Fanø Kommune

Politik for databeskyttelse

Fanø Kommune

Indholdsfortegnelse

Fanø Kommune

Introduktion

Hos Fanø Kommune er det afgørende, at vore borgere, samarbejdspartnere, leverandører og medarbejdere har tillid til kommunens behandling af personoplysninger og at beskyttelsen af personoplysninger sker med størst mulige sikkerhed. Vi skal konstant sikre, at tilgængelighed, fortrolighed og integritet mellem Fanø Kommune og vore borgere, samarbejdspartnere, leverandører og medarbejdere ikke kompromitteres med deraf følgende brud på persondatasikkerheden.

På denne baggrund har Fanø Kommune 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 Fanø Kommunes krav til behandling og beskyttelse af personoplysninger.
- Registreredes rettigheder, som beskriver borgeres, samarbejdspartneres, leverandørers og medarbejderes 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

Fanø Kommune 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 borgere, samarbejdspartnere, leverandører og medarbejdere, 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 Fanø Kommune og bidrager med en fælles forståelse af, hvad databeskyttelse indebærer, og den tilgang Fanø Kommune har til arbejdet med personoplysninger. Politikken bidrager desuden til at sikre og påvise overholdelse af gældende persondatalovgivning og at Fanø Kommune lever op til principperne om databeskyttelse i databeskyttelsesforordningen og databeskyttelsesloven, samt iagttager de krav der stilles til forvaltningens databehandling fra lovgiverne i særlovgivnigen.

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 i Fanø Kommune er følgende:

- Fanø Kommune lever op til gældende lovgivning og myndighedskrav inden for persondatabeskyttelse.
- Fanø Kommune fremstår som en organisation med troværdig beskyttelse af sine persondata.
- Fanø Kommunes medarbejdere forstår deres ansvar og efterlevelse af politik for databeskyttelse, der indgår som en naturlig del i det daglige arbejde.
- Fanø Kommune har en høj system-, data og driftssikkerhed og styrer risici for nedbrud og deraf følgende brud på persondatasikkerheden.
- Fanø Kommunes krav til tekniske og organisatoriske sikkerhedsforanstaltninger er operationelle og passende, baseret på risikovurderinger.
- Fanø Kommune 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, eksterne konsulenter, samarbejdspartnere, leverandører samt øvrige interessenter, der måtte få adgang til Fanø Kommunes 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

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 Fanø Kommunes direktion. Enhver afvigelse fra kravene i databeskyttelsespolitikken kræver forudgående risikovurdering og dokumentation herfor, herunder konsultation hos DPO'en (databeskyttelsesrådgiveren).

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

Godkendelsesprocedure og ajourføring

Databeskyttelsespolitikken er gældende, når den er godkendt af direktionen i Fanø Kommune.

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 administrationschefen, som sørger for, at afdelingslederne og funktionschefer har de fornødne hjælpemidler til at sikre, at kravene efterleves i de daglige forretningsgange i deres afdelinger.

Fanø Kommune har udpeget en databeskyttelsesrådgiver der skal medvirke til at sikre, at Fanø Kommune overholder persondatalovgivningen samt databeskyttelsespolitikken, blandt andet igennem information, rådgivning, uddannelse og overvågning af reglernes overholdelse samt samarbejde med tilsynsmyndigheden.

Databeskyttelsesrådgiveren hos Fanø Kommune har følgende opgaver:

- Rådgive ledelsen og ansatte om forhold, der vedrører behandling af persondata indenfor lovens rammer
- Rådgive ledelsen om beskyttelse af personoplysninger i forbindelse med større projekter
- Overvåge overholdelsen databeskyttelsesforordningen og databeskyttelsesloven, samt overholdelse af politikker om beskyttelse af personoplysninger.
- Skal sikre nødvendig uddannelse af personalet og iværksætte awareness-kampagner
- Medvirke til udarbejdelse af procedurer og kontroller for behandling af persondata
- Være SPOC i dialogen med registrerede, der ønsker at udøve deres rettigheder
- Validere indholdet forud for accept af databehandleraftaler
- Sikre at der føres tilsyn med Databehandlere
- Være kontaktperson for kommunen i samarbejdet med Datatilsynet i spørgsmål om behandling af persondata og når det er hensigtsmæssigt at rådgive sig med Datatilsynet

Databeskyttelseskrav

Fanø Kommune skal til enhver tid tilrettelægge arbejdet med beskyttelse af personoplysninger ud fra en risikobaseret tilgang, som tager udgangspunkt i en løbende vurdering af Fanø Kommunes 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 Fanø Kommune 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 Fanø Kommune, herunder også personoplysninger, placeret hos databehandlere, underdatabehandlere osv.

Fanø Kommune varetager drift af fagsystemer, webbaserede løsninger samt både internt – og eksternt afviklede systemer til indsamling, opbevaring og behandling af personoplysninger om borgere, samarbejdspartnere, leverandører og medarbejdere mv. Fanø Kommune har udarbejdet en fortegnelse over behandlingsaktiviteter i henhold til databeskyttelsesforordningen. Fortegnelsen giver overblik over de behandlinger, som Fanø Kommune er ansvarlig for.

