

DATABEHANDLERAFTALE

Mellem

Vejle Kommune
Konkurrenceudsættelse
Skolegade 1
7100 Vejle
CVR. nr.: 29189900
(herefter "Kommunen")

og

[Leverandørens navn]
[adresse]
[postnr. og by]
CVR. nr.: [XXXX]
(herefter "Leverandøren")

er der indgået nedenstående databehandleraftale (herefter "Aftalen") om Leverandørens
behandling af personoplysninger på vegne af Kommunen:

1. Generelt

- 1.1** Aftalen vedrører Leverandørens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen).
- 1.2** I Aftalen er indarbejdet de krav, som Databeskyttelsesforordningen stiller til databehandleraftaler.
- 1.3** Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.
- 1.4** Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder i ”hovedaftalen”.
- 1.5** Denne databehandleraftale frigør ikke leverandøren for forpligtelser, som efter Databeskyttelsesforordningen, Databeskyttelsesloven eller enhver anden lovgivning direkte er pålagt Leverandøren.
- 1.6** Til denne aftale hører 3 bilag. Bilagene fungerer som en integreret del af databehandleraftalen.

2. Formål

- 2.1** Leverandøren behandler i medfør af aftale med Kommunen om Automatisk indbrudsalarmanlæg (AIA) og adgangskontrolalarmanlæg (ADK) (herefter ”Hovedaftalen”) personoplysninger for Kommunen, hvor Leverandørens behandlinger og formålet med behandlingerne er beskrevet.

3. Kommunens rettigheder og forpligtelser

- 3.1** Kommunen er dataansvarlig for de personoplysninger, som Kommunen instruerer Leverandøren om at behandle. Kommunen har ansvaret for, at de personoplysninger, som Kommunen instruerer Leverandøren om at behandle, må behandles af Leverandøren, herunder at behandlingen er nødvendig og saglig i forhold til Leverandørens opgavevaretagelse.
- 3.2** Kommunen har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Aftalens pkt. 1.1 samt Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesloven).

4. Leverandørens forpligtelser

- 4.1** Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Kommunen, jf. pkt. 6 og bilag 3. Leverandøren har som databehandler de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Aftalens pkt. 1.1.
- 4.2** Leverandøren behandler alene de overladte personoplysninger efter dokumenteret instruks fra Kommunen, jf. pkt. 6 og bilag 3, og alene med henblik på opfyldelse af Hovedaftalen.
- 4.3** Leverandøren skal løbende føre fortegnelser over behandlingen af personoplysninger samt fortegnelser over alle brud på persondatasikkerheden, jf. bilag 1.
- 4.4** Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, svarende til de kategorier af personoplysninger, der behandles, samt de risici behandlingen indebærer for de registrerede, jf. bilag 1 – Sikkerhed.
- 4.5** Leverandøren skal på opfordring fra Kommunen hjælpe med at opfylde Kommunens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, udlevering af borgerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af borgerens oplysninger, samt Kommunens forpligtelser i forhold til underretning af den registrerede ved brud på persondatasikkerheden, i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.
- 4.6** Leverandøren skal hjælpe Kommunen med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36, jf. Databeskyttelsesforordningens artikel 28, stk. 3, litra f.
- 4.7** Leverandøren garanterer at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Kommunens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
- 4.8** Leverandøren er forpligtet til at oplyse med præcise adresseangivelser, hvor Kommunens personoplysninger opbevares, jf. bilag 2. Leverandøren skal ajourføre oplysningerne over for Kommunen ved enhver ændring.

5. Underleverandør (underdatabehandler)

- 5.1** Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Kommunen.
- 5.2** Leverandøren har ret til at anvende andre underdatabehandlere end dem, som er angivet i bilag 2, herunder at foretage udskiftning af disse, til at behandle de personoplysninger, som Kommunen har overladt til Leverandøren i medfør af Hovedaftalen. Leverandøren skal ajourføre oplysninger om underdatabehandlere i bilag 2 ved enhver ændring, og underrette Kommunen om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give Kommunen mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være Kommunen i hænde minimum 60 dage før anvendelsen eller ændringen skal træde i kraft. Såfremt Kommunen har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til Leverandøren inden 30 dage efter modtagelsen af underretningen.
- 5.3** Kommunen kan nægte at godkende skift eller tilføjelse af underdatabehandlere.
- 5.4** Hvis Leverandøren overlader behandlingen af personoplysninger, som Kommunen er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.
- 5.5** Leverandøren skal i aftalen med underdatabehandlere indføre Kommunen som begunstiget tredjemand i tilfælde af databehandlerens konkurs.
- 5.6** Underdatabehandleraftalen, jf. pkt. 5.4, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Aftalen, herunder, at underdatabehandleren garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
- 5.7** Når Leverandøren overlader behandlingen af personoplysninger, som Kommunen er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Kommunen ansvaret for underdatabehandlerens overholdelse af disses forpligtelser, jf. pkt. 5.4 .
- 5.8** Kommunen kan til enhver tid forlange dokumentation fra Leverandøren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Leverandøren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Kommunen.
- 5.9** Al kommunikation mellem Kommunen og underdatabehandleren sker via Leverandøren.

