UDENRIGSMINISTERIET

PERSONDATAPOLITIK FOR BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I UDENRIGSMISTERIET

INDHOLD

1. BAGGRUND

Europa-Parlamentet og Rådet har ved forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (herefter benævnt databeskyttelsesforordningen) vedtaget nye regler om behandling af personoplysninger. Fra og med den 25. maj 2018 gælder data-beskyttelsesforordningen direkte i alle medlemslande.

Herudover vil der i Danmark også fra den 25. maj 2018 gælde lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter benævnt data-beskyttelsesloven), som er vedtaget den 17. maj 2018.

De nye regler viderefører til dels tidligere regler om behandling og beskyttelse af persondata , men indfører også væsentligt stram-mere regler på bestemte områder.

2. FORMÅL

Formålet med Udenrigsministeriets persondatapolitik for behandling og beskyttelse af personoplysninger (herefter benævnt persondatapolitikken) er at fastlægge rammerne for behandling og beskyttelse af personoplysninger i Udenrigsministeriet. Denne politik skal være med til at sikre, at Udenrigsministeriet behandler personoplysninger i overensstemmelse med gældende regler samt politikker og retningslinjer herfor. Endvidere har persondatapolitikken til formål at sikre, at der i Udenrigsministeriet sker en løbende kontrol med efterlevelsen af de til enhver tid gældende regler samt politikker og retningslinjer for behandling og beskyttelse af personoplysninger.

Udenrigsministeriets udarbejder løbende politikker, retningslinjer og skabeloner, som vil blive udgivet på Persondata-portalen. Her vil der også være link til Datatilsynets vejledninger og skabeloner, som bl.a. kan anvendes i de tilfælde, hvor Udenrigsministeriet endnu ikke har udarbejdet egne vejledninger eller skabeloner.

3. OMFANG

Udenrigsministeriets persondatapolitik finder anvendelse i hele Udenrigsministeriets departement, dvs. i forhold til behandling af persondata i både hjemmetjenesten og på de danske repræsentationer i udlandet.

Persondatapolitikken finder også anvendelse for de af Udenrigsministeriets samarbejdspartnere, der udfører opgaver vedrørende behandling og beskyttelse af personoplysninger på Udenrigsministeriets vegne, f.eks. i kraft af en databehandleraftale.

Fiskeristyrelsen er en del af Udenrigsministeriets ressort og hører under ministeren for fiskeri og ligestilling og ministeren for nordisk samarbejde. Fiskeristyrelsen har, som selvstændig offentlig myndighed, selv ansvaret for styrelsens overholdelse af gældende regler om behandling og beskyttelse af personoplysninger. Persondatapolitikken finder ikke anvendelse for Fiskeristyrelsen.

4. DEFINITIONER

I denne persondatapolitik benyttes følgende definitioner:

- **Personoplysninger**
  Enhver form for information om en fysisk person, der enten i sig selv identificerer personen, eller som kan være med til at identificere personen. Der er tale om al information, der direkte eller indirekte kan identificere en fysisk person. Også en kombination af forskellige oplysninger kan identificere en person, ligesom oplysninger, som kun særligt indviede personer vil kunne identificere en fysisk person ud fra, er omfattet af begrebet.

  Begrebet "personoplysninger" skal fortolkes bredt.

- **Behandling (af personoplysninger)**
  Enhver aktivitet eller række af aktiviteter, som personoplysninger gøres til genstand for. Det kan f.eks. være indsamling, registrering, organisering, systematisering, opbevaring, ændring, søgning, formidling, videregivelse, genfinding og sletning mv.

  Begrebet "behandling" skal fortolkes bredt.

- **Den registrerede person**
  Den fysiske person, som de behandlede personoplysninger vedrører. Det kan f.eks. være en borger, en kunde, en medarbejder, en leverandør eller en samarbejdspartner m.fl.

- **Dataansvarlig**
  Den person eller institution, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger.

  Hvis Udenrigsministeriet er dataansvarlig, vil det som udgangspunkt være ministeriet som sådan (myndigheden), der er dataansvarlig.

- **Databehandler**
  Den person eller institution, der behandler personoplysninger på den dataansvarliges vegne, dvs. arbejder efter og under instruks fra den dataansvarlige.

- **Risiko for den registrerede person**
  Risikoen for, at den registrerede person udsættes for en fysisk, materiel eller immateriel skade, herunder tab af kontrol over sine personoplysninger, begrænsning af sine rettigheder, forskelsbehandling, identitetstyveri, finansielle tab eller sociale konsekvenser som f.eks. skade på omdømme.

