Resumé af Fresenius Kabis bindende virksomhedsregler

Dette dokument er et resumé og erstatter ikke det fulde dokument med bindende virksomhedsregler. Det fulde dokument med bindende virksomhedsregler vil i alle tilfælde være det eneste dokument, der er juridisk gældende.

1 Et passende og ensartet niveau af databeskyttelse

Fresenius skal følge mange databeskyttelseslove verden over. De bindende virksomhedsregler fastsætter et ensartet og passende niveau af databeskyttelse. Dette muliggør intern udveksling af persondata mellem Fresenius' relevante enheder.

2 Gælder verden over

De bindende virksomhedsregler gælder følgende Fresenius-enheder:

- Fresenius Kabi AG, herunder alle datter- og koncernselskaber
- Fresenius Digital Technology (FDT)
- Fresenius SE & Co. KGaA

Gælder visse aktiviteter

De bindende virksomhedsregler gælder følgende aktiviteter vedrørende persondatabehandling:

- Alle aktiviteter i europæiske enheder
- Aktiviteter i ikkeeuropæiske enheder:
  - når de indsamler persondata på vegne af en europæisk Fresenius-enhed, eller
  - når de samarbejder med en europæisk Fresenius-enhed
  - når de modtager persondata fra europæiske enheder
  - når de indsamler persondata fra personer i Europa med henblik på udbydelse af varer og tjenester eller i forbindelse med adfærdsovervågning.

De bindende virksomhedsregler gælder både papir- og IT-baserede processer.

De bindende virksomhedsregler gælder alle processer, der muliggør struktureret søgning på persondata.

3 De bindende virksomhedsregler fastsætter minimumsniveauet

Hvis lokale databeskyttelseslove kræver strengere eller yderligere regler vedrørende persondatabehandling, skal disse også overholdes.

Hvis en lokal lov er i strid med de bindende virksomhedsregler, skal databeskyttelsesrådgiveren underrettes. Databeskyttelsesrådgiveren skal vurdere indvirkningen heraf og løse problemet.

Hvis en enhed modtager en ordre fra en myndighed om at videregive persondata i strid med de bindende virksomhedsregler, skal databeskyttelsesrådgiveren underrettes. Databeskyttelsesrådgiveren skal underrette tilsynsmyndigheden i Tyskland.

4 De bindende virksomhedsregler er bindende for organisationen og vores medarbejdere

De bindende virksomhedsregler skal overholdes og er bindende for:

- alle enheder; de underskriver en kontrakt
- alle medarbejdere; de har pligt til at følge virksomhedens politikker baseret på deres ansættelseskontrakt.

Organisationer og medarbejdere kan opnå rettigheder i henhold til disse forpligtelser.

Håndhævelsen af de bindende virksomhedsregler, herunder de potentielle sanktioner ved overtrædelse, er de samme som ved enhver anden politikovertrædelse.

5 Fresenius har etableret en databeskyttelsesorganisation

Fresenius-koncernen har etableret en organisation, der sikrer intern databeskyttelse, og har udpeget følgende roller og ansvar:

- Databeskyttelsesrådgiveren monitorerer, dvs. tjekker og overvåger, om de bindende virksomhedsregler, lokale love, regler og processer følges. Databeskyttelsesrådgiveren kan foretage revisioner, gennemgange og undersøgelser. Databeskyttelsesrådgiveren er også kontaktpunkt for databeskyttelsesmyndighederne i Europa.

  Kontaktoplysninger:

  Fresenius Kabi AG
  Data Protection Officer
  Else-Kröner-Straße 1
  D-61352 Bad Homburg
  Tyskland
  E-mail: dataprotectionofficer@fresenius.com

  Eller Datatilsynet www.datatilsynet.dk

- Den lokale databeskyttelseskonsulent hjælper og rådgiver lokale medarbejdere og procesejere, når de har spørgsmål eller bekymringer vedrørende databeskyttelse. Den lokale databeskyttelseskonsulent kan på anmodning, hvis der eksempelvis er sproglige udfordringer, yde støtte til den generelle databeskyttelseskonsulent og databeskyttelsesrådgiveren, f.eks. i forbindelse med disses overvågningsfunktion og kontakt med tilsynsmyndigheder.

  Kontrolorgan og ansvarlig lokal enhed for behandling af persondata ligger hos:

  Fresenius Kabi Danmark

  Islands Brygge 57

  2300 København S

  Telefon: 3318 1600

  E-mail: info-dk@fresenius-kabi.com

- Den generelle databeskyttelseskonsulent udfører støtte- og konsulentopgaver for den lokale databeskyttelseskonsulent og er ansvarlig for databeskyttelsessystemet. Den generelle databeskyttelseskonsulent kan på anmodning, hvis der eksempelvis er sproglige udfordringer, yde støtte til databeskyttelsesrådgiveren, f.eks. i forbindelse med dennes overvågningsfunktion og kontakt med tilsynsmyndigheder.