6. Instrukser

- 6.1** Leverandørens behandling af personoplysninger på vegne af Kommunen sker udelukkende efter dokumenteret instruks, jf. bilag 3, med mindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Leverandøren er underlagt. I så fald underretter Leverandøren Kommunen om dette retlige krav inden behandling, med mindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser. Det er Leverandørens ansvar at sikre, at eventuelle underdatabehandlere, jf. pkt. 5.4, får tilsendt Kommunens instruks, jf. bilag 3.
- 6.2** Leverandøren giver omgående besked til Kommunen, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 1.1 eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

- 7.1** Leverandøren skal, jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau svarende til de kategorier af personoplysninger, der behandles, samt de risici behandlingen indebærer for de registrerede.
- 7.2** Leverandøren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.
- 7.3** Leverandøren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Kommunens personoplysninger, om Leverandørens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt. 9.
- 7.4** Leverandøren er forpligtet til straks at underrette Kommunens Databeskyttelsesrådgiver om ethvert brud på persondatasikkerheden uanset, om dette sker hos Leverandøren eller hos en underdatabehandler jf. bilag 1.
- 7.5** Leverandøren må ikke hverken offentligt eller til tredjeparter kommunikere om brud på persondatasikkerheden, jf. pkt. 7.4, uden forudgående skriftlig aftale med Kommunen, med mindre Leverandøren har en retlig forpligtelse til sådan kommunikation.

8. Overførsler til andre lande

- 8.1** Leverandørens overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande), skal ske i overensstemmelse med Kommunens instruks herfor, jf. bilag 3, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Leverandøren er underlagt. I så fald underretter Leverandøren Kommunen om dette retlige krav inden behandling, med mindre den pågældende ret forbyder en sådan underretning.

- 8.2** Leverandøren er forpligtet til at holde sig ajour med Europa-Kommissionens fortegnelse over godkendte 3. lande, samt uden unødigt ophold at give Kommunen meddelelse om ændringer heri samt foretage foranstaltninger for lovliggørelse når ændringer i fortegnelsen har betydning for Leverandørens lovlige behandling af Kommunens oplysninger.
- 8.3** Leverandøren skal dog underrette Kommunen om eventuelle planlagte ændringer vedrørende behandlinger af persondata i 3. lande og derved give Kommunen mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være Kommunen i hænde minimum 60 dage før anvendelsen eller ændringen skal træde i kraft. Såfremt Kommunen har indsigelser mod ændringerne, skal Kommunen give meddelelse herom til leverandøren inden 30 dage efter modtagelsen af underretningen. Ved sådanne ændringer skal Leverandøren ajourføre oplysninger herom i bilag 3.
- 8.4** Kommunen kan nægte at godkende ændringer vedrørende behandlinger af persondata i 3. lande.
- 8.5** Hvis Kommunens personoplysninger overføres til en EU-medlemsstat, er det Leverandørens ansvar, at de til enhver tid gældende bestemmelser om sikkerhedsforanstaltninger, som er fastsat i den pågældende medlemsstat, overholdes.

9. Tavshedspligt og fortrolighed

- 9.1** Leverandøren er – under og efter Hovedaftalens ophør – pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse.
- 9.2** Leverandøren skal sikre, at alle, der behandler oplysninger omfattet af Aftalen, herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

10. Kontroller og erklæringer

- 10.1** Leverandøren er forpligtet til vederlagsfrit og uden ugrundet ophold at give Kommunen nødvendige oplysninger til, at Kommunen kan sikre sig, at Leverandøren overholder de krav, der følger af denne Aftale.
- 10.2** Kommunen, en repræsentant for Kommunen eller dennes revision (såvel intern som ekstern) har adgang til at føre tilsyn hos Leverandøren med henblik på at konstatere, at Leverandøren overholder de krav, der følger af denne Aftale. Omfang og proces for tilsyn, herunder Leverandørens pris herfor, aftales i Hovedaftalen, sekundært i separat

aftale mellem parterne, såfremt omfang og proces ikke er omfattet af Hovedaftalen. Kommunens omkostninger i forbindelse med dette tilsyn afholder Kommunen selv.

