This translation is provided for convenience only, in the event of any dispute or claim the English language version will take precedence.
Denne oversettelsen har kun praktisk betydning. Ved en eventuell tvist eller et krav, vil den engelske versjonen være gjeldende.

MAL FOR DATABEHANDLINGSAVTALE

mellom

[Sett inn kundens navn]
[Sett inn CVR-nr. eller foretaksnummer]
[Sett inn adresse]
(«behandlingsansvarlig» eller «kunden»)

og

Planday A/S
Dansk org.nr. (CVR) 2766 6248
Kuglegårdsvej 7-9-11, Bygning 181
1434 Copenhagen K
Denmark
(«databehandler» eller «Planday»)

(enkeltvis kalt en «part», sammen kalt «partene»)

om databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige.

1 FORMÅL OG BAKGRUNN

1.1 Den behandlingsansvarlige har samtykket til å gi databehandleren i oppdrag å levere programvare og tjenester i henhold til vilkårene i kontrakten.

1.2 Som en del av leveransen av programvare og tjenester vil databehandleren måtte behandle personopplysninger, som kan være knyttet til spesifikke fysiske personer som beskrevet i tillegg A.

1.3 Databehandlingsavtalen fastsetter vilkårene og betingelsene som gjelder for databehandlerens behandling av personopplysninger.

2 DEFINISJONER OG TOLKNING

2.1 Følgende ord og uttrykk har de betydningene som er nevnt nedenfor i databehandlingsavtalen, hvis ikke annet går fram av sammenhengen.

Tillegg	betyr tillegg til denne databehandlingsavtalen.
Virkedag	er en dag som ikke er lørdag, søndag eller offentlig høytidsdag.
Kontortid	er fra kl. 09.00 til 17.00 på en virkedag.
Kontrakt	betyr kundeavtalen mellom databehandleren og

	kunden angående levering av tjenester, og databehandlerens generelle vilkår og betingelser, inkl. alle eventuelle tidsplaner, tillegg og endringer av disse.
Behandlingsansvarlig	er kunden som er definert i kontrakten, og i henhold til definisjonen i gjeldende personvernlovgivning.
Databehandlingsavtale	er denne avtalen med tillegg.
Databehandlingstjenester	er tjenestene beskrevet i Tillegg A
Personvernlovgivning	er lovgivning, inkludert eventuelle tillegg og endringer, som beskytter enkeltpersoners grunnleggende rettigheter og friheter, og spesielt deres rett til personvern med hensyn til behandling av personopplysninger gjeldende for en behandlingsansvarlig i EØS-landet der den behandlingsansvarlige er etablert, inkludert personvernforordningen (GDPR), Storbritannias databeskyttelseslov 2018, direktivet om personvern og elektronisk kommunikasjon 2002/58/EC (som oppdatert av 2009/136/EC-direktivet og lovgivningen om personvern og elektronisk kommunikasjon 2003 (*SI 2003/2426*). En referanse til personvernlovgivning viser til gjeldende lovverk inkludert de endringer, utvidelser eller nye vedtak som gjelder til enhver tid.
En registrert person	er en identifisert eller identifiserbar fysisk person (en identifiserbar person er en som direkte eller indirekte kan identifiseres, spesielt ved referanse til en identifikator, f.eks. et navn, identifikasjonsnummer, lokaliseringsdata, en online-identifikator eller ved ett eller flere elementer som er spesifikke for denne fysiske personens fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet).
Tilintetgjøre/tilintetgjøring	betyr at personopplysninger ugjenkallelig slettes fra alle lagringsmedier de har vært oppbevart på, og at disse personopplysningene ikke på noen måte kan gjenopprettes, heller ikke av eventuelle underbehandlere. Dette gjelder alle lagringsmedier som brukes i forbindelse med databehandlingen, og inkluderer alle eksisterende kopier.
Distributør	betyr [sett inn den aktuelle distributørens navn, org.nr. og adresse].

EØS	betyr Det europeiske økonomiske samarbeidsområdet.
Sluttbrukerlisensavtale	er avtalen mellom Planday og en hvilken som helst registrert person som bruker vaktliste-programvaren med navnet «Planday» og/eller en annen programvare tilknyttet denne.
Personvernforordningen (GDPR)	er EU-forordning 2016/679 utstedt av Europaparlamentet og Det europeiske råd 27. april 2016, angående beskyttelsen av fysiske personer med hensyn til behandling av personopplysninger og om den frie flyten av slike opplysninger, som opphever EU-direktiv 95/46/EF (personverndirektivet).
Personopplysninger	Enhver informasjon, uansett form, som er relatert til den registrerte ,og som defineres nærmere i personvernlovgivning.
Brudd på personopplysningssikkerheten	er et sikkerhetsbrudd som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.
Behandle/behandling	viser til enhver operasjon eller rekke av operasjoner, automatiserte eller ikke, som gjøres med personopplysninger eller sett av personopplysninger, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller kombinering, begrensning, sletting eller tilintetgjøring.
Behandlingsoperasjoner	Som definert i tillegg A.
Databehandler	betyr Planday, som definert i databehandlingsavtalen og iht. definisjonen i gjeldende personvernlovgivning.
Returnering	betyr at alle personopplysninger returneres fysisk og elektronisk til den behandlingsansvarlige, og at alle kopier o.l. av opplysningene som eventuelt er i databehandlerens besittelse, eller som databehandleren har til disposisjon, inkl. personopplysninger som er overlevert til underbehandlere, skal tilintetgjøres.

