Bilag 1

Databehandlerinstruks

1. Databehandlerens ansvar

Databehandling omfattet af Databehandleraftalen skal ske i overensstemmelse med denne instruks.

2. Generelt

2.1 Databehandleren skal som minimum træffe de nedenfor beskrevne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandlingen af personoplysninger omfattet af Databehandleraftalen.

2.1.1 Såfremt mere omfattende tekniske og organisatoriske sikkerhedsforanstaltninger, beskrevet i punkt 17.2, er nødvendige for at sikre efterlevelse af Databehandleraftalens punkt 6.1, skal sådanne mere omfattende foranstaltninger altid træffes.

2.2 Databehandleren skal udpege et fast kontaktpunkt, som over for den Dataansvarlige skal varetage ethvert forhold i relation til behandlingen af personoplysninger på vegne af den Dataansvarlige, jf. punkt 17.3

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

3. Autorisation og adgangskontrol

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

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

3.2.1 Såfremt den Dataansvarlige stiller krav om, at personale hos Databehandleren, der har adgang til personoplysninger, skal være sikkerhedsgodkendt, skal dette fremgå af Databehandleraftalens 17.2.

3.3 Kun de personer hos Databehandleren, som autoriseres dertil, må have adgang til personoplysninger, der behandles i henhold til Databehandleraftalen. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles.

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

3.5 Databehandleren skal kunne dokumentere hvilke medarbejdere, der har autorisation til at tilgå personoplysninger, der behandles i henhold til Databehandleraftalen.

3.6 Autoriserede personer hos Databehandleren udstyres med en personlig brugeridentifikation og et personligt password, der skal anvendes hver gang, der logges på systemet. Der skal anvendes 2-faktor-autentificering ved adgang til systemer med følsomme personoplysninger via internettet eller andet usikkert netværk.

3.7 Databehandleren skal sikre, at dennes medarbejdere modtager den tilstrækkelig uddannelse og instruktioner for at sikre, , at personoplysninger behandles i overensstemmelse med relevant lovgivning samt Databehandlerens og den Dataansvarliges politikker og procedurer herfor.

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

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

3.10 Der skal mindst en gang hvert halve år foretages kontrol af, at brugerne kun er tildelt de adgange, som de har behov for. Denne kontrol kan f.eks. indebære, at der i systemerne dannes en statistik over den enkelte brugers anvendelse af systemet, således at det kan konstateres, om der er udstedte autorisationer, som ikke er anvendt, og som derfor eventuelt bør inddrages. Ved anvendelse af en sådan statistisk opfølgning vil der fortsat være behov for en konkret vurdering af, om medarbejderen har et fortsat arbejdsmæssigt behov for adgang.

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

4. Fysisk sikring

4.1 Databehandleren skal sikre, at it-udstyr, der anvendes i forbindelse med databehandlingen, er fysisk sikret i henhold til gældende lovkrav.

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

4.3 Ved reparation og service af udstyr, skal Databehandleren sikre, at reparations- og servicepersonalet behandler eventuelle personoplysninger, de bliver bekendt med under deres arbejde, fortroligt.

4.4 Ved kassation af udstyr og lagringsmedier, der indeholder personoplysninger, skal lagringsmedier destrueres eller afmagnetiseres, så der sker effektiv sletning af personoplysningerne. Dokumentation for, at kassation er foretaget i overensstemmelse med ovenstående, skal forevises, når den Dataansvarlige anmoder herom.

5. Kontrol med afviste adgangsforsøg og logning

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

5.2 Der skal foretages maskinel registrering (logning) ved al behandling af personhenførbare oplysninger. Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrører eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, med mindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode af hensyn til at kunne anvende loggen som værktøj til brug for efterforskning.

5.2.1 Aftales der en længere opbevaringstid for loggen, skal dette fremgå af Databehandleraftalens punkt 17.2.

5.3 Databehandleren skal efter ønske fra den dataansvarlige stille nødvendige loginformationer til rådighed for den Dataansvarlige til brug for gennemførelse af periodisk audit eller til undersøgelse af misbrug eller mistanke om misbrug.

6. Håndtering af ind- og uddatamateriale indeholdende personoplysninger

6.1 Inddatamateriale må kun anvendes af personer, som er beskæftiget med inddateringen. Inddatamateriale skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, der er indeholdt heri.

6.2 Når det ikke længere er nødvendigt at bevare inddatamaterialet, skal Databehandleren slette eller tilintetgøre inddatamaterialet. Fremgangsmåden herfor skal ske efter best practice.

6.3 Punkt 6.2 gælder ikke, såfremt materialet er omfattet af bevarings-/kassationsbestemmelser i henhold til anden lovgivning, eller hvis journaliseret materiale behandles efter de almindelige arkiv bestemmelser om bevaring, herunder aflevering af arkivalier til Statens Arkiver.

6.4 Uddatamateriale er omfattet af samme instrukser som inddatamateriale.

6.5 Udover bestemmelsen i punkt 6.4 må uddatamateriale kun anvendes af personer, der er beskæftiger med de formål, til hvilke behandlingen af personoplysninger foretages, samt i forbindelse med revision, teknisk vedligeholdelse, driftsovervågning og fejlretning mv.

7. Mobile lagringsenheder

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

7.2 Mobile lagringsmedier med personoplysninger må kun udleverestil autoriserede personermed henblik på revision eller drifts- og systemtekniske opgaver.

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

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

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

8. Sikkerhedskopier

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

8.2 Databehandleren skal sikre, at systemer og personoplysninger sikkerhedskopieres regelmæssigt. Sikkerhedskopierne skal opbevares adskilt fra serverne i et ikke tilstødende rum for at sikre, at disse ikke går tabt f.eks. som følge af brand eller oversvømmelse. Opbevaring af sikkerhedskopier skal altid ske på betryggende vis så de ikke fortabes.

8.3 Databehandleren skal regelmæssigt kontrollere, at sikkerhedskopier er læsbare. Dette skal blandt andet gøres ud fra et beredskabssynspunkt, f.eks. ved større ændringer af system teknisk set up.

9. Opdateringer og ændringer

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

9.1.1 For kritiske sikkerhedsopdateringer skal Databehandleren have procedurer, der sikrer at disse kan gennemføres inden for 48 timer.

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

10. Eksterne kommunikationsforbindelser

10.1 Der må kun etableres eksterne it-kommunikationsforbindelser med tilladelse fra den Dataansvarlige og der træffes foranstaltninger til at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

10.1.1 Der skal træffes foranstaltninger til beskyttelse af personoplysninger, der transmitteres over åbne net. Eventuelle uddybende beskrivelser af foranstaltningerne skal fremgå af Databehandleraftalens punkt 17.2.

11. IT-beredskab

11.1 Databehandleren skal have dokumenterede it-beredskabsprocedurer, der sikrer genetablering af services inden for rimeligtid i tilfælde af driftsafbrydelser.

12. Underretning om sikkerhedshændelser og assistance ved håndteringen

12.1 Databehandlerens skal have en procedure for håndtering og opfølgning på sikkerhedsbrud i overensstemmelse med kravene i ISO27001.

12.2 Databehandleren skal dokumentere de identificerede risici og hvordan risikoen er nedbragt til et acceptabelt niveau.

12.3 Oversigt over kontaktpersoner i forbindelse med underretning om sikkerhedshændelser skal fremgå af Databehandleraftalens punkt 17.3.