Politik for databeskyttelse

Indholdsfortegnelse

Introduktion

Hos AMU-Fyn er det afgørende, at vores medarbejdere, kursister og interessenter har tillid til AMU-Fyns behandling af personoplysninger, og at beskyttelsen af personoplysninger sker med størst mulige sikkerhed. Vi skal konstant sikre, at tilgængelighed, fortrolighed og integritet mellem AMU-Fyn og vores medarbejdere, kursister, samarbejdspartnere og interessenter ikke kompromitteres med deraf følgende brud på persondatasikkerheden.

På denne baggrund har AMU-Fyn udarbejdet nærværende politik for databeskyttelse, som består af følgende fire dele:

- Generelle forhold om databeskyttelsespolitikken, som beskriver de overordnede rammer samt formål og øvrige elementer.
- Databeskyttelseskrav og behandlingssikkerhed, som beskriver AMU-Fyns krav til behandling og beskyttelse af personoplysninger.
- Registreredes rettigheder, som beskriver medarbejdere, kursister og interessenters rettigheder i henhold til databeskyttelsesforordningen.
- Anmeldelse af og underretning om brud på persondatasikkerheden, som beskriver anmeldelse til Datatilsynet og underretning til registrerede ved brud på persondatasikkerheden.

Generelt om databeskyttelsespolitikken

Dokumenthierarki

AMU-Fyns beskyttelse af personoplysninger er inddelt i følgende niveauer:

- En politik for databeskyttelse (nærværende dokument).
- En offentlig privatlivspolitik, der indeholder politikker, rettigheder og oplysninger i forhold til medarbejdere, kursister og interessenter, udmøntet i medfør af politik for databeskyttelse.
- Dokumentation i form af databehandleraftaler, procedurer, kontroller og erklæringer, udmøntet i medfør af politik for databeskyttelse, for at sikre implementering af denne i organisationen.
- Fortegnelse over behandlinger af personoplysninger samt tilhørende risikovurderinger, som danner baggrund for fastlæggelse af politik for databeskyttelse.

Formål

Databeskyttelsespolitikken fastlægger databeskyttelsen i AMU-Fyn og bidrager med en fælles forståelse af, hvad databeskyttelse indebærer, og den tilgang AMU-Fyn har til arbejdet med personoplysninger. Politikken bidrager desuden til at sikre og påvise overholdelse af gældende persondatalovgivning, og at AMU-Fyn lever op til principperne om databeskyttelse i databeskyttelsesforordningen og databeskyttelsesloven.

En væsentlig del af beskyttelsen af personoplysninger, er vores tilgang til og anvendelse af it samt vores medarbejderes holdninger og arbejdsgange ved behandling og beskyttelse af personoplysninger.

Målene for databeskyttelse hos AMU-Fyn er følgende:

- AMU-Fyn lever op til gældende lovgivning og myndighedskrav inden for persondatabeskyttelse.
- AMU-Fyn medarbejdere forstår deres ansvar og efterlevelse af politik for databeskyttelse, der indgår som en naturlig del i det daglige arbejde.
- AMU-Fyn har en høj system-, data og driftssikkerhed og styrer risici for nedbrud og deraf følgende brud på persondatasikkerheden.
- AMU-Fyn krav til tekniske og organisatoriske sikkerhedsforanstaltninger er operationelle og passende, baseret på risikovurderinger.
- AMU-Fyn overvåger tilsidesættelse af sikkerhedsforanstaltninger på en sådan måde, at disse bliver opdaget og kan tilbageføres til den ansvarlige.

Afgrænsning

Databeskyttelsespolitikken gælder for al behandling af personoplysninger som dataansvarlig, dvs. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse, hvad enten det være sig elektroniske eller papirbaserede personoplysninger.

Alle medarbejdere uanset ansættelsesform, der måtte få adgang til AMU-Fyns personoplysninger, er omfattet af denne databeskyttelsespolitik. Alle har et medansvar for databeskyttelsen og er forpligtet til at efterleve databeskyttelsespolitikken og tilhørende procedurer og retningslinjer.

