|  |  |
| --- | --- |
|  | Databehandleraftale |
| vedrørende | Sikkert Samfunds bistand til og behandling af personoplysninger i forbindelse med Skoleberedskab |

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

mellem

CVR

herefter ”den dataansvarlige”

og

Sikkert Samfund ApS

CVR 40 05 90 91

Fjeldhammervej 5-9

2610, Rødovre

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

1. Indhold

[2. Præambel 4](#_Toc30147576)

[3. Den dataansvarliges rettigheder og forpligtelser 4](#_Toc30147577)

[4. Databehandleren handler efter instruks 5](#_Toc30147578)

[5. Fortrolighed 5](#_Toc30147579)

[6. Behandlingssikkerhed 5](#_Toc30147580)

[7. Anvendelse af underdatabehandlere 6](#_Toc30147581)

[8. Overførsel til tredjelande eller internationale organisationer 7](#_Toc30147582)

[9. Bistand til den dataansvarlige 8](#_Toc30147583)

[10. Underretning om brud på persondatasikkerheden 9](#_Toc30147584)

[11. Sletning og returnering af oplysninger 10](#_Toc30147585)

[12. Revision, herunder inspektion 10](#_Toc30147586)

[13. Parternes aftale om andre forhold 10](#_Toc30147587)

[14. Ikrafttræden og ophør 10](#_Toc30147588)

[15. Kontaktpersoner hos den dataansvarlige og databehandleren 11](#_Toc30147589)

[Bilag A Oplysninger om behandlingen 12](#_Toc30147590)

[Bilag B Underdatabehandlere 13](#_Toc30147591)

[Bilag C Instruks vedrørende behandling af personoplysninger 14](#_Toc30147592)

[Bilag D Parternes regulering af andre forhold 19](#_Toc30147593)

Dette er **version 1**, sidst opdateret den [10-02.] januar 2023

# 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 Skoleberedskabsservice, herunder skoleberedskabsabonnementet, -løsningen og -applikationen, 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 tre bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
10. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

# 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]](#footnote-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.

# 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 er, uagtet pkt. 4.1., berettiget til at anvende de personoplysninger, som behandles på vegne af den dataansvarlige, med henblik på at (videre)udvikle og forbedre produktet. Anvendelsen af de pågældende personoplysninger skal i videst muligt omfang ske i aggregeret og/eller pseudonymiseret form, og hvis muligt i anonymiseret form. Databehandleren er i denne henseende selvstændig dataansvarlig, og Databehandleren vil derfor iagttage databeskyttelsesforordningen og -loven i nødvendigt omfang.
3. 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.

# 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.

# 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:

* 1. Pseudonymisering og kryptering af personoplysninger
  2. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
  3. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
  4. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

1. 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.
2. 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.

# Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.
3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 kalenderdages 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.

1. 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.
2. 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.
3. 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.

# 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:
   1. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
   2. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
   3. 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.

# 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:

* 1. oplysningspligten ved indsamling af personoplysninger hos den registrerede
  2. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
  3. indsigtsretten
  4. retten til berigtigelse
  5. retten til sletning (”retten til at blive glemt”)
  6. retten til begrænsning af behandling
  7. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
  8. retten til dataportabilitet
  9. retten til indsigelse
  10. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

1. 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:
2. 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
3. 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
4. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
5. 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.
6. 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.

# 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:
   1. 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
   2. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
   3. 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.

# 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.

# Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

# 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.

# 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 skriftligt varsel af begge parter.
5. Underskrift

På vegne af den dataansvarlige

|  |  |  |
| --- | --- | --- |
| På vegne af den dataansvarlige  Sted:  Dato:  Navn:  Stilling:  Telefonnummer:  E-mail: |  | På vegne af databehandleren  Sted: Rødovre  Dato: 10-02-23 Navn: Benjamin R. Bay  Stilling: Direktør  Telefonnummer: 40515114  E-mail: Bay@sikkertsamfund.dk |
|  |  |  |
|  |  |  |

# 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.

|  |  |  |
| --- | --- | --- |
| **Den dataansvarlige**  Navn:  Stilling:  Telefonnummer:  E-mail: |  | **Databehandleren**  Navn: Benjamin R. Bay  Stilling: Direktør  Telefonnummer: 40515114  E-mail: Bay@sikkertsamfund.dk |

# Bilag A Oplysninger om behandlingen

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

* 1. Formålet med databehandlerens behandling af personoplysninger er at levere, administrere og løbende vedligeholde den skoleberedskabsservice, som den dataansvarlige får leveret af databehandleren.