Underbehandler	viser til en annen behandler som er engasjert av databehandleren for å utføre bestemte behandlingsaktiviteter på vegne av den behandlingsansvarlige.
Planday-system	er ethvert informasjonsteknologisystem eller -systemer som databehandlingstjenestene utføres på i henhold til denne databehandlingsavtalen.

2.2 Hvis annet ikke spesifiseres eller går fram av sammenhengen, viser ord i entallsform også til flertall, og ord i flertallsform omfatter også entall.

2.3 Alle ord som kommer etter begrepene «inkludert», «inkluderer», «spesielt», «for eksempel» eller lignende uttrykk, skal oppfattes som illustrerende eksempler og skal ikke begrense de relaterte generelle ordenes generelle gyldighet.

2.4 Alle unntak fra eller øvre begrensninger av ansvar i kontrakten skal også gjelde for databehandlerens ansvar i henhold til denne databehandlingsavtalen.

3 OMFANG

3.1 Databehandlingsavtalen gjelder all behandling av personopplysninger som utføres av databehandleren i tilknytning til utførelsen av databehandlingstjenestene for den behandlingsansvarlige, som definert i tillegg A (virkeområdet).

3.2 Kunden og Planday er innforstått med at kunden er behandlingsansvarlig og Planday databehandler med hensyn til alle personopplysninger som formidles til Planday av eller på vegne av kunden, inkludert personopplysninger som beskrevet i tillegg A, under leveringen av databehandlingstjenestene.

3.3 Databehandlingens art og formål, ulike typer personopplysninger og kategorier av registrerte personer er beskrevet i tillegg A.

3.4 Ingenting i denne databehandlingsavtalen skal ha innvirkning på Plandays rettigheter og forpliktelser som er fastsatt i sluttbrukerlisensavtalen.

4 DATABEHANDLERENS FORPLIKTELSER

4.1 Databehandleren skal:

a) kun behandle personopplysninger i henhold til dokumenterte instrukser fra den behandlingsansvarlige, som angitt i denne databehandlingsavtalen og med de formålene som er angitt i tillegg A;

b) utføre sine aktiviteter i henhold til denne databehandlingsavtalen med all nødvendig dyktighet, påpasselighet og nøyaktighet;

c) føre en protokoll som beskrevet i art. 30 av GDPR i sine vanlige forretningslokaler, over all behandling av personopplysninger som gjøres under utførelsen av databehandlingstjenestene, og over databehandlerens overholdelse av forpliktelsene som beskrevet i denne databehandlingsavtalen («protokoller»);

d) sørge for at personer som er autorisert til å behandle personopplysninger, har avlagt bindende taushetsløfte, eller at de har en gjeldende lovpålagt konfidensialitetsplikt;

e) innføre hensiktsmessige tekniske og organisatoriske tiltak for å beskytte personopplysninger mot utilsiktet eller ulovlig tilintetgjøring eller utilsiktet tap, endring, ulovlig spredning eller tilgang og mot alle andre ulovlige behandlingsmetoder, inkludert kravene i forbindelse med slike tiltak i henhold til personvernlovgivningen, som angitt i paragraf 6;

f) bare kopiere personopplysningene i den grad det er absolutt nødvendig, som blant annet kan omfatte sikkerhetskopiering, speiling, sikkerhet, katastrofegjenoppretting og testing av personopplysningene;

g) bare utkontraktere aktiviteter til underbehandlere i samsvar med kravene i paragraf 7;

h) øyeblikkelig informere den behandlingsansvarlige hvis en instruks etter databehandlerens vurdering utgjør et brudd på personvernlovgivningen;

i) assistere den behandlingsansvarlige ved å, så langt det er mulig, innføre hensiktsmessige tekniske og organisatoriske tiltak for å oppfylle den behandlingsansvarliges forpliktelse til å svare på forespørsler om utøvelse av registrerte personers ikke-eksklusive rettigheter til tilgang, rettelse, sletting og dataportabilitet, slik disse er beskrevet i personvernlovgivningen;