Databeskyttelsespolitikkens indhold er baseret på følgende grundlag:

- Databeskyttelsesforordningen
- Databeskyttelsesloven
- Vejledninger fra Datatilsynet, EU-Kommissionen og Artikel 29-gruppen

AMU-Fyns behandling af personoplysninger som databehandler fremgår af databehandleraftalen samt tilhørende instruks.

Afvigelser

Der kan som udgangspunkt ikke afviges fra kravene i databeskyttelsespolitikken. Såfremt der er forretningsmæssige eller tekniske begrundelser for at afvige, skal dette godkendes af AMU-Fyns ledelse. Enhver afvigelse fra kravene i databeskyttelsespolitikken kræver forudgående risikovurdering og dokumentation herfor, herunder konsultation hos datasikkerhed behandler gruppen på AMU-Fyn.

Brud på databeskyttelsespolitikken kan resultere i disciplinære handlinger, herunder ansættelsesretlige konsekvenser og sanktioner mod underdatabehandlere og samarbejdspartnere. Der henvises i øvrigt til de skærpende omstændigheder i databeskyttelsesforordningen i forbindelse med brud på persondatasikkerheden.

Godkendelsesprocedure og ajourføring

Databeskyttelsespolitikken er gældende, når den er godkendt af ledelsen hos AMU-Fyn.

Databeskyttelsespolitikken ajourføres og godkendes en gang årligt.

Indholdet af databeskyttelsespolitikken kommunikeres til medarbejdere og andre relevante interessenter.

Rolle- og ansvarsfordeling

Ansvaret for implementeringen og efterlevelsen af databeskyttelsespolitikken er uddelegeret til datasikkerhed behandler gruppen, som sørger for, at uddannelsescheferne har de fornødne hjælpemidler til at sikre, at kravene efterleves i de daglige forretningsgange i deres afdelinger.

Databeskyttelseskrav

AMU-Fyn skal til enhver tid tilrettelægge arbejdet med beskyttelse af personoplysninger ud fra en risikobaseret tilgang, som tager udgangspunkt i en løbende vurdering af AMU-Fyns behandlingsaktiviteter.

Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører AMU-Fyn passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

Omfattede personoplysninger

Databeskyttelsespolitikken omfatter alle fysiske personers personoplysninger, som tilhører AMU-Fyn, herunder også personoplysninger, placeret hos underdatabehandlere osv.

AMU-Fyn varetager drift af webløsninger og internt afviklede systemer til indsamling, opbevaring og behandling af personoplysninger om medarbejdere, kursister, samarbejdspartnere, leverandører samt øvrige interessenter mv. AMU-Fyn har udarbejdet en fortegnelse over behandlingsaktiviteter i henhold til databeskyttelsesforordningen. Fortegnelsen giver overblik over de behandlinger, som AMU-Fyn er ansvarlig for.

Behandling af personoplysninger er en forudsætning for, at AMU-Fyn kan indgå ansættelsesaftaler, leverandørkontrakter, behandling af kursist oplysninger og de dertil knyttede ydelser.

Personoplysningerne behandles og arkiveres i forbindelse med:

- Indsamling af stamdata og sygdomsoplysninger på ansatte og kursister med henblik på at give den bedste service, jf. Amu-Fyns formålspolitik.
- Personaleadministration, herunder rekruttering, ansættelse, fratrædelse og udbetaling af løn mv.
- Stamdata for leverandører.

- Elever og kursisters stamdata i forbindelse med tilmelding på kurser

I behandlingen af personoplysninger kategoriseres disse i:

- Almindelige personoplysninger i henhold til databeskyttelsesforordningens artikel 6.
- Særlige kategorier af personoplysninger (følsomme personoplysninger), der kan indeholde oplysninger om de registreredes fysiske og/eller psykiske helbred i henhold til databeskyttelsesforordningens artikel 9.