- **Sikkerhedsforanstaltninger**
  (også kaldet sikkerhedskontroller)
  Sikkerhedsforanstaltninger omfatter såvel tekniske som organisatoriske sikkerhedsforanstaltninger og skal være med til at sikre, at uvedkommende ikke får adgang til systemer mv., der håndterer personoplysninger.

  Tekniske sikkerhedsforanstaltninger kan bl.a. omfatte autorisation og adgangskontroller, logning, kryptering, firewalls og antivirusprogrammer samt VPN og kryptering ved fjernarbejdspladser og brug af mobile devices, etc.

  Organisatoriske sikkerhedsforanstaltninger kan bl.a. bestå i at Udenrigsministeriets medarbejdere er instrueret i og uddannet til at håndtere behandlingen af personoplysninger korrekt og sikkert, samt foranstaltninger vedrørende den fysiske sikkerhed, herunder fysisk adgangskontrol, etc.

  Ovenstående eksempler på tekniske og organisatoriske foranstaltninger er ikke udtryk for en udtømmende opregning.

- **Udenrigsministeriet**
  Udenrigsministeriets departement dvs. både ude- og hjemmetjenesten.

- **Enhed**
  Et kontor eller en repræsentation inden for Udenrigsministeriets departement.

5. ROLLER OG ANSVAR

Nedenstående skema giver et overblik over roller og ansvar i Udenrigsministeriet i relation til behandling og beskyttelse af personoplysninger.

Ledelse og medarbejdere i Udenrigsministeriet er forpligtet til at handle i henhold til nedenstående i forhold til de til enhver gældende regler for behandling og beskyttelse af personoplysninger.

Gruppe / funktion	Roller og ansvar
Øverste ledelsesniveau (Direktionen)	Den øverste ledelse (dvs. direktionen i Udenrigsministeriet) har det overordnede og endelige ansvar for, at Udenrigsministeriet efterlever gældende regler om behandling og beskyttelse af personoplysninger, herunder reglerne i databeskyttelsesforordningen. Den øverste ledelses rolle er at træffe endelige beslutninger om behandlingen og beskyttelsen af personoplysninger i Udenrigsministeriet.
Daglig ansvarlig leder	Den daglige ansvarlige leder er den person, der inden for en enhed har det daglige ansvar for, at enheden administrerer i overensstemmelse med gældende regler om behandling og beskyttelse af personoplysninger, herunder bl.a. at sikre, at persondatapolitikken samt tilhørende retningslinjer er kommunikeret klart og tydeligt til medarbejderne i enheden. Den daglige ansvarlige leder har en koordinerende rolle i forhold til at implementere de sikkerhedstiltag, som der er vurderet et behov for i forhold til behandlingen og beskyttelsen af personoplysninger i enheden. I Udenrigsministeriet er den daglige ansvarlige leder enhedschefen.

Gruppe / funktion	Roller og ansvar
Databeskyttelsesrådgiver (DPO)	Databeskyttelsesrådgiverens rolle er at yde rådgivning og vejledning om persondataret og persondatabeskyttelse til ministeriets organisation samt at kontrollere, at Udenrigsministeriet overholder gældende regler for behandling og beskyttelse af personoplysninger. Databeskyttelsesrådgiveren er endvidere Udenrigsministeriets kontaktperson udadtil, i forhold til registrerede personer, i forhold til tilsynsmyndighederne og i forhold til andre samarbejdspartnere. Databeskyttelsesrådgiveren rapporterer til det øverste ledelsesniveau.
Systemejer	Systemejeren er den ansvarlige for driften og vedligeholdelsen af et system, der indeholder og behandler personoplysninger. I Udenrigsministeriet opereres der dels med "forretningssystemer", der anvendes af alle enheder og medarbejdere, f.eks. F2, og dels "fagsystemer", der kun anvendes af én eller enkelte enheder, f.eks. UM-VIS. Der er udpeget en ansvarlig systemejer for alle systemer i Udenrigsministeriet. Listen over systemejere kan findes her: Systemejerlisten.
Medarbejdere	Medarbejdere, der behandler personoplysninger, er ansvarlige for at gøre sig bekendt med formålene med behandlingen, samt de regler, politikker og retningslinjer, der er relevante for udførelsen af deres arbejde i forbindelse med behandling og beskyttelse af personoplysninger.