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

* 1. Generel og løbende varetagelse af skoleberedskabsservicen, herunder den skoleberedskabsapplikation, der er en central del af den dataansvarliges beredskab.
  2. I visse særlige tilfælde videregivelse af personoplysninger til relevante myndigheder, som f.eks. brandvæsnet og politiet.

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

* 1. Databehandleren vil behandle almindelige, ikke-følsomme oplysninger i form af telefonnummer på de brugere af mobilapplikationen, der har verificeret sig. Oplysningerne er omfattet af databeskyttelsesforordningens artikel 6.
  2. I visse særlige tilfælde vil databehandleren behandle oplysninger om lokation samt lyd- og billedoptagelser. Oplysningerne vil som udgangspunkt udgøre almindelige, ikke-følsomme personoplysninger omfattet af databeskyttelsesforordningens artikel 6. Lyd- og billedoptagelserne vil imidlertid i enkelte situationer kunne udgøre oplysninger om strafbare forhold omfattet af databeskyttelsesforordningens artikel 10, og databeskyttelseslovens § 8, såfremt f.eks. en særligt voldsom, aggressiv eller truende adfærd optages.

**A.4. Behandlingen omfatter følgende kategorier af registrerede**

4.1. Medarbejdere tilknyttet den dataansvarlige, og i visse særlige tilfælde fysiske personer (børn, unge, ældre m.fl.) som befinder sig på den dataansvarliges arealer og i den dataansvarliges lokaler.

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

* 1. Personoplysningerne (telefonnummer), der behandles i forbindelse med løbende og generel varetagelse af den dataansvarliges skoleberedskab, behandles, indtil den enkelte medarbejder ikke længere er tilknyttet den dataansvarlige, eller indtil den dataansvarlige og/eller databehandleren opsiger/ophæver aftalen, som nærværende databehandleraftale udspringer af.
  2. De yderligere personoplysninger (lokation, billed- og lydoptagelser), der i visse særlige tilfælde behandles, opbevares i 30 dage fra det tidspunkt, oplysningerne er indsamlet, hvorefter de slettes/destrueres.

# Bilag B Underdatabehandlere

**B.1. Godkendte underdatabehandlere**

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

| NAVN | CVR | ADRESSE | BESKRIVELSE AF BEHANDLING |
| --- | --- | --- | --- |
| Amazon Web Services EMEA SARL (AWS) | B186284 | 38 Avenue John F. Kennedy, L-1855 Luxembourg | Opbevaring af data i database, behandling af data i containere og udsendelse af e-mails, SMS og push-notifikationer |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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**

C.1.1. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige foretages med henblik på iværksættelse, vedligeholdelse og administration og den dataansvarliges skoleberedskab.

**C.2. Behandlingssikkerhed**

2.1. Sikkerhedsniveauet skal afspejle:

Databehandleren skal etablere et passende sikkerhedsniveau under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

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 udføre en risikovurdering for alle systemer, inden de anvendes til at behandle den dataansvarliges personoplysninger.

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

**Fysisk sikkerhed**

Databehandleren gennemfører følgende fysiske sikkerhedsforanstaltninger:

1. Databehandlerens kontorlokaler kan aflåses.
2. Databehandleren har alarmsystem til at opdage og forhindre indbrud.
3. Databehandlerens udstyr (herunder PC’er, eventuelle servere m.v) er sikret bag låste døre og vinduer.
4. Sikre kontrol af og sikring af alle flytbare elektroniske enheder, der indeholder personoplysninger, fx USB-stik, CD’er eller flytbare harddiske.
5. Der er overvågning af databehandlerens bygninger, lokaler og faciliteter eller adgangsveje (billede- eller videoovervågning).
6. Databehandleren anvender nøglestyring, dvs. udleverer nøgler til de relevante og nødvendige medarbejdere mv.
7. Databehandleren destruerer eller fjerner alle personoplysninger fra medier, f.eks. pc’er og smartphones, samt fra harddiske før bortskaffelse.
8. Fysiske backups af personoplysninger skal opbevares off-site eller i ild- og vandtætte beholdere.

