# BILAG 14 - DATABEHANDLERAFTALE

Offentligt indkøb

af

en SaaS løsning til digitale eksamener Aarhus Universitet

Aarhus Universitet
Nordre Ringgade 1
DK-8000 Aarhus C

## Standardkontraktsbestemmelser

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

mellem

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

herefter "den dataansvarlige"

og

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

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

# Indholdsfortegnelse

## 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 eksamensløsning 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.

## 2. 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.

## 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. 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.

## 4. 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.

## 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.

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

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.

## 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 specifik 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 fire måneder inden anvendelsen af

den pågældende underdatabehandler. 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, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

## 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 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.

## 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 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.

## 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 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.

## 12. 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 | |

## 13. 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] |

## Bilag A Oplysninger om behandlingen

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

Databehandleren skal hoste den digitale eksamensløsning.

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

Databehandleren opbevarer data.

### A.3. Behandlingen omfatter følgende kategorier af registrerede

Kategorier af registrerede personer

I. Studerende

II. Undervisere/ Censorer

III. Administrative medarbejdere

### A.4. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Kategorier af personoplysninger

ad) I: Navn, studienummer, AUID, mailadresse, telefonnummer, rolle
ad) II: Navn, AUID, mailadresse, telefonnummer, rolle
ad) III: Navn, AUID, mailadresse, telefonnummer, rolle

Særlige kategorier af personoplysninger

ad) I: Ingen
ad) Ii: Ingen
ad) III: Ingen

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

Uanset Aftalens formelle aftaleperiode skal Aftalen vedblive at gælde, så længe Databehandleren behandler de personoplysninger, som den Dataansvarlige er dataansvarlig for.

## Bilag B Underdatabehandlere

### B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

| NAVN | CVR | ADRESSE | BESKRIVELSE AF BEHANDLING | GYLDIGT OVERFØRSELSGRUNDLAG, HVIS RELEVANT |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

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.

### B.2. Varsel for godkendelse af underdatabehandlere

Databehandleren skal indgive anmodningen om en specifik godkendelse mindst fire måneder inden anvendelsen af den pågældende underdatabehandler.

## 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:

Databehandleren hoster data i forbindelse med en digital eksamensløsning, udbudt af databehandleren.

### C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter en større mængde personoplysninger, hvorfor der skal etableres et passende 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:

1. **Databehandlerens ansvar**

Databehandleren må alene handle efter denne instruks og kun vedrørende de opgaver, databehandleren har i henhold til databehandleraftalen og hovedaftalen.

2. **Tekniske og organisatoriske sikkerhedsforanstaltninger**

Databehandleren skal som minimum træffe de nedenfor beskrevne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandlingen af personlysninger på vegne af den dataansvarlige.

Såfremt mere omfattende tekniske og organisatoriske sikkerhedsforanstaltninger er nødvendige for at sikre efterlevelse af databehandleraftalen, skal sådanne mere omfattende foranstaltninger altid træffes.

**Risici for sikkerhed**

1. Databehandleren skal tage de nødvendige skridt til at identificere, vurdere og begrænse enhver, med rimelighed forudsigelig, intern og ekstern risiko for tilgængeligheden, fortroligheden, og/eller integriteten af alle personoplysninger omfattet af databehandleraftalen.

2. Databehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Databehandleren skal desuden, hvor det er nødvendigt, evaluere og forbedre effektiviteten af sådanne forholdsregler.

3. Databehandleren skal dokumentere de identificerede risici og – for enhver af disse risici – hvordan risikoen er nedbragt til et acceptabelt niveau.

4. Databehandleren skal have formelle processer for håndtering af sikkerhedshændelser.

5. Databehandleren skal ved hændelser, hvor personoplysningers fortrolighed, integritet eller tilgængelighed kan være eller have været negativt påvirket, underrette den dataansvarlige uden ugrundet ophold.

**Autorisation og adgangskontrol**

1. Autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere, redigere eller slette personoplysninger.

2. Databehandleren skal sikre, at der foretages et efter omstændighederne passende baggrundstjek for alt personale, der i forbindelse med deres ansættelse vil have adgang til personoplysninger omfattet af databehandleraftalen, uanset i hvilket format personoplysninger måtte være tilgængelige.

3. Kun de personer, som autoriseres dertil, må have adgang til de personoplysninger, der behandles, og kun i forhold til det formål opgaven vedrører.