j) etter ønske fra den behandlingsansvarlige tilintetgjøre eller returnere alle personopplysningene til den behandlingsansvarlige, enten i løpet av eller etter denne databehandlingsavtalens gyldighetsperiode, jf. paragraf 11;

k) gi den behandlingsansvarlige tilgang til all nødvendig informasjon for å bevise overholdelse av personvernlovgivningen, f.eks. årlig samsvarsattest iht. ISO27001, hvis tilgjengelig;

l) i tilknytning til paragraf 4.1 (k) tillate og bidra til revisjoner hvis det er juridisk og teknisk mulig, inkludert inspeksjoner utført av den behandlingsansvarlige eller av andre som er utnevnt av den behandlingsansvarlige, som beskrevet i paragraf 8;

m) oppfylle sine forpliktelser i henhold til personvernlovgivningen, inkludert, der det er aktuelt, å utnevne en personvernrådgiver.

4.2 Hvis databehandleren mottar en klage, et varsel eller annen kommunikasjon som direkte eller indirekte er forbundet med behandlingen av personopplysninger eller med en av partenes overholdelse av personvernlovgivningen, skal databehandleren øyeblikkelig gi beskjed til den behandlingsansvarlige, og samarbeide med og assistere den behandlingsansvarlige så langt det er mulig i forbindelse med alle slike klager, varsler eller kommunikasjoner.

4.3 Databehandlerens ansvar i henhold til kontrakten, inkludert databehandlingsavtalen, har begrensninger og fraskrivelser i henhold til vilkårene i kontrakten.

4.4 Databehandleren skal uten unødig opphold informere den behandlingsansvarlige hvis databehandleren får kjennskap til eller blir klar over brudd på personopplysningssikkerheten.

4.5 Databehandleren skal ha rett til å ta separat betalt fra den behandlingsansvarlige for alle eventuelle kostnader (inkl. interne ressurser, til databehandlerens standardpriser) som kan påløpe i forbindelse med assistanse som vist til under paragraf 4.1 (a–m).

5 DEN BEHANDLINGSANSVARLIGES FORPLIKTELSER

5.1 Den behandlingsansvarlige er alene ansvarlig for og forpliktet til å overholde det gjeldende lovverket for behandlingsansvarlige. Den behandlingsansvarlige skal sørge for at den overholder all personvernlovgivning før den bruker programvaren og mottar tjenester i henhold til kontrakten, på en måte som omfatter behandling av personopplysninger, f.eks. i tilknytning til formidling av nødvendig informasjon/meddelelser til og/eller godkjennelser fra registrerte personer og/eller tilsynsmyndigheter i forbindelse med databehandlingen.

5.2 Den behandlingsansvarlige skal omgående gi beskjed til databehandleren hvis den blir oppmerksom på at behandlingen av den behandlingsansvarliges personopplysninger kan være i strid med personvernlovgivningen.

5.3 Den behandlingsansvarlige garanterer at om databehandleren følger alle instrukser fra den behandlingsansvarlige nøyaktig, vil dette ikke føre til brudd på gjeldende personvernlovgivning.

5.4 Den behandlingsansvarlige vil holde databehandleren skadesløs fra alle tap som følger av at den behandlingsansvarlige ikke oppfyller sine forpliktelser i henhold til denne avtalen.

6 SIKKERHETSTILTAK

6.1 Databehandleren er forpliktet til å implementere egnede tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er hensiktsmessig i forhold til risikoene databehandlingen medfører, spesielt for utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet, der det tas i betraktning hvor oppdatert løsningen er, implementeringskostnader og databehandlingens art, omfang, bakgrunn og formål samt sannsynligheten for forekomst og alvorlighetsgraden av risikoene fysiske personers rettigheter og friheter utsettes for, inkludert bl.a., etter hva som er relevant:

a) pseudonymisering og kryptering av personopplysninger;

b) evnen til å sikre kontinuerlig konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene;

c) evnen til å gjenopprette tilgjengelighet og tilgang til personopplysninger innen rimelig tid dersom en fysisk eller teknisk hendelse oppstår;

d) en prosedyre for regelmessig testing, analysering og vurdering av hvor effektive databehandlingens tekniske og organisatoriske sikkerhetstiltak er.

6.2 Databehandleren skal innføre tiltak for å sikre at enhver fysisk person som utfører handlinger på vegne av databehandleren, og som har tilgang til personopplysningene, bare skal behandle

personopplysningene etter instruks fra den behandlingsansvarlige, med mindre noe annet kreves i henhold til personvernlovgivning.

6.3 De spesifikke tekniske og organisatoriske sikkerhetstiltakene databehandleren har innført, er beskrevet i tillegg B (sikkerhetstiltak).