6. ANSVARLIGHED

Udenrigsministeriet udviser altid ansvarlighed, når der foretages behandling af personoplysninger. Det sker bl.a. ved at dokumentere:

- de beslutninger, der træffes
- de foranstaltninger og aktiviteter, der udføres, samt
- de retningslinjer og kontroller, der implementeres om behandlingen og beskyttelsen af personoplysninger.
- Samtlige ansatte i Udenrigsministeriet er forpligtet til at kende og holde sig opdateret om ministeriets persondatapolitik samt ministeriets retningslinjer om behandling og beskyttelse af persondata. Retningslinjerne kan findes på intranettet under Politik og retningslinjer.

7. GRUNDPRINCIPPERNE FOR BEHANDLING AF PERSONOPLYSNINGER

Formålet er at fastlægge de overordnede rammer for, hvordan Udenrigsministeriet lovligt og forsvarligt behandler og beskytter personoplysninger.

Databeskyttelsesforordningens artikel 5, 6 og 9.

I Udenrigsministeriet behandles personoplysninger i overensstemmelse med de gældende regler i databeskyttelsesforordningen, herunder de grundprincipper for lovlig behandling i forordningens artikel 5, der gælder for al behandling af personoplysninger.

Det betyder, at personoplysninger kun behandles til lovlige, rimelige og legitime formål, der kan dokumenteres.

Udenrigsministeriet indsamler, opbevarer og behandler mv. kun personoplysninger, der er nødvendige for varetagelsen og opfyldelsen af det eller de angivne formål med behandlingen. Indsamlingen og behandlingen mv. af personoplysninger vil i den forbindelse blive minimeret til det, der er absolut nødvendigt af hensyn til opgavevaretagelsen.

Udenrigsministeriet begrænser behandlingen af personoplysninger, således at personoplysninger ikke behandles på en måde, der er uforeneligt med det formål, hvortil personoplysningerne oprindeligt blev indsamlet.

Endvidere sikrer Udenrigsministeriet, at personoplysninger ikke opbevares i et længere tidsrum, end hvad der er nødvendig for at opfylde formålet med behandlingen.

Når behandlingen af personoplysninger ikke længere er nødvendig, sikres det, at oplysningerne enten slettes i overensstemmelse med forordningens regler om sletning, eller at der træffes andre tekniske eller organisatoriske foranstaltninger, således at den registrerede ikke længere kan identificeres ud fra oplysningerne.

Såfremt behandlede personoplysninger viser sig at være urigtige, ufuldstændige eller mangelfulde i forhold til de formål, hvortil de er indsamlet og behandles, vil de blive rettet, opdateret eller slettet i overensstemmelse med forordningens regler.

Kravene til grundprincipperne for behandling af personoplysninger vil blive uddybet i "Retningslinje om lovlig behandling af personoplysninger".

Kravene til opbevaring mv. vil blive uddybet i "Retningslinje om opbevaringsbegrænsning, herunder om sletning og anonymisering af personoplysninger".

8. LOVLIG BEHANDLING AF PERSONOPLYSNINGER

Formålet er at sikre, at Udenrigsministeriet kun behandler personoplysninger, når der foreligger et lovligt behandlingsgrundlag (hjemmel) herfor.

Databeskyttelsesforordningens artikel 6-10.

Udenrigsministeriet sikrer, at der altid foreligger et lovligt behandlingsgrundlag (hjemmel) for behandlingen af personoplysninger.

Der skal således altid foreligge et af databeskyttelsesforordningens behandlingsgrundlag (hjemler), herunder særligt mindst ét af følgende behandlingsgrundlag:

Behandlingsgrundlag (hjemmel) for behandling af almindelige personoplysninger, jf. databeskyttelsesforordningens artikel 6:

- **Samtykke** – den registrerede person har givet samtykke til behandling af sine almindelige personoplysninger til et eller flere specifikke formål, jf. art. 6, stk. 1, litra a.
- **Kontrakt** – behandlingen er nødvendig for at kunne opfylde eller indgå en kontrakt, som den registrerede person er en del af, jf. art. 6, stk. 1, litra b.
- **Retlig forpligtelse** – behandlingen er nødvendig for at overholde en retlig forpligtelse. En retlig forpligtelse kan f.eks. være fastsat ved lov eller i en bekendtgørelse, eller følge af internationale regler, herunder EU-retlige regler, jf. art. 6, stk. 1, litra c.
- **Vitale interesser** – behandlingen er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser, jf. art. 6, stk. 1, litra d.

