Persondatapolitik for Møller & Rothe til alle medarbejdere - vedrørende behandling af personoplysninger.

Indhold:

Persondatapolitik for Møller & Rothe.
Dette dokument har to formål: Dels at tjene som et praktisk instrument i vores arbejde med beskyttelsen af persondata, dels som en skriftlig dokumentation af vores indsats for at overholde Databeskyttelsesforordningen.

Møller & Rothes persondatapolitik er udformet i sammenhæng med vores overordnede strategi, værdier og visioner og er på den måde en integreret del af, hvordan vi arbejder. Politikken er godkendt af ledelsen, og alle medarbejdere er gjort bekendt med den og deres ansvar i forhold til persondata. Hvis der opstår mistanke om, at persondata ikke håndteres korrekt, skal nærmeste leder kontaktes og informeres om problematikken.
Persondatapolitikken bliver gennemgået og opdateret hvert år. Ved ansættelse bliver alle nye medarbejdere gjort bekendt med persondatapolitikken og skal ved underskrift på ansættelseskontrakten bekræfte sit kendskab til- og forståelse af politikken.

1. Definitioner
Møller & Rothe behandler persondata i forbindelse med vores virksomhedsdrift og kundeadministration. Nedenfor vil kernebegreber fra lovgivningen blive defineret for at lette forståelsen af persondatapolitikken.

Databeskyttelsesforordningen	Den lovgivning, som pr. 25. maj 2018 regulerer behandlingen af persondata (træder sammen med Databeskyttelsesloven i stedet for Persondataloven)
Personoplysninger	Enhver oplysning om en identificeret eller identificerbar fysisk person, fx navn, adresse, telefonnummer, billede, nummerplade, cpr-nummer eller lignende. Oplysninger om enkeltmandsfirmaer er derfor også personoplysninger
Følsomme personoplysninger	Eksempelvis helbredsoplysninger, fagforenings-tilhørsforhold, race, etnicitet, politisk overbe-visning, oplysninger om strafbare forhold mv.
Registrerede	Alle personer, hvis oplysninger er registreret hos Møller & Rothe, fx kunder, medarbejdere og leverandører
Behandling af data	Alt hvad virksomheden gør med data, inklusiv opbevaring og sletning
Dataansvarlig	Den, der beslutter formål, omfang og metoder til behandling af persondata
Databehandler	Den, der behandler data på vegne af den dataansvarlige, fx et firma, som håndterer løn eller en cloudtjeneste

2. Organisering og ansvar

Denne persondatapolitik gælder for virksomheden Møller & Rothe.
Ansvaret for, at alle medarbejdere overholder persondatapolitikken, påhviler dem selv og ledelsen. Kontrol med overholdelse af persondatapolitik skal dokumenteres skriftligt og opbevares af Jan Gelbjerg-Hansen (CEO). Hvis kontrollen viser, at der har været episoder, hvor persondatapolitikken ikke er blevet overholdt, er det ledelsens opgave at afhjælpe problemet.

3. Medarbejderinstruks

Det følgende er konkrete regler og retningslinjer, som alle medarbejdere i Møller & Rothe skal følge i forbindelse med behandling af persondata. Instruksen er baseret på Databeskyttelsesforordningens og Databeskyttelseslovens krav og vil sammen med øvrig dokumentation og vejledninger sikre efterlevelsen af forordningen. Hvert element i instruksen er delt op i formål (hvorfor gør vi det), procedure (hvordan gør vi det) og kontrol (har vi nu også gjort det).

3.1 Sikring af lovligt grundlag/hjemmel

Formål:

- Lovligt grundlag for at behandle data.

Procedure:

Før en databehandling påbegyndes, skal der ske en afklaring af den lovlige hjemmel. Dette gøres af ejeren af processen. Som hovedregel vil vi i forbindelse med kunder og leverandører anvende hjemlen opfyldelse af kontrakt og ved vores medarbejdere henvise til et gyldigt indhentet samtykke, interesseafvejning eller en retlig *forpligtelse*.

Det lovlige grundlag for behandlingen dokumenteres sammen med den pågældende proces i fortegnelsen over behandlingsaktiviteter.

Underskrevne/accepterede samtykkeerklæringer opbevares af Jan Gelbjerg-Hansen (CEO) og alle behandlingsaktiviteter gennemgås en gang om året mhp. at sikre lovligheden.

3.2 Sikring af formål og at data er relevante

Formål:

- Oplysninger som indsamles, er baseret på et klart formål og omfatter ikke mere, end hvad der kræves til opfyldelse af formålet med behandlingen.

Procedure:

For hver behandlingsaktivitet defineres hvilke personoplysninger, som er relevante for formålet, og det sikres, at der ikke indsamles flere oplysninger end nødvendigt for at understøtte dette formål.
Formålet med behandlingen af personoplysninger, samt hvilke typer personoplysninger, der behandles for hver behandlingsaktivitet, er defineret i "Fortegnelsen over behandlingsaktiviteter"
I tilfælde, hvor det kan være i vores interesse at indsamle flere oplysninger end nødvendigt, kræves juridisk gyldig samtykkeerklæring jf. afsnit 3.1.
Som kontrolfunktion skal alle behandlingsaktiviteter gennemgås en gang årligt, hvor kategorier af indsamlede oplysninger sammenholdes med formålet mhp. at sikre, at oplysningerne fortsat er nødvendige for formålet.

3.3 Sikring af oplysningspligt

Formål:
- Sikre gennemsigtigheden af vores behandling af personoplysninger, samt de registreredes viden om deres rettigheder.

Procedure:
Ved ansættelse bliver alle medarbejdere via deres ansættelseskontrakt informeret om:
- hvem der er dataansvarlig og dennes kontaktoplysninger,
- formålet med behandling af data
- hjemmel for behandling, samt vores legitime interesser heri,
- eventuelle andre modtagere af data, herunder overførsel til tredjelande
- opbevaringsperiode for data
- den registreredes rettigheder i forhold til data (indsigt, berigtigelse, sletning, begrænset behandling og dataportabilitet).
- retten til at tilbagekalde et eventuelt afgivet samtykke
- retten til at klage til Datatilsynet
- at der er pligt til at afgive oplysninger og konsekvenser ved ikke at gøre det
- hvor oplysningerne er indhentet, hvis dette ikke er fra den registrerede selv
- omfanget af automatiske afgørelser, herunder profilering og logikken bag

Hvis vi senere ønsker at behandle oplysninger til et andet formål end oplyst til den registrerede, bliver den registrerede oplyst om dette, før ny behandling indledes.

For at oplyse kunder, leverandører og samarbejdspartnere udformes en tekst, indeholdende de ovenstående punkter, til Møller/Rothes hjemmeside. Et link til denne tekst afgives elektronisk (fx pr. mail) eller via telefon til den registrerede ved første kontakt.

Som kontrolfunktion er det ledelsens ansvar at sikre, at reglen om oplysningspligt er overholdt, og en gang årligt gennemgås aktive medlemskaber.

3.4 Sikring af retten til indsigt

Formål:
- Sikre at den registrerede kan få indsigt i egne oplysninger.

Procedure:
Ved henvendelse skal den registrerede, uden unødigt ophold, på en let forståelig måde have indsigt i de oplysninger, som er registreret om den pågældende, herunder:
- formålet med behandling af data
- hvilke kategorier af oplysninger, som behandles
- eventuelle andre modtagere af data, herunder overførsel til tredjelande
- opbevaringsperiode for data
- den registreredes rettigheder i forhold til data (indsigt, berigtigelse, sletning, begrænset behandling og dataportabilitet)
- retten til at klage til datatilsynet
- hvor oplysningerne er indhentet, hvis dette ikke er fra den registrerede selv
- omfanget af automatiske afgørelser, herunder profilering og logikken bag.

