Databehandleraftale

Mellem

Den dataansvarlige:

Virksomhed:

CVR-nr.

Adresse

og

Databehandleren

WOBA ApS

CVR: 37609641

Gammel Kongevej 1

1610 København V

Danmark

1 Indhold

2 Baggrund for databehandleraftalen

1. Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Aftalen er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i *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 (Databeskyttelsesforordningen)*, som stiller specifikke krav til indholdet af en databehandleraftale.

3. Databehandlerens behandling af personoplysninger sker med henblik på opfyldelse af parternes hovedaftale/kontrakt.

4. Databehandleraftalen og Hovedaftalen er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige Hovedaftalen – erstattes af en anden gyldig databehandleraftale.

5. Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder i Hovedaftalen.

6. Til denne aftale hører tre bilag. Bilagene fungerer som en integreret del af databehandleraftalen.

7. Databehandleraftalens Bilag A indeholder nærmere oplysninger om behandlingen, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

8. Databehandleraftalens Bilag B indeholder den dataansvarliges betingelser for, at databehandleren kan gøre brug af eventuelle underdatabehandlere, samt en liste over de eventuelle underdatabehandlere, som den dataansvarlige har godkendt.

9. Databehandleraftalens Bilag C indeholder en nærmere instruks om, hvilken behandling databehandleren skal foretage på vegne af den dataansvarlige (behandlingens genstand), hvilke sikkerhedsforanstaltninger, der som minimum skal iagttages, samt hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

10. Databehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.

11. Denne databehandleraftale frigør ikke databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.

3 Den dataansvarliges forpligtelser og rettigheder

1. Den dataansvarlige har over for omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker inden for rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

2. Den dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.

3. Den dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, som databehandleren instrueres i at foretage.

4 Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det 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 i forordningen nævnt i afsnit 2.2.

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5 Fortrolighed

1. Databehandleren sikrer, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.

2. Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde databehandlerens forpligtelser over for den dataansvarlige.

3. Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

4. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

6 Autorisation og adgangskontrol

1. Login sikkerhed: Vores digitale system (”Woba”) leveres som en SaaS platform og enhver autoriseret bruger kan få adgang via Wobas applikation (til mobil, tablet og computer) og online analyseværktøj. Log-ind-adgang til systemet styres igennem unikke brugerrettigheder (alle brugere får tildelt et unik log-ind) på vores platform, der bliver tildelt virksomhedens ansatte efter et princip om ”mindst-mulig-adgang” for, at de kan løse deres opgaver. Al information ved log-ind og besvarelser, når brugeren er logget ind, er krypteret. Vi baserer brugerrettighedsstyringen til Woba på baggrund af kundens anvisninger (mail-liste) som tilsendes os inden opstart af undersøgelsen. Derigennem sikrer vi, at kun autoriserede respondenter (ansatte) og administratorer (HR/ledere) får adgang til vores platform til at kunne besvare og se resultater for undersøgelsen. Vi benytter os både af (MFA) ”multi-factor-autenthication” og midlertidige adgang-tokens. Dermed sikrer vi, at kun personer, som autoriseres hertil, har adgang til de personoplysninger, der behandles.
2. Datasikkerhed: Desuden skal det nævnes, at al persondata befinder sig på servere hos vores hosting-udbyder, Amazon Web Services (AWS), i Frankfurt i EU. AWS lever op til og er compliant med GDPR-forordningens standarder såsom ISO 27001 for fysisk sikkerhed og tilgængelig. AWS har mere end 500+ GDPR-features og services der fokuserer på teknisk sikkerhed (såsom blokering af uautoriseret trafik - firewalls) og compliance og udvikler nye features løbende. Derudover foretager AWS løbende penetrationstest for at forbedre deres sikkerhedsfeatures og processer.
   Adgang direkte til databasen er alene tilgængelig for virksomhedens CTO samt én betroet teknisk nøglemedarbejder, der fungerer som suppleant for virksomhedens CTO i tilfælde af dennes sygdom eller ulykke.

