



Danish Crown

Koncernpolitik for databeskyttelse

September 2024 – Version 2.0



Dokumentstyring

Styring	
Version	2.0
Udstederen	Lise Lotte Langston (LILOL)
Godkender	Thomas Ahle (TAH)
Udsendelsesdato	26-09-2024
Ansøgningsdato	26-09-2024
Omfanget	Danish Crown Group
Hyppighed af gennemgang	Hvert 2. år

Versionshistorik			
Vs.	Dato	Ændret af	Oversigt over ændringer og opdateringer
1.0	01.01.2018	Rasmus Schjoldager	Gennemførelse af politikken
1.1	01-01-2021	Jesper Green Schou (JEGSC)	Opdatering for forbedret kommunikation.
1.2	01-02-2022	Jonas Hvid (JONHV)	Opdateret i forbindelse med implementering af standarder og andre retningslinjer/SOP'er
1.3	02-05-2023	Jonas Hvid (JONHV)	Opdatering af udsteder og godkender
2.0	26-09-2024	Jonas Hvid (JONHV)	Generel opdatering af politikken

Link til relaterede gruppedokumenter	
Navn på dokumentfil	Dokumentets indhold
GDPR-Guideline	GDPR-retningslinje for alle medarbejdere
GDPR Guideline HR	GDPR-retningslinje for HR-medarbejdere
GDPR Guideline Manager	GDPR-retningslinje for ledere
SOP Conclusion of DPA	Procedure for indgåelse af aftaler med databehandlere.
GDPR-Guideline photos and statements	Vejledning til marketing- og HR-medarbejdere, der bruger billeder internt og online
SOP How to exercise data subject rights	Procedure for udøvelse af registreredes rettigheder
SOP Audit data processors	Procedure for sikring af audit af databehandlere
SOP Transfer of personal data to countries outside EU/EEA	Procedure for indgåelse af aftaler med databehandlere uden for EU/EØS
SOP Yearly GDPR documentation review	Procedure for at sikre en årlig opdatering af GDPR-dokumentationen
Information Security Policy	Politik for alle medarbejdere med krav til beskyttelse af oplysninger
IT Security Guideline	Vejledning til alle medarbejdere om krav til arbejde med IT-udstyr



Indhold

Kontrol af dokumenter	2
1. Vores politik	4
1.1 Vores forpligtelse.....	4
1.2 Vores kultur.....	4
1.3 Vores pligt til at fremme overholdelse.....	4
1.4 Globalt konsistente høje standarder.....	4
2. Beskyttelse af personoplysninger	5
2.1 Hvad er personoplysninger?.....	5
2.2 Behandling af personoplysninger.....	5
2.2.1 Principper for databeskyttelse.....	5
2.2.2 Retsgrundlag for behandling af almindelige og fortrolige personoplysninger.....	5
2.2.3 Retsgrundlag for behandling af følsomme personoplysninger.....	5
2.3 GDPR-retningslinjer.....	6
2.4 Leverandører, der behandler personoplysninger på vores vegne.....	6



1. Vores politik

1.1 Vores forpligtelse

Ledelsen i Danish Crown er stærkt engageret i at sikre, at koncernen overholder den gældende databeskyttelseslovgivning. Denne forpligtelse er en del af vores generelle forpligtelse som en ansvarlig koncern til at handle med integritet og opfylde kravene i den gældende lovgivning i de lande, hvor vi opererer.

Vores forpligtelse til at beskytte personoplysninger er et fælles ansvar, og hver af os er forpligtet til at forstå vores fælles ansvar for at drive vores forretning på en måde, der er i overensstemmelse med vores værdier og i overensstemmelse med denne politik.

1.2 Vores kultur

I Danish Crown understøtter vi en compliance-kultur og giver den nødvendige vejledning og obligatorisk træning til alle relevante medarbejdere. På den måde sikrer vi, at alle relevante medarbejdere har et stærkt kendskab til reglerne og evne til at overholde de vejledninger, der gives.

Vi fremmer aktivt en kultur, hvor "at spille efter reglerne er business as usual", og vi opfordrer medarbejderne til at tage potentielle compliance-problemer op åbent.