7 UNDERBEHANDLERE

7.1 Den behandlingsansvarlige gir herved databehandleren tillatelse til å engasjere underbehandlere til å utføre behandling av personopplysninger, inkludert, men ikke begrenset til, underbehandlere som er oppgitt i tillegg A, forutsatt at databehandleren inngår en skriftlig avtale med hver underbehandler der de binder seg til de samme forpliktelsene som pålegges databehandleren i henhold til denne databehandlingsavtalen. Etter å ha gitt rimelig forhåndsvarsel har den behandlingsansvarlige til enhver tid rett til å motta kopier av databehandlerens databehandlingsavtaler med alle underbehandlerne.

7.2 Databehandleren skal forhåndsinformere den behandlingsansvarlige via e-post om eventuelle planer om å engasjere flere eller bytte ut underbehandlere, og behandlingsansvarlig / registrert person skal ha muligheten til å protestere og/eller gi informert samtykke, der dette ikke skal holdes tilbake uten rimelig grunn. Den behandlingsansvarlige kan ikke protestere uten å ha en konkret, ekte og objektiv grunn, om ikke annet fremgår i ufravikelige lovbestemmelser. Hvis den behandlingsansvarlige protesterer mot å engasjere flere underbehandlere eller å erstatte en underbehandler, og forutsatt at denne protesten er basert på en konkret, ekte og objektiv grunn, har databehandleren rett til å avslutte databehandlingsavtalen med øyeblikkelig virkning ved å gi skriftlig beskjed om dette.

7.3 Hvis en underbehandler ikke oppfyller sine personvernforpliktelser i henhold til databehandlingsavtalen nevnt under paragraf 7.1, skal databehandleren fortsatt ha fullt ansvar overfor den behandlingsansvarlige for utførelsen av underbehandlerens oppgaver og oppfyllelsen av dennes personvernforpliktelser generelt.

8 REVISJONER

8.1 Med formål å revidere databehandlerens overholdelse av sine forpliktelser iht. denne databehandlingsavtalen, skal databehandleren etter å ha mottatt et rimelig forhåndsvarsel minst tretti (30) dager i forveien la den behandlingsansvarlige utføre en revisjon i løpet av kontortiden, men også uten forhåndsvarsel i tilfeller der det er rimelig grunn til å mistenke at databehandleren har brutt denne databehandlingsavtalen, der revisjonen omfatter, men ikke er begrenset til å:

a) få adgang til å inspisere og ta kopier av datapostene og all annen informasjon som oppbevares i databehandlerens lokaler eller i databehandlerens systemer i tilknytning til databehandlingstjenestene, og:

b) få tilgang til å inspisere behandlingssystemet.

8.2 Det skriftlige forhåndsvarselet skal omfatte et forslag til revisjonsplan. Hvis en del av revisjonens foreslåtte omfang er dekket av omfanget av en revisjonsrapport utstedt av en kvalifisert ekstern revisor i løpet av de siste 12 månedene, kan databehandleren be den behandlingsansvarlige om å vurdere om denne rapporten kan brukes i stedet for å utføre en revisjon. Databehandleren skal ha rett til å foreslå en revisjonsdato og -tidspunkt, slik at forretningsdriften påvirkes minst mulig, og kan foreslå at revisjonen

kombineres med andre behandlingsansvarliges revisjoner. Den behandlingsansvarlige kan ikke avslå slike forslag fra databehandleren uten å ha en konkret, ekte og objektiv grunn til det.

8.3 På skriftlig forespørsel fra den behandlingsansvarlige slik paragrafene 8.1 og 8.2 beskriver, har den behandlingsansvarlige (eller et kontrollorgan bestående av uavhengige medlemmer med de nødvendige faglige kvalifikasjoner og som har taushetsplikt, utnevnt av den behandlingsansvarlige eller et reguleringsorgan) rett til å utføre revisjoner av databehandlerens fasiliteter og sikkerhetsrutiner som er direkte forbundet med behandlingen av personopplysninger i henhold til kontrakten, for å kunne kontrollere samsvar med denne databehandlingsavtalen. Med unntak av tilfeller der det er rimelig grunn til å mistenke brudd på denne databehandlingsavtalen, eller der det tillates av ufravikelige lovbestemmelser, skal slike revisjoner begrenses til 1 revisjon i løpet av en 12-månedersperiode.

8.4 Den behandlingsansvarlige skal dekke alle kostnader forbundet med revisjoner, og databehandleren skal ha rett til å ta separat betalt fra den behandlingsansvarlige for alle rimelige kostnader (inkl. interne ressurser, til databehandlerens standardpriser) som databehandleren pådrar seg i forbindelse med sin assistanse ved slike revisjoner.