Behandling af personoplysninger er en forudsætning for, at kommunen kan udføre de lovregulerede pålagte services overfor borgere og de dertil knyttede ydelser, indgå ansættelsesaftaler, leverandørkontrakter, lejekontrakter etc.

Personoplysningerne behandles og arkiveres i forbindelse med:

- Indsamling af data på borgere med henblik på at give den bedste service.
- Personaleadministration, herunder rekruttering, ansættelse, fratrædelse og udbetaling af løn mv.
- Stamdata for leverandører og samarbejdspartnere.

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 medlemmers fysiske og/eller psykiske helbred i henhold til databeskyttelsesforordningens artikel 9.
- Straffedomme og lovovertrædelser, som vil fremgå af straffeattest behandles i henhold til databeskyttelsesforordningens artikel 10

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, særlove i forvaltningen samt praksis. Dette sker blandt andet ved efterlevelse af databeskyttelsespolitikken.

Fanø Kommune 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. Undtaget herfra er de data, som er omfattet af arkivloven og skal overføres til rigsarkivet med henblik på historisk arkivering.

- **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

Fanø Kommune 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, samt Kommunernes Landsforenings Emnesystematik (KLE) afgør hvilken behandlingshjemmel, der kræves for den konkrete behandling, og behandlingshjemmel fremgår af fortegnelsen over behandlingsaktiviteter.

Risikovurderinger

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

Fanø Kommune 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 indenfor den periode, der er angivet i Fanø Kommune procedurer, herunder årshjul. Eventuelle ændringer af informationssikkerhedspolitikken og andre sikkerhedstiltag skal godkendes af direktionen.

Konsekvensanalyser

Fanø Kommune 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 Fanø Kommune forud for behandlingen en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger.

Fanø Kommune foretager en løbende ajourføring af konsekvensanalyser, særligt når der er ændringer af den risiko, som behandlingsaktiviteterne udgør.

Fanø Kommune skal høre Datatilsynet inden en tiltænkt behandling, såfremt konsekvensanalysen viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger, truffet af Fanø Kommune for at begrænse risikoen.

Organisatoriske foranstaltninger

Databeskyttelsesrådgiveren
Fanø Kommune skal udarbejde en procedure, der sikrer, at databeskyttelsesrådgiveren løbende udfører overvågning af, at databeskyttelsespolitikken og tilhørende procedurer, kontroller og retningslinjer efterleves og dermed, at databeskyttelsesforordningen og databeskyttelsesloven overholdes.

Awareness
Fanø Kommune 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
Fanø Kommune 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, hjemmebesøg, websystemer og mailkorrespondance i tilknytning til Fanø Kommunes forvaltning og borgerservices
- Udveksling af data mellem Fanø Kommune og den/de kommuner, der har indgået aftale med Fanø Kommune om forpligtende samarbejde i forhold til bla. databehandling.
- Sikker mail benyttes til udveksling af information, hvor dette kræves af indholdet i e-mailen.

Opbevaring og sletning
Fanø Kommune skal indføre følgende overordnede retningslinjer for opbevaring og sletning af personoplysninger:

- Personoplysninger opbevares i it-fagsystemer 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 kunde/leverandørforhold slettes efter 5 år, når kravet om Bogføringslovens opbevaringspligt er opfyldt.
- 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.
- Printede dokumenter indeholdende personoplysninger, må ikke forlade rådhuset eller behandlingsstedet.
- Fortroligt materiale indeholdende personoplysninger må ikke videresendes til medarbejderens private mailadresse.

Fysisk sikkerhed
Fanø Kommunes administrationslokaler skal være beskyttet mod uautoriseret adgang til dokumenter og data, for de afsnit hvor behandling af persondata foretages. Kun personer med et arbejdsbetinget eller andet legitimt behov har adgang til kontorer.

Kunder, partnere og leverandører samt andre besøgende skal henvende sig i receptionen, der kontakter den relevante kontaktperson. Kontaktpersonen møder og følger den pågældende rundt i bygningen. Besøgende kan færdes frit i receptionsområdet og ved mødelokaler. Ingen udefrakommende personer, må færdes uledsaget i medarbejderområdet.

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 Fanø Kommunes informationssikkerhedspolitik.

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 selvstændigt at installere software på pc'er eller it-arbejdspladser. Ønskes anden software installeret, skal dette ske i samråd med it-afdelingen.

Arbejdsrelaterede persondata, 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 Fanø Kommunes informationssikkerhedspolitik.

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

Anvendelse af Fanø Kommunes interne drev og servere
Der må ikke lagres arbejdsrelaterede personoplysninger på lokale pc drev.

Alle drev på Fanø Kommune 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.

Anvendelse af Fanø Kommunes elektroniske sags- og dokumenthåndteringssystem (ESDH)
Der må ikke lagres arbejdsrelaterede personoplysninger på lokale pc drev.