4. Der må endvidere autoriseres personer, for hvem adgang til personoplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

5. De autoriserede brugere udstyres med en brugeridentifikation og et password, der skal anvendes hver gang, der logges på systemet. Passwords skal skiftes efter gældende regler hos dataansvarlige og skal have en tilstrækkelig længde og kompleksitet. Som udgangspunkt anvendes 2-faktor autentificering ved adgang til systemer med følsomme personoplysninger.

6. Autorisation gives til den dataansvarliges systemer af den dataansvar-lige efter den dataansvarliges indstilling.

7. Der skal træffes foranstaltninger til at sikre, at kun autoriserede brugere kan få adgang til personoplysninger, og at brugeren kun kan få adgang til de personoplysninger og anvendelser (behandlinger), som den pågældende er autoriseret til.

8. Generelt skal alle ansatte hos databehandleren, der har med elektronisk databehandling at gøre, udstyres med en brugeridentifikation og et password med henblik på adgang til databehandlerens netværk. Brugeridentifikation og password skal anvendes hver gang, brugeren skaber sig intern adgang til databehandling. Eksternt skal adgange til databehandling etableres med 2-faktor-autentifikation.

9. Databehandleren skal have restriktioner for fysisk adgang til de områder, hvor der sker behandling af personoplysninger.

10. Databehandleren skal have formelle procedurer for håndtering af nulstilling af adgangskoder i situationer, hvor den normale logiske adgangskontrol sættes ud af kraft.

11. Der skal mindst en gang hvert halve år foretages kontrol af, at brugerne kun er tildelt de adgange, som de har behov for.

12. Databehandleren skal uden ophold kunne inddrage autorisationer (og herunder adgange) for brugere, der ikke længere har behov for autorisationen i forbindelse med brugerens arbejde.

**Uddannelse og instruktion**

1. Databehandleren skal sikre, at databehandlerens medarbejdere modtager tilstrækkelig uddannelse og instruktioner, inklusiv – men ikke begrænset til – uddannelse der tilsigter mod at øge medarbejdernes gennerelle sikkerhedsbevidsthed, introduktion af relevante sikkerhedspolitikker og procedurer, samt adgang til og uddannelse i dokumenterede processer og arbejdsbeskrivelser særligt vedrørende behandling af personoplysninger.

2. Uddannelse og instruktioner skal omfatte de emner, der er relevante for at sikre, at personoplysninger behandles i overensstemmelse med såvel lovgivningen som databehandlerens og den dataansvarliges relevante politikker og procedurer.

**Kontrol med afviste adgangsforsøg og logning**

1. Der skal foretages registrering af alle afviste adgangsforsøg. Hvis der inden for en fastsat periode er registreret højst 5 på hinanden følgende afviste adgangsforsøg med samme brugeridentifikation, skal der blokeres for yderligere forsøg. Adgangen åbnes først, når årsagen til afviste adgangsforsøg er klarlagt.

2. Der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse, emnet der blev set på og det anvendte søgekriterium. Loggen skal opbevares i seks måneder, hvorefter den skal slettes, medmindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode, dog højest 5 år, af hensyn til at kunne anvende den som værktøj til brug ved efterforskning.

**Inddatamateriale som indeholder personoplysninger**

1. Inddatamateriale, som ikke indgår i en manuel sag eller et manuelt register, må kun anvendes af personer, som er beskæftiget med inddateringen. Inddatamateriale indeholdende fortrolige personoplysninger skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til personoplysningerne.

2. Inddatamateriale skal slettes eller tilintetgøres, når det ikke længere er nødvendigt at bevare det af hensyn til de formål, som behandlingen varetager eller til kontrol med de inddaterede personoplysninger. Ved tilintetgørelse af inddatamateriale skal der træffes de fornødne sikkerhedsforanstaltninger for at undgå, at materialet misbruges eller kommer uvedkommende i hænde.

3. Bestemmelsen vedrørende sletning eller tilintetgørelse gælder ikke, såfremt materialet er omfattet af bevarings-/kassationsbestemmelser fastsat i henhold til anden

lovgivning. Inddatamateriale, der er journaliseret i henhold til gældende journaliseringsbestemmelser, behandles efter de almindelige arkivbestemmelser om bevaring, herunder aflevering af arkivalier til Statens Arkiver.