8.5 Alle revisjoner skal utføres i samsvar med databehandlerens interne retningslinjer, og alle deltakere skal avkreves egnede skriftlige taushetsløfter. I den grad det er tillatt i henhold til gjeldende lovverk skal den behandlingsansvarlige gi databehandleren en kopi av revisjonsrapporten, forutsatt at alle konfidensielle opplysninger fjernes, og databehandleren skal ha rett til å bruke denne rapporten vederlagsfritt overfor andre behandlingsansvarlige.

8.6 Den behandlingsansvarlige kan bare bruke informasjonen som innhentes ved en revisjon, inkl. alle revisjonsrapporter, til å oppfylle sine revisjonsforpliktelser i henhold til personvernlovgivning. For å unngå tvil presiseres det at den behandlingsansvarlige ikke kan formidle noen deler av revisjonsrapporten til offentligheten uten skriftlig forhåndsgodkjennelse fra databehandleren, unntatt om dette kreves av ufravikelige lovbestemmelser.

8.7 Databehandleren skal gi all nødvendig assistanse til å utføre slike revisjoner i løpet av denne databehandlingsavtalens gyldighetsperiode (som fastsatt i paragraf 11).

8.8 Den behandlingsansvarlige, eller dennes eksterne representanter som beskrevet i paragraf 8.3, kan gjennomføre revisjoner av databehandlerens underbehandlere i den grad det er mulig i henhold til vilkårene og betingelsene som gjelder underbehandleren på tidspunktet da revisjonen ønskes utført.

9 OVERFØRINGER TIL TREDJELAND

9.1 Databehandleren kan bare behandle personopplysningene i land utenfor EØS-området i henhold til dokumenterte instrukser fra den behandlingsansvarlige, som spesifisert i tillegg A.

9.2 Hvis databehandleren behandler personopplysninger i et tredjeland (land utenfor EØS), skal databehandleren informere den behandlingsansvarlige om denne planlagte overføringen på forhånd, og den behandlingsansvarlige skal ha muligheten til å protestere på dette, og vil sørge for at følgende vilkår oppfylles:

a) databehandleren har sikret at nødvendige sikkerhetsforanstaltninger (herunder nødvendige juridiske mekanismer) er til stede i forhold til overførselen;

b) den registrerte har rettsgyldige rettigheter og effektive rettsmidler;

c) databehandleren yter tilstrekkelig grad av beskyttelse av alle overførte personopplysninger, og

d) databehandleren overholder rimelige instrukser med hensyn til behandlingen av personopplysningene, som den dataansvarlige har opplyst denne om på forhånd.

10 TAUSHETSPLIKT

10.1 Databehandleren bekrefter at personene som er autorisert til å behandle personopplysningene, har taushetsplikt, inkludert for all informasjon forbundet med kontrakten og partenes forretninger.

10.2 Bestemmelsene om taushetsplikt skal fortsatt gjelde etter at denne databehandlingsavtalen er avsluttet.

11 GYLDIGHETSPERIODE OG AVSLUTNING

11.1 Denne databehandlingsavtalen trer i kraft enten på ikrafttredelsesdatoen som er spesifisert i kontrakten, eller på datoen da den behandlingsansvarlige skriver under på signatursiden, etter det som kommer først, og skal gjelde gjennom hele gyldighetsperioden som fastsatt i kontrakten.

11.2 Ved avslutning av kontrakten skal denne databehandlingsavtalen også avsluttes.

11.3 Uavhengig av paragraf 11.2 ovenfor skal denne databehandlingsavtalen ikke utløpe før den behandlingsansvarlige har mottatt og akseptert dokumentasjonen angående sletting som beskrevet i paragraf 11.6(b), om den behandlingsansvarlige ikke uttrykkelig har godkjent noe annet.

11.4 Alle bestemmelser i denne databehandlingsavtalen som uttrykkelig eller implisitt er ment å tre i kraft eller å fortsatt gjelde etter avslutningen av denne databehandlingsavtalen, skal fortsatt gjelde fullt ut.

11.5 Avslutning av denne databehandlingsavtalen skal, uansett grunn, ikke ha innvirkning på opparbeidede rettigheter, rettsmidler, forpliktelser eller ansvar partene har ved avslutning av avtalen.

11.6 Ved avslutning eller oppsigelse av denne databehandlingsavtalen, uansett grunn:

a) skal databehandleren så snart det er rimelig mulig returnere eller tilintetgjøre (etter skriftlige instrukser fra den behandlingsansvarlige) alle personopplysninger og all informasjon eller annet materiell databehandleren har fått fra eller på vegne av den behandlingsansvarlige i tilknytning til denne databehandlingsavtalen;

b) hvis den behandlingsansvarlige velger tilintetgjørelse i stedet for returnering av materiellet nevnt i paragraf 11.6 (a) skal databehandleren så snart det er rimelig mulig, sørge for at det tilintetgjøres, og at alle personopplysninger slettes fra programvaren og fra Planday-systemet.