- **Samfundsmæssig interesse** – behandlingen er nødvendig for at kunne udføre en opgave i samfundets interesse, jf. art. 6, stk. 1, litra e.
- **Offentlig myndighedsudøvelse** – behandlingen er nødvendig for at kunne udføre en opgave, der hører under offentlig myndighedsudøvelse, jf. art. 6, stk. 1, litra e.

Behandlingsgrundlag (hjemmel) for behandling af følsomme personoplysninger, jf. databeskyttelsesforordningens artikel 9:

- **Samtykke** – den registrerede person har givet udtrykkeligt samtykke til behandling af sine følsomme personoplysninger til et eller flere specifikke formål, jf. art. 9, stk. 2, litra a.
- **Arbejds-, sundheds- og socialretlige forpligtelser og rettigheder** – behandlingen er nødvendig for at overholde den dataansvarliges eller den registrerede persons arbejds-, sundheds-, og socialretlige forpligtelser og specifikke rettigheder, jf. art. 9, stk. 2, litra b.
- **Vitale interesser** – behandlingen er nødvendig, for at beskytte den registreredes eller en anden fysisk persons vitale interesser, i tilfælde, hvor vedkommende er ude af stand til selv at afgive samtykke til behandlingen, jf. art. 9, stk. 2, litra c.
- **Offentliggjort af den registrerede person** – den registrerede person har selv offentliggjort personoplysningerne, jf. art. 9, stk. 2, litra e.
- **Retskrav** – behandlingen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares, jf. art. 9, stk. 2, litra f.
- **Samfundsmæssig interesse** – behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser, jf. art. 9, stk. 2, litra g.
- **Forebyggende medicin eller diagnostik** – behandlingen er nødvendig med henblik på forebyggende medicin eller forebyggelse af arbejds- og miljørelaterede sygdomme, jf. art. 9, stk. 2, litra h.

- **Samfundsinteresser på folkesundhedsområdet** – behandlingen er nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet, jf. art. 9, stk. 2, litra i.
- **Arkiv, videnskabelige, historiske og statistiske formål** – behandlingen er nødvendig til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål, jf. art. 9, stk. 2, litra j.

SAMTYKKE

Såfremt behandlingen foretages på baggrund af et indhentet samtykke fra den registrerede person, sikrer Udenrigsministeriet, at samtykket er afgivet frivilligt samt at erklæringen om samtykke er formuleret i et let forståeligt sprog, så den registrerede person ikke er tvivl om, hvad der gives samtykke til. Endvidere sikres det, at samtykket er afgivet ved en aktiv handling, således at den registrerede f.eks. skal klikke "okay" eller "ja", skrive under eller lign. for at acceptere samtykket.

Endelig sikres det, at den registrerede person bliver oplyst om, at samtykket altid kan trækkes tilbage.

Ovenstående beskrivelse af behandlingsgrundlag efter databeskyttelsesforordningens artikel 6 og 9 er ikke udtryk for en udtømmende opregning. Kravene til et lovligt behandlingsgrundlag vil blive uddybet i "Retningslinje om lovlig behandling af personoplysninger".

Kravene til et lovligt samtykke vil blive uddybet i "Retningslinje om samtykke som behandlingsgrundlag".

9. OVERFØRSEL AF PERSONOPLYSNINGER TIL LANDE UDEN FOR EU OG EØS (TREDJELANDE)

Formålet er at sikre, at der ikke overføres personoplysninger til lande uden for EU/EØS, uden at Udenrigsministeriet har et lovligt grundlag herfor.

Databeskyttelsesforordningens artikel 44-50.

En overførsel til et tredjeland eller en international organisation dækker både over den situation, hvor Udenrigsministeriet videregiver personoplysninger til en dataansvarlig uden for EU, og den situation, hvor Udenrigsministeriet overlader en behandling af personoplysninger til en databehandler uden for EU.

En overførsel kan ske ved f.eks. fremsendelse af oplysninger elektronisk, fremsendelse af en USB nøgle, eller at der f.eks. gives en ekstern konsulent uden for EU adgang til at kunne se oplysninger i et af Udenrigsministeriets systemer.

Tredjelande er alle andre lande end EU- og EØS-lande (Island, Liechtenstein og Norge).

Udenrigsministeriet overfører kun personoplysninger til lande uden for EU og EØS, såfremt der foreligger et lovligt, rimeligt og legitimt grundlag herfor, og såfremt der kan sikres et tilstrækkeligt beskyttelsesniveau i overensstemmelse med reglerne herom i databeskyttelsesforordningen.

