige skadesløsholder Databehandleren for eventuelle tab som følge af den Dataansvarliges undladelse af at overholde sine forpligtelser i henhold til aftalen.

6 SIKKERHEDSFORANSTALTNINGER

6.1 Den Dataansvarlige er forpligtet til at indføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, som er hensigtsmæssigt i forhold til de risici, der foreligger ved behandlingen, især mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse eller adgang til Personoplysninger, der sendes, lagres eller på anden måde behandles, når der tages højde for det aktuelle tekniske niveau, omkostningerne ved implementering og art, omfang, sammenhæng og formål med behandling såvel som risici vedrørende forskellig sandsynlighed og alvor af fysiske personers rettigheder og friheder, herunder bl.a. som hensigtsmæssigt:

a) pseudonymisering og kryptering af Personoplysninger,

b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester,

c) evnen til rettidigt at genoprette tilgængeligheden af og adgangen til Personoplysninger i tilfælde af en fysisk eller teknisk hændelse,

d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

6.2 Databehandleren skal tage skridt til at sikre, at en fysisk person, der handler på bemyndigelse fra Databehandleren, som har adgang til Personoplysninger, ikke behandler Personoplysningerne, undtagen efter instruks fra den Dataansvarlige, medmindre vedkommende skal gøre dette i henhold til Databeskyttelseslovgivning.

6.3 De specifikke tekniske og organisatoriske sikkerhedsforanstaltninger implementeret af Databehandleren er anført i Bilag B (Sikkerhedsforanstaltninger).

7 UNDERDATABEHANDLERE

7.1 Den Dataansvarlige bemyndiger herved Databehandleren til at engagere Underdatabehandlere, herunder uden begrænsning de Underdatabehandlere som anført i Bilag A, til at udføre behandling af Personoplysninger, under forudsætning af, at Databehandleren indgår en skriftlig aftale med hver Underdatabehandler, der pålægger samme forpligtelser på Databehandleren i henhold til denne Databehandlingsaftale. Den Dataansvarlige er til enhver tid efter rimelig forudgående skriftlig varsel berettiget til at modtage en kopi af Databehandlerens databehandlingsaftale med hver Underdatabehandler.

7.2 Databehandleren informerer den Dataansvarlige pr. e-mail om eventuelle tilføjelser eller udskiftninger af en underdatabehandler forud, hvilket giver den Dataansvarlige/den Registrerede mulighed for at gøre indsigelse og/eller give sit informerede samtykke, idet dette samtykke ikke må nægtes uden rimelig grund. Den Dataansvarlige må ikke gøre indsigelser uden en objektiv årsag i god tro, medmindre præceptiv lov foreskriver det. Hvis den Dataansvarlige gør indsigelser mod tilføjelse eller erstatning af en underdatabehandler, under forudsætning af, at indsigelsen bygger på en objektiv årsag i god tro, er den Dataansvarlige berettiget til at opsige Databehandlingsaftalen med øjeblikkelig varsel ved skriftlig meddelelse.

7.3 Hvis en Underdatabehandler undlader at opfylde sine databeskyttelsesforpligtelser i henhold til Databehandlingsaftalen i klausul7.1, er Databehandleren fortsat fuldt ansvarlig over for den Dataansvarlige for udførelsen af Underdatabehandlerens generelle opfyldelse af sine databeskyttelsesforpligtelser.

8 REVISIONER

8.1 Med henblik på at revidere Databehandlerens overholdelse af sine forpligtelser i henhold til denne Databehandlingsaftale skal Databehandleren give den Dataansvarlige rimeligt skriftligt varsel på ikke under tredive (30) dage til Databehandleren i Arbejdstiden, men uden varsel i tilfælde af Databehandlerens med rimelighed mistænkte brud på denne Databehandlingsaftale, udføre en Revision, herunder, men ikke begrænset til:

a) få adgang til at inspicere og tage kopier af fortegnelserne og andre oplysninger, som opbevares i Databehandlerens lokaler eller i Behandlingssystemet i forbindelse med Databehandlingsydelserne, og

b) få adgang til inspicere Behandlersystemet.

