

§ 1.

Databehandleren handler alene efter instruks af den dataansvarlige.

§ 2.

Databehandleren forpligter sig til, til enhver tid at overholde lovgivningsmæssige krav samt denne databehandlerinstruks.

§ 3.

Databehandleren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med Persondataloven og Justitsministeriets sikkerhedsbekendtgørelse.

§ 4.

Databehandleren skal især iagttage følgende vedrørende autorisation og adgangskontrol:

- 1.1. Autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette oplysninger.
- 1.2. Kun de personer, som autoriseres dertil, må have adgang til personoplysninger, der behandles.
- 1.3. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.
- 1.4. Der må endvidere autoriseres personer, for hvem adgang til oplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.
- 1.5. Autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger.
- 1.6. Den autoriserede bruger udstyres med en brugeridentifikationskode og et password, der skal bruges hver gang, der logges på systemet.
- 1.7. Autorisation foranstalles af systemejeren efter indstilling fra medarbejderens leder.
- 1.8. 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.
- 1.9. Alle ansatte, der har med elektronisk databehandling at gøre, udstyres med en brugeridentifikationskode og et password med henblik på adgang til databehandlerens netværk. Brugeridentifikationskode og password skal anvendes hver gang, brugeren skaber sig adgang til netværket.

Stk. 2. Der skal mindst én gang hvert halve år foretage kontrol af, at betingelserne i henhold til ovenstående punkter 1.1. – 1.9. overholdes. Autorisationer for brugere, der ikke længere har behov for autorisationen i forbindelse med brugerens arbejde, skal inddrages.

§ 5.

Databehandleren skal iagttage følgende vedrørende inddatamateriale, der indeholder personoplysninger:

- 1.1. Inddatamateriale, som ikke indgår i en manuel sag eller et manuelt register, må kun anvendes af personer, som er beskæftiget med inddateringen. Inddatamateriale, som er omfattet af anmeldelsesreglerne i kapitel 12 i Persondataloven, dvs. inddatamateriale indeholdende fortrolige personhenførbare oplysninger, skal opbevares aflåst, når det ikke anvendes.
- 1.2. Inddatamateriale, som er nævnt i punkt 1.1., skal slettes eller tilintetgøres, når det ikke længere er nødvendigt at bevare det af hensyn til de formål, som behandlingen varetager eller til kontrol med de inddaterede personoplysninger, dog senest 5 år efter, at oplysningerne ikke længere tilgodeser formålet med behandlingen, eller oplysningerne ikke længere er administrativ aktive.
- 1.3. Inddatamateriale, som er nævnt i punkt 1.1., skal slettes eller tilintetgøres, når det ikke længere er nødvendigt at bevare det af hensyn til de formål, som behandlingen varetager eller til kontrol med de inddaterede personoplysninger, dog senest 5 år efter, at oplysningerne ikke længere tilgodeser formålet med behandlingen, eller oplysningerne ikke længere er administrativ aktive.
- 1.4. Bestemmelsen i pkt. 1.2. gælder ikke, såfremt materialet er omfattet af bevarings-/kassationsbestemmelser fastsat i henhold til anden lovgivning. Inddatamateriale, der er journaliseret i henhold til gældende journaliseringsbestemmelser, behandles efter de almindelige arkivbestemmelser om bevaring, herunder aflevering af arkivalier til Statens Arkiver.
- 1.5. Ved tilintetgørelse af inddatamateriale skal der træffes fornødne sikkerhedsforanstaltninger for at undgå, at materialet misbruges eller, at materialet kommer til uvedkommendes kendskab.

§ 6.

Databehandleren skal iagttage følgende vedrørende lagringsmedier:

- 1.1. Lagringsmedier med personoplysninger skal være mærket og skal opbevares under opsyn eller under lås, når de ikke benyttes.
- 1.2. Lagringsmedier må kun udleveres til medarbejdere samt til autoriserede personer, der har adgang til oplysningerne, med henblik på revision eller drifts- og systemtekniske opgaver.
- 1.3. Der skal føres en fortegnelse over, hvilke lagringsmedier, der benyttes i forbindelse med databehandlingen.
- 1.4. Der skal udarbejdes skriftlige instrukser for anvendelse og opbevaring af udtagelige lagringsmedier.
- 1.5. 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 oplysningerne ikke hændeligt eller bevidst tilintetgøres, fortabes eller forringes eller, at oplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med Persondataloven.

