[indsæt projektnavn/løsningens navn]

Bilag C – instruks vedrørende behandling af personoplysninger

***INTERN VERSIONSHISTORIK (SKAL SLETTES INDEN UDSENDELSE TIL KOMMUNERNE)***

|  |  |  |  |
| --- | --- | --- | --- |
| ***Versionsnr.*** | ***Dato for ændring*** | ***Ansvarlig (initialer)*** | ***Beskrivelse af ændring*** |
| *4.0* | *06.07.2020* | *JBU/ATP* | *Opdateret til ny datatilsyns databehandlerskabelon* |
| *4.1* | *25.03.2021* | *KLB* | *Generelt review med rettelser* |
| *5.0* | *26.04.2021* | *KLB* | *Uploadet i metodematrix* |
| *5.1* | *16.06.2021* | *KLB* | *C.2: Præcisering vedr. formulering om sikkerhedsniveau.*  *C.4: Tilføjet ”i systemet”.*  *C.8.2: Rettet stavefejl. Slettet formuleringen ”I tilfælde af, at Datatilsynet ønsker at foretage en fysisk inspektion af foranstaltninger i henhold til disse Bestemmelser, forpligter KOMBIT og KOMBITs underdatabehandlere sig til uden yderligere omkostninger for den dataansvarlige at stille tid og ressourcer til rådighed herfor.”* |
| *6.0* | *16.08.2021* | *KLB* | *Uploadet i metodematrix* |
| *7.0* | *Februar 2025* | *SIA* | *Opdateret databehandleraftaleskabelon i samarbejde med Databehandlersekretariatet og uploadet i metodematrix* |

# C.1 Behandlingens genstand/instruks

Databehandlerens og underdatabehandlernes behandling af personoplysninger på vegne af den dataansvarlige sker ved, at disse udfører følgende:

Databehandlerens rolle er primært at varetage leverandørstyring i henhold til kontrakten med underdatabehandleren [navn på underdatabehandleren], mens [navn på underdatabehandleren] varetager rollen som leverandør af systemet.

I forbindelse med varetagelsen af disse opgaver for den dataansvarlige er underdatabehandleren instrueret i at behandle personoplysninger i forbindelse med udvikling, test, drift, vedligehold og videreudvikling af systemet. Formålet og karakteren af behandlingen af personoplysninger på vegne af den dataansvarlige er nærmere beskrevet i bilag A.

Oplysningerne må ikke behandles efter instruks fra andre end den dataansvarlige.

Som udgangspunkt behandler databehandleren ikke personoplysninger på vegne af den dataansvarlige, men overlader behandlingen af personoplysninger til underdatabehandleren.

For at kunne varetage forpligtelserne i tilslutningsaftalen, kan der dog i visse tilfælde blive tale om, at databehandleren behandler personoplysninger ud fra et arbejdsbetinget behov.

Der er tale om behandling af personoplysninger i forbindelse med databehandlerens ansattes mulighed for at benytte funktioner i systemet i overensstemmelse med givne rettigheder, fx ret til at se/læse, tilføje, søge, ændre/skrive, udtrække eller slette personoplysninger i overensstemmelse med formålet.

Databehandlerens ansatte har i den forbindelse underskrevet en fortrolighedserklæring, og proces for tildeling, ændring, fjernelse og kontrol af adgange for ansatte følges.

## C.1.1 FKI som datadistributør

FKI (Fælles Kommunal Infrastruktur) hører under databehandlerens domæne, der på vegne af kommunerne indkøber data og funktionalitet fra datakilder som fx SKAT, CPR- og CVR-registret, og efterfølgende udstiller disse services i Serviceplatformen. Dette sikrer at kommuner, ATP/UDK og it-leverandører kan benytte disse services til deres kommunale fagløsninger.

De specifikke instrukser under denne databehandleraftale er de af kommunen og ATP/UDK allerede godkendte serviceaftaler. For Kommunen omfatter denne databehandleraftale også de serviceaftaler, som kommunen løbende godkender i databehandleraftalens løbetid.

Serviceaftaler godkendes af kommunen og ATP/UDK i Systemets Administrationsmodul.