8.2 Den skriftlige meddelelse skal omfatte en foreslået revisionsplan. Hvis en del af det krævede revisionsomfang er dækket af omfanget af en revisionsrapport af en kvalificeret tredjeparts-revisor inden for de seneste 12 måneder, kan Databehandleren kræve, at den Dataansvarlige overvejer, om man kan lægge denne rapport til grund i stedet for en revision. Databehandleren er berettiget til at foreslå dato og tidspunkt for revisionen for at minimere forstyrrelse af driften og kan foreslå, at revisionen kombineres med revisioner fra andre Dataansvarlige. Den Dataansvarlige kan ikke nægte disse forslag fra Databehandleren, medmindre man har en objektiv årsag i god tro til nægtelsen.

8.3 På den Dataansvarliges skriftlige anmodning, i henhold til klausul 8.1 og 8.2, er den Dataansvarlige (eller) et besigtigelsesorgan sammensat af uafhængige medlemmer og i besiddelse af de nødvendige faglige kvalifikationer bundet af fortrolighedspligt og udpeget af den Dataansvarlige eller en Tilsynsmyndighed)

berettiget til at udføre revisioner af Databehandlerens anlæg og sikkerhedspraksis i direkte forbindelse med Behandlingen af Personoplysninger i henhold til Aftalen for at kunne overvåge overholdelsen af denne Databehandlingsaftale. Undtagen i tilfælde af et med rimelighed mistænkt brud på Databehandlingsaftalen eller som i øvrigt tilladt af præceptiv lov, skal denne revision være begrænset til en revision for hver periode på 12 måneder.

8.4 Den Dataansvarlige skal betale eventuelle omkostninger vedrørende revisioner, og Databehandleren er berettiget til at opkræve den Dataansvarlige separat for eventuelle rimelige omkostninger (herunder interne ressourcer til Databehandlerens standardtakster), som Databehandleren måtte pådrage sig i forbindelse med sin hjælp med disse revisioner.

8.5 En revision skal udføres i overensstemmelse med Databehandlerens interne politikker, og alle deltagende er underlagt hensigtsmæssige skriftlige fortrolighedsforpligtelser. I det omfang gældende lov tillader det, skal den Dataansvarlige forsyne Databehandleren med en kopi af revisionsrapporten, og hvis eventuelle Fortrolige Oplysninger fjernes, er Databehandleren berettiget til at anvende denne rapport uden beregning i forhold til andre Dataansvarlige.

8.6 Den Dataansvarlige må kun bruge de indhentede oplysninger i en revision, herunder en eventuel revisionsrapport, med henblik på at overholde sine revisionsforpligtelser i henhold til Databeskyttelseslovgivningen. For at undgå tvivl må den Dataansvarlige ikke videregive nogen del af revisionsrapporten til offentligheden, uden forudgående skriftligt samtykke fra Databehandleren, medmindre præceptiv lov kræver det.

8.7 Databehandleren skal yde al nødvendig hjælp til udførelsen af disse revisioner i aftaleperioden (som anført i klausul 11) i denne Databehandlingsaftale.

8.8 Den Dataansvarlige eller dennes tredjeparts-repræsentanter som anført i klausul 8.3 har tilladelse til at gennemføre revisioner hos Databehandlerens Underdatabehandlere i det omfang, det er muligt i henhold til vilkår og betingelser i den dagældende version af Underdatabehandlerens vilkår og betingelser.

9 OVERFØRSLER TIL TREDJELANDE

9.1 Databehandleren må kun behandle Personoplysninger i lande uden for EØS under forudsætning af dokumenterede instrukser fra den Dataansvarlige som anført i Bilag A.

9.2 Hvis Databehandleren behandler Personoplysninger i et tredjeland (dvs. et land uden for EØS), skal Databehandleren i forvejen informere den Dataansvarlige om denne tilsigtede overførsel, og således give den Dataansvarlige mulighed for at gøre indsigelser, og skal sikre, at følgende betingelser er opfyldt:

a) Databehandleren har sikret, at passende sikkerhedsforanstaltninger (herunder passende juridiske mekanismer) er til stede i forhold til overførslen,

b) Den Registrerede har retsgyldige rettigheder og effektive retsmidler,

c) Databehandleren yder en tilstrækkelige grad af beskyttelse af alle overførte Personoplysninger og

d) Databehandleren overholder rimelige instrukser, som den Dataansvarlige har oplyst denne i forvejen, med hensyn til behandlingen af Personoplysningerne.

