Databehandleraftale

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

mellem

Partneren

herefter ”den dataansvarlige”

og

Kanpla ApS
CVR 40369813
Inge Lehmanns Gade 10
8000 Aarhus C

herefter ”databehandleren”

der hver især er en ”part” og sammen udgør ”parterne”

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

Indhold

1. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Disse Bestemmelser 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).

3. I forbindelse med leveringen af en digital platform og app behandler Databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

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

7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som Databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med Databehandleren og eventuelle underdatabehandlere.

9. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

10. Disse Bestemmelser frigør ikke Databehandleren fra forpligtelser, som Databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

2. Databehandlerens rettigheder og forpligtelser

1. Databehandleren er over for den dataansvarlige ansvarlig for at sikre, at Databehandlerens behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se databeskyttelsesforordningens artikel 28, stk. 3), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

1 Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

3. Databehandleren er ifølge databeskyttelsesforordningens artikel 28, stk. 4, ansvarlig for at sikre, at Databehandleren pålægges de samme databeskyttelsesforpligtelser som dem, der er fastsat i kontrakten eller et andet retligt dokument mellem den dataansvarlige og Databehandleren som omhandlet i databeskyttelsesforordningens artikel 28, stk. 3, gennem en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i denne forordning.

4. Parterne har derfor indgået Bestemmelserne, der pålægger Databehandleren de samme databeskyttelsesforpligtelser som dem, der er fastsat i kontrakten eller et andet retligt dokument mellem den dataansvarlige og Databehandleren.

3. 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. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

2. Databehandler underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

4. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på Databehandlerens vegne, til personer, som er underlagt Databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt Databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

5. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

a. Pseudonymisering og kryptering af personoplysninger

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

c. evne 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.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal Databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for Databehandleren vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

   Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

6. Anvendelse af underdatabehandlere

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

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren har den Dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette Den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 14 dages varsel og derved give Den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke

behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

   Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82.

7. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af Databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
c. behandle personoplysningerne i et tredjeland

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

8. 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 III.

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

   a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
   b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
   c. indsigtsretten
   d. retten til berigtigelse
   e. retten til sletning (”retten til at blive glemt”)
   f. retten til begrænsning af behandling
   g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
   h. retten til dataportabilitet
   i. retten til indsigelse
   j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, med at assistere den dataansvarlige med:

   a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, 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.

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

9. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a skal Databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at Databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

    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. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

    c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

10. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

11. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, 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. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med Databehandleren og underdatabehandlere er nærmere angivet i bilag C.7. og C.8.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

12. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

13. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters accept heraf.

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

14. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Databehandleren har følgende kontaktperson:

   Databehandleren:

Navn	Peter Søren Bæch
Stilling	CEO
Telefonnummer	+45 93 92 04 12
E-mail	pb@kanpla.dk

2. Den dataansvarlige er forpligtet til løbende at orientere databehandleren om ændringer vedrørende kontaktpersoner.

Bilag A Oplysninger om behandlingen

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er at levere en digital platform og app samt de tilknyttede services til den dataansvarlige, herunder registrering af brugernes oplysninger, opbevaring af data, yde support på brugen af systemet, bistå med at flytte, kopiere eller slette data samt tage backup af de aftalte data.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Databehandlerens behandling af personoplysninger på vegne af Databehandleren drejer sig primært om:

- Indsamling
- Registrering
- Sletning

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Almindelige personoplysninger:

- Navn
- Adresse
- E-mailadresse
- Stilling / titel
- Virksomhed
- Personalenummer
- Kostpræferencer / diet
- Telefonnummer
- Betalingsoplysninger

Følsomme personoplysninger:

- Oplysninger om allergener (frivilligt for brugeren)

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Gæster i kantinen (medarbejdere, kunder og evt. øvrige gæster)

