

Vedtaget af:	Sidst opdateret:	Vedtages	Tilgængelighed:	Version:
Bestyrelsen	24-04-2018 07-05-2019	Årligt samt efter behov	Internt	1.1
Ejere:	Anvendelsesområde:	Retsgrundlag:	Sider:	
Corporate Compliance Officer	Behandling af personoplysninger	<ul style="list-style-type: none">Persondataforordningen, GDPR (General Data Protection Regulation) og national databeskyttelseslovgivning i Sverige og DanmarkForskrifter og generelle råd fra databeskyttelsesmyndighederne i Sverige og Danmark	15	

Politik for beskyttelse af privatlivets fred

OKQ8 Scandinavia

Vedtaget af bestyrelsen for OK-Q8 AB den 7. maj 2019

Indholdsfortegnelse

1	Indledning.....	3
1.1	Baggrund og formål.....	3
1.2	Definitioner.....	3
2	Organisation og ansvar.....	5
2.1	Logiske registre til fastsættelse af dataansvar.....	5
2.2	Ansvar, roller og samarbejdsformer.....	5
2.2.1	Roller og ansvarsområder.....	5
2.2.2	Samarbejdsformer.....	7
2.3	Liste over behandling af personoplysninger.....	7
3	Udgangspunkt for behandling af personoplysninger i OKQ8 Scandinavia.....	8
3.1	Generelt om behandling af personoplysninger.....	8
3.2	Grundlæggende principper for OKQ8 Scandinavias behandling af personoplysninger.....	8
4	Hvornår er det lovligt at behandle personoplysninger?.....	9
4.1	Generelt om lovlig behandling.....	9
4.2	Retsgrundlag ved direkte markedsføring.....	9
4.3	Retsgrundlag for behandling af personoplysninger om medarbejdere.....	10
4.4	Overførsel af personoplysninger til tredjeland.....	10
5	Den registreredes rettigheder.....	10
6	Sortering i personoplysninger.....	11
7	Persondatasikkerhed.....	12
7.1	Generelt.....	12
8	Videregivelse af personoplysninger.....	13
8.1	Videregivelse til eksterne databehandlere.....	13
8.2	Videregivelse til parter med eget dataansvar.....	13
8.3	Videregivelse af oplysninger til tredjeland.....	13
8.4	Anmodning fra myndigheder om oplysninger.....	13
9	Brud på persondatasikkerheden.....	14
10	Indberetning.....	14
11	Opfølgning og kontrol.....	14
12	Vedtagelse og opdatering.....	14

1 Indledning

1.1 Baggrund og formål

OK-Q8 AB og dets datterselskaber ('OKQ8 Scandinavia') håndterer en stor mængde personoplysninger i virksomheden. Personoplysningerne behandles blandt andet for, at OKQ8 Scandinavia skal kunne opfylde aftaler indgået med kunder, leverandører og medarbejdere, være i stand til at yde en god service til kunderne og kunne overholde forpligtelser i henhold til andre love og regler.

Indsamling af personoplysninger sker for eksempel, når en kunde giver sine oplysninger til OKQ8 Scandinavia i forbindelse med køb af serviceydelser, eller når en medarbejder påbegynder sin ansættelse i OKQ8 Scandinavia. Personoplysninger kan også indsamles uden en aktiv handling fra kundens side, f.eks. gennem cookies på hjemmesiden eller samkøring med eksterne adresseregistre.

Du kan finde yderligere information om hvilke personoplysninger, OKQ8 Scandinavia behandler, og til hvilke formål, på intranettet, eller du kan få dem udleveret af selskabsjuristerne. Du kan også finde ekstern information om behandling af personoplysninger på OKQ8 Scandinavias eksterne websites.

Denne politik indeholder generelle krav og retningslinjer, der skal sikre, at indsamling og behandling af personoplysninger i OKQ8 Scandinavia sker i overensstemmelse med gældende databeskyttelseslovgivning og andre gældende eksterne love og regler. Denne politik træder i kraft den 25. maj 2018.