10 FORTROLIGHED

10.1 Databehandleren anerkender, at de personer, der er bemyndige til at behandle Personoplysninger, er forpligtet til fortrolighed, herunder alle oplysninger i forbindelse med Aftalen og Parternes virksomhed.

10.2 Bestemmelserne om fortrolighed gælder stadig efter opsigelse af denne Databehandlingsaftale.

11 AFTALEPERIODE OG OPSIGELSE

11.1 Denne Databehandlingsaftale træder i kraft fra ikrafttrædelsesdatoen som anført i Aftalen eller på datoen for den Dataansvarliges underskrivelse på underskriftsiden, hvilket tidspunkt der ligger først, og fortsætter i kraft i Aftaleperioden som defineret i Aftalen.

11.2 Ved opsigelse af Aftalen ophører denne Databehandlingsaftale også.

11.3 Uanset ovennævnte klausul11.2 udløber denne Databehandlingsaftale ikke, før den Dataansvarlige har modtaget og accepteret dokumentation vedrørende sletning beskrevet i klausul 11.6(b), medmindre den Dataansvarlige særskilt accepterer noget andet.

11.4 En bestemmelse i denne Databehandlingsaftale, som udtrykkeligt eller underforstået er beregnet på at træde i kraft eller fortsætte i kraft eller efter ophøret af denne Databehandlingsaftale, skal forblive med fuld gyldighed.

11.5 Opsigelse af denne Databehandlingsaftale, uanset årsag, påvirker ikke de påløbne rettigheder, afhjælpninger, forpligtelser eller ansvar for parterne, der eksisterer ved opsigelsen.

11.6 Ved denne Databehandlingsaftales ophør, uanset årsag:

a) Databehandleren skal så snart som rimeligt muligt tilbagelevere eller tilintetgøre (som skriftligt anvist af den Dataansvarlige) alle Personoplysninger og alle oplysninger og alle andre materialer leveret til denne eller på vegne af den Dataansvarlige i forbindelse med denne Databehandlingsaftale,

b) hvis den Dataansvarlige vælger tilintetgørelse frem for tilbagelevering af materialerne i henhold til klausul 11.6(a) skal Databehandleren så snart som rimeligt muligt sikre, at de tilintetgøres og at alle Personoplysninger slettes fra Softwaren og Planday-systemet.

Uanset det ovenstående må Tilintetgørelse ikke finde sted, før Databehandleren har informeret den Dataansvarlige om den påtænkte Tilintetgørelsesmetode og modtaget den Dataansvarliges bekræftelse på, at Tilintetgørelse skal foregå i overensstemmelse med den metode. Hvis den Dataansvarlige ikke finder den påtænkte Tilintetgørelsesmetode tilstrækkeligt effektiv, skal den Dataansvarlige informere Databehandleren om, hvilken metode der anses for tilstrækkeligt effektiv.

11.7 Databehandleren skal give skriftlig bekræftelse på overholdelse af klausul 11 (a) senest 14 dage efter ophøret af denne Databehandlingsaftale.

12 ÆNDRINGER PÅ GRUND AF ÆNDRINGER I PRÆCEPTIV LOV

12.1 Hvis der sker ændringer i præceptiv Databeskyttelseslovgivning, er Databehandleren berettiget til at ændre denne Databehandlingsaftale i overensstemmelse hermed.

13 LOVVALG OG TVISTER

13.1 Denne Databehandlingsaftale er reguleret af og fortolkes i overensstemmelse med dansk lov. Dog må reglerne om lovkonflikt tilsidesættes i det omfang, at disse regler er deklaratoriske.

13.2 En tvist, der måtte udspringe af denne Databehandlingsaftale, herunder tvister vedrørende eksistensen eller gyldigheden af denne Databehandlingsaftale, skal indbringes for de danske domstole.