Ikke desto mindre skal tilintetgjørelsen ikke skje før databehandleren har informert den behandlingsansvarlige om den tiltenkte tilintetgjørelsesmetoden, og fått den behandlingsansvarliges bekreftelse på at tilintetgjørelsen skal utføres ved hjelp av denne metoden. Hvis den behandlingsansvarlige ikke vurderer den tiltenkte tilintetgjørelsesmetoden til å være effektiv nok, vil den behandlingsansvarlige informere databehandleren om hvilken metode som anses å være tilstrekkelig effektiv.

11.7 Databehandleren skal skaffe til veie en skriftlig bekreftelse på samsvar med paragraf 11 (a) ikke senere enn 14 dager etter avslutning av denne databehandlingsavtalen.

12 ENDRINGER GRUNNET ENDRINGER I UFRAVIKELIGE LOVER

12.1 Hvis påbudt personvernlovgivning endres, har databehandleren rett til å endre denne databehandlingsavtalen i henhold til disse endringene.

13 GJELDENDE LOVER OG LØSNING AV TVISTEMÅL

13.1 Denne databehandlingsavtalen er underlagt og skal tolkes i samsvar med dansk lovgivning. Imidlertid må lovvalgsregler og prinsipper for lovkonflikt ses bort fra der disse reglene ikke er påbudte.

13.2 Ethvert tvistemål som oppstår i forbindelse med denne databehandlingsavtalen, inkludert tvistemål som gjelder om denne databehandlingsavtalen eksisterer eller er gyldig, skal fremmes for danske domstoler.

Denne databehandlingsavtalen er utstedt i to originaleksemplarer, der hver part mottar én kopi.

SIGNATURARK FØLGER

SIGNATURARK FOR DATABEHANDLINGSAVTALE VEDRØRENDE DATABEHANDLERENS BEHANDLING AV PERSONOPPLYSNINGER PÅ VEGNE AV DEN BEHANDLINGSANSVARLIGE

For databehandleren:
Dato:
Navn:

_____

For den behandlingsansvarlige:
Dato:
Navn:

_____

Tillegg A til databehandlingsavtale

I forbindelse med databehandlerens levering av tjenester og oppbevaring av personopplysningene på vegne av den behandlingsansvarlige gir den behandlingsansvarlige databehandleren tillatelse til og instrukser om behandling av følgende personopplysninger med formålene som er angitt nedenfor:

1. Generell beskrivelse av og formålet med behandlingsoperasjonene

Behandlingsoperasjoner:

Databehandleren behandler den behandlingsansvarliges personopplysninger for å levere personalforvaltningstjenester.

2. Kategorier av registrerte personer

Kategoriene av registrerte personer kan justeres fra tid til annen, så lenge behandlingen av personopplysningene og formålene med den fortsatt omfattes av den generelle beskrivelsen.

(i) *ansatte*
(ii) *potensielle ansatte*
(iii) *tidligere ansatte*

3. Typer personopplysninger

Beskrivelse av typer av personopplysninger for hver kategori av registrerte personer

Fullt navn og initialer, adresse, e-postadresse, telefonnummer, kjønn, personnummer, bankinformasjon, fødselsdato, slektningers eller pårørendes fulle navn og telefonnummer, lønningsinformasjon, fotografi, informasjon i ansettelseskontrakt, informasjon i lønnsslipper, data som er lagt inn i egendefinerte felter opprettet av kunden som kan inneholde sensitive personopplysninger.

4. Hvem hos databehandleren har tilgang til personopplysningene?

Kun personer som arbeider med formålene personopplysningene behandles for, kan autoriseres til å ha tilgang til og behandle personopplysningene, inkludert ansatte som leverer:

- *støttetjenester*
- *vedlikeholds- og sikkerhetskopieringstjenester*
- *driftssystemer/støttepersonell*

5. Hvilke eksterne parter (i tillegg til databehandleren) har tilgang til alle eller deler av personopplysningene (underbehandlere), med hvilke formål, og hvor befinner de seg geografisk (inkl. om dette er utenfor EØS-området)?

Underbehandler	Beskrivelse	Fysisk adresse	Foretaksnummer	Kontakt
Netgroup	Drift av infrastruktur	Netgroup A/S Hørskætten 52630 Taastrup Denmark	26 09 35 03	info@netgroup.dk
Salesforce	Kunden registrerer ledende databehandler, som er nødvendig for salgs- og supportaktivitetene	Floor 26 Salesforce Tower 110 Bishopsgate London United Kingdom EC2N 4AY	05 09 40 83	privacy@salesforce.com
Intercom	Chat-tjeneste i sanntid innenfor	3rd Floor, Stephens	538158	compliance@intercom.com

	produkt til kunder og inproduct-meldinger.	Ct.18-21 St. Stephen's Green Dublin 2 Ireland		
Amazon Web Services	Drift av infrastruktur – data lagret innenfor EU/EØS	One Burlington Plaza Burlington Road Dublin 4 Ireland	566018	https://aws.amazon.com/contact-us/
Microsoft Azure	Drift av infrastruktur – data lagret innenfor EU/EØS	One Microsoft Place South County Business Park Leopardstown, Dublin 18 D18 P521 Ireland	256796	https://azure.microsoft.com/en-gb/support/options/

Tillegg B til databehandlingsavtalen

Sikkerhetstiltak

Databehandleren skal innføre hensiktsmessige tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er hensiktsmessig i forhold til risikoen ved behandlingen. Disse tiltakene inkluderer, men er ikke begrenset til:

1. Tilgangskontroll til lokaler og fasiliteter (fysisk)

1.1 Databehandleren er kontraktmessig forpliktet til å ha kommersielt rimelige fysiske sikkerhetssystemer ved alle underbehandlerens eller de driftede datasentre og administrasjonslokaler der behandling av personopplysninger utføres;
1.2 Databehandleren er kontraktsmessig forpliktet til å implementere fysisk adgangskontroll hos alle underbehandlerens eller de driftede datasentre (inkludert, kun som eksempel, ved å godkjenne adgangskontroll til datasentre sammen med underbehandleren, f.eks. om personell på stedet skal hindre uautorisert adgang til datasentre, eller at nødvendig biometrisk skanning eller videoovervåking er på plass, eller at korsbom er integrert med adgangskontrollesere for å kunne kontrollere fysisk adgang til enhver tid, ved å kreve at personell viser ID-kort med bilde før de får adgang til lokalene);
1.3 Databehandleren vil undersøke om underbehandlerens eller de driftede datasentre skal ha prosedyrer for utstedelse av ID-kort til autorisert personell og for å kontrollere fysisk tilgang til systemer under databehandlerens kontroll;
1.4 Databehandleren vil godkjenne via underbehandlerens eller de driftede datasentre om besøkende må forhåndsgodkjennes før de kommer til databehandlerens lokaler der personopplysninger behandles, vise identifikasjon og/eller skrive under på en besøkslogg og eskorteres kontinuerlig mens de er i lokalene.

2. Tilgangskontroll til systemer (virtuell)

2.1 Databehandleren vil innføre og opprettholde kommersielt rimelige sikkerhetsforanstaltninger mot utilsiktet eller uautorisert tilgang til, tilintetgjørelse av, tap av eller endring av personopplysningene i systemene som brukes til å behandle personopplysninger:

2.1.1 Adgang vil gis personell på bakgrunn av adgangsrettigheter og spesifikke roller gjennom dokumenterte anmodningsprosedyrer for adgang.
2.1.2 Tilgangskontroller skal finnes på operativsystem-, database- eller programnivå;
2.1.3 Administrativ tilgang vil begrenses for å unngå endringer av systemer og programmer;
2.1.4 Brukere vil bli tildelt en enkelt konto med multifaktorautorisasjon der det er mulig, og vil ikke kunne dele kontoene sine.

3. Tilgangskontroll for enheter og bærbare datamaskiner

3.1 Databehandleren vil implementere og opprettholde kommersielt rimelige sikkerhetstiltak med hensyn til mobile enheter og bærbare datamaskiner som brukes til behandling av personopplysninger.

4. Tilgangskontroll for personopplysninger

4.1 Tilgang vil kun gis etter fullførelse av en godkjent prosess, dvs. en LAN-innloggings-ID, programtilgangs-ID eller annen lignende identifikasjon.
4.2 En unik bruker-ID og passord vil utstedes til hver bruker.

4.3 Når brukerne er verifisert, vil de være autorisert til ulike tilgangsnivåer ut fra sine spesifikke roller og på bakgrunn av adgangsrettigheter.

5. Kontroll av overføring og utlevering

5.1 Databehandleren vil implementere og opprettholde kommersielt rimelige tiltak for å forhindre at personopplysninger blir lest, kopiert, modifisert eller fjernet uten autorisasjon gjennom elektronisk overføring eller transport, og for å gjøre databehandleren i stand til å sjekke og fastslå til hvilke organisasjoner overføringen av personopplysninger ved hjelp av dataoverføringsfasiliteter gjøres.
5.2 Databehandleren skal ha teknologi og prosesser som er utformet for å minimere tilgang for ulovlig databehandling, inkl. teknologi for kryptering av personopplysninger.