1.3 Vores pligt til at fremme overholdelse

En overtrædelse af den nationale og/eller EU's databeskyttelsesforordning kan få alvorlige konsekvenser for Danish Crown og den enkelte, der lider under et databrud eller uretmæssig behandling af hans/hendes personoplysninger. Derfor skal hver medarbejder være opmærksom på følgende forpligtelser:

- A) Alle medarbejdere forventes at bidrage aktivt til at overholde de gældende regler i databeskyttelseslovgivningen.
- B) Ingen medarbejder bør gå ud fra, at Danish Crowns interesser nogensinde kræver andet end overholdelse af reglerne;
- C) Ingen har bemyndigelse til at give ordrer eller anvisninger, der ville resultere i en overtrædelse af reglerne;
- D) Den enkelte medarbejder er forpligtet til at søge råd og vejledning hos sin nærmeste leder og/eller chefjuristen i tvivl. og.
- E) Enhver overtrædelse eller mistanke om overtrædelse skal rapporteres til Group General Counsel. Det er også muligt at indberette en bekymring i Danish Crown Whistleblowerordningen.

1.4 Samme høje standarder globalt

Denne politik gælder i alle jurisdiktioner, hvor vi opererer. Vores politik afspejler behovet for globalt konsistente og høje standarder for at demonstrere vores forpligtelse til at drive vores forretning på en måde, der er i overensstemmelse med vores værdier, uanset jurisdiktion. Vi anerkender, at der kan være potentielle forskelle i lokal lovgivning, der påvirker vores lokale aktiviteter, og Group General Counsel vil give yderligere rådgivning og instruktioner efter behov.



2. Beskyttelse af personoplysninger

2.1 Hvad er personoplysninger?

Personoplysninger betyder alle oplysninger, der kan relateres til en identificeret eller identificerbar fysisk person ("den registrerede").

Personoplysninger skal behandles i overensstemmelse med den generelle databeskyttelsesforordning ("GDPR").

Personoplysninger er opdelt i tre kategorier: almindelige personoplysninger, følsomme personoplysninger og fortrolige personoplysninger:

Almindelige personoplysninger omfatter alle personoplysninger, der ikke er klassificeret som følsomme personoplysninger eller fortrolige personoplysninger.

Følsomme personoplysninger er oplysninger, der ved lov er klassificeret som følsomme, såsom personoplysninger om helbred, fagforeningsmæssigt tilhørsforhold, race og etnisk oprindelse, seksuel og politisk overbevisning og biometriske oplysninger.

Fortrolige personoplysninger er oplysninger, der er klassificeret som almindelige, men samfundets almindelige opfattelse vil anse det for uhensigtsmæssigt, hvis oplysningerne ikke er tilstrækkeligt sikret. Fortrolige personoplysninger kan være CPR-nummer, pas, økonomisk indkomst, straffeattest mv.

2.2 Behandling af personoplysninger

Behandling af personoplysninger er grundlæggende alt, hvad du kan gøre med personoplysninger, både automatiseret behandling og manuel håndtering, såsom indsamling, strukturering, opbevaring, videregivelse, tilgængeliggørelse, sletning og destruktions.

Behandling af alle personoplysninger skal:

- være i overensstemmelse med databeskyttelsesprincipperne beskrevet nedenfor i afsnit 2.2.1
- har et retsgrundlag som defineret i databeskyttelseslovgivningen beskrevet nedenfor i afsnit 2.2.2 og 2.2.3 og
- være i overensstemmelse med GDPR-retningslinjen for alle medarbejdere.

2.2.1 Principper for databeskyttelse

De databeskyttelsesprincipper, der gælder i henhold til databeskyttelseslovgivningen, fastsætter, at personoplysninger skal:

- **Princip 1:** Personoplysninger skal behandles lovligt, retfærdigt og gennemsigtigt ved at sikre, at der gives en meddelelse om beskyttelse af personlige oplysninger til den registrerede;
- **Princip 2:** Personoplysninger må kun behandles til et specifikt, udtrykkeligt og legitimt formål;
- **Princip 3:** Personoplysninger, der behandles til et formål, skal være tilstrækkelige og relevante for det formål, hvortil de behandles. For mange data bør ikke behandles;
- **Princip 4: Personoplysninger**, der behandles, skal holdes nøjagtige og ajourførte.
- **Princip 5:** Personoplysninger, der behandles, skal slettes, når der ikke længere er brug for oplysningerne, og
- **Princip 6:** Personoplysninger, der opbevares eller overføres, skal opbevares sikkert ved hjælp af passende tekniske og organisatoriske foranstaltninger.

2.2.2 Retsgrundlag for behandling af almindelige og fortrolige personoplysninger

Ud over opfyldelsen af databehandlingsprincipperne (afsnit 2.2.1) skal enhver behandling have et retsgrundlag ("retsgrundlag"). Det nødvendige retsgrundlag kan indhentes, hvis behandlingen af personoplysninger er:

- baseret på den registreredes samtykke;
- nødvendige for opfyldelsen af en kontrakt
- nødvendigt for at overholde en retlig forpligtelse eller
- nødvendig med henblik på en legitim interesse, forudsat at en sådan behandling ikke anses for at være skadelig for den registrerede.

