

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

mellem

kunden, det vil sige "den dataansvarlige"

og

Incendium A/S
CVR 32287239
Vestermøllevej 32
Thisted
Danmark

herefter "databehandleren"

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

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

1. Indhold

<u>2.Præambel.....</u>	<u>3</u>
<u>3.Den dataansvarliges rettigheder og forpligtelser.....</u>	<u>3</u>
<u>4.Databehandleren handler efter instruks.....</u>	<u>4</u>
<u>5.Fortrolighed.....</u>	<u>4</u>
<u>6.Behandlingssikkerhed.....</u>	<u>4</u>
<u>7.Anvendelse af underdatabehandlere.....</u>	<u>5</u>
<u>8.Overførsel til tredjelande eller internationale organisationer.....</u>	<u>6</u>
<u>9.Bistand til den dataansvarlige.....</u>	<u>7</u>
<u>10.Underretning om brud på persondatasikkerheden.....</u>	<u>8</u>
<u>11.Sletning og returnering af oplysninger.....</u>	<u>8</u>
<u>12.Revision, herunder inspektion.....</u>	<u>8</u>
<u>13.Parternes aftale om andre forhold.....</u>	<u>9</u>
<u>14.Ikrafttræden og ophør.....</u>	<u>9</u>
<u>15.Kontaktpersoner hos den dataansvarlige og databehandleren.....</u>	<u>10</u>
<u>Bilag A, Oplysninger om behandlingen.....</u>	<u>11</u>
<u>Bilag B, Underdatabehandlere.....</u>	<u>12</u>
<u>Bilag C, Instruks.....</u>	<u>13</u>

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 IncidentShare 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.

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 medlemsstaternes¹ nationale ret og disse Bestemmelser.

¹

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

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.

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 specifik skriftlig godkendelse 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 14 hverdage 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 gennem-

føre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Side 6 af 13

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 herigenem 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. I tilfælde af databehandlerens konkurs skal underdatabehandlere være instrueret i at slette 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.

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.

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

9. Bistand til den dataansvarlige

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. indsigtretten
 - 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 unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
 - b. den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
 - 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, inden behandling, såfremt en konsekvensanalyse vedrørende databe-

skyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

Side 8 af 13

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 unødigt 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 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 dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.
2. Den Dataansvarlige har ret til at få data udleveret ved 14 dage inden tjenestens ophør skriftligt at anmode herom.

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

hed 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. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.
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 u hensigtsmæssigheder 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, 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	Thomas Baun
Stilling	Administrerende Direktør

Telefonnummer 22645991
E-mail thomas@incendium.dk

Side 10 af 13

Underskrift

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via bestemte kontaktpunkter.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpunkterne.

Den Dataansvarlige har på godkendelsestidspunktet oplyst kontaktpunktet via en opgivelsen af en emailadresse.

Incendium kan til daglig kontaktes på info@incendium.dk og på firmaets hovedtelefonnummer 71990396.

Bilag A, Oplysninger om behandlingen

Formålet med og karakteren af Incendiums behandling af personoplysninger på vegne af den Dataansvarlige i IncidentShare er:

Incendium hoster video streamingservere, der stilles til rådighed for den Dataansvarlige til brug for live videostreaming. Transmission af video til serverne kan ske via mobilenheder, som forbinder til internettet og sender video.

Formålet er altså at muliggøre live streaming af video fra steder og på tidspunkter, som den Dataansvarliges medarbejdere vælger, og gøre videoen tilgængelig på en måde, som er under den Dataansvarliges fulde kontrol. Personoplysningerne som indeholdes på live streaming kan være både almindelige og følsomme. Livestreaming opbevares ikke. De personoplysninger, som opbevares i systemet, er ikke følsomme.

Behandlingen kan finde sted hos Incendium A/S's underdatabehandlere (bilag B) eller på Incendium A/S' adresser i Danmark.

Dataflow

Dataflowet er således, at en medarbejder hos den Dataansvarlige påbegynder streaming. Det gøres via et sms link, som medarbejdere udsender. Det sker ved at medarbejderen indtaster modtagerens telefonnummer. Live streaming finder først sted, når en medarbejder har truffet beslutning om, at det skal aktiveres og modtageren af linket accepterer at video streaming kan påbegyndes. Videoen transmitteres via internettet på en krypteret forbindelse til Incendiums server. I op til 1 time efter modtagelsen af sms'en kan modtageren sende video og i den periode vil modtagerens telefonnummer optræde i systemet og kan aflæses af medarbejderen. Det er også muligt for medarbejdere at slette linket/telefonnummeret før der er gået 1 time. Medarbejderen har mulighed for at give videosamtalen en label, som er en lille hjælpetekst. Vi gemmer både label og telefonnummer i op til 30 dage i systemets log, hvorefter informationerne anonymiseres.

IncidentShare er webbaseret og den Dataansvarlige tilgår data gennem en webbrowser.