**Organisatorisk sikkerhed**

Databehandleren gennemfører følgende organisatoriske sikkerhedsforanstaltninger:

1. Alle medarbejdere er underlagt fortrolighedsforpligtelse, der gælder for alle behandlede personoplysninger.
2. Medarbejdernes adgang til personoplysninger i systemer og på eventuelle fysiske medier eller faciliteter er begrænset, sådan at det kun er de relevante medarbejdere, der har rollebaseret adgang og login til de relevante personoplysninger, og det sikres, at adgang og login kun kan ske fra autoriseret udstyr.
3. Hvis medarbejdere skifter job, skal det sikres, at de ikke bevarer adgange, som var nødvendige i deres tidligere job.
4. Databehandleren har en dokumenteret procesbeskrivelse for brud på persondatasikkerheden, der minimum tages op til revidering årligt.
5. Databehandleren har en it-sikkerhedspolitik.
6. Databehandleren har en fast proces, der sikrer, at der ved reparation, service og kassation af hardware sørges for sletning eller fortsat fortrolighed vedrørende personoplysninger på det berørte hardware.
7. Databehandlerens medarbejdere skal uddannes i, hvad et brud på persondatasikkerheden er, trænes i at genkende tegn derpå samt at foretage den passende reaktion.
8. Databehandlerens medarbejdere dokumenterer og rapporterer regelmæssigt brud på persondatasikkerheden eller risici herfor.
9. Databehandleren introducerer nye ansatte til informationssikkerhed og sikrer, at de læser og forstår IT-sikkerhedspolitikken.

**Teknisk sikkerhed: Adgang til personoplysninger (data)**

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende adgang til personoplysninger:

1. Databehandlerens systemer har logisk adgangskontrol ved brugernavn og adgangskode eller anden autorisation.
2. Databehandleren benytter antivirusprogrammer, som opdateres jævnligt, og hvor virusdefinitionerne opdateres mindst én gang ugentligt.
3. Databehandleren kræver, at medarbejdere anvender individuelle adgangskoder (passwords).
4. Databehandlerens PC’er har automatisk adgangsbeskyttelse ved inaktivitet, dvs. låst pauseskærm.
5. Der anvendes politik for sammensætningen af adgangskoder, herunder minimumskrav, især brug af stærke adgangskoder, periodisk opdatering af adgangskoder og sikring af, at medarbejderne ikke skriver adgangskoderne ned.
6. Der er procedure(r) for tilbagekaldelse af tilladelser, når en medarbejder stopper hos Databehandleren eller skifter afdeling. Tilsvarende gælder eksterne konsulenter og vikarer.
7. Der er procedure(r) for tildeling af autorisationer til it-systemer ved en medarbejders ansættelse.
8. Databehandleren skal sikre, at enhver person, der udfører arbejde for Databehandleren og får adgang til personoplysningerne, kun behandler sådanne oplysninger efter den Dataansvarliges instruks.

**Teknisk sikkerhed: Adgang til og beskyttelser af systemer**

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende adgang til og beskyttelse af systemer:

1. Databehandleren foretager regelmæssig gennemgang og kontrol af brugerautorisationer til specifikke systemer.
2. Databehandleren foretager regelmæssig gennemgang af systemkontrol.
3. Databehandleren tildeler enkelte eller grupper af brugere autorisationer til at tilgå, ændre og slette behandlede personoplysninger.
4. Databehandleren har procedure(r) for at genskabe/reetablere data fra backup.
5. Databehandleren sikrer, at al indgående og udgående trafik på computere scannes for vira, hvilket også foretages for enhver diskette eller CD, der benyttes. Databehandlerens computere scannes for vira mindst én gang ugentligt.
6. Når databehandlerens computere er tilkoblet internettet, benyttes en firewall, fotrinsvist en ’next generation firewall’, en anti-DDOS finder og et indtrægnings-sporings-system (intrusion detection system).
7. Databehandleren sikrer tilgængeligheden og adgang til personoplysningerne i tilfælde af en sikkerhedshændelse, inklusiv gennem backups.