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Behandlingen er ved Bestemmelsernes indgåelse ikke tidsbegrænset, idet behandlingen fortsætter indtil, at den mellem parterne indgåede aftale om levering af en digital platform og app ophører.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	ADRESSE	BESKRIVELSE AF BEHANDLING
Google Cloud Platform	Server located at Frankfurt, Germany (europe-west3), samt enkelte funktioner i St. Ghislain, Belgium (europe-west1).	Bruges til opbevaring og behandling af dataen, herunder gennem Database (Firebase) og til statistik.
Intercom R&D Unlimited Company	2nd Floor, Stephen Court, 18-21 Saint Stephen's Green, Dublin.	Behandler oplysningerne for at give en skræddersyet supportoplevelse.
Reepay A/S	Pilestræde 28a, 2. sal, 1112 København K, Danmark. Server located at AWS Ireland.	Behandler oplysningerne for at facilitere betalinger på platformen.
Elastic NV	Keizersgracht 281, Amsterdam. Server located at GCP - Belgium (europe-west1).	Bruges til statistik og for at registere ændringer til bestillinger mv.
Mailjet SAS	4, rue Jules Lefebvre, 75009 Paris, France. Server located at GCP - Belgium (europe-west1) and Germany (europe-west3).	Behandler oplysningerne for at udsende e-mails, herunder ved bestilling, betaling mv.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarlige skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 14 dages forudgående skriftligt varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Databehandleren underretter den dataansvarlige per e-mail til kontaktpersonen hos Den dataansvarlige, som er anført i Bestemmelsernes pkt. 16.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Den dataansvarlige instruerer hermed Databehandleren i at foretage behandling af den dataansvarliges oplysninger til brug for levering af databehandlerens digitale platform og app.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

At behandlingen omfatter en større mængde almindelige personoplysninger, og der skal derfor etableres et almindeligt sikkerhedsniveau.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

IT-sikkerhedspolitik

IT-sikkerhedspolitik

Databehandleren skal have informationssikkerhedspolitikker og procedure, som revurderes årligt og godkendes af Databehandlerens ledelse.

Databehandleren skal have procedurer for udvikling / change mangement, som tager udgangspunkt privacy-by-default og standard-indstillinger.

Databehandleren skal, hvor det er nødvendigt, foretage en risikovurdering af de behandlingsaktiviteter der involverer persondata. Risikovurderingen skal tage udgangspunkt i data subjektets integritet, fortrolighed og tilgængelighed.

Passwordpolitik og brugerstyring

Databehandleren skal have passwordpolitikker og brugerstyringspolitikker for almindelige konti og strengere retningslinjer for administrative og servicekonti, som revurderes årligt og godkendes af Databehandlerens Tech Lead.

Adgang gives efter princippet om ”least priveliged access”. Dvs. der gives kun adgang til brugere der har en nødvendig behov herfor.

Bærbare medier

Databehandleren skal have procedurer til styring af bærbare- og lagermedier, herunder bortskaffelse af medier, der ikke er i brug længere og dermed modvirke at uautoriseret adgang.

Mobilt udstyr og fjernarbejdspladser

Der skal være understøttende sikkerhedsforanstaltninger til styring af risici ved anvendelse af mobilt udstyr og adgang til fjernarbejdspladser hos Databehandleren.

Oversigt over IT-aktiver

Databehandleren skal føre en opdateret liste over IT-Aktiver herunder PCér og serverer hvorpå den dataansvarliges data opbevares.

Håndtering af medarbejdere – før, under og efter ansættelsen

Uddannelse og bevidstgørelse

Databehandleren skal sørge for relevant uddannelse og sikre, at nye medarbejdere hos Databehandleren modtager Databehandlerens informationssikkerhedspolitikker samt politikker for behandling af personoplysninger og, at medarbejdere er beviste om politikkerne i deres arbejdstilrettelæggelse.

Databehandleren skal sikrer, at alle ansatte der behandler persondata er underlagt den fornødne tavshedspligt.