7 Behandlingssikkerhed

1. Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risici af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske

og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

2. Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering og herefter gennemføre foranstaltninger for at imødegå identificerede risici.

8 Sikring af data

Da data ikke fysisk opbevares i firmaet, men alene eksisterer på eksterne, administrerede servere, følger vores besvarelse af dette punkt de ovenstående besvarelser omkring sikkerheden i systemet. Dette indbefatter opbevaring af data i Frankfurt (inden for EU og i overensstemmelse med GDPR), kryptering af data både over netværk og "at rest", backups på eksterne servere (ligeledes i Frankfurt) samt sikring af at underleverandører overholder retningslinjerne for sikker afskaffelse af udtjent hardware m.m.

Adgang til systemet tildeles for vores medarbejderes vedkommende på "mindst mulig adgang" basis og begrænses derved altid mest muligt.

Vi stiller skrappe krav til, at vores underleverandører af bl.a. vores database og system-hosting er ISO 27001 certificerede, hvilket også sikrer ordentlig, fysisk sikring af vores data, både med adgangskontrol til hosting-centre, brandslukning og monitorering samt fail-over systemer.

Hvad angår adgang til data udefra, sker al den tekniske sikkerhed på vores platform og hos vores hosting-udbyder, hvorfor der ingen tekniske fordele er ved at befinde sig på en specifik, fysisk adresse. Den fysiske sikkerhed i virksomheden går derfor på at sikre eventuel fysisk persondata. Her følges tidligere angive retningslinjer for behandling af inddata og uddata.

Nye medarbejdere instrueres og oplæres ved ansættelsen. Hvis vores retningslinjer opdateres eller udvides, instrueres virksomheden samlet, senest en måned efter de nye retningslinjer træder i kraft. Der gennemføres årlige opfrisknings-kurser for alle ansatte i de samlede retningslinjer, ligesom medarbejderne efterfølgende testes i deres forståelse af retningslinjerne.

9 Sikkerhedsbrister

Der foreligger interne processer for håndering af brud på datasikkerheden, der angiver hvilke personer, der er ansvarlige for hvilke opgaver, herunder tekniske, kommunikative og organisatoriske opgaver. Inden for de første 24 timer er hovedopgaverne at stoppe bruddet, sikre oplysninger til efterfølgende undersøgelser, afdække omfanget og kontakte alle påvirkede kunder samt myndigheder. Vi samarbejder fuldt ud med alle vores kunder og sikrer, at alle har adgang til al nødvendig information til overholdelse af deres lovmæssige forpligtelser ved brud på datasikkerheden.

Alle i virksomheden har et ansvar for at indrapportere enhver mistanke om brud på datasikkerheden, hvad enten denne mistanke beror på kontakt fra en kunde, en leverandør eller egne oplevelser. Så snart et brud er bekræftet, vurderes det om bristen fortsat er til stede (fysisk eller teknisk) og såfremt dette er tilfældet, spærres adgang til bristen øjeblikkeligt, i yderste instans ved at systemet tages offline indtil bristen er fjernet.

10 Overtrædelse af sikkerhedsbestemmelser

Vi sætter datasikkerhed og overholdelse af persondataforordningen i højsædet og samtlige ansatte er forpligtede til, uden ophold, at gøre vores kunder opmærksomme på såvel overtrædelser som risiko for overtrædelser, så snart sådanne identificeres.

Bliver vi opmærksomme på overtrædelser gøres kunden med det samme opmærksomme herpå, enten ved kontakt til den person, der udviser uhensigtsmæssig adfærd eller ved direkte kontakt til vores kontaktperson hos kunden.

Ved identificeret overtrædelse sikres nødvendige data for efterfølgende udforskning af forløbet, overtrædelsen stoppes, hvis den fortsat er aktiv og omfanget afdækkes. Såfremt overtrædelsen af sikkerhedsbestemmelserne har haft indflydelse på kunder, informeres disse uden ugrundet ophold og så hurtigt, at de kan overholde eventuelle lovmæssige forpligtelser omkring indrapportering.