Serviceaftalerne er for Kommunen ikke blot lig en juridisk specifik instruks under denne databehandleraftale, men tjener også som en teknisk sikkerhedsforanstaltning, som teknisk sikrer, at der ikke udveksles personoplysninger uden en behørig godkendelse af den dataansvarlige, herunder en nødvendig specifik instruks fra den dataansvarlige.

Databehandleren godkender alene serviceaftaler på kommunernes vegne, som medfører behandling, som databehandleren og databehandlerens underdatabehandlere i forvejen har bemyndigelse til, jævnfør denne instruks eller tidligere specifikke instrukser i allerede indgåede serviceaftaler.

## C.1.2 Datastrømme

I forbindelse med behandlingen modtages og afsendes data fra og til følgende datastrømme:

| **Organisation/enhed** | **System** | **Data ind/ud** |
| --- | --- | --- |
| Social -og Indenrigsministeriet(CPR) | Det centrale personregister (CPR) | Ind |
| Udviklings- og forenklingsstyrelsen (UFST) | eIndkomst/indkomstregisteret, R75 og årsopgørelsen,MUL, GUL og evt. andre dataudvekslingplatforme som UFST anvender til at udveksle skattemæssige oplysninger | Ind |
| STAR | Feriekonto | Ind |
| Udenrigsministeriet | Udlændinge Information System | Ind |
| STAR | Det Fælles Data Grundlag | Ind/Ud |
| Udbetaling Danmark/ATP | Kontanthjælpssystem | Ind/Ud |
| Digitaliseringsstyrelsen | Digital Post | Ud |
| Kommunen selv | LIS-systemer som kommunen anvender (fx FLIS) | Ud |
| Danmarks Statistik | Dataload | Ud |
| Andre kommuner ( udveksling af personoplysninger mellem dataansvarlige kommuner) eller datastrøm som alene foregår internt i den samme kommune | SAPA, jobcenterløsninger og ESDH-system og udveksling internt i KY mellem dataansvarlige kommuner, fx når borgere flytter. | Ud/Ind |
| Digitaliseringsstyrelsen | Digital Post | Ud |
| Digitaliseringsstyrelsen | Digital Post | Ind |
| Kommunen selv | Kommunens økonomisystemer ( debitor- og kreditorsystemer) | Ud/Ind |
| Kommunen selv | Kommunens fjernprintleverandør | Ud |
| Erhvervsministeriet | Det Centrale Virksomhedsregister | Ind |
| Digitaliseringsstyrelsen | Nem-login og digital fuldmagt | Ud/Ind |

## C.1.3 Udfasning af nuværende it-system

I forbindelse med udfasning af [navn på eksisterende system(er)] sker der desuden en behandling af personoplysninger fra de eksisterende systemer ([navn på eksisterende system(er)]). Behandling af personoplysninger fra disse systemer er nødvendig i forbindelse med [aktiviteter, der kræver behandling] i [navn på nyt projekt] og konvertering af data i forbindelse med flytningen af personoplysninger til [navn på nyt projekt].

Data flyttes fra eksisterende systemer til det nye system via en *sikret FTP-forbindelse, som er krypteret. Desuden kræver adgangen både autentificering og autorisering før denne kan tilgås. Den endelige tilgang af data vil udelukkende være til autoriserede personer, som kun vil tilgå denne når det er relevant for udførslen af projektarbejdet.*

# C.2 Behandlingssikkerhed

**Oplysninger om behandlingen:**

Behandlingen omfatter følgende antal registrerede:

Under 1000 (1 point)

1000 - 10.000 (2 point)

Over 10.000 (3 point)

Behandlingen omfatter behandling af følgende type personoplysninger:

Almindelige personoplysninger, art. 6 (0 point)

Følsomme personoplysninger, art. 9 (3 point)

Andre beskyttelsesværdige / fortrolige personoplysninger, (F.eks. oplysninger om private forhold omfattet af straffelovens § 152, jf. forvaltningslovens § 27, personnumre, jf. databeskyttelseslovens § 11, samt oplysninger om strafbare forhold, jf. databeskyttelseslovens § 10) (2 point)

Behandlingsaktiviteter der betydeligt påvirker den registrerede (F.eks. Overvågning, kortlægning af adfærd, profilering, automatiske behandlinger) (2 point)