I behandlingen af personoplysninger skal de tekniske og organisatoriske sikkerhedsforanstaltninger tilrettelægges og implementeres til sikring af:

- Fortrolighed:
  - Personoplysninger skal til enhver tid beskyttes mod uautoriseret adgang.
  - Adgang, ændring og visning af personoplysninger skal til enhver tid kunne dokumenteres via logning.

- Integritet
  - Personoplysninger skal til enhver tid være valide og korrekte.
  - Personoplysninger skal til enhver tid beskyttes mod utilsigtede og uautoriserede ændringer.

- Tilgængelighed
  - Personoplysninger skal til enhver tid være tilgængelige for autoriserede personer.
  - Sikkerhedskopiering af alle personoplysninger skal ske dagligt.

Generelle behandlingsprincipper

Alle behandlinger af personoplysninger skal overholde gældende persondatalovgivning samt praksis. Dette sker blandt andet ved efterlevelse af databeskyttelsespolitikken.

AMU-Fyn skal ved enhver behandling af personoplysninger overholde og kunne dokumentere overholdelsen af de generelle behandlingsprincipper i databeskyttelsesforordningen og databeskyttelsesloven.

- **God databehandlingsskik**
  Data skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.

- **Formål**
  Data skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforeneligt med disse formål.

- **Dataminimering og proportionalitetsprincippet**
  Data skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

- **Korrekte data**
  Data skal være korrekte og om nødvendigt ajourførte.

- **Opbevaringsbegrænsning**
  Data skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles.

- **Integritet og fortrolighed**
  Data skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger.

Behandlingshjemmel

AMU-Fyn behandler kun personoplysninger, hvor der er et lovligt og legitimt grundlag herfor i særlovgivningen, databeskyttelsesforordningen, databeskyttelsesloven eller ved indhentelse af samtykke fra den registrerede.

Formål og kategori af personoplysninger afgør hvilken behandlingshjemmel, der kræves for den konkrete behandling, og behandlingshjemmel fremgår af fortegnelsen over behandlingsaktiviteter.

Risikovurderinger

Databeskyttelsesrådgiver gruppen skal i samarbejde med it-afdelingen iværksætte initiativer, der imødegår det trusselsbillede, som AMU-Fyn til enhver tid står over for, således at sikkerhedsforanstaltningerne er passende og risikoen for sikkerhedsbrud reduceres til et passende niveau.

AMU-Fyn foretager en løbende vurdering af, hvilket sikkerhedsniveau der er passende. I vurderingen tages der hensyn til de risici, som behandlingen udgør, særligt ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Som grundlag for ajourføring af de tekniske og organisatoriske foranstaltninger foretager it-afdelingen en gang årligt en overordnet risikovurdering. Vurderingen skal belyse sandsynligheden for og konsekvenserne af hændelser, der kan true beskyttelsen af personoplysninger trusler, herunder tilfældige, forsætlige og uforsætlige hændelser.

Risikovurderingen skal foreligge inden for den periode, der er angivet i AMU-Fyns procedurer, herunder årshjul. Eventuelle ændringer af sikkerhedspolitikken og andre sikkerhedstiltag skal godkendes af ledelsen.

Konsekvensanalyser

AMU-Fyn udarbejder i påkrævet omfang konsekvensanalyser i overensstemmelse med databeskyttelsesforordningen.

Hvis en behandling af personoplysninger, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder, foretager AMU-Fyn forud for behandlingen en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger.

AMU-Fyn foretager en løbende ajourføring af konsekvensanalyser, særligt når der er ændringer af den risiko, som behandlingsaktiviteterne udgør.

AMU-Fyn skal hører Datatilsynet inden en tiltænkt behandling, såfremt konsekvensanalysen viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger, truffet af AMU-Fyn for at begrænse risikoen.

Organisatoriske foranstaltninger

AMU-Fyn skal udarbejde en procedure, der sikrer, at databeskyttelsesrådgiver gruppen på AMU-Fyn løbende udfører overvågning af, at databeskyttelsespolitikken og tilhørende procedurer, kontroller og retningslinjer efterleves og dermed, at databeskyttelsesforordningen og databeskyttelsesloven overholdes.