6 8 databeskyttelsesprincipper, der skal følges iht. de bindende virksomhedsregler

Når vi behandler persondata, følger vi en lang række principper for at beskytte personers grundlæggende rettigheder og frihedsrettigheder i henhold til de bindende virksomhedsregler. De enkelte enheder skal opfylde følgende principper, når de behandler persondata:

6.1 Princip 1: Lovlighed

Der skal foreligge et dokumenteret juridisk grundlag for indsamling, anvendelse og behandling af persondata. Der er udarbejdet en ikkeudtømmende liste over juridiske grundlag. Eksempler:

- Databehandlingen er nødvendig for udarbejdelsen af en kontrakt med en person, f.eks. en medarbejder- eller salgskontrakt
- Personen har givet sit samtykke
- Fresenius' legitime interesse er større end de negative konsekvenser for de(n) pågældende person(er)
- Der er behov for at opfylde andre juridiske forpligtelser, f.eks. skattelove, overvågningskrav eller GxP-krav.

Særlige kategorier af data, f.eks. helbredsoplysninger, kræver supplerende juridiske grundlag.

Hvis lokal lovgivning indeholder yderligere eller divergerende bestemmelser, skal disse også følges (kan f.eks. være relevant for medarbejderdata).

6.2 Princip 2: Gennemsigtighed og rimelighed

Personoplysninger skal behandles på en rimelig og gennemsigtig måde. De registrerede personer skal før eller på tidspunktet for indsamling og anvendelse af persondata informeres om følgende:

- Hvem der er ansvarlig, og hvordan vi kan kontaktes
- Hvilke data der indsamles
- Hvordan dataene indsamles
- Hvorfor vi har brug for dataene (formål)
- Hvilke organisationer dataene deles med
- Hvorvidt dataene deles med andre lande
- Hvor længe dataene vil blive opbevaret
- Det juridiske grundlag for indsamling og anvendelse af data samt en nærmere forklaring af dette (princip 1)
- Hvorvidt de registrerede profileres
- Hvorvidt vi træffer automatiserede beslutninger
- Hvorvidt dataene skal afgives, og hvad der sker, hvis de ikke afgives
- Kontaktoplysninger på databeskyttelsesrådgiveren og den relevante myndighed
- De rettigheder, som de registrerede har.

Alle disse oplysninger skal gives på en grundig og letforståelig måde i et klart og enkelt sprog.

6.3 Princip 3: Begrænsning af formålet

Persondata må kun anvendes til de specificerede, eksplicitte og legitime formål, der ligger til grund for indsamlingen. Yderligere anvendelse er ikke tilladt, medmindre en sådan yderligere anvendelse er i overensstemmelse med det oprindelige formål, og/eller hvis der træffes yderligere foranstaltninger.

Yderligere anvendelse, der generelt anses for at være i overensstemmelse med det oprindelige formål, er:

- Arkivering
- Intern revision
- Undersøgelser

Den (lokale eller generelle) databeskyttelseskonsulent kan give vejledning om, hvorvidt en formålsændring kan tillades. Hvis en formålsændring tillades, skal de registrerede informeres om ændringen.

6.4 Princip 4: Dataminimering

Der må kun indsamles og anvendes persondata, der er nødvendige til det definerede formål, sådan som det er formidlet til den registrerede. Det skal således sikres, at persondataene er relevante og passende i omfang i forhold til formålet.

6.5 Princip 5: Nøjagtighed

Persondataene skal være nøjagtige og opdaterede. Der skal anvendes procedurer, som sikrer, at unøjagtige data slettes, rettes eller opdateres så hurtigt som muligt.

6.6 Princip 6: Begrænsning af opbevaringen

Persondata må ikke opbevares længere end nødvendigt for det formål, som de er indsamlet til, medmindre det er påkrævet ved lov. I så fald skal adgangen til dataene være begrænset. Persondata skal slettes eller anonymiseres, hvis der ikke længere foreligger juridisk grund eller formål.

6.7 Princip 7: Sikkerhed, integritet og fortrolighed

Der skal træffes passende tekniske og organisatoriske foranstaltninger til at beskytte persondata mod destruktion, tab, ændring, videregivelse eller adgang til persondata (f.eks. via konceptet passende roller og rettigheder, backup og gendannelse eller ved hjælp af kryptering).

Ved gennemførelsen af sådanne foranstaltninger skal der tages hensyn til risikoen for de registrerede. IT-systemernes sikkerhed skal vurderes i lyset af disse risici, når de installeres og vedligeholdes.