**Sikkerhedsniveau:**

På baggrund af de ovenfor angivne oplysninger om behandlingen, og under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål, samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder etableres følgende sikkerhedsniveau: [Markér det relevante sikkerhedsniveau]

[Skemaet her nedenfor kan anvendes i forbindelse med angivelse af sikkerhedsniveauet]:

|  |  |  |  |
| --- | --- | --- | --- |
| **Meget lav (1-2 point)** | **Lav (3-4 point)** | **Middel (5-6 point)** | **Høj (7-10 point)** |
|  |  |  |  |

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 understøtte den Dataansvarlige i dennes arbejde med at dokumentere de identificerede risici og hvordan risikoen er nedbragt til et acceptabelt niveau og gennemføre de foranstaltninger, der er nødvendige for at imødegå identificerede risici.

På baggrund af det etablerede sikkerhedsniveau implementeres procedurer for revisioner i overensstemmelse med punkt C.7 og C.8.

Afsnit C.2.1 beskriver hvilke sikkerhedsforanstaltninger, der er implementeret for at etablere det nødvendige og aftalte sikkerhedsniveau i forbindelse med udvikling, test, drift, vedligehold og videreudvikling af systemet.

Databehandleren og/eller dennes underdatabehandler skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger som er aftalt med den dataansvarlige:

**C.2.1 Sikkerhedsforanstaltninger etableret**

**C.2.1.1 Krav til pseudonymisering og kryptering af personoplysninger**

Krav til pseudonymisering af personoplysninger

Der foretages pseudonymisering af persondata, hvor den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers grundlæggende rettigheder og frihedsrettigheder tilsiger det.

Krav til kryptering af personoplysninger

Der foretages kryptering af persondata, hvor den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers grundlæggende rettigheder og frihedsrettigheder tilsiger det. Der anvendes altid kryptering af personoplysninger ved enhver transmission af fortrolige og følsomme personoplysninger via eksterne kommunikationsforbindelser.

**C.2.1.2 Krav vedrørende evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester**

* 1. Der foretages mindst én gang årligt en risikovurdering for hver af de behandlingssystemer og tjenester, hvori den Dataansvarliges personoplysninger behandles. Databehandler foretager loyalt og professionelt mitigerende foranstaltninger baseret på risikovurderingens resultater.
  2. Der foretages løbende mitigerende foranstaltninger af teknisk og organisatorisk karakter, når dette viser sig påkrævet.

Det sikres endvidere, at:

* 1. Adgang til de personoplysninger, som aftalen vedrører, er begrænset til personer, der har et sagligt formål.
  2. Der er tekniske og/eller organisatoriske foranstaltninger, som sikrer, at alene disse autoriserede personer, har adgang. Autorisationen omfatter også personer, som udfører konsulentopgaver eller nødvendige revisions- drifts- og systemtekniske opgaver.
  3. Der skal løbende foretages kontrol af, om brugerne er tildelt de adgange og autorisationer, som de bør have.
  4. Ansatte og eventuelle samarbejdspartnere skal til stadighed være bekendt med og have tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker, arbejdsgange og om deres tavshedspligt.

**C.2.1.3 Krav vedrørende evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en hændelse**

Det sikres, at

* 1. Der skal være opdaterede og effektive beredskabsplaner og -procedurer, der sikrer genetablering af personoplysninger og adgange inden for rimelig tid i tilfælde af driftsafbrydelser/forstyrrelser.
  2. Effektiviteten af de tekniske og organisatoriske foranstaltninger skal regelmæssigt afprøves og evalueres til sikring af behandlingssikkerhed gennem afholdelse af it-beredskabsøvelser. Den Dataansvarlige kan anmode om at få dokumentation for gennemførelsen stillet til rådighed.
  3. Det skal sikres, at der foretages regelmæssig backup af personoplysninger, der er omfattet af aftalen.