Hvis vi modtager et ønske om indsigt, skal Jan Gelbjerg-Hansen (CEO) kontaktes mhp. at besvare henvendelsen. Oplysninger udleveres i papirform eller elektronisk form, baseret på hvilket format, den registrerede ønsker.

Det sikres, at der meddeles oplysninger til den rette person. Der må kun udleveres oplysninger, når vedkommende har legitimeret sig, eller når der på anden måde er skabt sikkerhed for, at den, der fremsætter en indsigtsbegæring, er identisk med den person, som oplysningerne vedrører eller er i besiddelse af en fuldmagt fra denne.

Telefoniske henvendelser
Ved telefoniske henvendelser skal det sikres, at der kun gives oplysninger til rette person. Det kan f.eks. være nødvendigt at stille kontrolspørgsmål, fx spørge efter adresse og CPR-nr., eller foretage en kontrolopringning til et telefonnummer for at sikre, at det er den rette person, som anmoder om oplysningerne. Hvis medarbejderen ikke kan få den nødvendige sikkerhed, må oplysningerne i stedet sendes pr. post til den adresse, der er registeret på vedkommende.

Henvendelser via brev og e-mail
Hvis navn og adresse i brevet/e-mailen er identisk med de oplysninger, som i forvejen fremgår af systemet, kan oplysningerne normalt sendes til den registrerede på den registrerede post- eller e-mail-adresse. Er dette ikke tilfældet, bør forholdet undersøges nærmere.

Indsigt på andres vegne (fuldmagt)
Den registrerede kan give en anden fuldmagt til at få indsigt i egne oplysninger. Fuldmagten kan være specifik eller generel. Er der tale om en advokat, er det normalt ikke nødvendigt at efterspørge en fuldmagt.

Som kontrolfunktion gennemgås en gang årligt, hvorvidt evt. henvendelser om indsigt er besvaret uden unødigt ophold.

3.5 Sikring af retten til berigtigelse

Formål:
- Sikre, at de registrerede kan få berigtiget deres oplysninger.

Procedure:
Ved henvendelse fra den registrerede skal vi berigtige/rette eventuelle forkerte eller vildledende oplysninger om den pågældende.

Modtager vi besked om, at der behandles forkerte oplysninger, skal Jan Gelbjerg-Hansen (CEO) kontaktes, som herefter sørger for at korrigere oplysningerne. Den registreredes identitet bliver sikret, før oplysninger rettes, jf. afsnit 3.4.

Som kontrolfunktion gennemgås henvendelser om berigtigelse en gang årligt mhp. at sikre, at oplysningerne er korrekte og evt. rettet i systemet.

3.6 Sletteplig og sikring af retten til sletning

Formål:
- Oplysninger slettes, når de ikke længere er nødvendige for formålet med behandlingen
- Sikring af at kunne imødekomme den registreredes ret til sletning

Procedure:
I "Fortegnelsen over behandlingsaktiviteter" er der taget stilling til opbevaringsperioder for hver behandlingsaktivitet.

Personoplysninger opbevares centralt på dertil indrettede drev og systemer, for at mindske spredning af personoplysninger i organisationen og effektivisere sletteprocessen. Hvis medarbejderne har behov for midlertidigt at have personoplysninger liggende lokalt på deres maskiner eller skriveborde, skal disse fjernes, så snart arbejdet er udført.

Det sikres, at oplysninger også slettes hos eventuelle databehandlere.

Oplysninger slettes løbende:
Medarbejdere sletter løbende e-mails indeholdende personoplysninger, når disse er arkiveret andre steder, eller ikke længere er nødvendige for formålet med behandlingen.

Medarbejderne makulerer løbende fysiske dokumenter med personoplysninger, når disse ikke længere er nødvendige for formålet med behandlingen.

De ansvarlige for systemer indeholdende personoplysninger sletter/uigenkaldeligt afidentificerer løbende oplysninger i systemerne, som ikke længere er nødvendige for formålet med behandlingen.