- 10.3** Med mindre der er fastsat et hyppigere interval herfor i Hovedaftalen, skal Leverandøren én gang årligt vederlagsfrit fremsende en erklæring om overholdelse af Aftalen. Erklæringen skal udarbejdes i overensstemmelse med gældende, anerkendte branchestandarder på området og skal omfatte både Leverandørens og eventuelle underdatabehandlers databehandling. Den første erklæring skal foreligge senest 12 måneder efter Hovedaftalens eller Databehandleraftalens indgåelse.
- 10.4** I tilfælde af, at Datatilsynet og/eller andre relevante offentlige myndigheder ønsker at foretage en uanmeldt fysisk inspektion af de ovennævnte foranstaltninger, forpligter Leverandøren og Leverandørens underleverandører sig til uden yderligere omkostninger at stille tid og ressourcer til rådighed herfor.

11. Ændringer i Aftalen

- 11.1** Kommunen kan til enhver tid, med et forudgående varsel på 60 dage, foretage ændringer i Aftalen og instruksen, jf. bilag 3. Ændringsprocessen og omkostningerne herved aftales skriftligt mellem Kommunen og Leverandøren i Hovedaftalen, sekundært i separat skriftlig aftale mellem parterne, såfremt vilkår for ændringsprocesser og omkostninger forbundet hermed ikke er reguleret i Hovedaftalen. Leverandøren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlerne tillige forpligtes af ændringerne.
- 11.2** I det omfang ændringer i lovgivningen, jf. pkt. 3.2 eller tilhørende praksis, giver anledning til dette, er Kommunen berettiget til at foretage ændringer i Aftalen uden varsel, og uden at dette medfører krav om betaling fra Leverandøren.

12. Sletning af data

- 12.1** Kommunen træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Hovedaftalen.
- 12.2** Kommunen skal inden Hovedaftalens ophør skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til Kommunen. I begge tilfælde skal Leverandøren ligeledes slette eventuelle kopier, med mindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne. Leverandøren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Kommunens meddelelse.
- 12.3** Tilbagelevering af data skal ske i et åbent, offentligt anerkendt læsbart format.

- 12.4** Leverandøren skal fremsende dokumentation for, at den påkrævede sletning, jf. pkt. 12.2, er foretaget.

13. Misligholdelse og tvistigheder

- 13.1** Misligholdelse og tvistigheder er reguleret i Hovedaftalen.

14. Erstatning og forsikring

- 14.1** Erstatnings- og forsikringsspørgsmål er reguleret i Hovedaftalen jf. pkt. 2.1.
- 14.2** Såfremt erstatningsspørgsmålet ikke er reguleret i Hovedaftalen er Leverandøren erstatningsansvarlig efter Produktansvarsloven samt dansk rets almindelige regler om erstatning.
- 14.3** Såfremt forsikringsspørgsmålet ikke er reguleret i Hovedaftalen er Leverandøren i hele rammeaftalens løbetid forpligtet til at opretholde en erhvervs- og produktansvarsforsikring med en dækningssum på minimum 10 mio. kr. pr. år. Leverandøren skal på ordregiverens anmodning godtgøre forsikringens eksistens og omfang.

15. Ikrafttræden og varighed

- 15.1** Aftalen indgås ved begge parterers underskrift og løber indtil ophør af Hovedaftalen.
- 15.2** Aftalen er dog gældende, så længe behandlingen består. Uanset ”hovedaftalens” og/eller databehandleraftalens opsigelse, vil databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos Leverandøren og eventuelle underdatabehandlere.

16. Formkrav

16.1 Aftalen skal foreligge skriftligt, herunder elektronisk, hos Kommunen og Leverandøren.

For Kommunen

For Leverandøren

Navn og titel:

Navn og titel:

Dato:

Dato:

Underskrift:

Underskrift:

Bilag:

Bilag 1 – Sikkerhed

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører
(underdatabehandlere)

Bilag 3 – Instruks

Bilag 1 – Sikkerhed

1. Indledning

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Leverandøren i medfør af Aftalen har ansvar for at gennemføre, overholde og sikre overholdelse af hos dennes underdatabehandlere, som er angivet i bilag 2.