6. Inndatakontroll

6.1 Databehandleren skal ha system- og databaselogger som viser tilgangen til alle personopplysninger den har kontroll over;
6.2 Alle behandlingssystemer må konfigureres med hendelseslogging for å kunne identifisere systembrudd, uautorisert tilgang eller andre sikkerhetsbrudd. Loggene må være beskyttet mot uautorisert tilgang eller endring;
6.3 Kunden/databehandleren skal ha inndatakontroller i systemene sine.

7. Kontroll av personell

7.1 Databehandleren skal innføre prosedyrer for å sikre at databehandlerens ansatte og alle andre personer som utfører handlinger under databehandlerens ledelse der de kan komme i kontakt med eller på annen måte ha tilgang til og behandle personopplysninger, er pålitelige, f.eks. ved å foreta en bakgrunnsundersøkelse før ansettelsesforholdet inngås.
7.2 Databehandleren skal innføre prosedyrer for å sikre at databehandlerens personell kjenner til forpliktelsene databehandleren har i henhold til avtalen. Alle personer databehandleren autoriserer for tilgang til personopplysningene, skal databehandleren instruere og lære opp om personvernlovgivningen, så vel som alle gjeldende sikkerhetsstandarder, og autoriserte personer skal skriftlig binde seg til å overholde taushetsplikten, personvernlover og andre relevante sikkerhetsstandarder.
7.3 Databehandleren skal omgående tilbakekalle brukertilgangen til kundens/databehandlerens personopplysninger når brukeren fratrer sin stilling, jobbfunksjonen endres eller hvis brukeren er inaktiv eller fraværende over en forlenget periode.
7.4 Databehandleren skal ha innført en personvernpolicy og en policy for lagring av dokumenter som personalet må følge.

8 Avviksbehandling

8.1 Databehandleren vil innføre og opprettholde en avviksbehandlingsprosedyre som gjør det mulig for databehandleren å informere den behandlingsansvarlige om en relevant hendelse innen den påkrevde tidsrammen .
8.2. Hvis en (potensiell) hendelse berører personopplysninger, skal databehandleren gi beskjed til den behandlingsansvarlige i samsvar med paragraf 4 i databehandlingsavtalen.
8.3 Avviksbehandlingsprosedyren omfatter regelmessig evaluering av gjentatte problemer og hendelser som kan indikere sikkerhetsbrudd.
8.4 Databehandleren vil regelmessig gjennomgå alle tidligere hendelser med hensikt å lære av det.

9. Tilgangskontroll

9.1 Databehandleren skal beskytte personopplysningene mot utilsiktet tilintetgjøring eller tap ved å sikre følgende:

- 9.1.1 Arbeidsstasjoner skal beskyttes av kommersiell programvare som forhindrer angrep av virus og skadelig programvare, og som regelmessig skal oppdateres med nye virusdefinisjoner.
- 9.1.2 Når virus eller skadelig programvare identifiseres, skal databehandleren øyeblikkelig sette i verk tiltak for å hindre spredning av og skader fra viruset eller den skadelige programvaren, og for å fjerne denne.
- 9.1.3 Servere skal beskyttes av kommersielle brannvegger og systemer for inntrengingsbeskyttelse og -forebygging.

10. Driftskontinuitet og endringsledelse

10.1 Databehandleren vil implementere, opprettholde og regelmessig gjennomgå en driftskontinuitets- og katastrofegjennopprettingsplan, som bl.a. vil sørge for at databehandleren kan gjenopprette tilgjengelighet og tilgang til personopplysningene innen et rimelig tidsrom partene vil bli enige om, dersom en fysisk eller teknisk hendelse inntreffer.
10.2 Databehandleren vil innføre endringsledelse for å kontrollere organisasjonen, forretningsprosesser, systemer og underbehandlerforhold, som har innflytelse på informasjonssikkerheten.
10.3 Som en del av prosedyren for endringsledelse, gjennomgår databehandleren alt som kan ha en potensiell påvirkning på personvernsikkerheten, med hensikt å lære av det

11. Instrukskontroll

11.1 Databehandleren vil innføre og opprettholde prosedyrer for å sikre at personopplysninger bare behandles i samsvar med den behandlingsansvarliges instrukser.

12. Separasjonskontroll

12.1 Databehandleren vil innføre og opprettholde prosedyrer for å sikre at personopplysninger som samles inn med ulike formål, vil bli behandlet separat, i den utstrekning databehandleren uttrykkelig er blitt informert om slik ulikhet i formålene og bedt om å gjøre dette, og forutsatt at databehandleren kan fakturere sine kostnader i form av tidsbruk og utgifter som databehandleren har pådratt seg for å etterkomme denne forespørselen.

13. Regelmessig testing av sikkerhetstiltak

14.1 Databehandleren vil stadig teste, bedømme og evaluere hvor effektive dennes tekniske og organisatoriske sikkerhetstiltak er.

***