

Databehandleraftale (v. 1)

Indhold

Standardkontraktbestemmelser	2
1. Parterne	2
2. Præampel	2
3. Den dataansvarliges rettigheder og forpligtelser	2
4. Databehandleren handler efter instruks	2
5. Fortrolighed	2
6. Behandlingssikkerhed	3
7. Anvendelse af underdatabehandlere	3
8. Overførsel til tredjelande eller internationale organisationer	3
9. Bistand til den dataansvarlige	4
10. Underretning om brud på persondatasikkerheden	4
11. Sletning af oplysninger	4
12. Revision, herunder inspektion	4
13. Parternes aftale om andre forhold	5
14. Ikrafttræden og ophør	5
Bilag A. Oplysninger om behandlingen	6
A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige	6
A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig om (karakteren af behandlingen)	6
A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede	6
A.4. Behandlingen omfatter følgende kategorier af registrerede	6
Bilag B. Underdatabehandlere	7
B.1. Godkendte underdatabehandlere	7
Bilag C. Instruks vedrørende behandling af personoplysninger	8
C.1. Behandlingens genstand/instruks	8
C.2. Behandlingssikkerhed	8
C.3. Bistand til den dataansvarlige	8
C.4. Opbevaringsperiode/sletterutine	9
C.5. Lokalitet for behandling	9
C.6. Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren	9

Standardkontraktsbestemmelser

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

1. Parterne

mellem

NAVN:

CVR:

ADRESSE:

POSTNR OG BY:

LAND:

herefter "den dataansvarlige"

og

Edubutler ApS

CVR: 46018362

Damhus 1,

6600 Vejen

Danmark

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.

2. Præampel

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

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).

I forbindelse med leveringen af juniormesterlære.nu behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

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

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

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.

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

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.

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

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

3. Den dataansvarliges rettigheder og forpligtelser

Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes [1] nationale ret og disse Bestemmelser.

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.

Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

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

4. Databehandleren handler efter instruks

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.

Databehandleren 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.

5. Fortrolighed

Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges 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.

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

6. Behandlingssikkerhed

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.

Pseudonymisering og kryptering af personoplysninger.

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

Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.

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 den dataansvarlige 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.

7. Anvendelse af underdatabehandlere

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).

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

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. 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.

Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren sørge for at kunne fremskaffe en lignende kontrakt eller andet retsligt dokument, såsom en databehandlaftale (Data processing agreement) fra den pågældende underleverandør til den dataansvarlige. Det er op til den dataansvarlige på baggrund af det af databehandleren anskaffede materiale at vurdere, om de af underleverandøren gældende bestemmelser lever op til den dataansvarliges krav og instrukser.

Databehandleren er derfor ansvarlig for at fremskaffe det nødvendige materiale fra underdatabehandleren, for at der kan laves en vurdering af disse bestemmelser.

Underdatabehandlaftale(r) og eventuelle senere ændringer her til 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 underdatabehandlaftalen, skal ikke sendes til den dataansvarlige.

8. Overførsel til tredjelande eller internationale organisationer

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.

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.

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

overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation

overlade behandling af personoplysninger til en underdatabehandler i et tredjeland

behandle personoplysningerne i et tredjeland

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.

Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser 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.

9. Bistand til den dataansvarlige

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 sikre overholdelsen af:

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
- b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
- c. indsigtsheden
- 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

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, den dataansvarlige med:

den dataansvarliges forpligtelse til uden unødigt 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

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

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

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.

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.

10. Underretning om brud på persondatasikkerheden

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

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.

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, kategoriene og det omtrentlige antal berørte registrerede samt kategoriene 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.

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.

11. Sletning af oplysninger

Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til, når det ikke længere er nødvendigt at behandle personoplysninger, at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

Databehandleren forpligter sig til alene at behandle personoplysningerne til de formål, i den periode og under de betingelser, som disse regler foreskriver.

12. Revision, herunder inspektion

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.