Awareness
AMU-Fyn skal løbende afholde uddannelser om, hvordan medarbejdere forventes at behandle og beskytte personoplysninger. Disse uddannelser bliver tilpasset organisationens behov. Lederne for de respektive afdelinger har ansvaret for at motivere medarbejderne og sørge for, at medarbejderne efter behov har mulighed for at efteruddanne sig.

Alle medarbejdere skal modtage instruktion i behandlingen af personoplysninger samt, hvordan personoplysninger skal beskyttes.

Dataindsamling og udvekslingsmetoder
AMU-Fyn skal indføre procedurer for behandling og beskyttelse af ind- og uddata med udgangspunkt i, at indsamling og udveksling af personoplysninger sker som følger:

- Dataindsamling sker via fagsystemer, hvortil kun personale med arbejdsbetinget behov har adgang.
- Dataindsamling sker i forbindelse med personlige møder, telefonsamtaler eller skypekonsultationer i tilknytning til, at AMU-Fyn stiller services til rådighed omkring lægekonsultation, psykologer og socialrådgivere. Data indtastes direkte på fagpersonens computer og lagres herefter på diskområde, forbeholdt faggruppen.
- Udveksling af data mellem læge, psykolog og/eller socialrådgiver og patient/medlem/klient sker via e-boks.
- Udveksling af data mellem socialrådgiver og kommune sker via sikker mail.
- Sikker mail benyttes til udveksling, hvor dette kræves af indholdet i e-mailen.

Opbevaring og sletning
AMU-Fyn skal indføre følgende overordnede retningslinjer for opbevaring og sletning af personoplysninger:

- Personoplysninger opbevares i it-systemer og på serverdrev med begrænset adgang.
- Personoplysninger opbevares ikke længere, end hvad der er nødvendigt for formålet med behandlingen.
- Personoplysninger for medarbejdere slettes fem år efter endt ansættelse, og personoplysninger om ansøgere slettes efter seks måneder.
- Personoplysninger og oplysninger i relation til psykologisk rådgivning slettes tidligst efter 5 år i henhold til psykologloven.

- Personoplysninger i fysiske dokumenter og bærbare medier gælder, at USB-nøgler og eksterne harddiske mv. skal opbevares i aflåst skuffe eller skab, og at fysiske mapper, der indeholder dokumenter med personoplysninger, skal være placeret i aflåste skabe. Personoplysninger i fysiske mapper slettes ved makulering.

Fysisk sikkerhed
AMU-Fyns lokaler skal være beskyttet mod uautoriseret adgang. Kun personer med et arbejdsbetinget eller andet legitimt behov har adgang til kontorer og lignende med adgangskort og tilhørende personlig kode.

Sikkerhedsmæssige foranstaltninger skal indføres for områder/steder, hvor der foretages behandling af personoplysninger, for at forhindre uvedkommendes adgang til sådanne oplysninger.

Tekniske foranstaltninger

Regler for medarbejderes anvendelse af it
Alle medarbejdere, der i medfør af deres arbejde har en it-arbejdsplads stillet til rådighed, skal ved ansættelsen have udleveret et eksemplar af AMU-Fyns personalehåndbog, herunder også Amu-Fyns it sikkerhedspolitik

Regler for brug af pc og it-arbejdsplads
Alle pc'er eller it-arbejdspladser skal være beskyttet med antivirus-software, som under ingen omstændigheder må fjernes eller deaktiveres af medarbejdere. Det er ikke tilladt for medarbejderne selv at installere software på pc'er eller it-arbejdspladser. Ønskes anden software installeret, skal dette ske i samråd med it-afdelingen.

Arbejdsrelaterede data, herunder særlige kategorier af personoplysninger (følsomme personoplysninger), må ikke gemmes på pc'ens lokale drev c-drev.

Hvis arbejdspladsen forlades, skal medarbejderen låse pc'en.

Medarbejderes brug af internet og e-mail
Medarbejdere, der har fået stillet en pc til rådighed, skal følge retningslinjer for internetadgang og brug af e-mail. Retningslinjer fremgår af AMU-Fyns internet- og e-mail-politik.