11 Anonymisering, pseudonymisering og kryptering af personoplysninger

Al data interaktion (dataindsamling, resultatvisning m.m.) mellem vores brugere og digitale platform er ”default” krypteret af vores system og alle individuelle besvarelser er som udgangspunkt anonymiserede.

Data beholds i systemet, så længe kontrakten med kunden stipulerer, at der er formål. Herefter slettes data og eventuelle udtræk, rapporter og andet genereret på grundlag af denne data, vil ikke længere være tilgængelige.

Hvis en undersøgelse er sat op som anonym, giver analyseværktøjet alene mulighed for at se resultater, når datagrundlaget overstiger den satte, nedre grænse for anonymitet (pt. 5 besvarelser).

Alle individuelle besvarelser bliver tildelt et krypteret ID-nummer, hvorfor den enkeltes besvarelser og dermed navn, efternavn og arbejdsmail er anonyme og ikke kan genkendes. Fri-tekst kommentarer vises alene med angivelse af måned for besvarelsen, afdelingen (hvis flere end 5 besvarelser i afdelingen) samt den tilhørende, numeriske besvarelse (0 til 4).

Åbne undersøgelser er ikke pseudonymiserede.

Al data interaktion (dataindsamling, resultatvisning m.m.) mellem vores brugere og digitale platform er ”default” krypteret af vores system. Der er en række sikkerhedsforanstaltninger for dette, men grundlæggende sker al kommunikation imellem vores individuelle systemer samt med bru-

geren over krypterede forbindelser (SSL). Data er krypteret "at rest" for at forhindre uønsket adgang ved brud på databasesikkerheden. Hvis persondata skal overleveres digitalt, skal dette på nuværende tidspunkt ske ved at gemme data f.eks. på en USB-nøgle og fysisk overbringe denne til os, da vi på denne måde kan sikre, at data ikke bliver kompromitteret.

12 Backup

Vores systemer samt database har alle krypterede PITR-backups på eksterne servere inden for EU. Systemer kan genskabes til et vilkårligt stadie tilbage i tid uden begrænsning. Databasen kan genskabes til et vilkårligt tidspunkt, 14 dage tilbage i tiden.

Såfremt undersøgelsens formål ikke mere er gyldig eller en bruger henvender sig og vil have sin data og bruger slettet fra vores system, bliver data gemt via back-up i op til 30 dage, såfremt kunden ønsker at reetablere aftalen. Hvis ikke, bliver sletteprocessen automatisk fuldført herefter. Derudover er vi dækket af Trygs cyberforsikring ("eProtect") som hjælper os med at forebygge angreb såsom virus eller DDoS, hvor vi har adgang til at få professionel assistance 365 dage om året til at afværge angreb eller komme lynhurtigt tilbage på sporet.

13 Registreredes rettigheder

1. Berigtigelse af oplysninger

   Hvis vi modtager en anmodning (telefonisk eller via mail til vores supportafdeling) fra en registreret bruger, der har mistanke om eller er blevet opmærksom på, at vi har fået forkerte eller urigtige personoplysninger om vedkommende selv, berigtiger vi oplysningerne "uden unødig forsinkelse" inden for 48 timer. Vores supportteam kan kun få adgang til en slutbrugers konto og oplysninger, hvis den registrerede har givet samtykke til at give dem adgang.
   I vores tilfælde handler "urigtige oplysninger" ofte om, at rette fx faktuelle oplysninger om navn, mailadresse, afdeling osv., som kan rettes direkte fra vores Content Management System. Inden vi retter de urigtige oplysninger, skal vi have en bekræftelse fra kundens administrator (personen som har videregivet de forkerte oplysninger – ofte HR chefen) på, at korrektionen er korrekt. Her informerer vi om, hvilke tidligere afgivne oplysninger der er ukorrekte samt de korrekte oplysninger.