For enhver revision, inspektion eller tilsvarende aktivitet, der iværksættes af eller på vegne af den dataansvarlige, faktureres den tid, som databehandleren og/eller dennes rådgivere medgår, til DKK 7.500 (syvtusinde femhundrede danske kroner) pr. påbegyndt time eksklusiv moms. Dette inkluderer tid anvendt på forberedelse, gennemførelse, rejsetid og efterfølgende opfølgning.

Forud for gennemførelse af revision eller inspektion skal den dataansvarlige overføre et depositum på DKK 93.750 (treoghalvfemstusinde syvhundredeoghalvtreds danske kroner) til databehandlerens bankkonto. Beløbet dækker op til 10 arbejdstimer. Eventuelt merforbrug faktureres særskilt efterfølgende. Beløbet refunderes ikke, medmindre den dataansvarlige aflyser revisionen med mindst 10 dages varsel.

Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.6

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.

13. Parternes aftale om andre forhold

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.

14. Ikrafttræden og ophør

Bestemmelserne træder i kraft ved den af den dataansvarlige indsendte erklæring om at have læst og accepteret bestemmelserne under oprettelse af en konto på [Juniormesterlære.nu](https://www.juniormesterlaere.nu).

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

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.

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 skriftlig varsel af begge parter.

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 sikre drift, vedligeholdelse og support af det digitale system, som anvendes af den dataansvarlige. Behandlingen omfatter administration af personoplysninger vedrørende brugere hos den dataansvarlige, herunder oprettelse og håndtering af elev-, lærer- og forældreprofiler samt registrering og sammenknytning af brugernes aktiviteter og handlinger i systemet.

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

Databehandlerens behandling af personoplysninger omfatter indsamling, registrering, lagring, strukturering, opbevaring, brug og sletning af oplysningerne med henblik på drift, support og vedligeholdelse af det digitale system, der stilles til rådighed for den dataansvarlige.

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

Navn

Email adresse

Telefon

Skole

Fraværsregistreringer

Praktikaftaler

A.4. Behandlingen omfatter følgende kategorier af registrerede

Elever

Lærere

Forældre/værge

Virksomhedskontaktpersoner

Bilag B. Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere.

NAVN	FORMÅL	DETALJER	LINKS
SUPABASE	Drift i forbindelse med vores database, backend server applikation og automatiske emails.	Supabase, Inc. Europæisk server lokaliseret i Sverige	Data processing agreement
HOSTINGER	Web hosting af hjemmeside, behandling af kontaktformular	Litauen	Data processing agreement
VERCEL	Hosting af applikationens kode	Vercel, Inc. San Francisco, California	Data processing agreement

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges 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.

Bilag C. Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Drift, vedligeholdelse og support af et digitalt system til styring af elever og praktikaftaler. Dette inkluderer behandling af personoplysninger relateret til oprettelse og håndtering af elevprofiler, udfyldelse af praktikaftaler, og registrering af fremmøde. Behandlingen sker udelukkende i henhold til den dataansvarliges instrukser.

C.2. Behandlingssikkerhed

Behandlingen omfatter almindelige personoplysninger såsom navn, e-mail, telefonnummer, og skolerelation. Da oplysningerne anvendes i forbindelse med elevforhold og potentielt danner grundlag for skolegang, er det væsentligt, at oplysningerne beskyttes mod uautoriseret adgang, manipulation og tab. Der er dog ikke tale om følsomme personoplysninger efter databeskyttelsesforordningens artikel 9.

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

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

Kryptering:

Personoplysninger i transit og ved opbevaring krypteres ved brug af TLS i hvert lag. Der følges industristandarder, og data opbevares med AES256 (256 bit) kryptering. Cipher suiten i TLS overførsel af data sker efter udveksling af krypteringsnøgler mellem server og klient, som udgangspunkt det stærkest mulige, fx Elliptic Curve Diffie-Hellman.