For OK-Q8 Bank AB findes der en separat politik for beskyttelse af privatlivets fred, der også tager hensyn til andre love og regler, der gælder for banker og pengeinstitutter.

1.2 Definitioner

Behandling af personoplysninger

Enhver handling eller række af handlinger, der foretages i forbindelse med personoplysninger, uanset om det sker automatisk eller ej, f.eks. indsamling, registrering, organisering, opbevaring, behandling, ændring, begrænsning, justering, sletning eller tilintetgørelse, videregivelse ved fremsendelse, formidling, eller hvor oplysninger stilles til rådighed på anden vis, sammenfattes eller samkøres.

Databeskyttelseslovgivning

Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger samt enhver anden national eller international lov, forordning, direktiv, myndighedsforskrift eller generelle råd, der til enhver tid er gældende for OKQ8 Scandinavias behandling af personoplysninger.

OKQ8 Scandinavia GDPR-forum

Et tværfunktionelt forum i OKQ8 Scandinavia, der skal sikre høj overholdelse af reglerne i forbindelse med styring og gennemførelse af persondatabehandlingen.

Aftale om datadeling

En aftale mellem alle virksomheder og foreninger inden for OK/OKQ8-sfæren med henblik på at overholde de lovmæssige krav til den nødvendige og juridiske deling, udveksling og behandling af personoplysninger inden for OK/OKQ8-sfæren.

Databeskyttelsesforum

Et forum bestående af databeskyttelseskontakter fra alle virksomheder og foreninger inden for OK/OKQ8-sfæren. Databeskyttelsesforummet behandler og drøfter spørgsmål vedrørende ændringer i aftalen om datadeling, specifikationer samt databeskyttelseskontakternes mandat og arbejdsopgaver.

Interne regelsæt

OKQ8 Scandinavias interne politik, der består af politikker, instruktioner, procedurer og tjeklister i forbindelse med behandling af personoplysninger.

OK/OKQ8-sfæren

Alle virksomheder i OKQ8 Scandinavia, OK Detaljhandel AB samt alle OK-foreninger og franchisetagere, der driver virksomhed under OKQ8 Scandinavias varemærker.

Personoplysninger

Alle oplysninger, der vedrører en identificeret eller identificerbar fysisk person, der er i live. Med en identificerbar fysisk person menes en person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator, som f.eks. et navn, et identifikationsnummer, lokaliseringsdata eller et online-ID eller ved et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Dataansvarlig

Den juridiske person, der alene eller sammen med andre fastlægger formålene med og midlerne til behandlingen af personoplysningerne.

Databehandler

En juridisk person, der behandler personoplysninger på vegne af den dataansvarlige, f.eks. OKQ8 Scandinavias IT-leverandører.

2 Organisation og ansvar

Ved hver behandling af personoplysninger kan en aktør inden for OK/OKQ8-sfæren være en enkelt dataansvarlig, en fælles dataansvarlig eller en databehandler. I lyset af den gældende databeskyttelseslovgivning skal det fremgå tydeligt og være dokumenteret, hvem der inden for OK/OKQ8-sfæren er dataansvarlig for hver enkelt behandling af personoplysninger.

For OK/OKQ8-sfæren er ansvarsfordelingen dokumenteret i aftalen om datadeling samt i den pågældende virksomheds/forenings liste over behandling af personoplysninger.

2.1 Logiske registre til fastsættelse af dataansvar

Inden for OKQ8 Scandinavia er dataansvaret fordelt på baggrund af 'logiske registre'. De logiske registre er en logisk gruppering af de personoplysninger, der behandles til et bestemt formål, uanset hvilke IT-systemer der bruges til behandlingen.

Hvert enkelt logisk register er knyttet til en eller flere virksomheder i OKQ8 Scandinavia med dataansvar.