Retningslinjerne har til hensigt at sikre en hensigtsmæssig anvendelse af internet og e-mail i relation til Amu-Fyns tilrettelæggelse af arbejdet og persondatasikkerheden. Retningslinjerne skal være gældende, uanset om brugen sker på arbejdspladsen eller eksternt, såfremt brugen indebærer opkobling til AMU-Fyns netværk.

Anvendelse af AMU-Fyns interne drev og servere
Der må ikke lagres arbejdsrelaterede eller særlige kategorier af personoplysninger på lokale pc drev. Persondata af følsom karakter, skal derfor øjeblikkelig overføres til de respektive fortrolige netværksdrev efter brug og slettes fra lokal eller ekstern harddisk.

Alle drev på AMU-Fyns servere skal være tilgængelig for brugerne til arbejdsrelaterede formål. Den enkelte bruger skal dog kun have adgang til de drev, som brugeren har et arbejdsmæssigt behov for at have adgang til. Alle medarbejdere hos AMU-Fyn skal som udgangspunkt have adgang til et personligt drev og et afdelingsdrev samt til de nødvendige fællesdrev.

Brugerrettighedsstyring
For at sikre fortrolighed og integritet, skal medarbejdere kun tildeles de adgange til data i it-systemerne, som der er arbejdsbetinget behov for. Det er lederen af den enkelte afdeling,

der har ansvaret for, at den enkelte medarbejder er tildelt de korrekte rettigheder. Endvidere er det uddannelseschefens ansvar, at medarbejderes brugerkonti øjeblikkelig nedlægges ved arbejdsophør i forbindelse med medarbejderes fratrædelse. It-afdelingen er - i samarbejde med uddannelseschefen - ansvarlig for at definere, hvilke systemer og data, som medarbejderne skal have fri adgang til.

Password-politik
Alle medarbejdere skal øjebliklig efter tiltrædelse ændre sit midlertidige password til sit eget hemmelige password. Password skal som minimum være på 8 karakterer og være komplekst, herunder være en blanding af tal og tegn samt indeholde både store og små bogstaver. Password skal skiftes hver 180. dag, når systemet giver besked herom. Password kan genbruges efter 10. gange.

Passwords er strengt personlige og må ikke gives til andre. Hvis en medarbejder har mistanke om, at andre har kendskab til vedkommendes password, skal medarbejderen øjeblikkelig skifte det. Såfremt medarbejderen har mistanke om misbrug af password og brugerkonti, skal medarbejderen uden unødigt ophold henvende sig til lederen for afdelingen.

Databeskyttelse gennem design og standardindstilling
AMU-Fyn gennemfører - både på tidspunktet for fastlæggelse af processer og systemer til behandling og på tidspunktet for selve behandlingen - passende tekniske og organisatoriske foranstaltninger, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper.

I gennemførelsen af de passende tekniske og organisatoriske foranstaltninger tages der hensyn til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, som behandlingen indebærer.

AMU-Fyn gennemfører passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles. Sådanne foranstaltninger skal navnlig gennem standardindstillinger sikre, at personoplysninger ikke uden den pågældende fysiske persons indgriben stilles til rådighed for et ubegrænset antal fysiske personer.

Beskyttelse mod virus
Alle AMU-Fyns servere og pc'er skal være beskyttet med opdateret antivirus software til beskyttelse af it-systemer og data mod virusangreb. Det er it-afdelingens ansvar, at antivirussoftwaren er opdateret med seneste version.
Firewall
For at beskytte AMU-Fyns netværk mod indtrængen fra eksterne kilder, skal der opsættes en firewall. It-afdelingen er ansvarlig for, at adgangen til netværket er beskyttet via en firewall og har således ansvaret for konfigurationen af firewall samt administration og vedligeholdelse heraf, herunder sikre, at dette sker i takt med udviklingen i trusselsbilledet.
Ændringer af opsætning af firewallen skal registreres automatisk i en log.