**Teknisk sikkerhed: Kryptering**

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende kryptering:

1. Databehandlerens computere har krypterede harddiske.
2. Databehandlerens medarbejdermaskiner er krypterede med bitlocker eller lignende krypteringsteknologi.
3. Databehandlerens hjemmesider anvender HTTPS (Hyper Text Transfer Protocol Secure).
4. Personoplysninger krypteres i relevante systemer og/eller på opbevaringsmedier.
5. Databehandleren anvender kryptering og pseudonymisering af alle personoplysninger, når det overføres via internettet og i øvrigt, når det er muligt.

**Teknisk sikkerhed: Kontrol af transmission**

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende kontrol af transmission:

1. Retningslinjer for brug af arbejdsmail, herunder brug af arbejdsmail til privat brug, passende brug, kryptering, sikker brug mv.
2. Databehandleren anvender og har retningslinjer for sikker e-mail.

**Teknisk sikkerhed: Tilgængelighed og robusthed**

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende tilgængelighed og robusthed:

1. Kun autoriserede medarbejdere har adgang til databehandlerens eventuelle egne servere.
2. Serverrum har airconditionsystem.
3. Der er regler og retningslinjer for backup af data.
4. Der er regler og retningslinjer for genskabelse af data fra backup.
5. Der foretages regelmæssig backup (både egen og hos leverandør).
6. Der anvendes uafbrudt strømforsyning (UPS).
7. Databehandleren har procedurebeskrivelse(r) for brud på persondatasikkerheden, der minimum tages op til revidering og testning årligt.
8. Databehandleren har et sårbarhedsledelsesprogram (vulnerability management program), som overvåger potentielle sårbarheder og gennemfører penetrtionstests af netværk og systemer, som anvendes til behandling af personoplysninger. Programmet skal inkludere sårbarhedsscanninger på ekstern perimeter mindst hvert kvartal.
9. Databehandleren gennemfører penetrationstests på eksterne netværk perimetre mindst hvert kvartal.
10. Databehandleren foretager opfølgning og udbedring af svagheder, som er blevet identificeret ved disse tests.
11. Databehandleren skal løbende holde netværk og systemer opdaterede med nye versioner, opdateringer og patches.
12. Databehandleren skal have en business continuity plan i tilfælde af alvorlige sikkerhedshændelser og teste planen mindst én gang årligt.
13. Databehandleren skal periodisk teste, vurdere og sikre effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger.
14. Databehandleren skal sikre procedure for at følge op på manglende compliance.

**Teknisk sikkerhed: logning**

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende logning af aktiviteter:

1. Databehandleren fører log over fejlslagne loginforsøg, herunder tidspunkt for forsøg, brugeren samt blokerer adgang efter et givent antal fejlslagne forsøg.
2. Databehandleren skal logge aktiviteter vedrørende personoplysninger med angivelse af tidspunkt, bruger, søgninger, søgekriterier, adgang, ændringer, lukning, print, eksportering.
3. Den dataansvarlige kan på anmodning få udleveret en liste over de personer, som har haft adgang til den dataansvarliges personoplysninger hos databehandleren.

**Samarbejde med myndigheder**

Hvis en myndighed indgiver en anmodning om at få adgang til den dataansvarliges personoplysninger, skal databehandleren straks og uden ugrundet ophold videresende anmodningen til den dataansvarlige, medmindre det ifølge lovgivningen er påkrævet, at databehandleren behandler anmodningen. I så fald skal databehandleren underrette den dataansvarlige herom, herunder med en henvisning til det juridiske grundlag for anmodningen. Databehandleren kan dog undlade at underrette den dataansvarlige, såfremt underretning vil stride mod en eventuel lovmæssig tavshedspligt, som databehandleren er pålagt.