2.2 Ansvar, roller og samarbejdsformer

2.2.1 Roller og ansvarsområder

Ansvaret for, at personoplysninger behandles i henhold til gældende databeskyttelseslovgivning, denne politik samt andre interne og eksterne regler, omfatter alle niveauer inden for OKQ8 Scandinavias organisation fra bestyrelse til operativt udførende funktioner. Ansvaret for behandling af personoplysninger inden for OKQ8 Scandinavia er fordelt som beskrevet i denne politik.

Bestyrelsen

Bestyrelsen har ansvar for at fastlægge denne politik og de andre politikker, der skal til for at sikre overholdelse af gældende databeskyttelseslovgivning.

Administrerende direktør

Den administrerende direktør har ansvar for at udarbejde og opdatere denne politik, og for at alle medarbejdere og leverandører har adgang til politikken. Den administrerende direktør er ansvarlig for at sikre, at der findes en fungerende organisation og mulighed for, at databeskyttelsesrådgiveren kan udføre sit arbejde i overensstemmelse med databeskyttelseslovgivningen.

Databeskyttelsesrådgiver/Corporate Compliance Officer

OKQ8 Scandinavias Corporate Compliance Officer er blevet udnævnt til databeskyttelsesrådgiver for alle virksomheder i OKQ8 Scandinavia. Corporate Compliance Officer har det overordnede ansvar for at udarbejde, implementere og sørge for at følge op på interne regler, der gør det muligt for OKQ8 Scandinavia at håndtere personoplysninger i overensstemmelse med gældende databeskyttelseslovgivning og denne politik.

Corporate Compliance Officer har ansvar for at uddanne og støtte OKQ8 Scandinavias medarbejdere i spørgsmål og forhold vedrørende behandling af personoplysninger samt for at varetage kontakten til de kompetente databeskyttelsesmyndigheder.

Kontraktunderskriver og databehandler

Databehandleren behandler personoplysninger på ordre af OKQ8 Scandinavia og på OKQ8 Scandinavias vegne. Mellem den dataansvarlige og hver enkelt databehandler kræves der en skriftlig aftale med et bestemt indhold (databehandlingsaftale) i henhold til databeskyttelseslovgivningen. En sådan databehandlingsaftale skal udformes i overensstemmelse med Corporate Compliance Officers instruktioner og OKQ8 Scandinavias aftaleskabelon. Kontraktunderskriveren er ansvarlig for at sikre, at der findes en korrekt databehandlingsaftale for alle databehandlere. Afvigelser fra aftaleskabelonen skal godkendes på forhånd af Corporate Compliance Officer eller selskabsjuristerne. Kontraktunderskriveren har også ansvar for at sikre, at databehandlingsaftalen indeholder specifikationer og tilstrækkelige instruktioner i forbindelse med opgaven. Kontraktunderskriveren har ansvar for at kontakte Corporate Compliance Officer eller selskabsjuristerne, hvis der er behov for det.

Datakoordinatorer

OKQ8 Scandinavias datakoordinatorer har ansvar for at sikre, at den driftsmæssige behandling af personoplysningerne overholder gældende databeskyttelseslovgivning, denne politik og andre interne regler. Den enkelte datakoordinator har ansvar for et eller flere logiske registre med personoplysninger, autoriseret behandling, regler for sortering osv. Ansvarer omfatter desuden implementering og løbende opdatering af processer, rutiner og tjeklister, der sikrer korrekt håndtering af personoplysninger, samt indberetning af spørgsmål vedrørende personoplysninger til Corporate Compliance Officer.