2. Sletning af oplysninger

   Den enkelte bruger, som benytter Woba, ejer al egen data, som uploades til vores digitale platform og har som udgangspunkt ret til at få slettet alle oplysninger om sig selv *uden unødig forsinkelse* med en slettefrist på 48 timer. Dvs. al information om brugeren (navn, efternavn, arbejdsmail, arbejdsplads og afdeling) og dennes svar på Wobas spørgeskema-

undersøgelse samt resultater kan til hver en tid slettes. Data slettes på anmodning fra både database, logs, backups samt i fysisk form efter berigtigelse af henvendelse (at henvendelsen kommer fra den person der bedes slettet). På den måde sletter vi personoplysninger på en sådan måde, at de ikke kan genskabes. Med andre ord sletter vi den registrerede brugers personoplysninger, hvis:1) Det ikke længere er nødvendig for vores behandlingsformål at have oplysninger om den registrerede 2) Vi baserer vores behandling af vedkommendes persondata med samtykke (”terms & conditions”), og hvis den pågældende bruger trækker sit samtykke tilbage, og vi samtidig ikke har en hjemmel for behandlingen eller 3) Hvis brugerens oplysninger på nogen måde behandles i strid med databeskyttelsesforordningen (for mere om dette se WBIs databehandleraftale punkt 11). Udover at underrette den henvendte bruger om sletningen, underretter vi også personen hos kunden som har videregivet oplysningerne om den slettede bruger i sin tid.

3. Indsigtsret

Ved henvendelse til support (telefonisk og mail) informeres om alle registrerede data fra vores systemer efter berigtigelse af henvendelse (at henvendelsen kommer fra en person, der har ret til at bede om dem). Ved brugerens henvendelse og anmodning til os har vedkommende altid retten til at se personoplysninger, som vi behandler om pågældende i vores system, hvorfra vedkommende vurderer om indholdet af oplysningerne er korrekte, skal redigeres eller slettes m.m. Vi tilsender derefter den registrerede en elektronisk gratis kopi af selve oplysninger via vedkommendes mail. Inden e-mailen med oplysningerne afsendes, sender vi en sikkerhedsgodkendelse til vedkommendes mailadresse (den ansattes arbejdsmail, som vi har fået oplyst af kunden), som skal verificeres fra indbakken for at få tilsendt oplysningerne. På den måde sikrer vi, at vi sender oplysningerne til den korrekte person. Det er KUN oplysninger om den registrerede selv, der tilsendes som kopi.

4. Dataportabilitet

Data fra vores database eksporteres i et nemt læseligt og overskueligt CSV-format. Data, der kan eksporteres, er brugernes historiske besvarelser inklusive tidsangivelse af samme samt de påkrævede personlige oplysninger, vi har på den registrerede (navn, e-mail, arbejdsplads og afdeling/team). Den registrerede vil således let kunne få adgang til og kontrol over de oplysninger, som vi har registreret i systemet, og vil ligeledes let kunne overføre sine personoplysninger videre til et andet IT-miljø.

Alle brugere i Woba har ret til at modtage egne personlysninger og upload af besvarelser til systemet samt analyseresultater, hvori pågældendes besvarelse indgår - og kan til hver en tid modtage dem i et nemt og overskueligt format. Vores procedure for modtagelse følger samme standard som i punkt 3 under indsigtsretten i nærværende dokument.

5. Afgivelse af samtykke

Ved login accepteres og samtykkes til vores "terms & conditions" vilkår og betingelser (der skal tages *aktiv stilling* – det er ikke muligt at logge ind uden accept). Ved at acceptere vores vilkår og betingelser samtykker den enkelte bruger altså til, at systemet indsamler, arkiverer og benytter dennes besvarelser til undersøgelsens formål og gøres tilgængelig for brugerens arbejdsgiver.

6. Tilbagekaldelse af samtykke

Enhver bruger af Woba ejer af al data som er uploadet til vores digitale system. Vi oplyser derfor også i vores vilkår og betingelser, når brugeren første gang logger ind i Woba, at det er muligt for enhver bruger at tilbagekalde sit samtykke. Hvis brugeren henvender sig til os, via vores supportafdeling, omkring tilbagekaldelse af samtykke til, at Woba kan behandle vedkommendes personoplysninger, sletter vi han/hendes data uden unødig forsinkelse inden for 48 timer.