Netværk
Ansvaret for opbygning og vedligeholdelse af netværket skal placeres i it-afdelingen. it-afdelingen vedligeholder en topologi med oversigt over netværket. Alle eksterne forbindelser til AMU-Fyns netværk skal godkendes af it-afdelingen, som løbende opdaterer en oversigt med alle eksterne forbindelser til netværket.

Sikkerhedskopiering
Alle data, der er centralt lagret på AMU-Fyns servere, skal indgå i sikkerhedskopieringen af systemer og data. Det er it-afdelingens ansvar at foretage sikkerhedskopiering af centralt lagrede data, og at sikkerhedskopierne opbevares på forsvarlig vis. Endvidere er det it-afdelingens ansvar at teste genskabelse af data på baggrund af sikkerhedskopien.

Alle arbejdsrelaterede data skal sikkerhedskopieres, således at de kan genskabes i tilfælde af systemnedbrud eller lignende. For at sikre data, skal alle medarbejdere lagre data, herunder ind- og udgående elektroniske dokumenter, databaser, regneark m.v., på de centrale servere.

Sikker bortskaffelse af datamedier
Alle datamedier skal bortskaffes på en sådan måde, at oplysninger, der måtte befinde sig på datamediet, ikke kan tilgås og derved komme til uvedkommendes kendskab. Ved datamedier forstås enhver form for enhed opbevaring af data. Alle trykte dokumenter skal lægges i aflåst makulatorboks, som afhentes og destrueres på forsvarligvis. Alle harddiske, bånd, disketter, usb-nøgler og tilsvarende medier skal fysisk destrueres, så læsning og genskabelse af data umuliggøres.

Tidligere anvendte pc'er kan genanvendes inden for AMU-Fyn, uden at harddisken destrueres. Såfremt pc'en genanvendes inden for egen juridisk enhed, er det tilstrækkeligt, at harddisken formateres og overskrives gentagende gange, før den tages i brug af en anden medarbejder. Ved andre tilfælde skal harddiske destrueres.

Systemdokumentation
Der skal foreligge dokumentation for AMU-Fyns lokale it-systemer. Der er her tale om dokumentation af systemernes konfiguration, indhold samt anvendelse, både for systemer som leveres af leverandører samt egenudviklede systemer. Formålet er, at systemer kan genskabes efter eventuelle nedbrud.

Kontrol og overvågning

For at sikre en optimal og sikker drift kan IT-afdelinegn til hver en tid overvåge den enkeltes brug af netværk og PC. En evt. overtagelse af en brugers PC sker aldrig uden aftale med brugeren.

Brug af databehandlere

Databehandlere, underdatabehandlere og enhver anden, der udfører arbejde for AMU-Fyn, og som har adgang til personoplysninger, må kun behandle sådanne oplysninger efter instruks fra den dataansvarlige, medmindre det kræves i henhold til lovgivningen.

AMU-Fyns anvendelse af databehandler som dataansvarlig
Forinden en databehandler får adgang til eller påbegynder behandling af personoplysninger, skal databehandleren stille de fornødne garantier for, at denne vil gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandling opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

AMU-Fyn skal som dataansvarlig indgå en skriftlig databehandleraftale med databehandleren, der opfylder kravene i databeskyttelsesforordningen, og som skal godkendes af administrationschefen. Databeskyttelsesrådgiveren skal udføre rådgivning herom. Databehandleraftalen udgør den instruks, som databehandleren skal følge ved behandling af personoplysninger for AMU-Fyn

Databehandleren skal dokumentere, at denne lever op til ovenstående punkter, eksempelvis ved udlevering af en ISAE 3000 erklæring eller tilsvarende dokumentation.

AMU-Fyns anvendelse af underdatabehandler som databehandler
Forinden AMU-Fyn i sin egenskab af databehandler anvender en underdatabehandler til behandling af personoplysninger, skal underdatabehandleren stille de fornødne garantier for, at denne vil gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandling opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder. AMU-Fyn skal tillige indhente en forudgående specifik eller generel skriftlig godkendelse hos den dataansvarlige vedrørende underdatabehandleren i henhold til databehandleraftalen.