**C.2.1.4 Krav vedrørende procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden**

Der skal foreligge procedurer, som sikrer, at der sker regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

Der skal til enhver tid være tidssvarende procedurer for gennemførelse af:

* 1. Regelmæssig kontrol, vurdering, tilpasning og forbedring af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren er underlagt efter den til enhver tid gældende lovgivning, retspraksis, Datatilsynets afgørelser, anbefalinger og retningslinjer samt vilkårene i nærværende databehandleraftale.
  2. Kontrol af, at sikkerhedsforanstaltningerne faktisk efterleves i forhold til den til enhver tid værende risiko for de registreredes rettigheder og frihedsrettigheder.
  3. Kontrol af brugeradgang for medarbejdere eller andre autoriserede.
  4. Kontrol af at backuppen er læsbar, skrivebeskyttet, har det rette omfang og kan reetableres.
  5. Kontrol af at der sker korrekt kryptering, herunder at krypteringsnøglen opbevares sikkert.
  6. Kontrol med at sikkerhedsloggene er tilstrækkelige og relevante.
  7. Kontrol med at det fysiske sikkerhedsniveau er afstemt med det til enhver tid værende trusselsbillede.
  8. Databehandleren har formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering.
  9. For kritiske sikkerhedsopdateringer skal Databehandleren have procedurer, der sikrer, at disse kan gennemføres uden unødig forsinkelse.
  10. At der føres ekstraordinære kontroller ved større ændringer af systemteknisk set-up og efter brud på persondatabeskyttelsen.

**C.2.1.5 Krav vedrørende adgang til oplysninger via internettet**

Når der tilgås systemer indeholdende personoplysninger over internettet, så skal autentifikationen af brugeren ske ved flerfaktorautentificering. Der må kun oprettes forbindelse til personoplysninger omfattet af disse bestemmelser igennem sikre krypterede forbindelser.

**C.2.1.6 Krav vedrørende beskyttelse af oplysninger under transmission**

Der skal anvendes tilstrækkelige sikkerhedsforanstaltninger i forbindelse med transmission af personoplysninger. Sikkerhedsforanstaltningerne skal leve op til de til enhver tid anerkendte og gældende branchestandarder for behandling af personoplysninger.

Det sikres i denne forbindelse, at personoplysninger er krypteret i forbindelse med transmissionen. Krypteringen skal løbende holdes opdateret, og følge den til enhver tid værende anerkendte og gældende branchestandard.

**C.2.1.7 Krav vedrørende beskyttelse af oplysninger under opbevaring**

Under opbevaring af personoplysninger skal der etableres tilstrækkelige sikkerhedsforanstaltninger under hensyntagen til karakteren af de behandlede personoplysninger, og risikoen for de registreredes rettigheder.

Det sikres, at personoplysningerne er krypteret under opbevaring. Krypteringen skal løbende holdes opdateret, og følge den til enhver tid værende anerkendte og gældende branchestandard.

**C.2.1.8 Krav vedrørende fysisk sikring af lokaliteter, hvor der behandles oplysninger**

Det sikres, at der er passende sikkerhedsforanstaltninger mod enhver uautoriseret adgang til lokationer, hvor den Dataansvarliges data behandles.

Sikkerhedsforanstaltninger skal være afstemt med det aktuelle trusselsbillede samt den følsomhed og mængde af persondata som behandles for den Dataansvarlige.

Behandlingen foregår fra lokationer, som er beskyttet mod skader forårsaget af fysiske forhold som f.eks., - men ikke begrænset til - brand, overophedning, vandskade, magnetisme, forsyningssvigt, tyveri eller hærværk.

Det skal sikres, at alt anvendt udstyr, der anvendes i forbindelse med behandlingen af personoplysninger er underlagt passende tekniske foranstaltninger.

Mobile lagringsmedier:

I det omfang der anvendes mobile lagringsmedier med personoplysninger skal disse være mærket og opbevares med tilstrækkelig stærk kryptering under opsyn eller under lås, når de ikke benyttes.

Mobile lagringsmedier med personoplysninger må kun udleveres til autoriserede personer med henblik på revision eller drifts- og systemtekniske opgaver.

Der skal føres en fortegnelse over, hvilke mobile lagringsmedier der benyttes i forbindelse med databehandlingen.

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

Reparation, service og kassation af udstyr:

I forbindelse med reparation og service af udstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes fornødne foranstaltninger for at sikre, at personoplysningerne ikke hændeligt eller bevidst tilintetgøres, fortabes eller forringes eller, at personoplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med gældende lov.

