# DPA

## Standardkontraktsbestemmelser

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

mellem

SMTP.dk
CVR 29849439
Refshalevej 163A
1432 København K
Danmark

herefter "databehandleren"

[NAVN]
[CVR-NR]
[ADRESSE]
[POSTNUMMER OG BY]
[LAND]

herefter "den dataansvarlige"

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

## 1. Indhold

## 2. 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 SMTP mail relay service 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. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

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

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

## 3. Den dataansvarliges rettigheder og forpligtelser

1. 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.

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.

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, 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. 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. 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

1. 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.

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

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

## 6. 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 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

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 skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 30 dage inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

   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 30 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. 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, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

## 8. 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.

## 9. 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 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, 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.

## 10. 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.

## 11. Sletning og returnering af oplysninger

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

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

## 12. 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 nærmeret 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.

## 13. 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.

## 14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift 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 skriftlig varsel af begge parter.

5. Underskrift

   På vegne af den dataansvarlige

   | | |
   |---|---|
   | Navn | [NAVN] |
   | Stilling | [STILLING] |
   | Telefonnummer | [TELEFONNUMMER] |
   | E-mail | [E-MAIL] |

   Underskrift

   På vegne af databehandleren

   | | |
   |---|---|
   | Navn | [NAVN] |
   | Stilling | [STILLING] |
   | Telefonnummer | [TELEFONNUMMER] |
   | E-mail | [E-MAIL] |

   Underskrift

## 15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

| | |
|---|---|
| Navn | [NAVN] |
| Stilling | [STILLING] |
| Telefonnummer | [TELEFONNUMMER] |
| E-mail | [E-MAIL] |

| | |
|---|---|
| Navn | [NAVN] |
| Stilling | [STILLING] |
| Telefonnummer | [TELEFONNUMMER] |
| E-mail | [E-MAIL] |

**De behandlede oplysninger**

De personoplysninger, som Databehandler behandler på vegne af Dataansvarlig, vedrører de kategorier af persondata, som er afleveret af Dataansvarlig til Databehandler i dokumentet:

- Genstanden for og varigheden af behandlingen,
    - Det af Dataansvarlig uploadede data benyttes til alle former for Dataansvarligs e-mailkommunikation til tredjeparter. Data opbevares på systemet i 30 dage
- Behandlingens karakter og formål,
    - Afsendelse af Dataansvarligs e-mails til alle former for kommunikation, der foregår med Databehandlers SMTP sendeprotokol
- Typen af personoplysninger
    - Almindelige oplysninger, som databehandleren skal behandle på vegne af dataansvarlig:
        - E-mailadresser, FRA og TIL
- Kategorierne af registrerede
    - Afsenderen af e-mails samt e-mailadresser for disses kunder
- den fysiske lokation (af servere etc.) hvor persondata bliver behandlet:

ADEO Data Center Herstedvang 8  2620 Albertslund

## Bilag B Underdatabehandlere

**Underdatabehandlere**

| NAVN | CVR | ADRESSE | BESKRIVELSE AF BEHANDLING |
|---|---|---|---|
| AdeoDC | 37593184 | Herstedvang 8<br>2620 Albertslund<br>Danmark | Hosting af SMTP platform.<br>(Danmark) |
| VIP Support v/Morten Linder | 28014201 | Herstedvang 8<br>2620 Albertslund<br>Danmark | Assistance vedrørende storage systemer og VMware.<br>(Danmark) |
| Expertlance v/Radu Milcoveanu | | Bulevardul luliu Maniu 7 Corp T061072 Bucharest<br>Rumænien | Udvikling og support af SMTP platform.<br>(Rumænien) |

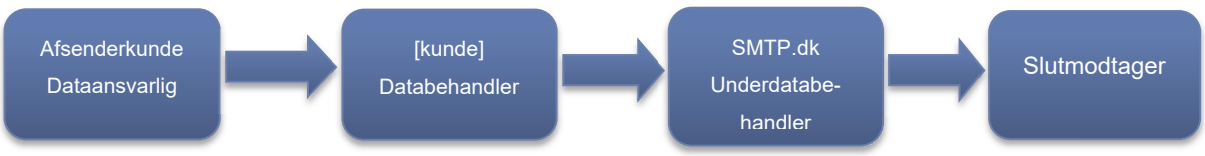
Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne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

## Bilag C Instruks vedrørende behandling af personoplysninger

**C.1. Behandlingens genstand/instruks**
Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

[kunde] fremsender e-mails til SMTP.dk server hvorfra e-mails sendes videre til slutmodtagere i en digital transaktion. Transaktionsdetaljer/log slettes efter 30 dage fra modtagelse af e-mails på SMTP.dk server.