Vi tilsender derefter brugeren en elektronisk gratis kopi af selve sletteoplysningerne via vedkommendes mail. Inden e-mailen med sletteoplysningerne afsendes, sender vi en sikkerhedsgodkendelse til vedkommendes mailadresse (den ansattes arbejdsmail, som vi har fået oplyst af kunden), som skal verificeres fra indbakken for at få modtage sletteoplysningen. Brugeren skal bekræfte tilsendelsen, før vi påbegynder sletningen af vedkommendes data.

7. Profilering (automatiske individuelle afgørelser)

Enhver bruger af Woba har mulighed for ikke at blive underlagt en automatisk behandling af vedkommendes personoplysninger i vores analyseundersøgelser på arbejdspladsen. Hvis kunden vælger det til, har kundens ansatte mulighed for at få foretaget en individuel profilering baseret på dennes besvarelser af undersøgelsen. Profilering i vores systemer er en matematisk beregning af den ansattes svar. Disse profiler ("resultater") er kun tilgængelige for den enkelte respondent og derved får hverken arbejdsgiver eller andre virksomheder adgang til disse. Såfremt kunden har valgt, at de ansatte skal modtage sit individuelle resultat, er det beskrevet i vores vilkår og betingelser, som den enkelte aktivt samtykker til inden sin besvarelse.

14 Eksterne kommunikationsforbindelser

Al kommunikation med vores platform sker via krypterede forbindelser, uanfægtet om der er tale om almindelig anvendelse af platformen eller synkronisering af kode eller arbejde med database.

15 Inddata- og uddatamateriale

1. Inddata: Det er kun teknisk og faglige kyndigt personale som beskæftiger sig med inddatering i WOBA, der får adgang til inddatamateriale. Denne adgang sikrer vi igennem autoriseret adgangskontrol. Derudover har alle firmacomputere personlige sikkerhedsgodkendte adgangskoder, så vi sikrer os, at ansatte, der ikke beskæftiger sig med inddatering, heller ikke får adgang til materialet. Inddata (i vores kontekst f.eks. medarbejderlister og organisationsstrukturer tilsendt digitalt) slettes fra mail og harddisk inden for 4 uger efter behandling er afsluttet. De 4 uger sikrer, at inddata er tilgængeligt ifald, der opdages fejl eller ønskes en anden behandling.

Såfremt inddata leveres i fysisk form, makuleres dette ligeledes inden for 4 uger efter behandlingen er afsluttet.

2. 2. Uddata: Uddatamateriale (herunder rapporter, præsentationer og dataudtræk) genereres digitalt af vores platform på kundens anmodning og kan downloades af de ansatte, kunden giver autoriseret adgang til. Al data interaktion (dataindsamling, resultatvisning m.m.) mellem vores brugere og digitale platform er ”default” krypteret af vores system.

Det er kun teknisk og faglige kyndigt personale som må beskæftige sig med uddatamateriale i WOBA. Uddata genereret af det udvalgte personale (ex penetrationstest eller papirbaserede rapporter) slettes og/eller makuleres inden for 4 uger, når behovet for brug af resultaterne ophører. Vi har implementeret klare sikkerhedstandarder – fx hvis en ansat i WOBA får stjålet en mappe med kunderelaterede rapporter – hvor kunden underrettes og hændelsen anmeldes uden unødig forsinkelse.

16 Logning

Al interaktion med vores digitale platform logges i vores database, hvilket gør, at vi til hver en tid kan spore den enkelte brugers operationer og interaktioner. Hver log indeholder informationer om, hvem der gjorde hvad (bruger, type af anvendelse m.m.), og på hvilket tidspunkt anvendelsen blev udført. Hver log etableres via forespørgsler til vores database og opbevares i min. 6 måneder. Ud over registreringen i databasen opbevares serverlogs på separate servere.