Ved kassation af udstyr og lagringsmedier, der indeholder personoplysninger, skal lagringsmedier destrueres eller renses, så der sker effektiv sletning af personoplysningerne. Dokumentation for, at kassation er foretaget i overensstemmelse med ovenstående, skal opbevares i den periode, databehandlingen foregår og forevises, på den Dataansvarliges anmodning.

**C.2.1.9 Krav vedrørende anvendelse af hjemme-/fjernarbejdspladser**

Hjemme-/fjernarbejdspladser skal være sikret med tekniske kontroller, der sikrer, at behandlingen af personoplysninger sker i overensstemmelse med gældende lovgivning og den Dataansvarliges og Databehandlerens retningslinjer.

Det skal sikres, at uvedkommende ikke får adgang til personoplysninger, der behandles ved hjemmearbejdspladser, ligesom de enkelte medarbejdere skal instrueres i, hvordan uvedkommende ikke får adgang.

Det sikres, at der anvendes kryptering af kommunikationsforbindelser. Fjernadgange skal være sikret af en VPN-løsning eller anden sikkerhedsteknologi, så det kun er autoriserede personer, som kan få adgang til personoplysninger.

Autentifikation af personer som får adgang til personoplysninger skal være baseret på en risikovurdering af den data, der skal beskyttes som beskrevet i eksempelvis Digitaliseringsstyrelsens National Standard for Identiteters Sikringsniveauer (NSIS). Risikovurderingen vil udmunde i et påkrævet sikringsniveau for at kunne tilgå systemet. Leverandøren har ansvaret for at håndhæve det påkrævede sikringsniveau, så data ikke kan tilgås af brugere uden det nødvendige sikringsniveau.

**C.2.1.10 Krav vedrørende logning**

Der skal foretages maskinel registrering (logning) ved al behandling af personoplysninger.

Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte eller det anvendte søgekriterium.

Loggen skal opbevares i seks måneder, hvorefter den skal slettes, medmindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode af hensyn til at kunne anvende den som værktøj til brug ved efterforskning.

Der føres løbende kontrol med, at loggen indeholder de nødvendige oplysninger, som fremgår af disse bestemmelser.

Ved mistanke om misbrug eller brud på persondatasikkerheden skal der vederlagsfrit udleveres en log over brugeraktivitet. Det skal sikres, at loggen er forståelig og indeholder de relevante aktiviteter.

**C.2.1.11 Øvrige foranstaltninger**

Opdateringer og ændringer

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

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

Awareness / kendskab til informationssikkerhed

Ansatte og eventuelle samarbejdspartnere, som har adgang til personoplysninger omfattet af disse Bestemmelser, skal gennemgå regelmæssig uddannelse vedrørende behandling af personoplysninger, som sikrer et vedvarende kendskab til databeskyttelsesreglerne, samt procedurer for behandlingen af personoplysninger

Test og udvikling

Personoplysninger, der anvendes til udvikling, test, supportsager eller lignende, er omfattet af samme grad af tekniske og organisatoriske foranstaltninger som produktionsmiljøer.

Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.

# C.3 Bistand til den dataansvarlige

Databehandleren og dennes underdatabehandlere skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 8.1 og 8.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Databehandleren og dennes underdatabehandlere bistår den dataansvarlige med de tekniske og organisatoriske foranstaltninger som fremgår under C.2.

Underretning af den dataansvarlige om anmodninger fra de registrerede

Databehandleren skal uden unødig forsinkelse, efter at være blevet opmærksom herpå, skriftligt underrette den dataansvarlige om enhver anmodning rettet til databehandleren eller dennes underdatabehandlere fra en registreret om udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren er ikke berettiget til at besvare anmodninger fra en registreret vedrørende udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret. Databehandleren skal på anmodning fra den dataansvarlige hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til de registreredes rettigheder i henhold til gældende databeskyttelsesret.

Bistand ved sikkerhedsbrud, herunder underretning af den dataansvarlige om sikkerhedsbrud

Databehandlerens bistand i forbindelse med den dataansvarliges forpligtelser efter databeskyttelsesforordningens artikel 33 og 34 sker ved, at databehandleren indgiver de oplysninger, der følger af Bestemmelse 9.3, til den dataansvarlige inden for den frist, der følger af Bestemmelse 9.2. Databehandleren skal efterfølgende bistå den dataansvarlige ved på den dataansvarliges anmodning at stille de oplysninger til rådighed, som er nødvendige for, at den dataansvarlige kan foretage anmeldelse af brud på persondatasikkerheden til den kompetente tilsynsmyndighed eller som er nødvendige for, at den dataansvarlige kan underrette den registrerede herom.

Bistand i forbindelse med risikovurderinger og konsekvensanalyser

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

Sikring af tekniske og organisatoriske foranstaltninger

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

# C.4 Opbevaringsperiode/sletterutine

Personoplysningerne opbevares hos databehandlerens underdatabehandler, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret i overensstemmelse med bestemmelse 10.1.

Der sker løbende sletning af personoplysninger i henhold til de krav, der er stillet til sletterutiner i systemet i overensstemmelse med lovgivning, så det ikke er muligt at identificere de registrede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles.

# C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger sker på følgende lokaliteter:

|  |  |  |
| --- | --- | --- |
| Beskrivelse af hvilke underdatabehandlere eller under-underdatabehandlere, der anvender lokationen | **Lokalitet for behandling** | **Eventuelt overførselsgrundlag** |
| [indsæt navn på underdatabehandler/under-underdatabehandler – fra bilag B] | [indsæt adresse] | [relevant hvis lokation er uden for EU/EØS] |

Ved ændringer i brug af lokaliteter skal processen i henhold til bestemmelse 6.3 følges.

## C.5.1 Lokationskrav

*[Punkt C.5.1 skal kun udfyldes, hvis systemet er underlagt lokationskravet i databeskyttelseslovens § 3, stk. 9. Lokationskravet indebærer, at personoplysninger, der behandles i en række specifikke it-systemer, helt eller devist skal opbevares i Danmark. Det er Justitsministeriet, der beslutter, om et it-system skal på listen over it-systemer, der skal føres her i landet, Punkt C.10 skal slettes, hvis systemet ikke er underlagt lokationskravet.]*

*[Her beskrives de fastsatte lokationskrav.]*

# C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

[Alternativ 1 – vælges, hvis personoplysninger ikke må overføres til tredjelande]

Databehandleren og dennes underdatabehandlere må ikke overføre personoplysninger til tredjelande.

[Alternativ 2 – vælges, hvis personoplysninger må overføres til tredjelande]

Databehandleren og dennes underdatabehandlere må overføre personoplysninger til følgende tredjelande:

[*KOMBIT eller KOMBITs underdatabehandler udfylder*]

Gyldigt overførselsgrundlag for overførslerne er:

[*Udfyldes i forhold til hvilke(t) tredjeland, de dataansvarlige har godkendt overførsel til.*]

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.

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

## C.7.1 Årligt tilsyn og revision af databehandleren

Databehandleren skal én gang årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart angående databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Revisionserklæringen skal være af typen ISAE 3000 GDPR type 2 med høj grad af sikkerhed udarbejdet efter opbygningen i FSR standarden dækkende kravene beskrevet i denne databehandleraftale. Revisionserklæringen kan indeholde yderligere kontroller, som kan hidrøre fra ISAE 3402 samt ISO 27001 og 27002 i det omfang det er relevant for det pågældende system. Revisionserklæringen fremsendes til den dataansvarlige, eller en uafhængig revisor bemyndiget af den dataansvarlige.

Revisionserklæringen anvendes til at dokumentere databehandlerens overholdelse af dennes forpligtelser overfor den dataansvarlige. Databehandleren følger op på, at eventuelle anmærkninger i revisionserklæringen bliver udbedret og dokumenterer dette i overensstemmelse med databehandlerens procedurer herfor.

Revisionserklæringen og tilhørende dokumentation fra databehandleren udarbejdes uden beregning for den dataansvarlige. Når revisionserklæringen er færdigbehandlet, sendes den til den dataansvarlige sammen med databehandlerens dokumentation for opfølgning på eventuelle anmærkninger.