Head of Information & IT Security

Head of Information & IT Security implementerer koordineringen af informationssikkerhedsarbejdet i OKQ8 Scandinavia og forvalter politik, de tilhørende retningslinjer og instrukser samt den generelle handlingsplan inden for informationssikkerhedsområdet. Ansvarer omfatter også opfyldelse af krav til IT- og informationssikkerhed i OKQ8 Scandinavias IT-miljøer samt bemanning og administration af de specialistrøler, der er nødvendige for at opfylde kravene. Håndtering af hændelser inden for IT-sikkerhedsområdet, rapportering til informationssikkerhedsgruppen og opfølgning over for leverandører er andre ansvarsområder inden for IT- og informationssikkerhedsområdet. Om nødvendigt bistår Head of information & IT Security Corporate Compliance Officer med risikoanalyser og konsekvensanalyser for at sikre princippet om indbygget databeskyttelse (privacy by design).

Alle medarbejdere

Alle medarbejdere og, hvor det er relevant, leverandører, der arbejder under OKQ8 Scandinavias ledelse, har et eget ansvar for at håndtere personoplysninger i overensstemmelse med gældende databeskyttelseslovgivning, denne politik og interne regler. I tilfælde af tvivl om, hvorvidt en

behandling af personoplysninger er tilladt, skal Corporate Compliance Officer eller selskabsjuristerne altid kontaktes.

Alle kontomedarbejdere og, hvor det er relevant, leverandører, der arbejder under OKQ8 Scandinavias ledelse, skal gennemgå en obligatorisk GDPR-uddannelse, som OKQ8 Scandinavia har udviklet.

2.2.2 Samarbejdsformer

Der er etableret interne regler, OKQ8 Scandinavias GDPR-forum og tydelig funktionel rapportering mellem de styrende og de udførende funktioner til behandling af personoplysninger for at sikre høj overensstemmelse og høj grad af bevidsthed i forbindelse med behandling af personoplysninger i hele OKQ8 Scandinavia.

Intern politik

På baggrund af denne politik for beskyttelse af privatlivets fred, der er vedtaget af bestyrelsen for OKQ8 Scandinavia, findes der udførlige og specifikke instruktioner til at sikre og tydeliggøre, hvilket ansvar de forskellige enheder og medarbejdere har vedrørende behandling af personoplysninger. Sådanne instruktioner er tilgængelige på intranettet eller udleveres af selskabsjuristerne. Corporate Compliance Officer er ansvarlig for at sikre, at datakoordinatorerne holdes ajour med de aktuelle instrukser og procedurer.

OKQ8 Scandinavia GDPR-forum

OKQ8 Scandinavias GDPR-forum er et tværfunktionelt forum, der skal sikre overholdelse af gældende databeskyttelseslovgivning i OKQ8 Scandinavias driftsaktiviteter. GDPR-forummet har det overordnede ansvar for at sikre, at reglerne for databehandlingen overholdes. Ansaret udøves på baggrund af de krav, der stilles i databeskyttelseslovgivningen.

Corporate Compliance Officer har ansvar for at organisere og lede arbejdet i GDPR-forummet. Datakoordinatorerne deltager i og rapporterer resultater, status og planlagte aktiviteter fra deres eget ansvarsområde og har ansvar for at informere om de vedtagne aktiviteter og sørge for de forudsætninger, der skal til for at gennemføre beslutningerne. Derudover deltager relevante personer fra IT, forretningsaktiviteter og de udførende funktioner efter behov. Corporate Compliance Officer sørger for mødeindkaldelse. Alle møder føres til protokols, og mødereferaterne arkiveres af Corporate Compliance Officer.

2.3 Liste over behandling af personoplysninger

Corporate Compliance Officer har ansvar for at sikre, at listen over behandling af personoplysninger overholder kravene i den gældende databeskyttelseslovgivning. Alle de behandlinger, som virksomheder inden for OKQ8 Scandinavia foretager, skal indtastes i en liste. Den enkelte persondatakoordinator har til gengæld ansvar for at sikre, at indholdet er fuldstændigt og korrekt på sigt, både hvad angår behandling af personoplysninger og databehandlere.