§ 7.

Databehandleren skal iagttage følgende vedrørende uddatamateriale som indeholder personoplysninger:

- 1.1. Uddata må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages.
- 1.2. Udover bestemmelsen i punkt 1.1. må uddatamateriale anvendes af personer, som er beskæftiget med sikkerheds- og/eller forvaltningsmæssig revision eller drifts- og systemtekniske opgaver vedrørende det pågældende system og systemets anvendelse.
- 1.3. Uddatamateriale skal både fysisk og teknisk opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, som er indeholdt i materialet.
- 1.4. Uddatamateriale skal tilintetgøres, når det ikke længere er nødvendigt til de formål, som behandlingen varetager, dog senest 5 år efter, at oplysningerne ikke længere tilgodeser formålet med behandlingen eller oplysningerne ikke længere er administrativ aktive.
- 1.5. Bestemmelsen i punkt 1.4. gælder ikke, såfremt materialet er omfattet af bevarings-/kassationsbestemmelser i henhold til anden lovgivning.
- 1.6. Uddatamateriale, der er journaliseret i henhold til vedtagne journaliseringsbestemmelser, behandles efter de almindelige arkivbestemmelser om bevaring, herunder aflevering af arkivalier til Statens Arkiver.
- 1.7. Ved tilintetgørelse af uddatamateriale skal der træffes de fornødne sikkerhedsforanstaltninger for at undgå, at materialet misbruges eller, at materialet kommer til uvedkommendes kendskab.
- 1.8. Bestemmelserne i punkterne 1.1. – 1.5. gælder ikke for uddatamateriale, som indgår i en manuel sag eller i et manuelt register.

§ 8.

Databehandleren må ikke foretage databehandling fra ad hoc arbejdspladser (fjernarbejdspladser eller hjemmearbejdspladser), jf. dog § 9.

§ 9.

Databehandleren skal iagttage følgende vedrørende eksterne kommunikationsforbindelser:

- 1.1. Der må kun etableres eksterne IT-kommunikationsforbindelser, hvis der efter tilladelse og efter nærmere aftale herom træffes foranstaltninger til at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.
- 1.2. Der skal foretages foranstaltninger, der sikrer at data, der transmitteres over åbne net som for eksempel Internettet, ikke fortabes, ændres eller kommer til uvedkommendes kendskab under transmissionen.
- 1.3. Den dataansvarlige fastlægger retningslinjer herfor og angiver, hvilke særlige foranstaltninger, der konkret skal træffes for at efterleve disse krav.

§ 10.

Databehandleren skal iagttage følgende vedrørende kontrol med afviste adgangsforsøg og logning:

- 1.1. 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 afviste adgangsforsøg er klarlagt.
- 1.2. Der skal foretages maskinel registrering (logning) af alle anvendelser 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.
- 1.3. Bestemmelsen i punkt 1.2. finder ikke anvendelse for personoplysninger, som indgår i tekstbehandlingsdokumenter og lignende, der ikke foreligger i endelig form. Det samme gælder sådanne dokumenter, som foreligger i endelig form, hvis der sker sletning inden for 30 dage.
- 1.4. Bestemmelsen i punkt 1.2. finder ikke anvendelse, hvis behandlingen af personoplysninger sker ved afvikling af programmer, som foretager en foruddefineret massebehandling af personoplysninger, eller hvis behandlingen sker med henblik på statistiske eller videnskabelige undersøgelser, og identifikationsoplysningerne forinden enten er krypteret eller erstattet med kodenummer eller lignende. Der skal dog i begge tilfælde foretages maskinel logning af brugeren og tidspunktet for behandlingen, jf. punkt 1.2.

Dato:

For databehandler:
