# Databehandleraftale

mellem

## Parterne

Sundhedsdatastyrelsen
<Organisationens navn>
Ørestads Boulevard 5
<Adresse>
2300 København S
<Postnummer og by>
33257872
<CVR-nummer>

(Herefter kaldt den **Dataansvarlige**)

Og

<Organisationens navn>

<Adresse>

<Postnummer og by>

<CVR-nummer>

(Herefter kaldt **Databehandleren)**

Er der indgået nedenstående databehandleraftale (herefter **Databehandleraftalen**) om Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige.

# 1. Definitioner

| | |
|---|---|
| Dataansvarlig | En fysisk eller juridisk person, en offentlig myndighed, en institution eller andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den Dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret. |
| Databehandler | En fysisk eller juridisk person, en offentlig myndighed, en institution eller andet organ, der behandler personoplysninger på den Dataansvarliges vegne. |
| Hovedaftale | Den aftale eller kontrakt, der er indgået mellem parterne vedrørende udførelse af de opgaver, hvortil Databehandleraftalen er knyttet. |
| Sikkerhedsgodkendelse | Ved sikkerhedsgodkendelse forstås en status, som en person tildeles efter en personundersøgelse, således at denne kan få adgang til klassificeret materiale eller -områder. I Danmark foretages personundersøgelser og sikkerhedsgodkendelser af Politiets Efterretningstjeneste. |
| Tredjelande og internationale organisationer | Et tredjeland er et land, som ikke er medlem af EU eller EØS (Island, Liechtenstein og Norge).<br><br>En international organisation kan f.eks. være Røde Kors, WHO, FN, OECD m.fl. For at reglerne i forordningens kapitel V finder anvendelse på internationale organisationer, er det en forudsætning, at den internationale organisation befinder sig i et tredjeland. |
| Underdatabehandler | En Databehandler, som Databehandleren har overladt hele eller dele af den behandling, som Databehandleren foretager på vegne af den Dataansvarlige. |

## 2. Generelt

2.1 Denne databehandleraftale vedrører den Dataansvarliges og Databehandlerens forpligtelse til at efterleve EUROPA-PARLAMENTETS OG RÅDETS FORORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om ophævelse af direktiv 95/46EF (generel forordning om databeskyttelse) samt lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

2.2 Principperne og anbefalingerne i ISO27001 med senere ændringer vil på alle relevante områder finde anvendelse i det omfang, andet ikke fremgår af nærværende Databehandleraftale.

2.3 Databehandleren skal behandle personoplysninger i overensstemmelse med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

2.4 Er det i forbindelse med indgåelsen af nærværende Databehandleraftale aftalt, at Databehandleren forpligter sig til at gøre sig bekendt med og efterleve den Dataansvarliges informationssikkerhedspolitik eller andre sikkerhedsretningslinjer, skal dette fremgå af punkt 17.2.

2.5 Databehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.

## 3. Formål

3.1 Databehandlerens opgave og formålet med databehandlingen fremgår af punkt 17.1.

3.2 Databehandleren må ikke behandle oplysninger omfattet af denne Databehandleraftale til egne formål.

## 4. Den Dataansvarliges rettigheder og forpligtelser

4.1 Den Dataansvarlige har overfor omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

4.2 Den Dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.

4.3 Den Dataansvarlige er blandet andet ansvarlig for, at der foreligger hjemmel til den behandling, som databehandleren instrueres i at foretage.

## 5. Databehandlerens generelle forpligtelser

5.1 Databehandleren er Databehandler for de personoplysninger, som behandles på vegne af den Dataansvarlige iht. Hovedaftalen og Databehandleraftalen.

5.2 Databehandleren handler alene efter dokumenteret instruks fra den Dataansvarlige og alene i det omfang, det er nødvendigt for, at Databehandleren kan opfylde sine forpligtelser iht. Hovedaftalen og Databehandleraftalen. jf bilag 1 Databehandlerinstruks, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, jf. punkt 10.1.

5.3 Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter Databehandlerens mening er i strid med Databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5.4 Databehandleren har de forpligtelser, som er pålagt Databehandleren i medfør af lovgivningen, jf. punkt. 2.1 .

5.5 Databehandleren er forpligtet til at oplyse med præcise adresseangivelser, hvor den Dataansvarliges personoplysninger opbevares, jf. punkt 17.1. Databehandleren skal underrette den Dataansvarlige om enhver ændring.

5.6 Denne databehandleraftale frigør ikke Databehandleren for de forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt Databehandleren.

## 6. Tekniske og organisatoriske sikkerhedsforanstaltninger

6.1 Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal

gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

6.2 Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:

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

6.3 Databehandleren skal i forbindelse med ovenstående – i alle tilfælde – som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag 1.

6.4 Databehandleren skal mindst en gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandling af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed iagttages.

6.5 Databehandleren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af den Dataansvarliges personoplysninger, om Databehandlerens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. punkt 11 samt bilag 1 Databehandlerinstruks.

## 7. Anvendelse af ad hoc arbejdspladser

7.1 Anvendelse af ad hoc arbejdspladser (fjern- eller hjemmearbejdspladser) skal være godkendt af den Dataansvarlige.

7.2 Såfremt Databehandleren foretager databehandling fra ad hoc arbejdspladser, skal Databehandleren sikre, at disse lever op til de sikkerhedsmæssige krav i denne Databehandleraftale med bilag samt Datatilsynets IT-sikkerhedstekster herom.

7.2.1 I det omfang databehandlingen sker fra ad hoc arbejdspladser, skal Databehandleren i punkt 17.2 beskrive

- Hvilken krypteret forbindelse, der anvendes mellem ad hoc arbejdspladsen og Databehandlerens/Dataansvarliges netværk
- Anvendelse af 2-faktor-autentifikation

- Databehandlerens instruks til egne medarbejdere om anvendelse af ad hoc arbejdspladser.

## 8. Underretningspligt og assistance

8.1 Databehandleren forpligter sig til uden unødig forsinkelse og skriftligt, at orientere den Dataansvarlige om afvigelser fra kravene i databehandleraftalen, f.eks.:

- Ved enhver fravigelse fra givne instrukser
- Ved enhver afvigelse fra det aftalte om tilgængelighed
- Ved planlagte releases, opgraderinger, tests mv.
- Ved enhver mistanke om brug på fortroligheden, misbrug, fortabelse og forringelse af data mv.

8.2 Yderligere forpligter Databehandleren sig til uden unødig forsinkelse og senest 24 timer efter, at denne er blevet bekendt med bruddet skriftligt at orientere den Dataansvarlige om brud på persondatasikkerheden, f.eks.:

- Ved enhver konstatering af misbrug, fortabelse og forringelse af data mv.
- Ved enhver hændelig eller uautoriseret videregivelse af eller adgang til personoplysningerne behandlet efter denne databehandleraftale

Sådan at den Dataansvarlige har mulighed for at efterleve forpligtelsen til at anmelde bruddet til tilsynsmyndigheden inden for 72 timer

En underretning om brud på persondatasikkerheden skal indeholde følgende oplysninger:

- karakteren af bruddet på datasikkerheden og, hvis det er muligt, hvem der er omfattet, antal berørte og antal berørte registreringer af personoplysninger
- beskrivelse af de sandsynlige konsekvenser der er af bruddet
- beskrivelse af de foranstaltninger databehandleren har truffet eller foreslår truffet for at håndtere databruddet og hvad der kan gøres for at begrænse dets mulige skadevirkninger

8.3 Databehandleren skal følge op på sikkerhedshændelsen og underrette den Dataansvarlige om de nærmere omstændigheder, herunder udarbejde en situationsrapport samt oplyse om, hvilke personoplysninger, der er kompromitteret, samt hvilke tiltag Databehandleren har iværksat eller påtænker at iværksætte.

8.4 Databehandleren og dennes underdatabehandlere må hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud uden forudgående skriftlig aftale med den Dataansvarlige om indholdet af en sådan kommunikation, medmindre Databehandleren er retligt forpligtet til sådan kommunikation.

8.5 Databehandleren og denne eventuelle Underdatabehandlere skal uden unødig forsinkelse bistå den Dataansvarlige med håndteringen af enhver henvendelse fra en registrerede,

herunder anmodning om indsigt, berigtigelse, blokering eller sletning, hvis de relevante personoplysninger behandles af Databehandleren. Databehandleren og denne eventuelle Underdatabehandlere skal ligeledes bistå den Dataansvarlige med at overholde øvrige forpligtelser, der måtte påhvile den Dataansvarlige efter gældende ret, hvor bistanden er forudsat, samt bistand er nødvendigt for, at den Dataansvarlige kan overholde sine forpligtelser.

## 9. Databehandlerens brug af Underdatabehandler[1]

9.1 Databehandleren må ikke uden udtrykkelig skriftligt samtykke fra den Dataansvarlige anvende andre underdatabehandlere end dem, der er angivet i bilag 2, til at behandle personoplysninger, som den Dataansvarlige har overladt til Databehandleren i medfør af databehandleraftalen og Hovedaftalen. Den Dataansvarlige er berettiget til at stille vilkår for et sådant samtykke.

9.2 Databehandleren skal indgå en skriftlig aftale med sin underdatabehandleren, hvor det sikres, at underdatabehandleren som minimum kan opfylde de forpligtelser, som Databehandleren har påtaget sig ved denne Databehandleraftale, for så vidt angår den behandling af personoplysninger, der varetages af underdatabehandleren. Databehandleren indestår for kontraktsmæssigheden og lovligheden af underdatabehandlerens behandling af personoplysninger. Det forhold, at databehandleren indgår aftale med en underdatabehandler, fritager ikke Databehandleren for pligten til at efterleve nærværende Databehandleraftale.

9.3 Den Dataansvarlige kan til enhver tid forlange dokumentation fra Databehandleren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Databehandleren anvender i forbindelse med opfyldelsen af sine forpligtelser over for den Dataansvarlige.

9.4 Det er Databehandlerens ansvar at sikre og dokumentere, at eventuelle underdatabehandlere, er bekendt med og efterlever den Dataansvarliges instruks (bilag 1).

9.5 Al kommunikation mellem den Dataansvarlige og underdatabehandleren skal som udgangspunkt ske via Databehandleren.

9.6 Ved ophør af en aftale med en underdatabehandler skal Databehandleren give den Dataansvarlige meddelelse herom. Databehandleren skal i den forbindelse sikre, at underdatabehandleren sletter data behørigt i overensstemmelse med kravene i punkt 13.

### Skift af underdatabehandler i aftaleperioden

9.7 Databehandleren kan udpege en ny Underdatabehandler, såfremt den nye Underdatabehandler (1) overholder gældende love om databeskyttelse og (2) er bundet af

[1] Såfremt underdatabehandleren er etableret i et tredjeland, skal reglerne i kapitel 11 ligeledes iagttages.

en databehandleraftale og (3) har et sikkerhedsniveau som er mindst den samme som den nuværende Underdatabehandler.

9.8 Databehandleren skal orientere den Dataansvarlige i tilfælde af, at der vælges en ny Underdatabehandler. Orienteringen skal ske senest 3 måneder inden den nye Underdatabehandler tages i anvendelse.

9.9 Såfremt den Dataansvarlige ikke mener, at en af Databehandleren udpeget Underdatabehandler lever op til et eller flere af de ovennævnte krav under punkt (1), (2) og (3), vil det blive betragtet som væsentlig misligholdelse og der henvises til punkt 14 om misligholdelse. Inden væsentlig misligholdelse gøres gældende skal den Dataansvarlige underrette sin Databehandler om forholdet og give en passende frist til at udbedre misligholdelsen.

## 10. Overførsel af personoplysninger til tredjelande eller internationale organisationer

10.1 Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt; i så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. databeskyttelsesforordningens art. § 28, stk. 3, litra a.

10.2 Uden den Dataansvarlige instruks eller godkendelse kan Databehandleren – indenfor rammerne af Databehandleraftale – derfor bl.a. ikke;

a) videregive personoplysninger til en Dataansvarlige i et tredjeland eller i en international organisation,
b) overlade behandlingen af personoplysninger til en underdatabehandler i et tredjeland [2],
c) lade oplysningerne behandle i en anden af Databehandlerens afdelinger, som er placeret i et tredjeland.

10.3 Den Dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af dennes aftales punkt 17.2.

[2] Se også pkt. 9

## 11. Tavshedspligt og fortrolighed

11.1 Personoplysninger omfattet af denne aftale er fortrolige.

11.2 Databehandleren sikrer, at de personer, de er autoriseret til at behandle personoplysninger på vegne af den Dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

11.3 Det påhviler Databehandleren og dennes eventuelle underdatabehandlere at informere egne ansatte, samarbejdspartnere, eksterne konsulenter, vikarer m.fl. om udstrækningen af tavshedspligten og om konsekvenserne ved en eventuel overtrædelse.

11.4 Kun de personer hos Databehandleren eller dennes underdatabehandlere, der autoriseres hertil, må have adgang til de personoplysninger, der behandles og brugerne må kun autoriseres til anvendelser, de har behov for i forhold til at kunne opfylde Databehandlerens forpligtelser over for den Dataansvarlige.

11.5 Databehandleren og dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.

11.6 Databehandlerens forpligtelser om tavshedspligt og fortrolighed gælder også efter aftalens ophør.

## 12. Audit og revisionserklæringer

12.1 Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige de nødvendige oplysninger til, at denne kan påse forpligtelserne i henhold til denne aftale samt at der er truffet passende tekniske og organisatoriske sikkerhedsforanstaltninger. Endvidere skal Databehandleren kunne dokumentere, at identificerede sårbarheder bliver imødegået ud fra en risikobaseret vurdering.

12.2 Såfremt den Dataansvarlige, en repræsentant for den Dataansvarlige, dennes revision (intern eller ekstern) eller en relevant offentlig myndighed, særligt Datatilsynet, ønsker at foretage fysisk inspektion (audit) af de foranstaltninger, som Databehandleren har etableret i medfør af aftalen, forpligter Databehandleren sig til - med et rimeligt varsel – at stille tid og ressourcer til rådighed herfor. Databehandleren forpligter sig til på samme måde at sikre, at sådanne audits kan gennemføres hos sine eventuelle underdatabehandlere.

12.3 Som supplement eller alternativ til de overfor nævnte audits kan der indgås aftale om, at Databehandleren og eventuelle underdatabehandlere for egen regning sørger for, at en uafhængig ekspert årligt udarbejder en revisionserklæring på grundlag af en anerkendt standard angående Databehandlerens overholdelse af kravene til sikkerhedsforanstaltninger fastsat i Databehandleraftalen. Erklæringen skal være

formuleret konkret i forhold til den opgave, som Databehandleren løser for den Dataansvarlige. En sådan aftale skal fremgå af punkt 17.2.

## 13. Håndtering af data efter aftalens ophør

13.1 Databehandleren og dennes eventuelle underdatabehandlere forpligter sig til at tilbagelevere og/eller slette personoplysninger, når databehandlingen i henhold til Hovedaftalen med den Dataansvarlige ophører medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

13.2 Den Dataansvarlige skal inden Hovedaftalens ophør skriftligt meddele Databehandleren, hvorvidt alle personoplysninger skal slettes eller tilbageleveres til den Dataansvarlige. Fristen herfor aftales mellem parterne.

13.3 Databehandleren er ansvarlig for, at sletning af oplysningerne sker på en sådan måde, at det ikke er muligt at genskabe oplysningerne. Databehandleren er herunder ansvarlig for at oplysningerne også slettes fra backup samt hos eventuelle underdatabehandlere.

13.4 Hvis oplysningerne tilbageleveres til den Dataansvarlige, skal Databehandleren slette eventuelle kopier af oplysningerne.

13.5 Når sletningen er gennemført, skal Databehandleren fremsende en skriftlig erklæring på, at data er slettet som aftalt.

13.6 Såfremt Databehandleren eller dennes underdatabehandlere i forbindelse med konkurs eller lignende ophører med at behandle personoplysninger for den Dataansvarlige, skal alle personoplysninger uden ugrundet ophold tilbageleveres på en måde, der gør det muligt for den Dataansvarlige at anvende disse fremadrettet. Databehandler, dennes konkursbo e.l. er herefter forpligtet til at slette oplysninger fra deres egne systemer i overensstemmelse med pkt. 13.1-13.5.

## 14. Misligholdelse

14.1 Bestemmelserne i dette afsnit har forrang ift. Hovedaftalen, for så vidt angår behandlingen af personoplysninger. Såfremt dette ikke er tilfældet, angives det i pkt. 17.1.

14.2 Ved Databehandlerens misligholdelse af Databehandleraftalen er den Dataansvarlige berettiget til at gøre sædvanlige misligholdelsesbeføjelser gældende med de tilføjelser og præciseringer, som fremgår af bestemmelserne i dette afsnit.

14.3 Ved væsentlig misligholdelse af Databehandleraftalen er den Dataansvarlige berettiget til at ophæve Hovedaftalen og dermed også Databehandleraftalen. Som udgangspunkt betragtes det som væsentlig misligholdelse, såfremt Databehandleren ikke overholder forpligtelserne i Databehandleraftalen, den til enhver tid gældende lovgivning vedrørende databeskyttelse samt kravene i de dokumenter, der udgør bilag til Databehandleraftalen.

14.4 Den Dataansvarliges ophævelse af Hovedaftalen og Databehandleraftalen indebærer ikke, at den Dataansvarlige giver afkald på sin ret til at kræve erstatning, hvis betingelserne herfor er opfyldt, jf. pkt. 14.7.

14.5 Såfremt den Dataansvarlige vælger ikke at ophæve Hovedaftalen og Databehandleraftalen i ét eller flere tilfælde, selvom den Dataansvarlige er berettiget hertil, medfører dette ikke, at den Dataansvarlige mister retten til at ophæve Hovedaftalen og Databehandleraftalen i andre tilfælde.

14.6 Ved ophævelse af Hovedaftalen og Databehandleraftalen, er Databehandleren forpligtet til at levere databehandling i henhold til Hovedaftalen og denne Databehandleraftale, indtil databehandlingen er sikret hos en anden databehandler. Databehandleren er ligeledes forpligtet til at levere relevant ophørsassistance til den Dataansvarlige, herunder i relation til eventuelle underdatabehandlere, som Databehandleren måtte have overladt en del af databehandlingen til.

14.7 Databehandleren er erstatningsansvarlig i overensstemmelse med dansk rets almindelige regler i tilfælde af misligholdelse af Databehandleraftalen. Såfremt den Dataansvarlige af tredjemand gøres erstatningsansvarlig for Databehandlerens og/eller eventuelle Underdatabehandleres manglende overholdelse af Databehandleraftalen, herunder Databehandleraftalens bilag, og/eller overtrædelse af gældende lovgivning vedrørende databeskyttelse, skal Databehandleren holde den Dataansvarlige skadesløs for alle omkostninger, gebyrer, erstatningsbeløb, udgifter eller tab, som den Dataansvarlige har afholdt eller pådraget sig som følge heraf.

14.8 Den Dataansvarlige er berettiget til at stille krav om, at Databehandleren bistår med at forsvare den Dataansvarliges interesser i en eventuel rets- eller voldgiftssag, uagtet Databehandlerens eventuelle indsigelser i forhold til den påberåbte misligholdelse, såfremt Databehandlerens bistand er af væsentlig betydning for varetagelsen af den Dataansvarliges interesser.

## 15. Lovvalg og værneting

15.1 Medmindre lovvalg og værneting er direkte reguleret i Hovedaftalen, finder følgende bestemmelser anvendelse:

15.1.1 Denne Databehandleraftale inklusiv ethvert spørgsmål om Databehandleraftalens gyldighed er undergivet dansk ret.

15.1.2 Såfremt der opstår uoverensstemmelser mellem Parterne i forbindelse med Databehandleraftalen, skal Parterne med en positiv, samarbejdende og ansvarlig holdning søge at indlede forhandlinger med henblik på at løse tvisten.

15.1.3 Hvis enighed ikke kan opnås via forhandling eller på anden vis, skal tvisten løses ved de danske domstole ved den Dataansvarliges hjemting.

## 16. Ikrafttræden og varighed

16.1 Nærværende Databehandleraftale indgås ved begge parters underskrift og gælder indtil behandlingen af personoplysninger i henhold til Hovedaftalen er ophørt og Databehandleren har slettet data, jf. pkt. 13.

16.2 Den Dataansvarlige og Databehandleren er solidariske ansvarlige for at sikre, at der foretages de nødvendige opdateringer i databehandleraftalen ved lovændringer, hvis den dataansvarlige forpligtes til at efterkomme nye sikkerhedsstandarder eller hvis der sker ændringer af tekniske eller organisatoriske forhold hos den Dataansvarlige og/eller Databehandleren

# 17. Specifikke forhold vedr. databehandlingen

(Såfremt Databehandlerens opgave, jf. Hovedaftalen, vedrører flere forskellige databehandlinger, skal der udfyldes og vedlægges tilhørende kopier af afsnit 17, så der fremgår dokumentation for hver enkelt databehandling, som Databehandleraftalen omfatter)

**17.1 Generelle forhold**

| | |
|---|---|
| Databehandlingens navn | Adgang til services på den Nationale Serviceplatform (NSP) |
| ID i den Dataansvarliges fortegnelse over databehandlinger | ID i den dataansvarliges fortegnelse fremgår af oversigten over services på NSPOP |
| ID i Databehandlerens fortegnelse | |
| Hovedaftale/kontrakt (dato for indgåelse, journal-ID) | Serviceaftale |
| Databehandlingens formål | Formålet med databehandlingen er at give lokale anvendere adgang til services på den nationale serviceplatform via leverandørens/databehandlerens it-løsning |
| Generel beskrivelse af behandlingen | En række anvendere af Sundhedsdatastyrelsens services på NSP tilgår disse gennem databehandlerens it-løsning (LPS-system/EOJ-system), ved at databehandlerens it-løsning er integreret til NSP. |
| Registrerede personer (kategorier af personer, der indgår i databehandlingen) | Patienter<br>Sundhedspersonale |
| Kategorier af personoplysninger | Almindelige personoplysninger: Navn, kontaktoplysninger<br>Fortrolige personoplysninger: CPR-nummer<br>Følsomme personoplysninger: Helbredsoplysninger |

| | |
|---|---|
| Evt. modtagere af oplysninger | Praktiserende læger og personale ansat hos disse. Ansatte i hjemmeplejen. |
| Sletningsfrister | Oplysninger opbevares ikke hos databehandleren. |
| Evt. lov/bestemmelse, der hjemler databehandlingen | Sundhedsloven §220a |
| Databehandlerens opgave | Databehandleren står for integration mellem sin it-løsning og services på NSP. I den forbindelse har databehandleren opgaven med at sikre, at den dataansvarlige er bekendt med, hvilke brugere, der anvender databehandlerens løsning til at tilgå services på NSP samt at sikre, at brugerne er bekendt med reglerne for at tilgå services. |
| Lokationer for databehandlingen | (angives af serviceaftager) |

**17.2 Særlige forhold vedr. databehandlingen (hvis ikke relevant, markeres dette)**

| | |
|---|---|
| Evt. andre lovkrav, som databehandlingen er underlagt (f.eks. krav om, at data skal opbevares i Danmark eller evt. specifikke samtykkekrav) | Ikke relevant |
| Evt. andre krav, som den dataansvarlige pålægger databehandleren | Databehandleren skal efter instruks fra den dataansvarlige sikre, at anvendere af services på NSP er bekendt med reglerne for anvendelsen. Reglerne for anvendelsen fremgår af bilag 2 til serviceaftageraftalen.<br>Herudover skal databehandleren hvert ½ år (april og oktober) fremsende en oversigt over, hvilke anvendere, der tilgår hvilke services på NSP via deres it-løsning. |
| Aftale mellem parterne om helt eller delvist fravigelse af krav i databehandleraftalen<br><br>(Beskriv aftalte fravigelser og eventuelle kompenserende sikkerhedsforanstaltninger) | Ikke relevant |
| Databehandleren forpligter sig til at efterleve den dataansvarliges informationssikkerhedspolitik og/eller retningslinjer.<br><br>(Angiv relevante dokumenter) | Den koncernfælles informationssikkerhedspolitik og databeskyttelsespolitik for Sundheds- og Ældreministeriet fremsendes årligt til databehandleren |

| | |
|---|---|
| Den dataansvarlige har givet instruks om eller godkendelse af overførsel af personoplysninger til tredjeland eller international organisation (anfør også overførselsgrundlag efter databeskyttelsesforordningens kapitel 5). | Der må ikke overføres personoplysninger til tredjeland eller internationale organisationer |
| Særlige tekniske eller organisatoriske sikkerhedsforanstaltninger, som skal etableres hos Databehandleren<br><br>(f.eks. sikkerhedsgodkendelse af medarbejdere) | Ikke relevant |
| Beskrivelse af sikkerhedsforanstaltninger ved anvendelse af ad hoc arbejdspladser efter aftale med den Dataansvarlige | Ikke relevant |
| Beskrivelse af sikkerhedsforanstaltninger ved eksterne kommunikationsforbindelser | Adgang til services på NSP sker via LPS- eller EOJ-systemet på sundhedsdatanettet med anvendelse af virkshomhedscertifikat. Brugerne autoriserer sig i LPS- eller EOJ-systemet. |

| | |
|---|---|
| Uddybende beskrivelse af foranstaltninger til beskyttelse af transmission af personoplysninger over åbne netværk | Ikke relevant |
| Opbevaringstid for log (hvis længere end 6 måneder, jf. punkt 5.2 i databehandlerinstruksen). | |
| Evt. aftale om udarbejdelse af revisionserklæring, herunder angivelse af type | ISAE3000 erklæring fremsendes årligt på forlangende fra den dataansvarlige |

**17.3 Kontaktoplysninger i forbindelse med underretning om sikkerhedshændelser**

| | |
|---|---|
| **Kontaktpersoner hos den dataansvarlige ved almindelige afvigelser fra normal drift** | |
| Funktion | SDS National Servicedesk |
| Navn | SDS National Servicedesk |
| E-mail | Se bemærkninger |
| Telefon | 7222 8601 |
| Bemærkninger | https://www.nspop.dk/category/sup |
| **Kontaktpersoner hos den dataansvarlige ved kritiske fejl og sårbarheder samt ved mistanke herom** | |
| Funktion | SDS National Servicedesk |
| Navn | SDS National Servicedesk |
| E-mail | Se bemærkninger |
| Telefon | 7222 8601 |
| Bemærkninger | https://www.nspop.dk/category/sup |
| **Kontaktpersoner hos databehandleren ved almindelige afvigelser fra normal drift** | |
| Funktion | |
| Navn | |
| E-mail | |
| Telefon | |
| Bemærkninger | |
| **Kontaktpersoner hos databehandleren ved kritiske fejl og sårbarheder samt ved mistanke herom** | |
| Funktion | |
| Navn | |
| E-mail | |
| Telefon | |
| Bemærkninger | |

For den Dataansvarlige

Dato:

Navn:

_____

For Databehandleren

Dato:

Navn:

_____

## 18. Bilagsliste

Bilag 1: Databehandlerinstruks
Bilag 2: Sundheds- og Ældreministeriets koncernfælles informationssikkerhedspolitik.

| | |
|---|---|
| For den Dataansvarlige | For Databehandleren |
| Dato: | Dato: |
| Navn: | Navn: |
| _____ | _____ |

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.

Bilag 2

# Informationssikkerhedspolitik

## Sundheds- og Ældreministeriet

| Version | Dato | Ansvarlig | Kommentarer |
|---|---|---|---|
| 1.0 | 20131215 | Pia Jespersen | Godkendt i KLF 20131121 |
| 1.1 | 20151110 | Pia Jespersen | Revision af informationssikkerhedspolitik |
| 1.1 | 20160127 | Pia Jespersen | Rettelser fra KLF møde indføjet. Godkendt i KLF20160126 |
| 1.2 | 20170912 | Pia Jespersen | Rettelse vedr. årlig godkendelse. Forelagt KIS |
| 1.3 | 20180406 | Susanne Lyngby | Tilpasset til Databeskyttelsesforordningen |
| 1.4 | 20180418 | Pia Jespersen | Tilføjelse vedr. koncernfælles funktioner |
| 2.0 | 20180423 | Pia Jespersen | Godkendt i KLF 20180423 |

SUNDHEDS- OG ÆLDREMINISTERIET

## *1. Generelt*

Denne informationssikkerhedspolitik er gældende for hele ministerområdet under **Sundheds- og Ældreministeriet.** Informationssikkerhedspolitikken skal til enhver tid understøtte **Sundheds- og Ældreministeriets** værdigrundlag, vision og de strategiske mål, der fastlægges for organisationen.

Ministeriet har ansvaret for en lang række data, der anvendes til behandlingsformål, kvalitetssikring, forskning, produktion, tilsyn, lægemiddelgodkendelse osv. Data anvendes såvel internt i ministeriet og institutionerne og stilles til rådighed for eksterne parter, herunder brugere andre steder i sundhedsvæsenet.

Dette stiller først og fremmest krav om, at data er tilgængelige for de relevante brugere, når og hvor der er behov for det. **Tilgængelighed** til data skal afpasses efter dette behov.

Tilsvarende er der et krav om **dataintegritet**, dvs. at data, der stilles til rådighed skal være korrekte og opdaterede. Det er særligt kritisk hvor data anvendes direkte i patientbehandling, hvor fejl eller manglende opdateringer kan have betydning for førlighed og helbred.

De oplysninger, der indgår i opgaveløsningen i sundhedsvæsenet, er typisk følsomme oplysninger, herunder personoplysninger, og der er derfor krav om høj grad af **fortrolighed**.

Ministeriets dataanvendelse er meget omfattende og kompleks, og der er behov for at fastlægge sikkerhedsniveauet for anvendelsen konkret i den enkelte databehandling i forhold til vurderingen af risici.

## *2. Formål*

Informationssikkerhedspolitikken skal bidrage til at sikre, at de informationer, som ministeriets institutioner er ansvarlige for, ikke hændeligt eller ulovligt tilintetgøres, fortabes, forringes eller kommer uvedkommende i hænde. Politikken har til formål

- at fastlægge de overordnede normer for informationssikkerhed i **Sundheds- og Ældreministeriet**
- at angive ansvarsfordeling og styring af informationssikkerhed i **Sundheds- og Ældreministeriet**
- at fastlægge et tidssvarende og tilstrækkeligt højt sikkerhedsmæssigt niveau i de it-løsninger, ministeriets institutioner er ansvarlige for
- 
- at skabe rammen for udarbejdelse af retningslinjer og procedurer vedr. informationssikkerhed. Det skal sikres, at der findes de nødvendige vedligeholdelses- og kontrolfunktioner, så informationsbehandlingen kan ske sikkert og i overensstemmelse med den vedtagne politik.

SUNDHEDS-
OG ÆLDREMINISTERIET

### *3. Gyldighedsområde/Omfang*

Informationssikkerhedspolitikken gælder alle institutioner under ministerområdet for **Sundheds- og Ældreministeriet**, hvor informationer behandles, herunder opbevares og anvendes, uanset i hvilken form.

Informationssikkerhedspolitikken omfatter alle brugere – medarbejdere, konsulenter og andre, der midlertidigt eller for en længere periode har adgang til informationer, som **Sundheds- og Ældreministeriet** eller underliggende institutioner er ansvarlige for.

Endvidere gælder politikken for og hos eksterne samarbejdspartnere, der udfører opgaver for **Sundheds- og Ældreministeriet**. Eksterne samarbejdspartnere skal gøres bekendt med og tiltræde relevante dele af Informationssikkerhedspolitikken.

### *4. Organisation og ansvar*

Departementet fører tilsyn med informationssikkerheden inden for ministerområdet. Formålet med departementets tilsyn er løbende at vurdere, om styringen af informationssikkerheden i de underliggende institutioner er tilrettelagt hensigtsmæssigt, pålideligt og sikkerhedsmæssigt forsvarligt, så informationers fortrolighed, integritet og tilgængelighed sikres i overensstemmelse med det regelgrundlag, institutionen er underlagt.

Den enkelte institutions og departementets ledelse har ansvaret for at informationssikkerhedspolitikken implementeres og efterleves inden for hver enkelt institution, herunder udvikling af lokale informationssikkerhedsstrategier og retningslinjer.

Institutioner, der har outsourcet it-driftsopgaver til en leverandør, eller som indgår i et driftsfællesskab har ansvaret for at fastsætte de nødvendige informationssikkerhedsmæssige krav i en aftale med leverandøren eller driftsfællesskabet i overensstemmelse med sikkerhedspolitikken.

Ministerområdets organisering af informationsanvendelsen betyder, at databehandling i vidt omfang foregår på tværs af institutionsgrænser og i samarbejde med enheder/organisationer uden for ministerområdet. Det er særligt vigtigt at være opmærksom på informationssikkerhed i disse relationer.

Der er i Sundhedsdatastyrelsen etableret en sekretariatsfunktion, der skal koordinere informationssikkerhedsarbejdet i hele **Sundheds- og Ældreministeriet**.

Koncernledelsen har til opgave at sikre en tværgående prioritering af økonomi og ressourcer til organisatoriske eller tekniske sikringsforanstaltninger inden for ministeriets område.

SUNDHEDS- OG ÆLDREMINISTERIET

Etablering af informationssikkerhedsudvalg og placering af roller og ansvar i relation til informationssikkerhedsarbejdet, herunder styring af arbejdet med informationssikkerhed, fastlægges for koncernen og for den enkelte institution og beskrives nærmere i henhold til ISO27001, se nedenfor.

## *5. Målsætninger*

Informationssikkerhedsforanstaltninger skal fastlægges ud fra en konkret vurdering og prioritering, idet der skal være et rimeligt forhold mellem nødvendigheden af en foranstaltning, dens effektivitet og omkostning, herunder, at foranstaltningerne skal gennemføres med mindst mulig ulempe for den daglige anvendelse af de informationer, **Sundheds- og Ældreministeriet** og underliggende institutioner er ansvarlige for.

Målene for informationssikkerheden på **Sundheds- og Ældreministeriets** område er at:

- **Sundheds- og Ældreministeriet** lever op til gældende lovgivning og standarder
- **Sundheds- og Ældreministeriet** er og fremstår som en organisation med en pålidelig it-service og med en troværdig beskyttelse af de informationer, den er ansvarlig for
- Der er størst mulig åbenhed om mål og midler i informationssikkerhedsarbejdet
- Alle kender deres rolle og ansvar
- Ingen uvedkommende kan få adgang til informationer eller informationssystemer, der kan anvendes til at skade borgere, patienter, virksomheder, medarbejdere eller **Sundheds- og Ældreministeriet** selv
- Beskytte fysiske personers rettigheder i forbindelse med behandling af personoplysninger ved at sikre, at de behandles på en lovlig, rimelig og gennemsigtig måde
- Personoplysninger indsamles til udtrykkeligt angivne og legitime formål, og ikke viderebehandles på en måde, der er uforenelig med disse formål
- Sikre dataminimering, så personoplysninger er tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt for at opfylde angive formål
- Personoplysninger behandlet inden for ministeriets område er korrekte
- Sikre at personoplysninger anonymiseres eller slettes, når de ikke længere er nødvendige til de formål, hvortil de pågældende personoplysninger behandles
- Etablere passende tekniske og organisatoriske foranstaltninger, der sikrer tilstrækkelig sikkerhed i ministeriets databehandling
- Informationssikkerheden er lokalt forankret og indgår som en naturlig del i det daglige arbejde
- Begrænse konsekvenser af eventuelle skader til en for **Sundheds- og Ældreministeriet** kendt og accepteret størrelse samt sikre, at en videreførelse af databehandlingen efter skade kan ske inden for en accepteret økonomisk ramme og tidshorisont
- Beskytte informationer og systemer ved at opbygge kapacitet til at imødegå og bekæmpe trusler og sårbarheder fra cyberangreb

- Omgåelse eller forsøg på omgåelse af sikkerhedsreglerne opdages og kan tilbageføres til den eller de ansvarlige personer
- Sikre dokumentation for, at organisationen til enhver tid efterlever de opsatte mål

## *6. Retningslinjer for informationssikkerhed*

Beskyttelsen af de informationer, **Sundheds- og Ældreministeriet** er ansvarlig for, skal afstemmes efter risiko, væsentlighed og økonomi samt overholde gældende lovkrav og indgåede aftaler.

Informationssikkerhedspolitikken er baseret på ISO/IEC 27001. Som udgangspunkt skal sikkerhedsniveauet svare til de sikringsforanstaltninger, der er beskrevet her. Hvis sikkerhedsniveauet afviger herfra, skal der foreligge en begrundelse herfor.

Informationssikkerhedspolitikken uddybes i specifikke retningslinjer og forretningsgange, der dækker hovedområderne inden for ISO/IEC 27001:

- Sikkerhedspolitik
- Organisering af informationssikkerhed
- Risikostyring
- Styring af aktiver
- Styring af informationssikkerhed
- Medarbejdersikkerhed
- Fysisk og miljømæssig sikkerhed
- Styring af kommunikation og drift
- Leverandørstyring
- Styring af informationssikkerhedshændelser
- Adgangsstyring
- Anskaffelse, udvikling og vedligeholdelse af it-systemer
- It-beredskabsstyring
- Overensstemmelse med lovbestemte krav

Derudover formuleres der retningslinjer og forretningsgange på baggrund af databeskyttelseslovgivningen samt krav og anbefalinger fra Digitaliseringsstyrelsen og Center for Cybersikkerhed, hvor dette er relevant.

Da der inden for ministerområdet er institutioner af forskellig størrelse og varierende kompleksitet og omfang af it-anvendelse, kan der være områder af de ovenfor nævnte, som ikke er relevante for alle institutioner. Ved udarbejdelse af retningslinjer m.v. tages der højde for dette.

SUNDHEDS- OG ÆLDREMINISTERIET

### 6.1. Risikostyring

Der foretages regelmæssigt en overordnet risikovurdering, så ledelsen kan holde sig informeret om det aktuelle risikobillede. Ligeledes foretages der en risikovurdering ved større forandringer i organisation, arbejdsopgaver eller teknologi. Risikovurderingen er ledelsens beslutningsgrundlag for implementering af nødvendige sikringsforanstaltninger.

I forbindelse med fx ibrugtagning af ny teknologi eller større forandringer i eksisterende teknologi, skal det vurderes, om der skal foretages en konsekvensanalyse. Hvis en behandling af personoplysninger sandsynligvis vil indebære en høj risiko for, at den registrerede får krænket sine rettigheder, foretages der en konsekvensanalyse forud for behandlingen, hvor databeskyttelsesrådgiveren konsulteres.

Hvis konsekvensanalysen viser, at behandlingen vil føre til en høj risiko, som ikke kan begrænses ved at indføre passende foranstaltninger, foretages en forudgående høring af Datatilsynet.

### 6.2. Leverandørstyring

Ved anvendelse af leverandører eller databehandlere i forbindelse med personoplysninger eller andre fortrolige informationer, skal der ved indgåelse af kontrakter eller leverandøraftaler sikres, at der etableres tilstrækkelige organisatoriske og tekniske sikkerhedsforanstaltninger, og der skal sikres løbende kontrol af sikkerheden ved leverandøren gennem ekstern revision, opfølgning på eventuelle observationer og tilsynsbesøg.

I det omfang, at koncernfælles funktioner fungerer som databehandlere for flere institutioner inden for Sundheds- og Ældreministeriet, skal det sikres, at den løbende kontrol og opfølgning på sikkerheden koordineres mellem de institutioner, der anvender databehandleren.

### 6.3. Styring af informationssikkerhedshændelser

Hvis en medarbejder opdager brud eller muligt brud på informationssikkerheden, skal det meddeles til den lokale informationssikkerhedsorganisation.

Ved brud på persondatasikkerheden skal Datatilsynet informeres uden unødig forsinkelse og senest 72 timer efter, at sikkerhedsbristen er opdaget, medmindre det er usandsynligt, at bruddet indebærer risiko for fysiske personers rettigheder.

Hvis et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for den registreredes rettigheder, skal den registrerede underrettes. Dette skal ske uden unødig forsinkelse, og underretningen afhænger ikke af tidspunktet for, hvornår der sker anmeldelse til Datatilsynet.

Medarbejdere, som overtræder informationssikkerhedspolitikken eller deraf afledte retningslinjer, er underlagt de sædvanlige personaleretlige disciplinære sanktioner.

Overtrædelser af straffeloven meldes som udgangspunkt til politiet.

SUNDHEDS- OG ÆLDREMINISTERIET

### 6.4. It-beredskabsstyring

Sundhedsdatastyrelsen har ansvaret for, at der som en del af retningslinjerne foreligger en it-beredskabsplan for håndtering af større informationssikkerhedsmæssige hændelser og tekniske uheld, og at alle relevante personer i organisationen og hos samarbejdspartnere er bekendt med deres pligter og opgaver i forbindelse med sådanne hændelser.

It-beredskabsplanen skal sikre, at skader begrænses mest muligt og at driften i vides muligt omfang kan opretholdes og genoprettes. For forretningskritiske systemer skal der tages stilling til, hvor hurtigt, der skal etableres nøddrift. Der skal foreligge forretningsmæssige nødprocedurer for alle kritiske forretningsområder.

Alle styrelser er part i den koncernfælles it-beredskabsplan. Lægemiddelstyrelsen har endvidere ansvaret for en it-beredskabsplan omfattende it-systemer og -infrastruktur, som ikke indgår i kundeaftalen med Sundhedsdatastyrelsen.

### 6.5. Informationssikkerhedsbevidsthed

Som dataansvarlige myndigheder er det institutionerne under Sundheds- og Ældreministeriets ansvar at tilse, at medarbejdere og øvrige brugere bliver informeret om, hvilket ansvar der påhviler dem, når de behandler informationer, som ministeriet er ansvarlig for.

Medarbejdere og øvrige brugere af disse informationer skal følge informationssikkerhedspolitikken og de retningslinjer, der er afledt heraf.

## *7. Opfølgning og revision*

Informationssikkerhedspolitikken skal revideres ved større ændringer eller som minimum hvert år og godkendes af koncernledelsen.

Hver institution og departementet rapporterer til koncernledelsen en gang om året eller efter behov jf. de gældende aftaler i Departementets tilsynskoncept for ministerområdet.

Godkendt i koncernledelsesforum 23.04.2018