Kravene til overførsel af personoplysninger til tredjelande, herunder om sondringen mellem sikre og usikre tredjelande, vil blive uddybet i "Retningslinje om overførsel af personoplysninger til lande uden for EU og EØS".

10. FORTEGNELSER OVER BEHANDLINGSAKTIVITETER

Formålet er at sikre, at Udenrigsministeriet fører de nødvendige fortegnelser over behandlingsaktiviteter, for at have et samlet overblik over disse, samt kunne fremvise fortegnelserne for tilsynsmyndighederne på deres anmodning, idet forordningen stiller krav herom.

Endvidere er formålet at sikre, at der foreligger et grundlag for vurderingen af risikoen ved behandlingen af de registrerede personers personoplysninger.

Databeskyttelsesforordningens artikel 30.

I overensstemmelse med reglerne i databeskyttelsesforordningens artikel 30 fører Udenrigsministeriet en række fortegnelser over de behandlinger af personoplysninger (behandlingsaktiviteter), som ministeriet foretager. Fortegnelserne opdateres løbende. Der er for de enkelte fortegnelser udpeget én eller flere enhed(er) i ministeriet, der er ansvarlig for den løbende opdatering.

Fortegnelserne skal stilles til rådighed for Datatilsynet, ved tilsyn, som dokumentation for ministeriets behandlingsaktiviteter. Endvidere har fortegnelserne til formål, at danne grundlag for vurdering af risiciene for den registrerede ved Udenrigsministeriets behandling af dennes personoplysninger.

Kravene til fortegnelserne vil blive uddybet i "Retningslinje om fortegnelser efter artikel 30".

11. DEN REGISTRERERE PERSONS RETTIGHEDER

Formålet er at sikre at behandlingen af personoplysninger tilgodeser den registrerede persons ret til at kontrollere hvornår, hvordan og i hvilket omfang dennes personoplysninger bliver behandlet i Udenrigsministeriet.

Databeskyttelsesforordningens artikel 12-23.

Udenrigsministeriet sikrer den registrerede persons rettigheder ved bl.a. at behandle personoplysninger på en åben og oplyst måde.

Det betyder, at Udenrigsministeriet oplyser en registreret person om, at ministeriet behandler dennes personoplysninger, samt om, hvordan de behandles. På den baggrund har en registreret person mulighed for at gøre sine rettigheder i henhold til databeskyttelsesforordningen og anden relevant persondataretlig lovgivning gældende over for Udenrigsministeriet.

Herudover hjælper Udenrigsministeriet den registrerede person med at udøve sine rettigheder og ministeriet håndterer anmodninger fra en registreret person, som gør sine rettigheder gældende.

Kommunikation til og med den registrerede person sker altid i kortfattet form og i et klart og letforståeligt sprog.

Nedenfor er listet, hvilke rettigheder Udenrigsministeriet hjælper den registrerede person med, såfremt vedkommende anmoder herom:

- Indsigt i de behandlinger af personoplysninger, som Udenrigsministeriet foretager om en registreret person (indsigtsretten), jf. art. 15.

- Berigtigelse, såfremt behandlede personoplysninger om en registreret person er forkerte eller mangelfulde, jf. art. 16.
- Sletning af behandlede personoplysninger om en registreret person., jf. art. 17.
- Begrænsning af behandling af personoplysninger om en registreret personer, jf. art. 18.
- Udlevering af personoplysninger samt transmission heraf til anden dataansvarlig (dataportabilitet), jf. § 20.
- Behandling af indsigelser fra en registreret person mod behandling af dennes personoplysninger, jf. art. 21.

Såfremt Udenrigsministeriet træffer afgørelser, som betydeligt påvirker den registrerede person, sikres det, at en sådan afgørelse ikke udelukkende er truffet ved en automatisk behandling eller profilering.

Udenrigsministeriet videregiver ikke personoplysninger til andre, medmindre den registrerede person har givet samtykke til dette eller Udenrigsministeriet er retligt forpligtet og berettiget til at videregive personoplysningerne. Det vil være tilfældet, hvis der foreligger det fornødne behandlingsgrundlag (hjemmel) herfor i enten databeskyttelsesforordningen eller andet retsgrundlag.

Såfremt Udenrigsministeriet har videregivet personoplysninger til andre uden for Udenrigsministeriet, sikres det, at modtagerne af personoplysningerne informeres om enhver berigtigelse, sletning eller begrænsning, som Udenrigsministeriet har truffet foranstaltninger om, jf. artikel 19, i databeskyttelsesforordningen.

Kravene til den registreredes rettigheder vil blive uddybet i "Retningslinje om de registreredes rettigheder".