**Uddatamateriale som indeholder personoplysninger**

1. Uddata må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages.

2. Ud over bestemmelsen i punkt 1 må uddatamateriale anvendes af personer, som er beskæftiget med sikkerheds- og/eller forvaltningsmæssig revision eller drifts- og systemtekniske opgaver vedrørende det pågældende system og systemets anvendelse.

3. Uddatamateriale skal både fysisk og teknisk opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, som er indeholdt i materialet.

4. Uddatamateriale skal tilintetgøres, når det ikke længere er nødvendigt til de formål, som behandlingen varetager.

5. Bestemmelsen om tilintetgørelse gælder ikke, såfremt materialet er omfattet af bevarings-/kassationsbestemmelser i henhold til anden lovgivning.

6. Uddatamateriale, der er journaliseret i henhold til vedtagne journaliseringsbestemmelser, behandles efter de almindelige arkivbestemmelser om bevaring, herunder aflevering af arkivalier til Statens Arkiver.

7. Ved tilintetgørelse af uddatamateriale skal der træffes de fornødne sikkerhedsforanstaltninger for at undgå, at materialet misbruges eller kommer uvedkommende i hænde.

8. Bestemmelserne i punkterne 1-5 gælder ikke for uddatamateriale, som indgår i en manuel sag eller i et manuelt register.

**Mobile lagringsmedier**

1. Mobile lagringsmedier med personoplysninger skal være mærket og skal opbevares krypteret under opsyn eller under lås, når de ikke benyttes.

2. Mobile lagringsmedier med personoplysninger må kun udleveres til medarbejdere samt til autoriserede personer, der har adgang til personoplysningerne med henblik på revision eller drifts- og systemtekniske opgaver.

3. Der skal føres en fortegnelse over hvilke mobile lagringsmedier, der benyttes i forbindelse med databehandlingen, og hvem der har benyttet dem.

4. Der skal udarbejdes skriftlige instrukser for anvendelse og opbevaring af udtagelige mobile lagringsmedier.

5. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes fornødne foranstaltninger for at sikre, at personoplysningerne ikke hændeligt eller bevidst tilintetgøres, fortabes eller forringes, eller at personoplysningerne kommer uvedkommende i hænde, misbruges eller i øvrigt behandles i strid med persondataloven.

**Sikkerhedskopier**

1. Der gælder de samme retningslinjer for sikkerhedskopier som for al anden behandling af personoplysninger i medfør af denne aftale.

2. Databehandleren skal sikre, at systemer og personoplysninger sikkerhedskopieres regelmæssigt medmindre andet aftales nærmere i databehandleraftalen.

3. Sikkerhedskopier skal opbevares sikkert og adskilt fra serveren i et ikke tilstødende rum eller anden bygning for at sikre, at disse ikke går tabt.

4. Databehandleren skal regelmæssigt kontrollere, at sikkerhedskopier er læsbare. Dette skal blandt andet gøres ud fra et beredskabssynspunkt, f.eks. ved større ændringer af et systems tekniske setup.

**Opdateringer og ændringer**

1. Databehandleren skal have formelle procedurer til sikring af, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid.

2. Databehandleren skal have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering. Proceduren skal understøttes af en effektiv funktionsadskillelse eller ledelsesopfølgning med henblik på at sikre, at ingen enkeltpersoner kan implementere en ændring alene.

**Driftsafbrydelser**

Databehandleren skal have dokumenterede beredskabsprocedurer, der sikrer genetablering af services inden for rimelig tid i tilfælde af driftsafbrydelser.

**Bortskaffelse af udstyr**

1. Databehandleren skal have formelle processer i overensstemmelse med best practice og kunne sikre, at der sker effektiv sletning af personoplysninger, således at de ikke kan gendannes på nogen måde inden bortskaffelse af elektronisk udstyr.

2. Ved bortskaffelse af udstyr skal databehandleren dokumentere fremgangsmåden herfor og kunne forevise denne dokumentation efter anmodning herom.

**Tilsyn**

Databehandleren skal føre og dokumentere et tilsyn med databehandlerens organisations overholdelse af lovkrav, politikker og procedurer.

### 3. 3. Ad hoc arbejdspladser

1. Databehandleren må ikke foretage databehandling fra ad hoc arbejdspladser (fjern-arbejdspladser eller hjemmearbejdspladser), medmindre det er beskrevet udførligt i databehandleraftalen, hvordan dette skal foregå på en sikker måde, herunder brug af 2-faktor-autentifikation.