Ethvert sikkerhedsbrud, der kan medføre en risiko for de registrerede, skal dokumenteres og rapporteres til databeskyttelsesorganisationen. Alt efter situationen skal sådanne brud også meddeles til tilsynsmyndigheden, de registrerede eller andre organisationer.

6.8 Princip 8: Ansvarlighed

Overholdelsen af de bindende virksomhedsregler skal kunne dokumenteres. Dette gøres ved at udforme og vedligeholde passende dokumentation som f.eks.:

- fortegnelser over behandlingsaktiviteter
- tekniske og organisatoriske foranstaltninger til opfyldelse af databeskyttelsesprincipperne og håndtering af risiciene.
- risikovurderinger vedrørende databeskyttelse og konsekvensanalyser

6.8.1 Brug af databehandlere

Der må kun benyttes databehandlere, som giver tilstrækkelige garantier i forhold til at gennemføre passende tekniske og organisatoriske foranstaltninger, så databehandlingen opfylder kravene i de bindende virksomhedsregler og de lokale databeskyttelseslove. Dette skal sikres gennem en databeskyttelsesaftale mellem den pågældende enhed og databehandleren.

6.8.2 Videreoverførsel/overførsel af persondata

Der skal gennemføres foranstaltninger til at beskytte overførsler af persondata til andre organisationer uden for EØS i overensstemmelse med de bindende virksomhedsregler. Dette kan gøres ved at blive enige med den pågældende organisation om de af Europa-Kommissionen vedtagne standardkontraktbestemmelser.

7 Risikovurdering vedrørende databeskyttelse

For hver databehandlingsaktivitet skal der foretages en risikovurdering vedrørende databeskyttelse. Vurderingen er en formel procedure til vurdering af aktivitetens betydning for de pågældende registrerede personers rettigheder og frihedsrettigheder.

De identificerede kontrolmangler og potentielle risici skal rapporteres og dokumenteres. Der skal gennemføres tekniske og organisatoriske foranstaltninger til imødegåelse heraf, inden databehandlingsaktiviteten påbegyndes.

8 Konsekvensanalyse vedrørende databeskyttelse

Hvis resultatet af risikovurderingen vedrørende databeskyttelse viser en høj risiko, skal der gennemføres en konsekvensanalyse vedrørende databeskyttelse. Der skal indhentes vejledning hos databeskyttelsesrådgiveren.

Hvis konsekvensanalysen viser et højt risikoniveau for en specifik databehandlingsaktivitet, skal der gennemføres passende tiltag til at mindske sådanne risici, inden behandlingsaktiviteten påbegyndes. Hvis konsekvensanalysen stadig viser et højt risikoniveau efter gennemførelsen af tiltagene, skal den relevante tilsynsmyndighed høres, inden dataene behandles.

9 Individuelle rettigheder

De registrerede skal kunne udøve deres rettigheder:

- **Ret til at tilgå sine persondata**: Den registrerede kan bede om at få adgang til/modtage information om sine persondata, der behandles af Fresenius (f.eks. formålet med databehandlingen, kategorierne af persondata, modtagerne, opbevaringsperioden og eventuel brug af automatiseret beslutningstagning).
- **Ret til at få rettet sine persondata:** Den registrerede kan bede om at få rettet unøjagtige eller ufuldstændige persondata.
- **Ret til at få slettet sine persondata:** Den registrerede kan bede om at få slettet sine persondata, medmindre der er lovkrav om, at de fortsat skal opbevares.
- **Ret til at få begrænset behandlingen af sine persondata:** Den registrerede kan bede om at få begrænset behandlingen af sine persondata, enten hvis nøjagtigheden af persondataene anfægtes, eller hvis databehandlingen er uretmæssig (ikke længere påkrævet til de angivne formål).
- **Ret til at modtage sine persondata i et flytbart format:** Den registrerede kan bede om at få tilsendt sine persondata i et almindeligt anvendt og maskinlæsbart format, hvis følgende betingelser er opfyldt:
    - Den registrerede har afgivet persondata
    - Databehandlingen er baseret på den pågældendes samtykke eller en kontrakt indgået med vedkommende
    - Databehandlingen foretages automatisk.
- **Ret til at gøre indsigelse mod behandlingen af sine persondata:** Den registrerede kan med henvisning til sin personlige situation gøre indsigelse mod behandlingen af sine persondata baseret på en legitim eller offentlig interesse. En sådan henvendelse skal vurderes. Derudover kan den registrerede gøre indsigelse mod direkte markedsføring og profilering. I disse tilfælde skal databehandlingen ophøre.
- **Ret til ikke at være genstand for automatiseret beslutningstagning:** Den registrerede har ret til ikke at være genstand for automatiseret beslutningstagning (herunder profilering), der kan have juridisk eller lignende væsentlig indvirkning på vedkommende, medmindre:
    - det er nødvendigt for indgåelse eller opfyldelse af en kontrakt mellem den registrerede og den pågældende enhed
    - det er baseret på den registreredes udtrykkelige samtykke.