2. Sikkerhedskrav

Leverandøren er berettiget og forpligtet til at træffe nærmere beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige (og forudsatte) sikkerhedsniveau omkring personoplysningerne. Leverandøren behandler personoplysningerne i overensstemmelse med nærværende Databehandleraftale og de bestemmelser i henholdsvis Databeskyttelsesforordningen og Databeskyttelsesloven, der er gældende for databehandlere.

Foranstaltningerne fastlægges ud fra overvejelser om:

1. Det aktuelle tekniske niveau
2. Implementeringsomkostningerne
3. Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. Instruksen (bilag 3)
4. Konsekvenserne for de registrerede ved brud på persondatasikkerheden
5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:
 - a) tilintetgørelse af oplysningerne
 - b) tab af oplysningerne
 - c) ændring af oplysningerne
 - d) uautoriseret videregivelse af oplysningerne
 - e) uautoriseret adgang til oplysningerne

Leverandøren gennemfører i alle tilfælde og som minimum følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger jf. Instruks (bilag 3) og som dermed opfylder Databeskyttelsesforordningens artikel 32.

Generelle sikkerhedsforanstaltninger

Leverandøren skal opretholde et formelt, velimplementeret og professionelt ledelsessystem for informationssikkerhed baseret på lovgivningens krav og god databehandlingsskik. Leverandøren skal fastsætte og implementere interne politikker og bestemmelser, der er fyldestgørende og afspejler de faktiske forhold. Derudover skal Leverandøren opretholde

procedurer for regelmæssig afprøvning, vurdering og evaluering af de tekniske og organisatoriske foranstaltninger, som Leverandøren har implementeret til sikring af personoplysningerne.

Håndtering af personoplysninger

Dokumenter og data (herunder mobile lagringsmedier), der indeholder personoplysninger, behandles så fortrolighed, integritet, tilgængelighed og robusthed bevares for at sikre, at de ikke mistes eller kommer i forkerte hænder samt for at hindre de skadevirkninger, sådanne brud måtte have for registrerede personer.

Instruktion af medarbejdere m.v.

Leverandøren sikrer at ansatte og eventuelle samarbejdsparter til stadighed er bekendt med og har tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker, arbejdsgange og om deres tavshedspligt.

Adgangsstyring og administration af brugeradgang

Kun medarbejdere, som har et arbejdsbetinget behov for at behandle personoplysninger i forhold til Aftalen, må være oprettet som brugere med adgang til Kommunens persondata. Kun de personer, der af den bemyndigede er autoriseret hertil, må have adgang til personoplysningerne. Leverandøren skal uden ugrundet ophold annullere autorisationer (og herunder adgange) for brugere, der ikke længere har et arbejdsbetinget behov for autorisation.

Der føres en liste over autoriserede medarbejdere med angivelse af, hvilken type adgang autorisationen dækker. Listen over autoriserede medarbejdere opdateres løbende iht. god databehandlingsskik. Efterspørger Kommunen listen, skal listen gøres tilgængelig uden unødigt ophold.

Ved ydelsens afslutning lukkes medarbejdernes adgang.

Derudover anvender leverandøren sikre identifikation og autorisationsteknologier, eksempelvis adgangskoder, biometri eller lignende. De anvendte autentifikationsmekanismer lever op til seneste vejledning fra Digitaliseringsstyrelsen, og god skik på området.

Kontrol med afviste adgangsforsøg

Med udgangspunkt i en risikobaseret tilgang foretager Leverandøren registrering af afviste adgangsforsøg og blokerer for yderligere forsøg efter fastlagte antal på hinanden følgende afviste adgangsforsøg.

Leverandøren skal endvidere opretholde procedurer, som sikrer rettidig opfølgning på alle afviste adgangsforsøg, hvor opfølgning er nødvendig for at forhindre brud på persondatasikkerheden og skadevirkninger for registrerede personer.

Fysisk sikring

Leverandøren skal opretholde fysiske sikringsforanstaltninger til sikring af lokaliteter, som anvendes til behandling af personoplysninger omfattet af Databehandleraftalen mod uvedkommendes adgang og manipulation.

Ændringshåndtering

Leverandøren har 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 og/eller ledelsesopfølgning for at sikre, at ingen enkeltpersoner kan kontrollere en ændring alene.

Opbevaringsperiode/sletterutiner

Personoplysningerne opbevares så længe, der er et sagligt grundlag herfor.

Driftsafbrydelser

Leverandøren skal have dokumenterede beredskabsprocedurer, der sikrer genetablering af services uden ugrundet ophold i tilfælde af driftsafbrydelser i henhold til hovedaftalen.

Eksterne kommunikationsforbindelser

Leverandøren har passende tekniske foranstaltninger til at beskytte systemer og netværk samt til at begrænse risikoen for uautoriseret adgang og/eller installering af skadelig kode.

I det omfang det er et krav i medfør af gældende lovgivning, god databehandlingsskik eller i øvrigt er omfattet af Aftalen anvender Leverandøren krypteringsteknologier og andre tilsvarende foranstaltninger.

Logning

Hvis der i systemet behandles følgende kategorier af personoplysninger:

- følsomme personoplysninger
- personoplysninger om straffedomme og lovovertrædelser
- oplysninger om cpr-nummer

skal der foretages logning af alle relevante hændelser i forbindelse med brugernes behandling af personoplysninger. Formålet med logningen er, at Leverandøren skal kunne hjælpe Kommunen med dokumentation og rapportering af hændelser samt brud på persondatasikkerheden. Loggen skal, når den efterspørges af Kommunen, gøres tilgængelig for Kommunen i maskinlæsbar format efter aftale.

Logningen skal have fokus på brugernes handlinger, herunder mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den/de personer, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.

Leverandøren foretager løbende afprøvning, vurdering og evaluering af effektiviteten af logningsaktiviteten, og underretter Kommunen om eventuelle u hensigtsmæssigheder.

Hændelsesloggen opbevares og slettes løbende efter 180 dage med mindre loggen udviser forhold, hvor leverandøren har underretningspligt over for Kommunen.

Under håndteringen af konkrete brud på persondatasikkerheden bevares loggen indtil bruddet er færdigbehandlet, idet Kommunen afgør, hvornår dette tidspunkt indtræder.

Sikkerhedskopiering

Der bliver dagligt foretaget sikkerhedskopiering af konfigurationsfiler og data. Sikkerhedskopierne opbevares betryggende i minimum 30 dage, og således at de ikke hændeligt eller ulovligt tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

Periodisk sker der test af, at data kan genskabes fra sikkerhedskopier.

Ad hoc og hjemmearbejdspladser

Såfremt Leverandøren foretager databehandling fra ad hoc og/eller hjemmearbejdspladser, skal Leverandøren sikre, at disse lever op til de sikkerhedsmæssige krav i denne Databehandlersaftale med bilag, lovgivning i øvrigt samt Datatilsynets vejledninger herom.

Leverandøren skal blandt andet opfylde og dokumentere følgende:

- Beskrivelse af anvendt krypteret forbindelse mellem ad hoc arbejdspladsen og Leverandørens/Kommunens netværk
- Leverandørens interne instruks til egne medarbejdere vedrørende ad hoc og hjemmearbejdspladser

Derudover skal Leverandøren, hvis det er teknisk muligt anvende 2-faktor-autentifikation.

Bortskaffelse af udstyr

Leverandøren skal have formelle processer med henblik på at sikre, at der sker en effektiv sletning af personoplysninger inden bortskaffelse af elektronisk udstyr.

Meddelelse og redegørelse i forbindelse med brud på datasikkerheden

I tilfælde af brud på persondatasikkerheden skal Leverandøren uden unødigt forsinkelse, umiddelbart efter at denne er blevet bekendt med bruddet, give Kommunen meddelelse herom med angivelse af:

- Karakteren af bruddet på persondatasikkerheden
- Kategorierne og det omtrentlige antal berørte registrerede, hvis det er muligt
- Kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
- Navn og kontaktoplysninger til kontaktpunkt, hvor yderligere oplysninger kan indhentes
- Beskrivelse af de sandsynlige konsekvenser af bruddet
- Beskrivelse af foranstaltninger der er truffet, eller foreslås truffet som led i håndteringen af bruddet og dets mulige skadevirkninger

Hvis det ikke er muligt at levere oplysningerne ovenfor samlet, skal de i stedet leveres trinvist.