Adgangsrettigheder

Databehandleren skal have procedure for håndtering af brugere og deres roller og rettigheder. Databehandleren skal have klarlagt ansvaret for tildeling af roller og rettigheder, herunder under ansættelsen og efter ansættelsens ophør således, at det sikres, at modstridende funktioner og ansvarsområder adskilles for at modvirke muligt sikkerhedsbrud.

Databrud og hændelseshåndtering

Databrud

Databehandleren skal sikre adskillelse af udviklings-, test og driftsmiljøer for at imødegå risikoen for databrud.

Hændelseshåndtering

Databehandleren skal have procedure for håndtering er databrud, herunder hvornår og hvordan der skal rapporteres til Databehandleren samt klassificering af databrud. Databrudsproceduren skal testes mindst en gang årligt.

Databehandleren skal føre en løbende oversigt over hændelser og databrud. Oversigten skal beskrive:

- Tidspunktet hvorpå hændelsen er sket og afsluttet.
- Konsekvenser af bruddet.
- Navn på anmelder og til hvem bruddet er rapporteret.
- Hvis muligt hvilke afhjælpningsmuligheder.
- Mitigerende handlinger for at undgå fremtidige lignende databrud.

Logning

Databehandleren foretager logning af brugen af databehandlerens IT-systemer.

Databehandleren skal opsætte alarmer der advarer Databehandleren såfremt der sker mistænkelig adfærd.

Fysisk sikkerhed

Databehandleren skal have procedure for Databehandleren fysisk sikkerhed for at sikre, at uvedkommende ikke får adgang til personoplysninger.

Servere og andet udstyr hvorpå der behandles personoplysninger, skal befinde sig i aflåst rum.

Serverrum skal beskyttes mod brand og tyveri.

Personoplysninger på papir eller andet fysisk eller manuelt medie opbevares aflåst, når de ikke er i brug.

Databehandleren skal have en procedurer for tilintetgørelsen af persondata på papir, USB-stik og andet manuelt medie.

Endpoint-security

Antivirus og Firewall

Databehandleren skal have passende antivirusprogrammer og firewall til beskyttelse mod hackerangreb, malware og andre skadelige programmer og koder.

Opdatering

Systemer, hvorved personoplysninger behandles skal løbene opdateres, så den databehandleren en minimerer risiko for programmeringsfejl og sårbarheder i databehandlerens IT-sikkerhed.

TLS-kryptering

Databehandleren skal have TLS eller tilsvarende kryptering til beskyttelse af informationer uanset om disse er stationære eller under transmission, herunder ved anvendelse, vedligeholdelse og beskyttelse af krypteringsnøgler gennem deres livscyklus. Endvidere skal der anvendes kryptering i overensstemmelse med relevante aftaler, lovgivning og branchestandarder, samt myndighedsanbefalinger.

Backup

Backup

Databehandleren skal foretage backups af persondata der tilhører den dataansvarlige.

Databehandleren skal sikre at backups er segregeret fra øvrige anvendte data lokationer for at mindske muligheden for at data går tabt.

Databehandleren skal udføre test af implementerede IT-sikkerhedsforanstaltninger, herunder log og backup.

Opbevaringsperiode/sletterutine

Personoplysninger på backup opbevares i 30 dage, hvorefter de overskrives hos databehandleren.

C.3 Bistand til den dataansvarlige
Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelsernes pkt. 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Databehandleren skal implementere processer, der understøtter bistand til den dataansvarlige med opfyldelse af de registreredes rettigheder iht. kapitel 3 i databeskyttelsesforordningen.

Databehandleren skal hurtigst muligt iværksætte tiltag for at reducere eller fjerne konstaterede sårbarheder.

Databehandleren skal gennemgå egne logs for at bekræfte om data er blevet tilgået af uautoriserede – og på anmodning fra den dataansvarlige udlevere disse logs.

Databehandleren skal kunne udlevere lister over berørte registrerede, der gør den dataansvarlige i stand til at identificere og underrette disse.