Før oplysninger slettes, sikres det, at oplysningerne ikke er nødvendige at opbevare i henhold til andre lovgivninger, herunder bl.a. bogføringsloven.

Retten til at blive glemt:
Når en registreret henvender sig med et ønske om at blive slettet, skal dette oplyses til Jan Gelbjerg-Hansen (CEO), som er ansvarlige for sletning og som foretager sletningen uden unødigt ophold, efter at have sikret sig, at formålet med behandlingen af oplysningerne ikke længere er til stede. Det skal hermed sikres, at den registrerede ikke har nogle udeståender med os, før sletningen foretages. Den registrerede orienteres om årsagen til, at anmodningen om sletning ikke kan imødekommes helt eller delvist. Den registrerede skal til enhver tid kunne få slettet oplysninger, som er indsamlet baseret på samtykke. Den registreredes identitet bliver sikret, før oplysninger slettes, jf. afsnit 3.4.

Som kontrolfunktion gennemgås behandlingsaktiviteten en gang årligt. Listen over fratrådte medarbejdere samt opbevarede ansøgninger gennemgås, og medarbejdere opfordres jævnligt til at slette overflødige data.

3.7 Sikring af retten til begrænset behandling

Formål:
- Begrænse behandlingen af personoplysninger til kun opbevaring.

Procedure:
Når en registreret henvender sig og fremsætter ønske om, at behandlingen af vedkommendes oplysninger begrænses, skal Jan Gelbjerg-Hansen (CEO), som er ansvarlig for begrænset behandling, straks oplyses herom. Behandlingen af personoplysningerne begrænses til blot at opbevare oplysningerne, indtil forholdet som er grundlag for den begrænsede behandling, løses. Den registreredes identitet bliver sikret, før behandlingen begrænses, jf. afsnit 3.4.

Som kontrolfunktion gennemgås behandlingsaktiviteten en gang årligt.

3.8 Sikring af retten til dataportabilitet

Formål:
- At personlysninger som behandles automatisk kan udleveres eller overføres i et struktureret, almindeligt anvendt og maskinlæsbart format.

Procedure:
Når en registreret henvender sig med et ønske om at få udleveret eller overført personlysninger, rettes der straks henvendelse til Jan Gelbjerg-Hansen (CEO), som er ansvarlig for dataportabilitet, og baseret på den registreredes ønske enten udleverer materialet i et struktureret, almindeligt anvendt, maskinlæsbart format eller, hvis teknisk muligt, overfører oplysningerne til en ny dataansvarlig, ønsket af den registrerede. Den registreredes identitet bliver sikret, før oplysninger udleveres eller overføres, jf. afsnit 3.4.

Som kontrolfunktion gennemgås behandlingsaktiviteten en gang årligt.

3.9 Sikring af retten til indsigelse

Formål:
- Imødekomme den registreredes ret til indsigelse mod profilering og direkte markedsføring.

Procedure:
Når en registreret oplyser, at denne ikke ønsker at vedkommendes oplysninger benyttes til profilering eller direkte markedsføring, skal der straks rettes henvendelse til Jan Gelbjerg-Hansen (CEO), som er ansvarlige for profilering og direkte markedsføring, og som derefter sørger for, at behandlingen af oplysningerne i forbindelse med profilering og direkte markedsføring stoppes. Den registreredes identitet bliver sikret, før behandlingen stoppes, jf. afsnit 3.4.

Det er sikret, at der er mulighed for, at en medarbejder kan behandle den registreredes personoplysninger fremfor en automatiseret proces.

Som kontrolfunktion gennemgås henvendelser om indsigelse en gang årligt for at kontrollere, at der ikke længere benyttes registrerede oplysninger til eks. profilering.

3.10 Databehandleraftaler

Formål:
- Sikring af, at der etableres databehandleraftaler med de, der behandler personoplysninger på vegne af os.

Procedure:
Der er indgået databehandleraftaler med de, der behandler personoplysninger på vegne af os.