12. DATAANSVARLIG OG DATABEHANDLER

Formålet er at sikre, at det er afklaret, hvorvidt Udenrigsministeriet er dataansvarlig eller databehandler i forhold til processer, der involverer behandling af personoplysninger.

Endvidere er formålet at sikre, at der er overblik over, hvilke databehandlere Udenrigsministeriet benytter, og at der er indgået de nødvendige databehandleraftaler.

Databeskyttelsesforordningens artikel 24-29.

Når Udenrigsministeriet behandler personoplysninger, vurderes det, hvornår Udenrigsministeriet er henholdsvis dataansvarlig, databehandler eller har et fælles/delt dataansvar med en anden institution (fælles dataansvarlige).

12.1 DATAANSVARLIG

Såfremt Udenrigsministeriet er dataansvarlig, sikres det, at de databehandlere der benyttes, kan stille de fornødne sikkerhedsgarantier for behandlingen og beskyttelsen af personoplysninger. Endvidere sikres det, at databehandlerne er instrueret i, hvordan de må behandle personoplysninger på Udenrigsministeriets vegne, samt at der er indgået en databehandleraftale, der overholde de til enhver tid gældende regler herfor.

12.2 DATABEHANDLER

Såfremt Udenrigsministeriet er databehandler, sikres det, at ministeriet kun behandler personoplysninger under instruks fra den dataansvarlige.

Endvidere sikres det, at Udenrigsministeriet ikke gør brug af andre databehandlere (underdatabehandlere) uden at anvendelsen heraf er godkendt af den dataansvarlige.

Såfremt anvendelsen af andre databehandlere (underdatabehandlere) er skriftligt godkendt af den dataansvarlige, sikres det, at den dataansvarlige underrettes, såfremt Udenrigsministeriet planlægger at udskifte anvendte databehandlere (underdatabehandlere) eller indgå aftale med nye, således at den dataansvarlige får mulighed for at gøre indsigelser mod sådanne ændringer.

Såfremt den dataansvarlige har godkendt, at Udenrigsministeriet bruger andre databehandlere (underdatabehandlere), sikres det, at de som minimum lever op til de krav, som den dataansvarlige har stillet til Udenrigsministeriet.

12.3 FÆLLES/DELT DATAANSVAR (FÆLLES DATAANSVARLIGE)

Hvis Udenrigsministeriet er fælles dataansvarlig med en anden institution, sikres det, at Udenrigsministeriet har fastlagt det delte ansvar i forhold til overholdelse af de til enhver tid gældende regler for behandling og beskyttelse af personoplysninger. Endvidere sikres det, at de forpligtelser, som Udenrigsministeriet har over for en registreret person, overholdes, herunder at det er fastlagt, hvem der gør oplysningerne tilgængelige for den registrerede person, samt at dette sker på en åben og oplyst måde. Den registrerede person kan dog altid frit vælge, hvilken dataansvarlig vedkommende vil udøve sine rettigheder over for.

Kravene, der stilles til henholdsvis dataansvarlige og databehandlere, vil blive uddybet i "Retningslinje om dataansvarlig, databehandler og fælles/delt dataansvar", mens kravene til databehandleraftaler vil blive uddybet i "Retningslinje om databehandleraftaler".

13. RISIKOVURDERING AF UDENRIGSMINISTERIETS BEHANDLING AF DEN REGISTREREDES PERSONOPLYSNINGER

Formålet er at identificere, hvilke potentielle risici for den registrerede person, der kan være i forbindelse med Udenrigsministeriets behandling af dennes personoplysninger.

Når Udenrigsministeriet behandler personoplysninger, vurderer ministeriet risiciene for den registrerede person ved behandlingen af dennes personoplysninger. Vurderingen foretages på baggrund af de foretagne behandlingsaktiviteter, herunder de anvendte systemer. Derved skabes et samlet overblik over de potentielle risici forbundet med en behandling.

Risiciene er beregnet og identificeret på baggrund af en mulig konsekvens for den registrerede person ved behandlingen af dennes personoplysninger, samt sandsynligheden for at konsekvensen indtræffer.

Risikovurderingen er dokumenteret og godkendes af det øverste ledelsesniveau.

Metoden til vurderingen af risiciene for den registrerede person ved behandling af dennes personoplysninger vil blive uddybet i "Retningslinje om risikovurdering for den registrerede".

