Persondatapolitik for

Kong Frederik den Syvendes Stiftelse paa Jægerspris

til alle medarbejdere –

vedrørende behandling af personoplysninger

Version	Dato	Ændret af	Godkendt af
1.0	25.07. 2018	NS	NS

Indhold

Persondatapolitik for Kong Frederik den Syvendes Stiftelse paa Jægerspris (Stiftelsen).

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

Stiftelsens persondatapolitik er udformet i sammenhæng med virksomhedens overordnede strategi, værdier og visioner og er på den måde en integreret del af, hvordan virksomheden 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 man straks kontakte sin nærmeste leder og informere denne om problematikken.

Persondatapolitikken bliver gennemgået og opdateret løbende. Ved ansættelse bliver alle nye medarbejdere gjort bekendt med persondatapolitikken.

1. Definitioner

Stiftelsen behandler persondata i forbindelse med ansøgninger, ansættelse, køb, salg, samarbejde og HR-funktioner. 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, fagforeningstilhørsforhold, race, etnicitet, politisk overbevisning, oplysninger om strafbare forhold mv.
Registrerede	Alle personer, hvis oplysninger er registreret hos Stiftelsen, 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 alle afdelinger, men det kan være nødvendigt at indføre specifikke instrukser i specifikke afdelinger. I så fald skal disse instrukser være i overensstemmelse med persondatapolitikken, have en klar ansvarsfordeling og en fast plan for opdatering.

Ansvaret for medarbejdernes overholdelse af denne persondatapolitik hviler først hos medarbejderne selv, dernæst hos afdelingslederne. Hvis kontrollen viser, at der har været episoder, hvor persondatapolitikken ikke er blevet overholdt, er det afdelingslederens opgave at afhjælpe problemet.

3. Medarbejderinstruks

Det følgende er de konkrete regler og retningslinjer, som alle ansatte i Stiftelsen skal følge i forbindelse med behandling af persondata. Instruksen er baseret på Databeskyttelsesforordningens og Databeskyttelseslovens krav. 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:

- Der er et lovligt grundlag for at behandle data

Procedure:

Før en databehandling påbegyndes skal der ske en afklaring af den lovlige hjemmel. Hvis et lovlig grundlag ikke kan identificeres, igangsættes behandlingen ikke.

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

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 bliver det klart defineret 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 virksomhedens interesse at indsamle flere oplysninger end nødvendigt, skal der med hjælp fra juridisk afdeling udarbejdes en samtykkeerklæring jf. afsnit 3.1.

3.3 Sikring af oplysningspligt

Formål:

- Sikre gennemsigtigheden af virksomhedens behandling af personoplysninger, samt de registreredes viden om deres rettigheder.

Procedure:

Ved ansættelsen bliver medarbejderne via deres ansættelseskontrakt på en letforståelig måde informeret om:

- formålet med behandling af personlige data,

- hjemmel for behandling,
- eventuelle andre modtagere af data,
- 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 de har pligt til at afgive oplysninger og konsekvenser ved ikke at gøre det,
- hvor oplysningerne er indhentet, hvis dette ikke er direkte fra den registrerede selv,

Hvis virksomheden senere ønsker at behandle oplysninger til et andet formål end oplyst til den registrerede, bliver den registrerede oplyst om dette før den nye behandling igangsættes.

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

3.4 Sikring af retten til indsigt

Formål:

- Sikre at den registrerede kan få indsigt i de oplysninger, som behandles om dem

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 direkte fra den registrerede selv.

Der må kun udleveres personlige oplysninger efter skriftlig henvendelse enten som brev eller via mail.

Oplysninger udleveres i papirform eller almindelige anvendt elektronisk form, baseret på hvilket format, den registrerede ønsker.

Det sikres, at den, der meddeles oplysninger til, er 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.

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-mailadresse. Er dette ikke tilfældet, bør forholdet undersøges nærmere.

Indsigt for børn under 18 år
Forældremyndighedens indehaver kan begære indsigt på barnets vegne. Barnet kan også selv få indsigt.

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.

3.5 Sikring af retten til berigtigelse

Formål:

- Sikre, at de registrerede kan få berigtiget deres oplysninger

Procedure:

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

En medarbejder, der modtager besked om at der behandles forkerte oplysninger, henvender sig til Stiftelsens administration, Slotsgården 20, 3630 Jægerspris, mail: kf@kongfrederik.dk, som sørger for at korrigere oplysningerne. Den registreredes identitet bliver sikret før oplysninger rettes, jf. afsnit 3.4.

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.

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 Stiftelsens administration, Slotsgården 20, 3630 Jægerspris, mail: kf@kongfrederik.dk, 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 virksomheden, før sletningen foretages. Medarbejderne, som håndterer anmodningen om sletning, orienterer den pågældende registrerede 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.

Sletning i backup:

I henhold til virksomhedens backup-strategi bliver backups overskrevet en gang månedligt, så alle sletninger i systemet bliver overskrevet i backuppen en gang månedligt.

3.7 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 Stiftelsens administration, Slotsgården 20, 3630 Jægerspris, , som 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.

3.8 Databehandleraftaler

Formål:

- Sikring af, at der etableres databehandleraftaler med andre juridiske enheder, som behandler personoplysninger på vegne af os.

Procedure:

Der er indgået databehandleraftaler med eksterne juridiske enheder, der behandler personoplysninger på vegne af Stiftelsen.

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.

3.9 Sikring af dokumentation

Formål:

- Imødekomme Databeskyttelsesforordningens krav om fortegnelse over behandlingsaktiviteter og konsekvensanalyse

Procedure:

Virksomheden har etableret en fortegnelse over behandlingsaktiviteter, som kan findes på GDPR Portalen. Fortegnelsen opdateres løbende, når der sker ændringer i virksomhedens behandlingsaktiviteter.

Medarbejderne er instrueret i at opdatere fortegnelsen i tilfælde af ændringer til deres 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 risiko områder udarbejdes der en handlingsplan for nedsættelse af risiko. Hvis risikoen ikke kan nedsættes konsulteres Datatilsynet.

3.10 Datasikkerhed

Formål:

- Der er etableret fornødne organisatoriske og tekniske foranstaltninger mod at personoplysninger 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.

Mails med personoplysninger
Mails med personoplysninger er begrænset til et absolut minimum.

3.11 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. Løbende, afhængig af mængden af bilag, kan personoplysninger fra aflåste skabe arkiveres i et aflåst arkiveringsrum.

3.12 Print og dokumenter med personoplysninger

Formål:

- Personlige oplysninger må ikke ligge frit tilgængeligt i papirform.

Procedure:

Print foregår altid med Follow You Print. 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 makuleres.

3.13 Sikring af medarbejder awareness

Formål:

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

Procedure:

Samtlige medarbejdere i Stiftelsen 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.

3.14 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 Stiftelsens direktør, der så hurtigt som muligt skal have overblik over bruddet. Større brud på datasikkerheden anmeldes til datatilsynet indenfor 72 timer via deres 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 mail.

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

3.15 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 Stiftelsen 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 Stiftelsen ikke har godkendt, herunder bl.a. private mail-applikationer, sin egen cloudløsning eller programmer, som kan downloades fra nettet til behandling af personoplysninger.