Videregivelse

Personoplysninger om medarbejdere bliver videregivet til offentlige myndigheder, fx SKAT og pensionsselskaber, leverandører og kommuner, i henhold til særlove. Personoplysninger i forbindelse med donationer bliver videregivet til SKAT med henblik på udnyttelse af reglerne om fradrag for støtte til velgørenhed.

I forbindelse med rejseaktiviteter sker der efter forudgående samtykke fra den registrerede overførsel af personoplysninger til tredjelande. Oplysningerne kan være både almindelige personoplysninger og særlige kategorier af personoplysninger (følsomme personoplysninger), og overførslen sker under iagttagelse af databeskyttelsesforordningens bestemmelser om overførsler af personoplysninger til tredjelande og internationale organisationer.

Registreredes rettigheder

AMU-Fyn iagttager den registreredes rettigheder, herunder retten til indsigt, tilbagetrækning af samtykke, berigtigelse, sletning og klageadgang til Datatilsynet mv. AMU-Fyn oplyser de registrerede om AMU-Fyns behandling af personoplysninger i den offentliggjorte privatlivspolitik.

Brud på persondatasikkerheden

I tilfælde af eller ved mistanke om brud på persondatasikkerheden skal databeskyttelsesrådgiver gruppen kontaktes omgående. Databeskyttelsesrådgiver gruppen vurderer, om der er tale om et brud på persondatasikkerheden, herunder om der skal ske anmeldelse til Datatilsynet og underretning til de registrerede.

Ved brud på persondatasikkerheden forstås enhver hændelse, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Hvis der er mistanke om, at misbrug af systemer og data har fundet sted og dermed sket et muligt brud på persondatasikkerheden, skal medarbejderen underrette nærmeste leder.

Anmeldelse til Datatilsynet

Ved brud på persondatasikkerheden skal AMU-Fyn anmelde dette til Datatilsynet, når AMU-Fyn er dataansvarlig.

Anmeldelse af brud på persondatasikkerheden skal ske uden unødig forsinkelse og om muligt senest 72 timer, efter at AMU-Fyn er blevet bekendt med bruddet. Bliver sikkerhedsbruddet ikke anmeldt inden for 72 timer, skal årsagen til forsinkelsen angives i anmeldelsen.

Anmeldelsen skal mindst indeholde:

- Beskrivelse af karakteren af bruddet på persondatasikkerheden, herunder kategorierne og det omtrentlige antal berørte registrerede.
- Angivelse af navn på ansvarlige kontaktperson hos AMU-Fyn.
- Beskrivelse af de sandsynlige konsekvenser af sikkerhedsbruddet.
- Beskrivelse af de foranstaltninger, som AMU-Fyn har truffet eller forslår truffet for at afhjælpe sikkerhedsbruddet.

Ved brud på persondatasikkerheden skal de dataansvarlige kontaktes uden unødig forsinkelse, efter AMU-Fyn er blevet opmærksom på sikkerhedsbruddet, når AMU-Fyn er databehandler.

Underretning til de registrerede

Som dataansvarlig, og når et persondatasikkerhedsbrud indebærer en høj risiko for de registrerede, skal AMU-Fyn uden unødig forsinkelse underrette den eller de registrerede. Underretningen skal formuleres i et klart og tydeligt sprog og mindst indeholde de samme oplysninger, som anmeldelsen til Datatilsynet.

Det er dog ikke nødvendigt at underrette den eller de registrerede, såfremt:

- AMU-Fyn har gennemført passende tekniske og organisatoriske foranstaltninger og de er blevet anvendt på de personoplysninger, som er berørt af sikkerhedsbruddet.
- AMU-Fyn har truffet efterfølgende foranstaltninger, som sikrer, at den høje risiko ikke længere er reel.
- Det ville kræve en uforholdsmæssig indsats fra AMU-Fyn side. I sådanne tilfælde skal AMU-Fyn i stedet foretage en offentlig meddelelse eller tilsvarende foranstaltning, hvor de registrerede underrettes på en effektiv måde.