**C.3 Bistand til den dataansvarlige**

3.1. 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:

* + 1. Hvis den dataansvarlige modtager en anmodning om udøvelse af den registreredes rettigheder efter databeskyttelsesforordningen eller -loven, og korrekt besvarelse af anmodningen kræver bistand fra databehandleren, skal databehandleren bistå den dataansvarlige med nødvendige og relevante oplysninger og dokumentation samt passende tekniske og organisatoriske sikkerhedsforanstaltninger.
    2. Hvis den dataansvarlige vil have hjælp til at besvare en anmodning fra en registreret, skal den dataansvarlige sende skriftlig anmodning herom til databehandleren, og databehandleren skal som svar herpå levere den nødvendige hjælp eller dokumentation hurtigst muligt og senest 7 kalenderdage efter modtagelse af anmodning herom.
    3. Hvis databehandleren modtager en anmodning om udøvelse af den registreredes rettigheder efter databeskyttelsesforordningen eller -loven fra andre end den dataansvarlige, og anmodningen vedrører personoplysninger behandlet på vegne af den dataansvarlige, skal databehandleren uden unødvendig forsinkelse videresende anmodningen til den dataansvarlige.

**C.4 Opbevaringsperiode/sletterutine**

4.1. Personoplysninger opbevares generelt i den periode, hvor databehandleren leverer tjenesten Skoleberedskab til den dataansvarlige, hvorefter de slettes hos databehandleren. Oplysninger vedrørende lokation samt billed- og lydoptagelser opbevares dog alene i 30 dage fra det tidspunkt, oplysningerne er indsamlet, hvorefter de slettes/destrueres.

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 dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

**C.5 Lokalitet for behandling**

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

Hos databehandlerens egne hovedkontorer og på hovedkontorerne for godkendte underdatabehandlere, som angivet i bilag B.

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

6.1. Personoplysningerne behandles kun af databehandleren på de lokationer, som er beskrevet i Bilag C.5.

6.2. Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

6.3. Overførsel af personoplysninger må i alle tilfælde kun ske som foreskrevet i Bestemmelserne, på den dataansvarliges instruks, og i det omfang databehandleren har sikret et passende overførelsesgrundlag i overensstemmelse med databeskyttelseslovgivningen.

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

7.1. Databehandleren skal på skriftlig anmodning dokumentere over for den dataansvarlige, at databehandleren:

* + 1. overholder sine forpligtelser efter denne databehandleraftale og instruksen, og
    2. overholder bestemmelserne i databeskyttelsesforordningen, for så vidt angår personoplysningerne, som databehandleren behandler på vegne af den dataansvarlige.

7.2. Databehandlerens dokumentation i henhold til pkt. 7.1. skal sendes til den dataansvarlige inden for rimelig tid efter modtagelsen af anmodningen herom.

7.3. Databehandleren skal herudover give mulighed for og bidrage til revisioner og inspektioner hver 12. måned, der foretages af revisorer udpeget af den dataansvarlige, de offentlige myndigheder i Danmark eller af anden kompetent jurisdiktion, i det omfang det er nødvendigt for at kontrollere, at databehandleren overholder Bestemmelserne og gældende databeskyttelseslovgivning. Den pågældende revisor skal være underlagt fortrolighed i henhold til lov eller aftale. Den dataansvarlige skal skriftligt varsle revisioner som beskrevet med mindst 14 kalenderdage.

7.4. Databehandleren er forpligtet til uden beregning én gang årligt at svare på et spørgeskema om overholdelsen af GDPR fra den dataansvarlige som led i den dataansvarliges revision.

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

8.1. Databehandleren skal minimum hver 12. måned for egen regning føre tilsyn med anvendte underdatabehandlere.

8.2. Revisionserklæringen eller andet tilstrækkeligt dokumentation af det gennemførte tilsyn fremsendes efter anmodning til den dataansvarlige uden unødig forsinkelse.

8.3. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

8.4. Den dataansvarlige afholder omkostningerne forbundet med udarbejdelsen af eventuelle yderligere erklæringer.

8.5. Baseret på resultaterne af erklæringen, 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.

1. Henvisninger til ”medlemsstat” i disse bestemmelser skal forstås som en henvisning til ”EØS-medlemsstater”. [↑](#footnote-ref-1)