2. Den dataansvarlige skal godkende brug af ad hoc arbejdspladser.

3. Der må kun etableres eksterne IT-kommunikationsforbindelser, hvis der efter godkendelse og efter nærmere aftale herom træffes foranstaltninger til at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

4. Der skal foretages foranstaltninger, der sikrer at personoplysninger, der transmitteres over åbne net som for eksempel Internettet, ikke fortabes, ændres eller kommer til uvedkommendes kendskab under transmissionen.

5. Den dataansvarlige fastlægger retningslinjer herfor og angiver, hvilke særlige foranstaltninger, der konkret skal træffes for at efterleve disse krav.

### 4. 4. Underretningspligt og assistance ved sikkerhedshændelse

Databehandleren har pligt til uden unødig ophold at underrette den data-ansvarlige, såfremt der er indtruffet en sikkerhedshændelse. Denne underretning skal således ske umiddelbart efter en sikkerhedshændelse er indtruffet eller opdaget af databehandleren.

En underretning vil derfor typisk være to delt:

5. En underretning om at en hændelse er indtruffet
6. En underretning om de nærmere omstændigheder, herunder men ikke udelukkende:
    a. En situationsrapport
    b. Hvilke personoplysninger der er kompromitteret.
    c. Hvilke tiltag databehandleren har iværksat eller påtænker at iværksætte.

**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 skal uden unødig forsinkelse, efter at være blevet opmærksom herpå, skriftligt underrette den dataansvarlige om enhver anmodning rettet til databehandleren eller dennes eventuelle underdatabehandlere fra en registreret om udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren er ikke berettiget til at besvare anmodninger fra en registreret vedrørende udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret.

Databehandleren skal på anmodning fra den dataansvarlige hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til de registreredes rettigheder i henhold til gældende databeskyttelsesret.

Databehandlerens bistand ifm. den dataansvarliges forpligtelser efter databeskyttelsesforordningens artikel 33 og 34 sker ved, at databehandleren indgiver de oplysninger, der følger af bilag D. Databehandleren skal efterfølgende bistå den dataansvarlige ved på den dataansvarliges anmodning at stille de oplysninger til rådighed, som er nødvendige for, at den dataansvarlige kan foretage anmeldelse af brud på persondatasikkerheden til Datatilsynet eller som er nødvendige for, at den dataansvarlige kan underrette den registrerede herom.

Såfremt den dataansvarlige vurderer, at behandlingen sandsynligvis vil indebære en høj risiko for de registreredes rettigheder og frihedsrettigheder, skal databehandleren på anmodning fra den dataansvarlige bistå den dataansvarlige ifm. dennes forpligtelser efter databeskyttelsesforordningens artikel 35 og 36 ved at indgive de oplysninger til den dataansvarlige, der er nødvendige for, at den dataansvarlige kan foretage en konsekvensanalyse i overensstemmelse med artikel 35 og foretage en forudgående høring af Datatilsynet i overensstemmelse med artikel 36.

Databehandleren skal endelig sikre, at dennes tekniske og organisatoriske foranstaltninger gør det muligt for den dataansvarlige at overholde sine forpligtelser efter databeskyttelsesforordningens art. 33-36, herunder f.eks. gennem de foranstaltninger der følger af bilag C.2.

**C.4 Opbevaringsperiode/sletterutine**
[BESKRIV EVENTUEL OPBEVARINGSPERIODE/SLETTERUTINE FOR DATABEHANDLEREN]

[EKSEMPELVIS]

*"Personoplysninger opbevares i [ANGIV TIDSPERIODE], hvorefter de slettes hos databehandleren.*

*Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret 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 dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

[ANGIV, HVOR BEHANDLINGEN FINDER STED] [ANGIV, HVILKEN DATABEHANDLER ELLER UNDERDATABEHANDLER, DER ANVENDER ADRESSEN]

**C.6 Instruks vedrørende overførsel af 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**
På anmodning fra den dataansvarlige skal databehandleren give den dataansvarlige de nødvendige oplysninger til, at denne kan påse forpligtelserne i henhold til Bestemmelserne samt

at der er truffet passende tekniske og organisatoriske sikkerhedsforanstaltninger. Endvidere skal databehandleren kunne dokumentere, at identificerede sårbarheder bliver imødegået ud fra en risikobaseret vurdering.