Alle medarbejdere med adgang til ESDH systemet KMD Nova har kun adgang til de dokumenter, hvortil de har et arbejdsmæssigt behov for at have adgang til.

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 IT-Chefen der har ansvaret for, at den enkelte medarbejder er tildelt de korrekte rettigheder. Endvidere er det IT-Chefens ansvar, at medarbejderes brugerkonti (roller og rettigheder) øjeblikkeligt nedlægges ved arbejdsophør i forbindelse med medarbejderes fratrædelse. IT-Chefen er ansvarlig for at definere, hvilke systemer og data, som medarbejderne skal have fri adgang til.

Password-politik
Alle medarbejdere skal øjeblikkeligt 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 90. dag, når systemet giver besked herom. Password kan genbruges efter 32. 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 øjeblikkeligt skifte det. Såfremt medarbejderen har mistanke om misbrug af password og brugerkonti, skal medarbejderen uden unødigt ophold henvende sig til sin nærmeste ledere eller IT-Chefen.

Databeskyttelse gennem design og standardindstilling
Fanø Kommune 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.

Den dataansvarlige 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 Fanø Kommunes servere og pc'er skal være beskyttet med opdateret antivirus software til beskyttelse af it-systemer og data mod virusangreb. Det er it-afdelingens eller outsourcingpartnerens ansvar, at antivirus-softwaren er opdateret med seneste version.

Firewall
For at beskytte Fanø Kommunes netværk mod indtrængen fra eksterne kilder, er der opsat en firewall. It-afdelingen er ansvarlig for, at adgangen til netværket er beskyttet via denne firewall og har således ansvaret for konfigurationen af firewall samt administration og vedligeholdelse heraf, herunder sikrer, 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 Fanø Kommunes 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 Fanø Kommunes servere, skal indgå i sikkerhedskopieringen af systemer og data også når disse fysisk befinder sig hos en outsourcingpartner. Det er it-afdelingens ansvar at foretage sikkerhedskopiering af centralt lagrede data uanset serverens fysiske placering, og at sikkerhedskopierne opbevares på forsvarlig vis. Endvidere er det it-afdelingens ansvar at teste muligheden for 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 og tilhørende fagsystemer.

Fjernarbejdspladser
Ved arbejdsbetinget behov skal medarbejdere kunne tilgå netværket uden for Fanø Kommunes lokaler ved opkobling via en sikker VPN-forbindelse der benytter 2 faktorgodkendelse via SMS.

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 til 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 Fanø Kommune, uden at harddisken destrueres. Såfremt pc'en genanvendes inden for egen juridiske 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 Fanø Kommunes lokale og outsourcede it-systemer. Der er her tale om dokumentation af systemernes konfiguration, indhold samt anvendelse, både for systemer som leveres af leverandører samt evt. egenudviklede systemer. Formålet er, at systemer kan genskabes efter eventuelle nedbrud.

Kontrol og overvågning
Fanø Kommune skal have procedure for overvågning og kontrol af medarbejderes brug af systemer, herunder brug af internettet og e-mail. Overvågningen og kontroller skal være baseret på opsat sikkerhedslogning.

Brug af databehandlere

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

Fanø Kommune 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 foranstaltninger på en sådan måde, at behandling opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

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

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

Videregivelse

Personoplysninger om borgere og medarbejdere bliver videregivet til offentlige myndigheder, fx SKAT og pensionsselskaber, leverandører og andre kommuner eller offentlige organisationer, i henhold til særlove.

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

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

Brud på persondatasikkerheden

I tilfælde af eller ved mistanke om brud på persondatasikkerheden skal databeskyttelsesrådgiveren kontaktes omgående. Databeskyttelsesrådgiveren 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.

Alle brud på persondatasikkerheden skal dokumenteres, herunder de faktiske omstændigheder, dets virkninger og de trufne afhjælpende foranstaltninger samt en vurdering af hvorvidt persondatasikkerhedsbruddet skal anmeldes til Datatilsynet og om den registrerede skal underrettes.

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 IT-Chefen eller nærmeste leder, der efterfølgende underretter IT-Chefen.

Anmeldelse til Datatilsynet

Ved brud på persondatasikkerheden skal Fanø Kommune anmelde dette til Datatilsynet, når Fanø Kommune er dataansvarlig.

Anmeldelse af brud på persondatasikkerheden skal ske uden unødig forsinkelse og om muligt senest 72 timer, efter at Fanø Kommune 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 databeskyttelsesrådgiveren i Fanø Kommune.
- Beskrivelse af de sandsynlige konsekvenser af sikkerhedsbruddet.
- Beskrivelse af de foranstaltninger, som Fanø Kommune har truffet eller forslår truffet for at afhjælpe sikkerhedsbruddet.

Underretning til de registrerede

Som dataansvarlig, og når et persondatasikkerhedsbrud indebærer en høj risiko for de registrerede, skal Fanø Kommune 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:

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