Hver gang der indgås en ny aftale med en samarbejdspartner, vurderes det, om ydelsen involverer behandling af personoplysninger på vegne af os. Hvis dette er tilfældet, indgås der en databehandleraftale.

Der udføres løbende kontrol med databehandlerne via indhentede erklæringer eller besøg.
Databehandleraftalerne gemmes centralt af Jan Gelbjerg-Hansen (CEO).

Hvis en medarbejder bliver opmærksom på fejl eller mangler i en databehandlers håndtering af personoplysninger, skal medarbejderen gøre nærmeste leder opmærksom på problemet. Lederen skal herefter undersøge problemet og eventuelt foretage den nødvendige opfølgning. Den øverste IT-ansvarlige i virksomheden inddrages i fornødent omfang, men orienteres som minimum.

Som kontrolfunktion gennemgås vores databehandler aftaler en gang årligt.
3.11 Sikring af dokumentation

Formål:
- Imødekomme Databeskyttelsesforordningens krav om fortegnelse over behandlingsaktiviteter og konsekvensanalyse.

Procedure:
Vi har etableret en fortegnelse over behandlingsaktiviteter, som kan findes hos Jan Gelbjerg-Hansen (CEO). Fortegnelsen opdateres løbende, når der sker ændringer i virksomhedens behandlingsaktiviteter.

For hver behandlingsaktivitet er der foretaget en risikovurdering baseret på sandsynligheden for, at personoplysninger mister fortrolighed, integritet eller tilgængelighed, samt hvilken konsekvens det har for den registrerede.

Risikovurderingen revurderes 1 gang årligt og for høj-risikoområder udarbejdes der en handlingsplan for nedsættelse af risiko. Hvis risikoen ikke kan nedsættes, konsulteres Datatilsynet.

Som kontrolfunktion gennemgås en gang årligt vores behandlingsaktiviteter mhp. at vurdere, om der er tale om en høj risiko, og hvorvidt der skal etableres en konsekvensanalyse og en handlingsplan mhp. at nedsætte risikoen.

3.12 Datasikkerhed

Formål:
- Der er etableret fornødne organisatoriske og tekniske foranstaltninger mod at person oplysninger kommer til uvedkommendes kendskab eller går tabt.

Procedure:
Begrænsning af adgangen til elektronisk persondata
Alle systemer/drev, der indeholder personoplysninger er omfattet af begrænset adgang, således at det kun er de medarbejdere, der har behov for adgangen til at udføre deres arbejde, der har adgang til systemer/drev med personoplysninger.

Som kontrolfunktion gennemgås en gang årligt adgangskoder til systemer og mapper for vores medarbejdere.

Mails med personoplysninger
Mails med personoplysninger er begrænset til et absolut minimum. Følsomme personoplysninger, der skal sendes via mail, skal sendes krypteret.

3.13 Fysisk sikkerhed

Formål:
- Der er forholdsregler, der sikrer mod uvedkommendes adgang til lokaler, hvor der foregår behandling af personoplysninger.

Procedure:
Områder med adgang til personoplysninger sikres således, at uvedkommende ikke kan få adgang til disse. Det sker ved at opbevare personoplysninger i aflåste skabe, når lokalet ikke er under opsyn.

Alle medarbejdere skal låse deres PC, når arbejdsstationen forlades.

Adgangsforhold til matriklen, kontorer mv. gennemgås løbende og nøgler udleveres alene på navn og til begrænset antal medarbejdere.

3.14 Gæster

Formål:
- Gæster skal håndteres sikkert.

Procedure:
Gæster, der skal opholde sig i længere tid eller alene i lokalerne skal registreres, og må ikke færdes alene. Gæster som opholder sig i lokaler, hvor der håndteres personoplysninger, skal informeres om deres tavshedspligt og evt. udfylde en tavshedserklæring, som opbevares.

Som kontrolfunktion gennemgås disse tavshedspligtserklæringer en gang årligt.

3.15 Print og dokumenter med personoplysninger

Formål:
- Personlige oplysninger må ikke ligge frit tilgængelige i papirform.