2.2.3 Retsgrundlag for behandling af følsomme personoplysninger

Det er generelt forbudt at behandle følsomme personoplysninger i Danish Crown, men der er nogle



tilfælde, hvor det er nødvendigt at behandle følsomme personoplysninger

f.eks. i forhold til sundhed og sikkerhed og HR. I disse tilfælde skal det overvejes, om behandling af følsomme personoplysninger er:

- baseret på den registreredes samtykke; eller
- nødvendige for overholdelse af regler og bestemmelser om beskæftigelse, social sikring eller social beskyttelse.

2.3 GDPR-retningslinjer

For at overholde databeskyttelseslovgivningen er der udarbejdet en række praktiske retningslinjer.

Retningslinjerne er en integreret del af denne politik for overholdelse af databeskyttelse og leveres til alle relevante medarbejdere som en del af den obligatoriske uddannelse, der gennemføres under vores program for overholdelse af databeskyttelse.

Yderligere information og retningslinjer for GDPR kan findes på Danish Crowns intranet om databeskyttelse, som kan findes her: [Link](#)

2.4 Leverandører, der behandler personoplysninger på vores vegne

For at overholde databeskyttelseslovgivningen er der udarbejdet en række praktiske retningslinjer.

Danish Crown er ansvarlig for at beskytte de registreredes personoplysninger. Dette gælder også, når en leverandør behandler vores data.

For at overholde GDPR er det obligatorisk at sikre, at der er indgået en databehandleraftale med en leverandør, hvis primære ydelse er at behandle personoplysninger på vegne af Danish Crown.

Danish Crown kan blive pålagt store bøder og sanktioner, hvis Danish Crown ikke indfører tilstrækkelige sikkerhedsforanstaltninger for databeskyttelse, herunder databehandleraftaler. Mere vejledning kan findes i GDPR-vejledningen, som du finder her: [Link](#)

2.5 IT-sikkerhed

Danish Crowns medarbejdere er forpligtet til at overholde Danish Crowns IT-sikkerhedsvejledning, som beskriver de tekniske og organisatoriske sikkerhedsforanstaltninger, som enhver medarbejder skal kende og overholde. IT-sikkerhedsvejledningen kan findes på Kronens intranetside om databeskyttelse, som kan findes her: [Link](#)

2.6 Brud på datasikkerheden

Danish Crown har etableret en proces, som alle medarbejdere skal følge i tilfælde af brud på sikkerheden. En

Brud på datasikkerheden kan defineres som en hændelse, der kan kompromittere fortroligheden, integriteten eller tilgængeligheden af en Registreredes personoplysninger eller Danish Crowns IT-infrastruktur, hvor personoplysninger behandles.

Eksempler på brud på sikkerheden:

- En e-mail, der indeholder fortrolige eller følsomme personoplysninger, sendes til en eller flere forkerte modtagere (både internt og eksternt).
- En e-mail med fortrolige eller følsomme personlige data vises, mens du deler skærmen under onlinemøder.
- En bærbar computer bliver stjålet eller glemt/efterladt uden opsyn.
- Fysiske dokumenter, der indeholder fortrolige eller følsomme personoplysninger, går tabt/forlægges.
- Cybersikkerhedsangreb, der involverer personoplysninger.
- Et dokument, der indeholder fortrolige eller følsomme personoplysninger, var utilstrækkeligt maskeret/skjult.

I tilfælde af brud på sikkerheden skal et sådant brud rapporteres hurtigst muligt via IT Service Desk. Danish Crowns IT-afdeling vil efterfølgende hjælpe med at inddæmme skaden og vurdere, om bruddet skal anmeldes til myndighederne.

Klik her for at rapportere et brud på sikkerheden: [Link](#)

Danish Crown har pligt til at vurdere, om en overtrædelse skal anmeldes til den relevante myndighed senest 72 timer efter, at Danish Crown er blevet bekendt med overtrædelsen.

2.7 Sådan søger du yderligere rådgivning

I Danish Crown anerkender vi, at en åben og ærlig dialog er en forudsætning for at bevare og løbende styrke vores integritet.

Som medarbejder i Danish Crown er det din ret og dit ansvar at få vejledning om enhver forretningsmæssig beslutning, du er usikker på. Det første kontaktpunkt i forhold til GDPR-spørgsmål bør være at kontakte GDPR@danishcrown.com