Dataflow:




Instruks:

## C.2. Behandlingssikkerhed

Databehandler har valgt et højt sikkerhedsniveau, for at kunne modtage personoplysninger omfattet af Databeskyttelsesordningens artikel 9 om "Særlige kategorier af personoplysninger"

Databehandleren er 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:

Sikkerhedsniveauet skal afspejle:

Risikostyring og risikovurdering

- Databehandleren skal anlægge en risikobaseret tilgang til sin styring af informationssikkerheden hos databehandleren. Risikostyringen skal baseres på en dokumenteret og regelmæssig opdateret risikovurdering. Vurderingen skal tage udgangspunkt i de registreredes rettigheder og databehandlerens behandlingsaktiviteter.

IT-sikkerhedspolitik

- Databehandleren skal have informationssikkerhedspolitikker og procedurer, som revurderes årligt og godkendes af databehandlerens ledelse.

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

- Databehandleren skal på anmodning fra dataansvarlige fremsende sin IT-sikkerhedspolitikker, herunder informations-sikkerheds procedure til dataansvarlige.

Passwordpolitik

- Databehandlerens passwordpolitik er sat ens for alle medarbejdere og afspejler et højt sikkerhedsniveau. Passwordpolitikken revurderes årligt i forbindelse med årlige revision og godkendes af databehandlerens ledelse.

Bærbare medier

- Databehandlerens politik tillader ikke uden specifik aftale med den dataansvarlige, at data opbevares på bærbare medier (laptop, telefoner, usbstick, eksterne harddiske eller lignende)

Mobilt udstyr og fjernarbejdspladser

- Databehandleren arbejder kun fra fjernarbejdspladser med sikker forbindelse og 2 faktor login.

Håndtering af medarbejdere – før, under og efter ansættelsen

Uddannelse og bevidstgørelse

- Medarbejdere der håndterer personoplysninger, gennemgår årligt GDPR og Databehandlerens GDPR-politikker, IT-sikkerhedspolitikker og informationssikkerhedspolitikker.

Social Engineering

- Databehandleren træner medarbejdere i at være bevidste overfor social engineering
  angreb mindst en gang årligt.

Adgangsrettigheder:

- Databehandleren gennemgår løbende tildeling og tilbagekaldelse af brugeradgang til
  Personoplysninger og systemer, der benyttes via adgangsrettigheder, brugertyper og
  privilegerede rettigheder m.m., herunder styring og jævnlig kontrol.

- Databehandleren vedligeholder en liste over personer og hvilke data de har adgang til.

Tavshedsforpligtelse og sanktionsvilkår:

- Databehandlerens ansatte underskriver en tavshedspligt under ansættelsen og ved ansættelsens ophører.

Ryddet skrivebord:

- Databehandleren har en generel cleandesk politik og politik om PC låses når den forlades, dertil kommer at materiale med persondata opbevares aflåst.

Kontrol og dokumentation

Databehandleren skal på den dataansvarliges anmodning dokumentere løbende overholdelse af GDPR. Den dataansvarlige kan i øvrigt til enhver til stille supplerende spørgsmål til databehandleren.

- Databehandlerens dokumentation skal sendes til dataansvarlige inden for rimelig tid efter modtagelsen af anmodningen herom.

Afhjælpning af afvigelser

- Databehandleren er forpligtet til at afhjælpe afvigelser, der er identificeret i forbindelse med revisionen. Databehandleren skal dokumentere planen for og implementeringen af afhjælpningen.

Databrud og hændelseshåndtering

Databrud

- Databehandleren har procedurer for at imødegå databrud, bl.a. i form af 2-factor login og begrænsede adgangsrettigheder.

Hændelseshåndtering

- Databehandleren har en procedure for håndtering er databrud, herunder hvornår og hvordan der skal rapporteres til dataansvarlig samt klassificering af databrud. Databrudsproceduren testes årligt som led i Dataansvarliges årlig kontrol af Databehandleren.

Fysisk sikkerhed

- Servere og andet udstyr hvorpå der behandles personoplysninger, befinder sig i aflåst rum. Servere hostes hos hostingfirma og databehandlers lokation er aflåst.