Procedure:
Print med personoplysninger må ikke efterlades i printerrummet.
Papirdokumenter, der indeholder personoplysninger, må i arbejdstiden ikke opbevares uden opsyn af en medarbejder.

Alle henvendelser (breve i papirformat, print af e-mails, papirlapper m.v.), som indeholder personoplysninger skal efter endt brug smides ud i en særlig aflåst papircontainer, som står i kopirummet eller makuleres. Indholdet af papircontainer bliver makuleret, når containeren er fyldt.

Som kontrolfunktion er alle medarbejdere opmærksomme på at fjerne print med personoplysninger el.lign.

3.16 Sikring af medarbejder awareness

Formål:
- Demonstrere at medarbejdere er bekendt med reglerne for behandling af persondata.

Procedure:
Samtlige nye medarbejdere skal underskrive en tavshedserklæring ved deres ansættelse.
Alle nye medarbejdere skal i forbindelse med deres ansættelse gøres bekendt med regler for behandling af personoplysninger og IT-sikkerhed.

Som kontrolfunktion gennemgås alle nyansættelser og tilhørende personalesager en gang årligt.

3.17 Notifikation ved brud på datasikkerheden

Formål:
- Datatilsynet, og under visse omstændigheder, den registrerede, bliver ved brud på datasikkerheden notificeret om muligt indenfor 72 timer efter et brud er konstateret.

Procedure:
Brud på datasikkerheden er defineret som en hændelse, der resulterer i, at der sandsynligvis er en risiko for, at personoplysninger er blevet udsat for uautoriseret adgang eller er gået tabt.

Hvis en medarbejder opdager brud på datasikkerheden, meddeles dette straks til Jan Gelbjerg-Hansen (CEO), som indenfor 72 timer, om muligt, skal have overblik over bruddet. Jan Gelbjerg-Hansen indsamler oplysninger om hændelsen, berørte datakategorier, antal lækkede data records, sandsynlige konsekvenser og hvilke tiltag, der er iværksat for at imødegå bruddet, som anmeldes til Datatilsynet indenfor 72 timer via Datatilsynets hjemmeside.

Brud, der sandsynligvis medfører en risiko for, at personoplysninger er blevet udsat for uautoriseret adgang eller er gået tabt, anmeldes til Datatilsynet.

Alle brud på sikkerheden noteres i Databrudsloggen.

Hvis sikkerhedsbruddet er af sådan karakter, at det er nødvendigt at informere de registrerede, gøres dette via e-mail.

Hvis virksomheden ikke har kontaktoplysningerne på de registrerede, sker orienteringen offentligt via Datatilsynets hjemmeside.

Som kontrolfunktion gennemgås en gang årligt, hvorvidt alle utilsigtede hændelser er anmeldt til Datatilsynet indenfor 72 timer.

3.18 Privacy by Design og Privacy by Default

Formål:
- Imødekommelse af Databeskyttelsesforordningens krav om Privacy by design and default.

Procedure:
Ved udvikling eller anskaffelse af nye it-systemer er virksomheden opmærksom på, at systemerne er sikre, og at de understøtter opdeling af adgangsrettigheder, således at personoplysninger kan beskyttes mod uautoriseret adgang og tab.

Medarbejderne må ikke benytte tjenester til behandling af personoplysninger, som ledelsen ikke har godkendt, herunder bl.a. private mail-applikationer, egne cloudløsninger eller programmer, som kan downloades fra nettet til behandling af personoplysninger.
Som kontrolfunktion gennemgås vores IT-system, og deres opsætning en gang årligt.

3.19 DPO

Formål:
- Vurdering af, om det er et krav, at virksomheden har en DPO

Procedure:
Det vurderes årligt, hvorvidt virksomheden har behov for en DPO, baseret på Databeskyttelsesforordningens kriterier for krav om DPO.

Det er ved indførelsen af nærværende retningslinjer maj 2018 vurderet, at Møller/Rothe ikke har brug for en DPO.