10 Overholdelse af de bindende virksomhedsregler

10.1 Adgang til de bindende virksomhedsregler

De bindende virksomhedsregler skal være tilgængelige for de registrerede personer på en passende måde. De bindende virksomhedsregler vil blive offentliggjort på inter- eller intranettet.

De registrerede kan også få adgang til de bindende virksomhedsregler ved at kontakte den relevante databeskyttelsesrådgiver eller en medarbejder i databeskyttelsesorganisationen.

10.2 Håndtering af klager relateret til de bindende virksomhedsregler

Den enkelte registrerede har ret til:

- at klage over overtrædelse af de bindende virksomhedsregler, lokale databeskyttelseslove, ordrer fra tilsynsmyndigheder, interne politikker og retningslinjer eller frivillige forpligtelser relateret til databeskyttelse
- at benytte sine individuelle rettigheder
- at påberåbe sig enhver anden rettighed iht. de bindende virksomhedsregler.

En sådan klage kan f.eks. indgives via telefon, e-mail eller brev, mundtligt ved henvendelse til den relevante databeskyttelsesrådgiver, den relevante (lokale) databeskyttelseskonsulent eller via vores klagehotline.

Hvis klagen vurderes at være berettiget, vil enheden træffe passende tiltag for at behandle klagen og underrette den registrerede inden for en måned.

10.3 Erstatningsansvar og håndhævelse

Registrerede, der har lidt skade eller lignende som følge af behandlingen af deres persondata, har ret til at påberåbe sig disse dele af de bindende virksomhedsregler og få tilkendt erstatning ved en kompetent domstol (hvis relevant).

Hvis det påvises, at parter uden for EU/EØS har overtrådt reglerne, vedkender FSE sig sit erstatningsansvar over for de registrerede. Den enhed, der har forårsaget skaden, skal bistå FSE i rimeligt omfang med henblik på at sikre en rettidig behandling af sådanne klager eller anmodninger.

10.4 Samarbejde med tilsynsmyndighederne

Den enkelte enhed skal samarbejde med tilsynsmyndighederne, efterleve rådgivningen vedrørende fortolkningen af de bindende virksomhedsregler og acceptere at blive revideret af de relevante tilsynsmyndigheder.

10.5 Kurser

Den enkelte enhed skal gøre det obligatorisk for sine medarbejdere at deltage i kurser vedrørende de bindende virksomhedsregler og databeskyttelse, herunder regelmæssige vedligeholdelseskurser. Der skal gennemføres generelle kurser mindst to gange om året for alle relevante medarbejdere. Derudover tilbydes der rollespecifikke kurser (f.eks. for HR- eller indkøbsafdelinger) for at tage højde for de specifikke behov hos visse roller/personer.

10.6 Revision

Alle parter skal være indstillet på at blive underkastet regelmæssig revision (planlagt revision eller ad hoc-revision), så det kan vurderes og testes, om de bindende virksomhedsregler bliver overholdt, og så der kan gennemføres passende og tilstrækkelige afhjælpningsmekanismer, hvis en enhed ikke overholder de bindende virksomhedsregler. Databeskyttelsesorganisationen følger op på en eventuel gennemført revision for at vurdere, om de foreslåede korrigerende handlinger er blevet korrekt gennemført, og dokumentere resultaterne i revisionsrapporten. Den enkelte enhed skal efter anmodning stille revisionsrapporter til rådighed for tilsynsmyndighederne.

10.7 Opdatering af de bindende virksomhedsregler

Parterne skal gennemgå de lokale databeskyttelseslove og angive, om det er nødvendigt at foretage ændringer i de bindende virksomhedsregler. Fresenius kan om nødvendigt foretage ændringer i de bindende virksomhedsregler. Alle væsentlige ændringer i de bindende

virksomhedsregler vil omgående blive rapporteret til den enkelte enhed og tilsynsmyndigheden. Andre mindre væsentlige ændringer i de bindende virksomhedsregler vil blive rapporteret til parterne så hurtigt som praktisk muligt.

11 Håndtering af enheder, der ikke længere er omfattet af reglerne

Hvis en enhed ophører med at tilslutte sig de bindende virksomhedsregler (dvs. ved opsigelse af den koncerninterne aftale), skal enheden enten

- returnere alle persondata til de parter, som der er modtaget data fra, eller
- destruere alle de pågældende persondata i henhold til de lokale opbevaringsregler, eller
- sikre tilstrækkelig beskyttelse af de pågældende persondata (f.eks. ved at blive enige om standardkontraktbestemmelser).