Leverandøren skal føre en fortegnelse over brud på persondatasikkerheden. Loggen skal som minimum indeholde informationer om:

- De faktiske omstændigheder ved bruddet
- Bruddets virkninger
- De afhjælpende foranstaltninger, der er truffet

Leverandøren er forpligtet til at bidrage aktivt til, at Kommunen modtager tilstrækkelige informationer til, at Kommunen kan håndtere en eventuel informationsforpligtelse til de registrerede og Datatilsynet.

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

1. Lokation(er) for behandlingen

[Leverandøren udfylder de steder, hvor Kommunens personoplysninger opbevares/behandles.]

2. Underdatabehandlere

Kommunen har ved databehandleraftalens ikrafttræden godkendt anvendelsen af følgende underdatabehandlere:

Navn	CVR-nr.	Adresse	Beskrivelse af behandling
[Navn]	[CVR-nr.]	[Adresse]	[Overordnet beskrivelse af behandlingen hos underdatabehandleren]
[Navn]	[CVR-nr.]	[Adresse]	[Overordnet beskrivelse af behandlingen hos underdatabehandleren]
[Navn]	[CVR-nr.]	[Adresse]	[Overordnet beskrivelse af behandlingen hos underdatabehandleren]
[Navn]	[CVR-nr.]	[Adresse]	[Overordnet beskrivelse af behandlingen hos underdatabehandleren]

Bilag 3 – Instruks

Instruks

Kommunen instruerer hermed Leverandøren om at foretage behandling af Kommunens oplysninger til brug for levering af ydelser, jf. Hovedaftale.

Overlader Leverandøren behandling af Kommunens oplysninger til underdatabehandlere, er Leverandøren ansvarlig for at indgå skriftlige (under)databehandleraftaler med disse, jf. Aftalens pkt. 5.4. Leverandøren er ansvarlig for, at Kommunens instruks fremsendes til eventuelle underdatabehandlere.

1.1 Behandlingens formål

Behandling af Kommunens oplysninger sker i henhold til formålet i Hovedaftalen.

Leverandøren må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end Kommunen.

1.2 Generel beskrivelse af behandlingen

Leverandøren foretager alene behandling inden for rammerne af formålet, som er beskrevet ovenfor.

1.3 Kategorier af oplysninger

Behandlingerne indeholder personoplysninger i de nedenfor afkrydsede kategorier. Leverandørens og eventuelle underdatabehandlers niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed, jf. bilag 1.:

Almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 6):

☒ Almindelige personoplysninger

Følsomme personoplysninger:

- ☐ Race eller etnisk oprindelse
- ☐ Politisk overbevisning
- ☐ Religiøs overbevisning
- ☐ Filosofisk overbevisning
- ☐ Fagforeningsmæssigt tilhørsforhold
- ☐ Genetiske data
- ☐ Biometriske data
- ☐ Helbredsoplysninger, herunder misbrug af medicin, narkotika, alkohol m.v.
- ☐ En fysisk persons seksuelle forhold eller seksuelle orientering

Personoplysninger om straffedomme og lovovertrædelser (jf. Databeskyttelsesforordningens artikel 10):

- ☐ Straffedomme
- ☐ Lovovertrædelser

Oplysninger om Cpr-nummer (jf. Databeskyttelseslovens §11):

- ☒ CPR-nummer

1.4 Kategorier af registrerede

Der behandles oplysninger om følgende kategorier af registrerede:

- A. ☐ Borgere, voksne
- B. ☐ Borgere, børn fra og med 13 år og til og med 17 år
- C. ☐ Borgere, børn til og med 12 år
- D. ☐ Pårørende
- E. ☒ Bipersoner
- F. ☒ Ansatte
- G. ☐ Tidligere ansatte
- H. ☐ Jobansøgere
- I. ☒ Politikere
- J. ☐ Afdøde personer (indenfor 10 år efter dødsfald)

1.5 Tredjelande (ikke EU-medlemslande)

Leverandøren må overføre personoplysninger til tredjelande, som Europa-Kommissionen har godkendt som sikre 3. lande, samt til underleverandører, der har tilsluttet sig certificeringer om overførselsgrundlag, som er godkendt af Europa-Kommissionen.

Der overføres data til følgende tredjelande:

Der overføres data til følgende underleverandører:

Overførselsgrundlaget er:

- ☐ Retligt bindende instrumenter mellem myndigheder
- ☐ Bindende virksomhedsregler
- ☐ Adfærdskodeks og certificeringsmekanismer
- ☐ Standardbestemmelser om databeskyttelse
- ☐ Ad-hoc kontrakter
- ☐ Samtykke