Såfremt den dataansvarlige, en repræsentant for denne, dennes revision (intern eller ekstern) eller en relevant offentlig myndighed, særligt Datatilsynet, ønsker at foretage fysisk inspektion (audit) af de foranstaltninger, som databehandleren har etableret i medfør af Bestemmelserne, forpligter databehandleren sig til - med et rimeligt varsel – at stille tid og ressourcer til rådighed herfor. Databehandleren forpligter sig til på samme måde at sikre, at sådanne audits kan gennemføres hos dennes eventuelle underdatabehandlere.

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

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

[BESKRIV PROCEDURERNE FOR DATABEHANDLERENS REVISIONER, HERUNDER INSPEKTIONER, MED BEHANDLINGEN AF PERSONOPLYSNINGER, SOM ER OVERLADT TIL UNDERDATABEHANDLEREN]

[EKSEMPELVIS]

*"Databehandleren skal [ANGIV TIDSPERIODE] for [EGEN/UNDERDATABEHANDLERENS] regning indhente en [REVISIONSERKLÆRING/INSPEKTIONSRAPPORT] fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.*

*Der er enighed mellem parterne om, at følgende typer af [REVISIONSERKLÆRINGER/INSPEKTIONSRAPPORTER] kan anvendes i overensstemmelse med disse bestemmelser:*

*[BESKRIV AFTALTE REVISIONSERKLÆRINGER/INSPEKTIONSRAPPORTER]*

*[REVISIONSERKLÆRINGEN/INSPEKTIONSRAPPORT] fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i [ERKLÆRINGEN/RAPPORTEN] og kan i sådanne tilfælde anmode om en ny [REVISIONSERKLÆRING/INSPEKTIONSRAPPORT] under andre rammer og/eller under anvendelse af anden metode.*

*Baseret på resultaterne af [ERKLÆRINGEN/RAPPORTEN], 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 uden unødig forsinkelse 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."*

[ELLER]

*"Databehandleren eller en repræsentant for databehandleren foretager [ANGIV TIDSPERIODE] en fysisk inspektion af lokaliteterne, hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.*

*Ud over det planlagte tilsyn, kan databehandleren gennemføre en inspektion med underdatabehandleren, når databehandleren (eller den dataansvarlige) finder det nødvendigt.*

*Dokumentation for sådanne inspektioner fremsendes uden unødig forsinkelse 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.*

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

[OG, HVIS RELEVANT]

*"Den dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, hvis den dataansvarlige vurderer, at databehandlerens inspektion hos underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker I overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.*

*Den dataansvarliges eventuelle deltagelse i en inspektion hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser."*

[OG, HVIS RELEVANT]

*"Databehandlerens og underdatabehandlerens eventuelle udgifter i forbindelse med en fysisk inspektion af underdatabehandlerens lokaliteter er den dataansvarlige uvedkommende – uanset om den dataansvarlige har initieret og deltaget i en sådan inspektion."*

## Bilag D Parternes regulering af andre forhold

D.1 I tilfælde af brud på datasikkerheden skal følgende information indgives til den dataansvarlige:

| | |
|---|---|
| Dato og tid: | Brud på persondatasikkerheden blev konstateret den [dato], klokken [klokkeslæt]. |
| Omstændighederne ved bruddet på datasikkerheden: | Bruddet skyldes [beskriv omstændighederne ved bruddet på datasikkerheden]. |
| Karakteren/arten af bruddet: | På nuværende tidspunkt bemærkes det, at [Indsæt information om karakteren/omfanget af sikkerhedsbruddet. Såfremt det er muligt at fastslå følgende:<br>1) Kategorier og det omtrentlige antal registrerede impliceret;<br>2) Kategorier og det omtrentlige antal persondataoplysninger impliceret.] |
| Andre oplysninger: | På nuværende tidspunkt bemærkes det, at [Angiv andre oplysninger om bruddet på datasikkerheden, der kan være brugbare for den dataansvarliges vurdering af indvirkningen af bruddet]. |
| Handlinger truffet: | Af hensyn til at begrænse omfanget af og konsekvenserne ved bruddet, har vi indtil videre [foranstaltninger truffet af databehandleren for at imødegå bruddet på persondatasikkerheden, herunder foranstaltninger truffet for at begrænse eventuelle skadevirkninger]. |
| Kontaktperson hos databehandleren: | [Kontaktoplysninger, herunder information på databehandlerens eventuelle DPO]. |