Databehandleren beslutter, hvornår revisionserklæringen udarbejdes, som dog skal udarbejdes første gang senest 12 måneder efter databehandleren er påbegyndt behandling af den dataansvarliges personoplysninger og herefter årligt med maksimalt 12 måneders mellemrum.

Baseret på resultaterne af revisionserklæringen 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.

## C.7.2 Yderligere tilsyn og inspektion hos databehandleren

Den dataansvarlige eller en repræsentant for den dataansvarlige har udover revisionen i C.7.1 adgang til at foretage yderligere tilsyn, herunder fysiske inspektioner, med lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige på baggrund af et sagligt grundlag finder det nødvendigt.

I det omfang den dataansvarlige måtte ønske at gennemføre yderligere tilsyn hos databehandleren end anført i C.7.1, kontakter den dataansvarlige databehandleren, som i rimeligt omfang giver den dataansvarlige adgang til relevante dokumenter og materialer fra databehandleren.

I tilfælde af, at Datatilsynet ønsker at foretage en fysisk inspektion hos databehandleren af foranstaltninger i henhold til disse Bestemmelser, forpligter databehandleren sig til uden yderligere omkostninger for den dataansvarlige at stille tid og ressourcer til rådighed herfor.

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

## C.8.1 Årligt tilsyn og revision af underdatabehandlere

Databehandleren træffer valg om, hvordan revision af underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og underdatabehandleraftalen foretages, herunder hvilken type af revisionserklæring og/eller inspektionsrapport, der indhentes. Typen og omfanget af revisionen skal afspejle karakteren af den behandling af personoplysninger, som underdatabehandleren foretager. Revisionserklæringer og/eller inspektionsrapporter fremsendes minimum 1 gang årligt til den dataansvarlige til orientering. Revisionserklæringen og tilhørende dokumentation fra databehandleren udarbejdes uden beregning for den dataansvarlige. Når revisionserklæringen er færdigbehandlet, sendes den til den dataansvarlige sammen med databehandlerens dokumentation for opfølgning på eventuelle anmærkninger.

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.

Databehandleren indhenter mindst én gang årligt en revisionserklæring fra sin underdatabehandler udarbejdet af en uafhængig tredjepart (statusautoriseret revisor) vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Revisionserklæringen skal være systemspecifik og af typen ISAE 3000 GDPR type 2 med høj grad af sikkerhed udarbejdet efter opbygningen i FSR standarden dækkende kravene beskrevet i denne databehandleraftale. Revisionserklæringen kan indeholde yderligere kontroller, som kan hidrøre fra ISAE 3402 samt ISO 27001 og 27002 i det omfang det er relevant for det pågældende system.

Revisionserklæringen fra underdatabehandleren anvendes til at dokumentere overholdelse af dennes forpligtelser overfor KOMBIT og de dataansvarlige. Databehandleren følger op på, at eventuelle anmærkninger i revisionserklæringen bliver udbedret og dokumenterer dette i overensstemmelse med databehandlerens procedurer herfor. Den dataansvarlige kan anvende disse oplysninger til at dokumentere, at den dataansvarlige har afløftet sin tilsynspligt.

Databehandleren beslutter, hvornår revisionserklæringen udarbejdes, som dog skal udarbejdes første gang senest 12 måneder efter underdatabehandleren er påbegyndt behandling af den dataansvarliges personoplysninger og herefter årligt med maksimalt 12 måneders mellemrum.

Baseret på resultaterne af revisionserklæringen, 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.

## C.8.2 Yderligere tilsyn og inspektion hos underdatabehandlere

Den dataansvarlige eller en repræsentant for den dataansvarlige har udover revisionen i C.8.1 adgang til at foretage yderligere tilsyn, herunder fysiske inspektioner, med lokaliteterne, hvorfra databehandlerens underdatabehandlere foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige på baggrund af et sagligt grundlag finder det nødvendigt.

Dokumentation for sådanne inspektioner fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.

I det omfang den dataansvarlige måtte ønske at gennemføre yderligere tilsyn hos databehandlerens underdatabehandlere end anført i C.8.1, kontakter den dataansvarlige databehandleren, som herefter forestår kontakten til underdatabehandlerne og i rimeligt omfang giver den dataansvarlige adgang til relevante dokumenter og materialer fra underdatabehandlere.