Databehandleren kan ikke kræve særskilt betaling for bistand for, at Databehandleren kan efterleve sine forpligtelser (f.eks. hvis Databehandleren vil ændre i oplysningstekster, ændre kontaktinformationer, trække data ud ved indsigtsanmodninger, ved anmodninger om sletning mv.)

Databehandleren skal udlevere risikovurderinger samt konsekvensanalyser og/eller bistå den dataansvarlige i at udarbejde risikovurderinger samt konsekvensanalyser for det pågældende system.

C.4 Opbevaringsperiode/sletterutine
Personoplysninger opbevares i hele den løbetid, som samarbejdet mellem parterne har, hvorefter Databehandleren tilbageleverer dem til den dataansvarlige, medmindre instruks om sletning er givet inden da.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal Databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med Bestemmelsernes pkt. 11.1, medmindre Databehandleren, efter instruks fra den dataansvarlige og efter underskriften af disse Bestemmelser, har ændret den dataansvarliges oprindelige valg. Sådanne ændringer dokumenteres og opbevares skriftligt, herunder elektronisk, i tilknytning til Bestemmelserne.

C.5 Lokalitet for behandling
Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den datasvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end Danmark og de aftalte lokationer for underdatabehandlere i bilag B.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Databehandleren er ikke berettiget til at foretage overførsel af personoplysninger til usikre tredjelande uden Databehandlerens udtrykkelige skriftlige forhåndsgodkendelse. Enhver overførsel af personoplysninger til usikre tredjelande skal opfylde betingelserne i databeskyt-

telsesforordningen, herunder om nødvendigt ved anvendelse af EU-Kommissionens Standardkontraktbestemmelser for tredjelandsoverførsler (Standard Contractual Clauses) som vedtaget af EU-Kommissionen den 4. juni 2021.

Hvis Databehandleren ikke i Bestemmelserne eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er Databehandleren ikke berettiget til inden for rammerne af Bestemmelserne at foretage sådanne overførsler.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til Databehandleren

Databehandleren skal hvert tredje år for databehandlerens regning indhente en ISAE 3000 revisionspåtegning. Erklæringen indeholder en uafhængig revisors erklæring, ledelses udtalelse, systembeskrivelse, og slutteligt Databehandleren kontrolmål, kontroller samt test og resultat heraf.

Baseret på resultaterne af revisionserklæring, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den uafhængige tredjepart skal behandle enhver information indhentet hos eller modtaget fra databehandleren fortroligt og må kun udlevere sine konklusioner til den dataansvarlige. databehandleren skal modtage en kopi af ekspertens rapport og være berettiget til at anvende denne som dokumentation overfor andre kunder i relevant omfang Revisionserklæring fremsendes uden unødig forsinkelse til den dataansvarlige til orientering.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren skal føre tilsyn med underdatabehandlerne ved hjælp af de virkemidler, der er nødvendige for at kunne vurdere om underdatabehandleren overholder sine forpligtelser.

Dokumentation for ført tilsyn fremsendes uden unødig forsinkelse til dataansvarlige. Den dataansvarlige kan anfægte rammerne for og/eller metoden af tilsynet og kan i sådanne tilfælde anmode om gennemførelsen af en nyt tilsyn under andre rammer og/eller under anvendelse af anden metode.

I det omfang en af databehandlerens anvendt underdatabehandlere stiller en erklæring fra uafhængig tredjepart til rådighed for databehandleren, fx i form af ISAE 3000, ISAE 3402 eller lignende, om underdatabehandlerens overholdelse af persondatalovgivningen, indhenter databehandleren sådan en erklæring.

I det omfang databehandleren er anmodet herom af den dataansvarlige, fremsender databehandleren snarest muligt efter modtagelse af sådan erklæring fra underdatabehandleren til den dataansvarlige eller gør en sådan kopi tilgængelig for den dataansvarlige på anden vis. I modsat fald redegør databehandlere skriftligt overfor den dataansvarlige for hovedtrækkene i en sådan erklæring, snarest mulig efter modtagelsen