17 Brugeradministration

Vores platform anvendes af to typer af brugere – personer der afgiver oplysninger (medarbejdere) og personer der analyserer dem (ledere/HR samt ”øverste instans”). En person kan godt være i begge kategorier samtidig. I forbindelse med afgivelse af oplysninger (besvarelsen af undersøgelsen), har brugeren log ind-adgang til at se egne, tidligere besvarelser samt virksomhedstotaler (hvis virksomheden har givet adgang dertil).

Personer der analyserer data (lederne) tildeles log ind-adgang til én eller flere organisatoriske enheder (afdelinger). Samtidig begrænses brugerens rettigheder baseret på rolle (administrator eller leder), hvor administrator har adgang til alle oplysninger og indstillinger, herunder også brugerlister, men kan ikke rette, skabe eller slette individuelle besvarelser. En afdelingsleder har læse-adgang til besvarelser fra egne afdelinger til udvalgte undersøgelser og kan få tildelt rettigheder til alle undersøgelser ud over de tildelte (dog stadig kun for egne afdelinger), rettigheder til at administrere (rette, skabe og slette) medarbejdere, administrere administratorer eller til at igangsætte undersøgelser.

Kryptering: Alle medarbejdere og ledere tildeles dermed unikke rettigheder via et krypteret ID-nummer, så de kun har adgang til at besvare, se, arkivere og slette de oplysninger som er relevant for dem. Al data interaktion (dataindsamling, resultatvisning m.m.) mellem vores brugere og digitale platform er "default" krypteret af vores system.

Med andre ord har ingen medarbejdere adgang til oplysninger, som de ikke har brug for i forbindelse med besvarelse af Wobas undersøgelser

18 Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2 og 4, for at gøre brug af en anden databehandler (underdatabehandler).

2. Databehandleren må således ikke gøre brug af en anden databehandler (underdatabehandler) til opfyldelse af databehandleraftalen uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige. Ved at underskrive denne databehandleraftale giver dataansvarlige sit skriftlige samtykke til, at databehandler må anvende de i denne databehandleraftale listede underdatabehandlere.

3. I tilfælde af generel skriftlig godkendelse skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

4. Den dataansvarliges nærmere betingelser for databehandlerens brug af underdatabehandlere fremgår af denne aftales Bilag B.

19 Overførsel af oplysninger til tredjelande eller internationale organisationer

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt

intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det 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.

2. Uden den dataansvarliges instruks eller godkendelse kan databehandleren – inden for rammerne af databehandleraftalen - derfor bl.a. ikke;

    a. videregive personoplysningerne til en dataansvarlig i et tredjeland eller i en international organisation,
    b. overlade behandlingen af personoplysninger til en underdatabehandler i et tredjeland,
    c. lade oplysningerne behandle i en anden af databehandlerens afdelinger, som er placeret i et tredjeland.

20 Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel 3.

    Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

    a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
    b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
    c. den registreredes indsigtsret
    d. retten til berigtigelse
    e. retten til sletning (»retten til at blive glemt«)
    f. retten til begrænsning af behandling
    g. underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
    h. retten til dataportabilitet
    i. retten til indsigelse
    j. retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering

2. Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyns-

tagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art 28, stk. 3, litra f.

Dette indebærer, at databehandleren under hensynstagen til behandlingens karakter skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

a. forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
b. forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
c. forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
d. forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
e. forpligtelsen til at høre tilsynsmyndigheden (Datatilsynet) inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen

21 Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en eventuel underdatabehandler.

   Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter at denne er blevet bekendt med bruddet, sådan at den dataansvarlige har mulighed for at efterleve sin eventuelle forpligtelse til at anmelde bruddet til tilsynsmyndigheden indenfor 72 timer.

2. I overensstemmelse med denne aftales afsnit 9.2., litra b, skal databehandleren - under hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne – bistå den dataansvarlige med at foretage anmeldelse af bruddet til tilsynsmyndigheden. Det kan betyde, at databehandleren bl.a. skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse til tilsynsmyndigheden:

a. Karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
b. Sandsynlige konsekvenser af bruddet på persondatasikkerheden
c. Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

22 Sletning og tilbagelevering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne. For yderlige specifikation af dette punkt se Bilag C, C.3.

23 Tilsyn og revision

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise databehandlerens overholdelse af 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.

2. Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

24 Ikrafttræden og ophør

1. Denne aftale træder i kraft ved begge parters underskrift heraf.

2. Aftalen kan af begge parter kræves genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i aftalen giver anledning hertil.

3. Opsigelse af databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af Hovedaftalen.

4. Aftalen er gældende, så længe behandlingen består. Uanset hovedaftalens og/eller databehandleraftalens opsigelse, vil databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.

25 Kontaktpersoner/kontaktpunkter hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner/kontaktpunkter:

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersonen/kontaktpunktet.

Primær kontakt hos den dataansvarlige	Primær kontakt hos databehandleren
Navn:	Navn: Nicolai Asmussen
Stilling:	Stilling: CTO
Telefon:	Telefon: 28 10 01 64
E-mail:	E-mail: nwa@workbalanceinstitute.com

26 Underskrift

På vegne af den dataansvarlige	På vegne af databehandleren
Navn:	Navn: Malene Madsen
Stilling:	Stilling: Adm. Direktør
Dato:	Dato: Den 09-01-2019
Underskrift:	Underskrift:

Bilag A Oplysninger om behandlingen

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er:

At levere en arbejdspladsvurdering til dataansvarlige der foretages gennem brugen af databehandlers (WOBA ApS) platform, Woba. Woba, består af en app, der indsamler kvantitative og kvalitative besvarelser fra medarbejderne samt et online analyseværktøj, som ledelsen og/eller HR får adgang til, således at de kan administrere resultaterne af de besvarelser, der kommer ind i app'en.

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om:

Behandlingens primære formål er at kortlægge arbejdsmiljøet hos dataansvarlige samt trivslen blandt dataansvarliges ansatte/brugere. Således skal data, og herunder behandlingen, benyttes til at *forebygge* fysiske og psykiske arbejdsskader som følge af arbejdsmiljøet samt benyttes til at fremme trivslen blandt arbejdspladsens ansatte.

Behandlingen sker automatisk ved, at Woba – herunder app og dashboard – automatisk genererer analyser ud fra de besvarelser, som dataansvarliges ansatte/brugere indrapporterer i app'en.

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

Navn, e-mailadresse og enhed i organisationen (fx afdeling, team eller område). Disse tre typer af oplysninger er standard og en forudsætning for, at dataansvarlige kan anvende Woba. Der efterspørges ikke flere oplysninger end ovenstående fra databehandlers side.

Behandlingen omfatter følgende kategorier af registrerede:

De registrerede er ansatte, der arbejder i dataansvarliges virksomhed, og som har indgået en aftale med databehandler, WOBA ApS. Ansatte gælder både medarbejdere og ledere.

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter denne aftales ikrafttræden. Behandlingen har følgende varighed:

Indtil formålet med behandlingen ophører jf. punktet 'Rettigheder til Data' i 'Hovedaftalen', eller indtil dataansvarlige ønsker, at behandlingen ophører, hvad der end måtte komme først.

Bilag B Betingelser for databehandlerens brug af underdatabehandlere og liste over godkendte underdatabehandlere

B.1 Betingelser for databehandlerens brug af eventuelle underdatabehandlere

Databehandleren har den dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere. Databehandleren skal dog underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være den dataansvarlige i hænde minimum 1 måned før anvendelsen eller ændringen skal træde i kraft. Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til databehandleren inden 2 uger efter modtagelsen af underretningen. Den dataansvarlige kan alene gøre indsigelse, såfremt den dataansvarlige har rimelige, konkrete årsager hertil.