Vedvarende fortrolighed, integritet, tilgængelighed og robusthed:

Systemet opbygges med henblik på at sikre kontinuerlig tilgængelighed og dataintegritet via overvågning, redundans og adgangsstyring. Brugeradgang skal kontrolleres via rollebaserede rettigheder og sikre loginmetoder.

Genopretning ved hændelse:

Der etableres backup-rutiner med minimum daglig sikkerhedskopiering og en disaster recovery-plan, som muliggør genoprettelse inden for 24 timer ved nedbrud eller datatab.

Regelmæssig test og evaluering:

Der foretages minimum én årlig sikkerhedstest og løbende evaluering af systemets tekniske og organisatoriske sikkerhedsforanstaltninger.

Adgang via internettet:

Adgang til systemet beskyttes af sikre login-protokoller, som minimum med brugernavn og adgangskode.

Beskyttelse under transmission:

Alle dataoverførsler mellem bruger og system samt til tredjepartsintegrationer skal ske via krypterede forbindelser (HTTPS, SFTP, mv.).

Beskyttelse under opbevaring:

Data opbevares i sikrede datacentre med adgangskontrol og kryptering. Adgang til produktionsdatabaser begrænses strikt til nødvendigt personale.

Logning:

Der føres log over adgang til personoplysninger, herunder loginforsøg, dataændringer og dataudtræk. Logs opbevares i minimum 6 måneder til sikkerhedsmæssige og revisionsformål.

C.3. Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Bistand ved sikkerhedsbrud, herunder teknisk analyse og dokumentation. Bistand ved anmodninger fra registrerede (f.eks. indsigt, sletning, rettelse). Bistand ved konsekvensanalyser (DPIA) samt samarbejde i forbindelse med tilsyn.

Tekniske og organisatoriske foranstaltninger inkluderer:

Etablering af procedurer for håndtering af registreredes rettigheder.

Adgang til relevante logfiler ved sikkerhedsbrud.

Besvarelse af forespørgsler fra den dataansvarlige inden for rimelig tid.

Tilvejebringelse af dokumentation for overholdelse af tekniske sikkerhedsforanstaltninger.

C.4. Opbevaringsperiode/sletterutine

Personoplysninger opbevares kun så længe det er nødvendigt for at opfylde formålet med behandlingen, og som aftalt med den dataansvarlige. Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren slette personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarliges oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelse.

C.5. Lokalitet for behandling

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

Supabase servere, Sverige - Databehandling og opbevaring af personoplysninger. Udbyder: Supabase Inc, USA.

Klaus Nissen, Damhus 1, 6000 Vejen - Adgang og support vedr. systemadministration og kundeservice. (Databehandler)

Lars Vindbjerg Hansen, Søndervangvej 5, 6600 Vejen - Adgang og support vedr. systemadministration og kundeservice. (Databehandler)

C.6. Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Den dataansvarlige eller en repræsentant for den dataansvarlige kan efter forudgående skriftlig aftale, dog maksimalt én gang om året, foretage en fysisk inspektion af lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse bestemmelser.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

For enhver revision, inspektion eller tilsvarende aktivitet, der iværksættes af eller på vegne af den dataansvarlige, faktureres den tid, som databehandleren og/eller dennes rådgivere medgår, til DKK 7.500 (syvtusinde femhundrede danske kroner) pr. påbegyndt time eksklusiv moms. Dette inkluderer tid anvendt på forberedelse, gennemførelse, rejsetid og efterfølgende opfølgning.

Forud for gennemførelse af revision eller inspektion skal den dataansvarlige overføre et depositum på DKK 93.750 (treoghalvfemstusinde syvhundredeoghalvtreds danske kroner) til databehandlerens bankkonto. Beløbet dækker op til 10 arbejdstimer. Eventuelt merforbrug faktureres særskilt efterfølgende. Beløbet refunderes ikke, medmindre den dataansvarlige aflyser revisionen med mindst 10 dages varsel.

Revision, inspektion eller lignende kan kun foregå efter gensidig aftale og med mindst 30 dages varsel.