Bilag B, Underdatabehandlere

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

Linode LLC, org no. 6719178, 249 Arch Street, Philadelphia, Pennsylvania 08090, USA

Behandlingsaktiviteten for Linode er, at fungere som hostingudbyder, der stiller virtuelle servere til rådighed for Incendium A/S og sørger for de den fysiske sikkerhed og drift af maskinerne.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt følgende lokaliteter for underdatabehandlere:

Linode LLC's datacenter: Equinix, Gutleutstrasse, Frankfurt a. M.

Den dataansvarlige har gjort sig bekendt med Linodes erklæringer om efterlevelse af forordningen <https://www.linode.com/eu-model/> og anser erklæringerne som fyldestgørende dokumentation for, at underdatabehandleren kontraktligt er bundet til at efterleve forordningen og bestemmelserne, som følger af denne aftale.

Onlinecity.io, cvr 27364276, Buchwaldsgade 50, 5000 Odense C.

Behandlingsaktiviteten for Onlinecity er, at fungere som gateway for afsendelse af sms'er.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt lokaliteter for underdatabehandlere, som fremgår af <https://gatewayapi.com/security-and-compliance/>

Den dataansvarlige har gjort sig bekendt med Onlinecity.io's erklæringer om efterlevelse af forordningen <https://gatewayapi.com/security-and-compliance/> og anser erklæringerne som fyldestgørende dokumentation for, at underdatabehandleren kontraktligt er bundet til at efterleve forordningen og bestemmelserne, som følger af denne aftale.

Bilag C, Instruks

Instruksen fra den Dataansvarlige til Incendium er at stille en eller flere virtuelle servere til rådighed, som indeholder software til håndtering af video og sørge for, at transmission af video til serveren kan foregå på en betryggende måde. Dette system kaldes "IncidentShare". Servere og transmission skal sikres med passende tekniske og organisatoriske foranstaltninger. Disse foranstaltninger er bl.a. firewall, backup, netværkssegmentering, logning og adgangskontrol.

Den fysiske sikring af servere varetages af underdatabehandlere.

Servere skal have så høj en opetid som mulig, men den Dataansvarlige beder Incendium om, altid at prioritere sikkerhed højest – også hvis det kræver at servere bliver utilgængelige i perioder. Den Dataansvarlige beder Incendium om, at opdateringer som udgangspunkt installeres den første tirsdag i hver måned, eller straks muligt, hvis der er tale om kritiske sikkerhedsopdateringer, og accepterer, at serveren kan være påvirket eller utilgængelig mens opdateringerne foregår. I den udstrækning, at der optræder informationssikkerhedsmæssige hændelser beder den Dataansvarlige om, at Databehandleren kontakter Den Databeskyttelsesansvarlige pr. email.

Bistand til den dataansvarlige

I forbindelse med efterlevelse af Databehandleraftalens §9, er proceduren, at Incendium A/S's Informationssikkerhedsudvalg udpeger en ansvarlig i firmaet, som står i direkte kontakt med den Dataansvarlige. Vi udbeder os en skriftlig anmodning fra den Dataansvarlige. Når denne anmodning er modtaget (per email), kan vi påbegynde arbejdet. Vi kontakter aldrig de registrerede direkte. Såfremt den Dataansvarlige bestiller begrænsning eller sletning af materiale udbeder vi os endnu en skriftlig anmodning. Når den er modtaget kan begrænsningen eller sletningen foretages. Materialet kan bestå logningsoplysninger, der kan indeholde oplysninger om telefonnumre og tidspunkter. Den Dataansvarlige er indforstået med, at den bistand, som Databehandleren giver i medfør af Databehandleraftalens §9 og §12 eller andre aktiviteter, der følger af bestemmelser reguleres af de almindelige betingelser for samarbejde. Det vil bl.a. sige at medgået tid faktureres særskilt.

Brud på Persondatasikkerhed

Ved brud eller mistanke om brud på Persondatasikkerheden (i strid med databeskyttelsesforordningen eller andre databeskyttelsesbestemmelser) orienteres den Dataansvarlige uden unødigt forsinkelse pr. email. Hvis det vurderes, at der foreligger en umiddelbar trussel for, at Persondatasikkerheden fortsat kan brydes på systemet, lukkes netværkssadgangen straks.

Senest 72 timer efter bruddet eller mistanken er opstået fremsendes en rapport til den Dataansvarlige med følgende indhold:

1. Bruddets karakter
2. Omfang
3. Konsekvenser
 - 3.a Kendte
 - 3.b Mulige
4. Foranstaltninger
 - 4.a. Trufne
 - 4.b. Forslag

Registrering og sletning

Vi registrerer telefonnumre på modtagerne af sms til video linket. Der opbevares ingen video, men vi har oplysninger om hvilke telefonnumre, der er blevet kontaktet og tidspunkter. Disse oplysninger anonymiseres efter 30 dage.