Denne Databehandlingsaftale er udfærdiget i to originaler, og hver Part modtager et eksemplar.

UNDERSKRIFTARK FØLGER

UNDERSKRIFTARK TIL DATABEHANDLINGSAFTALE VEDRØRENDE DATABEHANDLERENS BEHANDLING AF PERSONOPLYSNINGER PÅ VEGNE AF DEN DATAANSVARLIGE

For Databehandleren:	For den Dataansvarlige:
Dato:	Dato:
Navn:	Navn:
_____	_____

Bilag A til Databehandlingsaftale

I forbindelse med Databehandlerens levering af tjenester og hosting af Personoplysningerne på vegne af den Dataansvarlige giver den Dataansvarlige Databehandleren instruks og giver samtykke til behandling af følgende Personoplysninger til de nedennævnte formål:

1. Generel beskrivelse og formål med Behandlingsaktiviteterne
Behandlingsaktiviteter

Databehandleren behandler den Dataansvarliges Personoplysninger med det formål at levere ledelse af arbejdskraft.

2. Kategorier af Registrerede
Kategorierne af Registrerede kan til enhver tid ændres i det omfang, at behandlingen af Personoplysninger og formålene dermed fortsat hører ind under den generelle beskrivelse.

(i) *Medarbejdere*
(ii) *Potentielle medarbejdere*
(iii) *Tidligere medarbejdere*

3. Typer af Personoplysninger
Beskrivelse af typerne af Personoplysninger for hver kategori Registrerede

Fulde navn og initialer, adresse, e-mailadresse, telefon, køn, skatte-ID, bankoplysninger, fødselsdato, slægtninges eller nærmeste pårørendes fulde navn og telefonnummer, lønoplysninger, foto, oplysninger om ansættelsesaftale, oplysninger om medarbejderens lønseddel, data indtastet i tilpassede felter oprettet af Kunden, som kan indeholde følsomme Personoplysninger.

4. Hvem hos Databehandleren har adgang til Personoplysningerne
Kun personer, der er ansat til det formål, hvortil Personoplysningerne behandles, bemyndiges til at tilgå og behandle Personoplysninger, herunder medarbejdere, der leverer:

- *Supportydelser*
- *Vedligeholdelse og backup*
- *Driftssystem/supportpersonale*

5. Hvilke eksterne parter (ud over Databehandleren) har adgang til alle eller dele af Personoplysningerne (underbehandlere) til hvilket formål og deres geografiske placering (herunder hvis uden for EØS)?

Underdata-behandler	Beskrivelse	Postadresse	Virksomhedsregistrerings-nummer	Kontakt
Netgroup	Hosting af infrastruktur	Netgroup A/S Hørskætten 5, 2630 Taastrup	26 09 35 03	info@netgroup.dk
Salesforce	Kunden registrerer ledende databehandl er, der er nødvendig for Salgs- og Supportakti-viteter	Floor 26 Salesforce Tower 110 Bishopsgate London United Kingdom EC2N 4AY	05 09 40 83	privacy@salesforce.com
Intercom	Chat-support i realtid inden for produkter til kunder og	3rd Floor, Stephens Ct.18-	538158	compliance@intercom.com

	in-product meddelelser	21 St. Stephen's Green Dublin 2 Ireland		
Amazon Web Services	Hosting af infrastruktur – data lagret inden for EU/EØS	One Burlington Plaza Burlington Road Dublin 4 Ireland	566018	https://aws.amazon.com/contact-us/
Microsoft Azure	Hosting af infrastruktur – data lagret inden for EU/EØS	One Microsoft Place South County Business Park Leopardstown, Dublin 18 D18 P521 Ireland	256796	https://azure.microsoft.com/en-gb/support/options/

Bilag B til Databehandlingsaftalen

Sikkerhedsforanstaltninger

Databehandleren indfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der er hensigtsmæssigt i forhold til risikoen ved behandlingen. Disse foranstaltninger omfatter, men er ikke begrænset til:

1. Adgangskontrol til lokaler og anlæg (fysiske)

1.1 Databehandleren er kontraktligt forpligtet til at stille kommercielt rimelige fysiske sikkerhedssystemer til rådighed på alle underdatabehandlerens eller de hostede datacentre og administrationssteder, som anvendes til Persondatabehandling.
1.2 Databehandleren er kontraktligt forpligtet til at implementere fysisk adgangskontrol for alle underdatabehandlerens eller de hostede datacentre (herunder bl.a. kun ved at godkende adgangskontrol til datacentre sammen med underdatabehandleren, f.eks. om onsite-personale skal forhindre uautoriseret adgang til datacentre, eller at nødvendig biometrisk scanning eller videoovervågning forefindes, eller at korsbomme er integreret med adgangskontrollæsere med henblik på til enhver tid at kontrollere den fysiske adgang på alle steder, ved at kræve, at personalet viser foto-id, før de kan få adgang til stedet)
1.3 Databehandleren vil undersøge om underdatabehandlerens eller de hostede datacentre skal opretholde procedurer med henblik på at udstede identifikationskort til bemyndiget personale og kontrollere fysisk adgang til de systemer, der er under Databehandlerens kontrol,
1.4 Databehandleren godkender via underdatabehandlerens eller det hostede datacenter, om besøgende er forhåndsgodkendte, før de kommer til behandlingsstederne, som anvendes til at behandle Personoplysninger, og bliver anmodet om at fremvise identifikation og/eller underskrive en log over besøgende, og bliver til enhver tid ledsaget, når de befinder sig på stederne.

2. Adgangskontrol til systemer (virtuelle)

2.1 Databehandleren skal oprette og vedligeholde kommercielt rimelige sikkerhedsforanstaltninger mod hændelig eller uautoriseret adgang til, tilintetgørelse af, eller ændring af Personoplysningerne på systemerne, der anvendes til at behandle Personoplysninger:

2.1.1 der ydes adgang for personale på baggrund af adgangsrettigheder og specifikke roller gennem dokumenteret anmodningsprocedurer for adgang,
2.1.2 adgangskontrol muliggøres ved operativsystem, database eller på applikationsniveau,
2.1.3 administrativ adgang begrænses for at forhindre ændringer i systemer eller applikationer,
2.1.4 brugerne vil, hvor det er muligt, blive tildelt en enkelt konto med multifaktorgodkendelse og vil ikke kunne dele deres konti.

3. Adgangskontrol for udstyr og bærbare

3.1 Databehandleren indfører og opretholder kommercielt rimelige sikkerhedsforanstaltninger hvad angår mobilt udstyr og bærbære, der anvendes til at behandle Personoplysninger.

4. Adgangskontrol til Persondata

4.1 Adgang gives først efter fuldførelse af en godkendt proces, dvs. LAN Logon-ID, adgangs-ID til applikationer eller anden lignende ID.
4.2 Der udstedes unik bruger-ID og kodeord til brugerne.

4.3 Når brugerne er verificeret, bemyndiges de til adgangsniveauer på baggrund af deres specifikke rolle og på baggrund af adgangsrettigheder.

5. Kontrol med overførsel og videregivelse

5.1 Databehandleren skal indføre og opretholde kommercielt rimelige foranstaltninger for at forhindre, at Personoplysninger læses, kopieres, ændres eller fjernes uden bemyndigelse under elektronisk overførsel eller transport og muliggøre, at Databehandleren kontrollerer og fastslår, til hvilke organer overførslen af Personoplysninger via dataoverførselsanlæg forudses.
5.2 Databehandleren skal opretholde teknologi og processer beregnet på at minimere adgang til ulovlig behandling, herunder teknologi til kryptering af Personoplysninger.

6. Inputkontrol

6.1 Databehandleren skal opretholde system- og databaselogger til adgang til alle Personoplysninger, som Databehandleren kontrollerer,
6.2 Alle Databehandlerens systemer skal være konfigureret til at give logging af hændelser for at identificere systemlækager, uautoriseret adgang eller anden overtrædelse af sikkerheden. Logger skal beskyttes mod uautoriseret adgang eller ændring,
6.3 Kunden/Databehandleren skal opretholde inputkontrol på sine systemer.