14. KONSEKVENSANALYSER (DPIA)

Formålet er at sikre, at der foretages konsekvensanalyser forud for behandlingen af personoplysninger, der sandsynligvis indebærer en høj risiko for den registrerede person, for dermed at identificere tiltag, der kan reducere denne risiko.

Databeskyttelsesforordningens artikel 35 og 36.

Hvis det i forbindelse med registreredes risikovurdering er vurderet, at en bestemt behandling af personoplysninger sandsynligvis vil indebære en høj risiko for de registreredes rettigheder, udfører Udenrigsministeriet en konsekvensanalyse.

Konsekvensanalysen skal hjælpe med at fastlægge de foranstaltninger, som Udenrigsministeriet påtænker kan imødegå de risici, der er forbundet med en behandling af personoplysninger, der vurderes at indebære en bestemt høj risiko for de registrerede personer.

Såfremt de påtænkte tekniske og organisatoriske sikkerhedsforanstaltninger ikke i tilstrækkeligt omfang kan imødegå risiciene for de registrerede personer, rådfører Udenrigsministeriet sig hos Datatilsynet, inden ministeriet foretager den pågældende behandling af personoplysningerne. Udenrigsministeriet skal altid inddrage DPO'en i forbindelse med udarbejdelse af en DPIA.

Kravene til udarbejdelse af konsekvensanalyser vil blive uddybet i "Retningslinje om konsekvensanalyser (DPIA)".

15. BEHANDLINGSSIKKERHED

Formålet er at sikre, at der i Udenrigsministeriet er en tilstrækkelig sikkerhed ved behandlingen af personoplysninger, som afdækker de identificerede risici i risiko- og konsekvensanalyserne.

Databeskyttelsesforordningens artikel 25 og 32.

Udenrigsministeriet sikrer, at der vedvarende opretholdes et tilstrækkeligt sikkerhedsniveau – både teknisk og organisatorisk – ved behandlingen af personoplysninger.

15.1 SIKKERHEDSSTYRING

På baggrund af de udarbejdede risiko- og konsekvensanalyser defineres det, hvilket sikkerhedsniveau og hvilke sikkerhedstiltag, der skal implementeres for at sikre et tilstrækkeligt beskyttelsesniveau, når Udenrigsministeriet foretager behandling af personoplysninger.

I den forbindelse overvejes følgende forhold, jf. også artikel 32 i databeskyttelsesforordningen:

- Brugen af pseudonymisering, kryptering og anonymisering.
- Sikring af fortrolighed og integritet.
- Systemers tilgængelighed og modstandsdygtighed (robusthed).
- Muligheden for at genskabe tilgængelighed og adgang til behandlede personoplysninger inden rimelig tid (backup).
- De identificerede risici, som behandlingen af personoplysninger kan indebære, herunder hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til de behandlede personoplysninger, som kan føre til fysisk, materiel eller immateriel skade for den registrerede person.

Udenrigsministeriet vurderer løbende proceduren for sikkerhedstiltag. Ved ændringer testes og evalueres sikkerheden, for at sikre at sikkerhedsniveauet fortsat og til enhver tid er tilstrækkeligt.

15.2 DATABESKYTTELSE GENNEM DESIGN OG STANDARDINDSTILLINGER

Udenrigsministeriet sikrer, at løsninger, som ministeriet udvikler fremadrettet til brug for behandling og beskyttelse af personoplysninger, designes således at de reducerer graden af indgriben i den registrerede persons privatliv.

Endvidere efterstræbes det, at løsninger, der anvendes til behandling af personoplysninger, har sikkerhedsindstillingerne slået til som standard, således at der ikke indhentes eller behandles flere personoplysninger, end hvad der er nødvendigt til at opfylde behandlingens formål, samt at personoplysninger ikke opbevares i længere tid end nødvendigt.

Herudover sikres det, at personoplysninger ikke stilles til rådighed for andre, uden at der har været en fysisk person involveret, hvilket betyder, at udlevering af personoplysninger til andre ikke må ske automatisk, f.eks. som følge af en proces.

Kravene, der skal sikre en tilstrækkelig behandlingssikkerhed af personoplysninger, vil blive uddybet i "Retningslinje om behandlingssikkerhed af personoplysninger, herunder om sikker kommunikation mv.".

16. UDENRIGSMINISTERIETS PROCEDURE VED BRUD PÅ PERSONDATASIKKERHEDEN

Formålet er at sikre, at brud på persondatasikkerheden håndteres korrekt, herunder at der sker anmeldelse af bruddet til Datatilsynet, og at den registrerede underrettes, såfremt bruddet indebærer en høj risiko for den registrerede persons rettigheder.

Databeskyttelsesforordningens artikel 33 og 34.

16.1 ANMELDELSE TIL DATATILSYNET

Såfremt der sker et brud på persondatasikkerheden, anmelder Udenrigsministeriet bruddet til Datatilsynet. Anmeldelsen sker uden unødigt ophold og senest 72 timer efter, persons at Udenrigsministeriet har opdaget bruddet.

Hvis det er usandsynligt, at bruddet indebærer en risiko for den registrerede persons rettigheder, er Udenrigsministeriet ikke forpligtet til at anmelde bruddet til Datatilsynet.

16.2 UNDERRETNING TIL DEN REGISTRERERE

Hvis bruddet sandsynligvis vil indebære en høj risiko for den registrerede persons rettigheder eller frihedsrettigheder, vil Udenrigsministeriet uden unødig forsinkelse underrette den registrerede person om bruddet, samt oplyse om, hvilke sandsynlige konsekvenser bruddet måtte have for vedkommende.

Kravene, der sikrer en korrekt håndtering af brud på persondatasikkerheden, vil blive uddybet i "Retningslinje om brud på behandlingssikkerheden i forhold til personoplysninger og hvad der skal gøres i tilfælde af sikkerhedsbrud".

17. DATABESKYTTELSESRÅDGIVER (DPO)

Formålet er at sikre, at der er udpeget en databeskyttelsesrådgiver, samt at databeskyttelsesrådgiverens rolle, herunder stilling og opgaver, er fastlagt og opfyldes.

Databeskyttelsesforordningens artikel 37-39.

Som en offentlig myndighed, der foretager behandling af personoplysninger, er Udenrigsministeriet forpligtet til at udpege en databeskyttelsesrådgiver (DPO).

Databeskyttelsesrådgiveren i Udenrigsministeriet er udvalgt på baggrund af sine faglige kvalifikationer, herunder ekspertise inden for persondataret og persondatabeskyttelse.

Databeskyttelsesrådgiverens rolle er dels at kontrollere, at Udenrigsministeriet overholder de til enhver tid gældende regler for behandling og beskyttelse af personoplysninger. Endvidere skal databeskyttelsesrådgiveren yde både konkret og generel rådgivning om reglerne for behandling og beskyttelse af personoplysninger til Udenrigsministeriets organisation.

Endelig er Databeskyttelsesrådgiveren Udenrigsministeriets kontaktperson udadtil, både i forhold til registrerede personer og i forhold til tilsynsmyndighederne.

Medarbejdere i Udenrigsministeriet kan til enhver tid kontakte databeskyttelsesrådgiveren ved spørgsmål til indholdet af denne persondatapolitik eller de tilhørende retningslinjer, eller ved øvrige spørgsmål om, hvordan personoplysninger skal behandles og beskyttes, herunder hvordan de registrerede personers rettigheder skal efterleves mv.

KONTAKTOPLYSNINGER TIL DATABESKYTTELSESRÅDGIVEREN I UDENRIGSMINISTERIET:

Navn: Jake Lillethorup Mahs

E-mail: dpo@um.dk

Telefonnr.: 3392 1965 eller 2259 9632.

Databeskyttelsesrådgiverens rolle, herunder opgaver og ansvar, vil blive uddybet i "Retningslinje om databeskyttelsesrådgiveren (DPO)".

Der henvises endvidere til "Kommissorium for databeskyttelsesrådgiveren i Udenrigsministeriet".

18. KONTAKTEN TIL DATATILSYNET

Formålet er at sikre, at eventuelle tilsyn og henvendelser fra Datatilsynet håndteres korrekt, herunder at Datatilsynet får den rette dokumentation.

Databeskyttelsesforordningens artikel 51-59.

Såfremt Datatilsynet skulle foretage tilsyn eller rette henvendelse til Udenrigsministeriet, sikrer det øverste ledelsesniveau (Direktionen), at tilsynet får den efterspurgte og rette information, herunder fortegnelserne over behandlingsaktiviteter i henhold til databeskyttelsesforordningens artikel 30.

Endvidere sikres det, at Udenrigsministeriet til enhver tid overholder de tidsfrister, som Datatilsynet måtte stille i forbindelse med et tilsyn eller andre henvendelser til Udenrigsministeriet.

MINISTRY OF FOREIGN AFFAIRS OF DENMARK

2 Asiatisk Plads
DK-1448 Copenhagen K
Denmark

Tel +45 33 92 00 00
Fax +45 32 54 05 33
um@um.dk
www.um.dk