- Serverrum er beskyttet mod brand og tyveri.

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

Endpoint-sercurity

- Databehandlers data opbevares hos - se underdatabehandler liste bilag B, hvor der er høj beskyttelse.databehandleren vil på anmodning af den dataansvarlig fremsende revisionserklæringer fra hostingfirma, ISAE 3000, ISAE 3402 eller ISO 27001 dokumentation eller lignende.

- Databehandler udveksler primært data via SSH, kun hvor det ikke er muligt og kun med den dataansvarliges accept udveksles data via e-mail med tvungen End2End kryptering.

Backup

- Databehandler har backup af logdata, backup opbevares i 30 dage, hvorefter de overskrives hos underdatabehandleren.

- Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal **databehandleren** enten slette eller tilbagelevere personoplysningerne, medmindre dataansvarlige – efter underskriften af disse bestemmelser – har ændret oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

Data Loss Prevention

- Databehandler har opsatte processer og politikker, der evalueres årligt, som beskytter mod tab af personoplysninger.

Klassifikation

- Databehandler behandler og klassificerer al data, som var det følsom data.

Mobile device management

- Databehandler opbevarer ikke data på mobile enheder og mobile enheder har kun adgang til data via 2 faktor login.

**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:

Databehandleren bistår med vejledning i hvordan data indeholdende personoplysninger kan fremsendes og modtages via nævnte sikrede kanaler.

**C.4 Opbevaringsperiode/sletterutine**
Medmindre andet aftales vil personoplysninger blive opbevaret i 30 dage, hvorefter de slettes hos databehandleren.

**C.5 Lokalitet for behandling**
Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter.

**C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande**

Der må ikke overføres personoplysninger til tredjelande

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser 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 år for egen regning enten indhente en revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens generelle overholdelse af databeskyttelsesforordningen til udlevering til den dataansvarlige, eller uden beregning udfylde et GDPR Spørgeskema – "Kontrol af databehandlere", som den dataansvarlige sender til databehandleren. Den dataansvarlige kan i øvrigt til enhver tid stille supplerende spørgsmål til databehandleren.
Ovenstående fremsendes uden unødig forsinkelse til dataansvarlige til orientering.

Baseret på resultaterne af spørgeskemaet, 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 dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når dataansvarlige finder det nødvendigt.

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

Databehandler reviderer underdatabehandlere ved årlig indhentning af underdatabehandleres revisionserklæring eller lignende, udarbejdet af underdatabehandler for underdatabehandlers regning

Databehandleren skal som dokumentation for løbende overholdelse af GDPR og Bestemmelserne stille ISAE3000 type 1 erklæring eller lignende til rådighed for den dataansvarlige. Den Dataansvarlige kan i øvrigt til enhver tid stille supplerende spørgsmål til Databehandleren.

Revisionserklæringer eller lignende fremsendes uden unødig forsinkelse til databehandleren til orientering, som på anmodning af den dataansvarlige videresender dem til den dataansvarlige. Den dataansvarlige kan anfægte rammerne for og/eller metoden og kan i sådanne tilfælde anmode om en ny erklæring eller lignende under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne 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.

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når databehandleren (eller den dataansvarlige) finder det nødvendigt.

Dokumentation for sådanne inspektioner fremsendes på anmodning af den dataansvarlige til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om

gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode."

**Sikkerhedsbilag**

- Følsomme oplysninger er krypteret i transit via en sikker filoverførselsløsning i overensstemmelse med branchestandarder
- Databehandler benytter sig af antivirusprogrammer
- Databehandler har implementeret firewalls
- Databehandler sikrer kritiske netværksadgangspunkter, og at systemer løbende testes for svagheder
- Alle ansatte hos Databehandler, eller som arbejder for Databehandler, er tildelt en unik konto, som ikke må deles, og skal holdes fortrolig
- Alle kunder får tildelt en automatisk genereret kode ved første login.
- Adgangskodekonfigurationer bliver håndhævet for at sikre en minimumskonfiguration af:
    - Minimum 12 karakterer (indeholdende store små bogstaver, tal, special tegn)
- Nye brugere skal adgangsautoriseres af brugere med rettigheder hertil, før der gives adgang til systemer
- Alle adgangs- og nøglebegivenheder bliver logget og er tilgængelige for Databehandler, hvis nødvendigt
- Fjernadgang sker via krypteret forbindelse