7. Kontrol med arbejdet

7.1 Databehandleren skal indføre procedurer for at sikre sine medarbejderes pålidelighed og andre personers pålidelighed, der arbejder under Databehandlerens ledelse, som kan komme i kontakt med, eller på anden måde have adgang til og behandle Personoplysninger, såsom ved at gennemføre baggrundstjek forud for ansættelsen.
7.2 Databehandleren skal indføre procedurer til at sikre, at Databehandlerens personale er klar over sit ansvar i henhold til Aftalen. Databehandleren skal instruere og uddanne alle de personer, man bemyndiger til at have adgang til Personoplysningerne om Databeskyttelseslovgivningen samt om alle relevante sikkerhedsstandarder, og skal forpligte dem skriftligt til at overholde datahemmeligheden, Databeskyttelseslovgivningen og andre relevante sikkerhedsstandarder.
7.3 Databehandleren skal straks handle for at tilbagekalde Kundens/Databehandlerens Personoplysninger på grund af opsigelse, ændring i jobfunktion eller hvis det konstateres, at brugeren er inaktiv eller har forlænget fravær.
7.4 Databehandleren skal have en databeskyttelsespolitik på plads og en politik for opbevaring af dokumenter, som Databehandlerens personale skal overholde.

8. Hændelseshåndtering

8.1 Databehandleren skal indføre og vedligeholde en procedure for styring af hændelser, der gør det muligt for behandleren at informere den Dataansvarlige om evt. relevante hændelser inden for den krævede tidsramme.
8.2. Hvis en hændelse (potentielt) påvirker Personoplysninger, skal Databehandleren give den Dataansvarlige meddelelse i overensstemmelse med Klausul 4 i Databehandlingsaftalen.
8.3 Proceduren for hændelseshåndtering omfatter periodisk vurdering af tilbagevendende forhold, der kan indikere et sikkerhedsbrud.
8.4 Databehandleren vil regelmæssigt gennemgå eventuelle tidligere hændelser med henblik på læring.

9. Tilgængelighedskontrol

9.1 Databehandleren skal beskytte Personoplysninger mod hændelig tilintetgørelse eller tab ved at sikre:

9.1.1 Arbejdsstationer skal beskyttes af kommerciel software til at forhindre antivirus og malware, som jævnligt opdateres med af definitioner,

9.1.2 Ved opdagelse af en virus eller malware skal Databehandleren straks tage skridt til at standse spredning af virus og den ødelæggelse, som virus eller malware forårsager, og slette virus eller malware.

9.1.3 Servere skal beskyttes af kommercielle firewalls og systemer til beskyttelse mod indtrængen.

10. Driftskontinuitet og forandringsledelse

10.1 Databehandleren skal indføre, opretholde og regelmæssigt gennemgå en plan for driftskontinuitet samt en katastrofeberedskabsplan, der blandt andet gør det muligt for Databehandleren rettidigt at genskabe tilgængelighed og adgang til Personoplysningerne, som skal aftales af parterne, der er omfattet i tilfælde af en fysisk eller teknisk hændelse.
10.2 Databehandleren vil implementere forandringsledelse med henblik på at kontrollere organisationen, forretningsprocesser, systemer og underdatabehandlerforhold, som har indflydelse på sikkerheden.
10.3 Som led i proceduren for forandringsledelse, gennemgår Databehandleren eventuelle påvirkninger af persondatasikkerheden med henblik på læring.

11. Kontrol af instrukser

11.1 Databehandleren skal indføre og opretholde procedurer for at sikre, at Personoplysninger kun behandles i overensstemmelse med den Dataansvarliges instrukser.

12. Kontrol af adskillelse

12.1 Databehandleren skal indføre og opretholde procedurer for at sikre, at personoplysninger, der er indsamlet til forskellige formål, behandles separat i det omfang, at Databehandleren udtrykkeligt har fået meddelelse om disse forskellige formål og anmodet om at gøre dette på den betingelse, at Databehandleren kan fakturere sin tid og sine udgifter for at overholde denne anmodning.

13. Regelmæssig afprøvning af sikkerhedsforanstaltninger

14.1 Databehandleren skal ofte afprøve, vurdere og evaluere effektiviteten af sine tekniske og organisatoriske sikkerhedsforanstaltninger.

***