B.2 Godkendte underdatabehandlere

Den dataansvarlige har ved databehandleraftalens ikrafttræden godkendt anvendelsen af følgende underdatabehandlere:

Navn	Adresse	Beskrivelse af behandling
Heroku (a Salesforce company)	The Landmark @ 1 Market St. Suite 300 San Francisco, CA 94105, USA	Heroku hoster selve systemerne (der bearbejder data). Firmaet er amerikansk, men data ligger i "Region: EU" i Frankfurt i Tyskland. Heroku er hostet af Amazon Web Services på eu-central-1 og hører under EU lovgivning.
Postmark (a Wildbit company)	2400 Market Street, No. 200, Suite 235B, Philadelphia, PA 19103, USA	Postmark bruges som en Email-tjeneste til at sende mails ud med invitationer til at oprette sig eller logge ind i Woba. Postmark opbevarer ikke et fuld addressekartotek, men fungerer som et relay. - https://postmarkapp.com/eu-privacy#gdpr
Google	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Da vi bruger Gmail, opbevarer Google personoplysninger indsendt af vores kunder i forbindelse med support eller anden kommunikation. Data ligger fysisk placeret i EU - https://www.google.com/about/datacenters/inside/locations/index.html.
Expo (650 Industries Inc.)	624 University Ave # 1 Palo Alto, CA, 94301-2019, USA	Expo anvendes til at sende såkaldte 'push-notifikationer' ud til de ansatte/brugerne, når de skal mindes om, at det nu er tid til at besvare spørgsmålene i Woba, herunder app'en. Deres systemer benytter Amazons CDN-netværk.

Aiven Oy	Helsinki, Finland	Aiven hoster vores database. Firmaet er Finsk, men data ligger på en server hos eu-central-1, som er en del af Amazon Web Services (AWS). Eu-central-1 hos AWS ligger fysisk placeret i Frankfurt i Tyskland og hører under EU lovgivning.
Amazon Web Services (AWS)	Seattle, Washington, USA	AWS opbevarer vores filer (ikoner og Pdf'er), der opbevares på en server hos eu-central-1, der fysisk er placeret i Frankfurt i Tyskland og hører under EU lovgivning.

Den dataansvarlige har ved databehandleraftalens ikrafttræden specifikt godkendt anvendelsen af ovennævnte underdatabehandlere til netop den behandling, som er beskrevet ovenfor. Databehandleren kan ikke – uden den dataansvarliges specifikke og skriftlige godkendelse – anvende den enkelte underdatabehandler til en "anden" behandling end aftalt eller lade en anden underdatabehandler foretage den beskrevne behandling.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1 Behandlingens genstand

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Data analyseres og behandles automatisk af Woba samt manuelt af interne medarbejdere fastansat i WOBA. Til manuel behandling anvendes alene Excel.

C.2 Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

At der er tale om indsamling af personoplysninger af *ikke* særlig karakter, der måtte være personfølsomt. Som beskrevet ovenfor, indsamler vi e-mail, navn og enhed i organisationen (fx afdeling, team eller område) fra dataansvarliges ansatte/brugere som en forudsætning for at kunne anvende vores platform, Woba. Imidlertid er vi som databehandlere berettigede og forpligtede til at etablere de nødvendige og rette organisatoriske og tekniske sikkerhedsforanstaltninger omkring den indsamlede data.

C.3 Opbevaringsperiode/sletterutine

Personoplysningerne, herunder rådata, opbevares hos databehandler i op til 5 år, efter at samarbejdet med dataansvarlige er ophørt, medmindre at dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret. Perioden i op til 5 år tjener det formål, at databehandler (WOBA) skal bruge rådata i forsknings- og udviklingsmæssigt øjemed.

C.4 Lokalitet for behandling

Behandling af de i aftalen omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end den følgende:

Fruebjergvej 3, 2100 København Ø (adresse for behandleren, WOBA ApS).

Der gives i øvrigt ved underskrift af denne aftale tilladelse til, at ovennævnte underdatabehandlere må opbevare data på de listede adresser.

C.5 Nærmere procedurer for den dataansvarliges tilsyn med den behandling, som foretages hos databehandleren

Den dataansvarliges eventuelle udgifter i forbindelse med et fysisk tilsyn afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsagligt den tid), der er nødvendig for, at den dataansvarlige kan gennemføre sit tilsyn.