3 Udgangspunkt for behandling af personoplysninger i OKQ8 Scandinavia

3.1 Generelt om behandling af personoplysninger

OKQ8 Scandinavia skal overholde den til enhver tid gældende databeskyttelseslovgivning ved behandling af personoplysninger, der sker helt eller delvis automatisk, og i visse tilfælde også ved behandling af personoplysninger i manuelle registre. I tilfælde af tvivl om, hvorvidt databeskyttelseslovgivningen er brugbar for visse former for behandling, kontaktes Corporate Compliance Officer eller selskabsjuristerne. Ud over databeskyttelseslovgivningen findes der regler om behandling af personoplysninger i andre love og bestemmelser, der går forud for databeskyttelseslovgivningen. Når andre love og bestemmelser har forrang, skal dette dokumenteres i listen over behandling af personoplysninger. Corporate Compliance Officer har ansvar for at følge ændringer i databeskyttelseslovgivningen samt relaterede love og regler. Persondatakoordinatorer har ansvar for løbende at opdatere listen over behandling af personoplysninger og krav til ændringer i rutiner og IT-support.

3.2 Grundlæggende principper for OKQ8 Scandinavias behandling af personoplysninger

OKQ8 Scandinavia må kun behandle personoplysninger på en lovlige, korrekt og gennemskelig måde i forhold til den registrerede. Den dataansvarlige skal kunne bevise, at følgende punkter er opfyldt, for eksempel ved revision foretaget af den relevante databeskyttelsesmyndighed. Det betyder bl.a., at OKQ8 Scandinavias behandling af personoplysninger skal være i overensstemmelse med følgende grundlæggende principper:

- **Retsgrundlag:** Enhver behandling af personoplysninger skal ske på baggrund af et dokumenteret retsgrundlag, se desuden punkt 4.
- **Formålsbegrænsning:** Oplysningerne indsamles til specifikke, udtrykkeligt angivne og dokumenterede formål og må ikke efterfølgende behandles på en uforenelig måde.
- **Dataminimering:** Kun personoplysninger, der er adækvate, relevante og ikke for omfattende i forhold til formålet, må indsamles.
- **Rigtighed:** Oplysningerne skal være korrekte og opdaterede, og det skal være muligt at spore ændringer.
- **Opbevaringsbegrænsning:** Oplysningerne må ikke opbevares længere, end hvad der kræves til formålet, se desuden punkt 6.
- **Fortrolighed:** Personoplysninger skal beskyttes under anvendelse af passende tekniske og organisatoriske sikkerhedsforanstaltninger for at forhindre uautoriseret eller ulovlig behandling og tab, tilintetgørelse eller forvanskning af oplysningerne. Se desuden punkt 7.

4 Hvornår er det lovligt at behandle personoplysninger?

4.1 Generelt om lovlig behandling

Behandling af personoplysninger er kun lovligt, hvis mindst ét af følgende seks forhold gør sig gældende:

- Den registrerede har **givet samtykke** til behandling af sine personoplysninger til et eller flere specifikke formål.
- Behandling er **nødvendig af hensyn til opfyldelse af en kontrakt**, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt.
- Behandling er **nødvendig for at overholde en retlig forpligtelse**, som påhviler den dataansvarlige.
- Behandling er nødvendig for at **beskytte** den registreredes eller en anden fysisk persons **vitale interesser**.
- Behandling er **nødvendig af hensyn til udførelse af en opgave i samfundets interesse**, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.
- Behandling er **nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse**, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

Retsgrundlag for OKQ8 Scandinavias behandling af personoplysninger skal sikres og være dokumenteret i den dataansvarliges liste. I tilfælde af tvivl kontaktes Corporate Compliance Officer eller selskabsjuristerne.

4.2 Retsgrundlag ved direkte markedsføring

Ved målrettet markedsføring eller profilering skal der kun indhentes samtykke, hvis der ikke findes nogen anden lovlig grund. OKQ8 Scandinavia har en generelt legitim interesse i at markedsføre sine tjenester. Det betyder, at afhængigt af omstændighederne kan OKQ8 Scandinavia foretage visse markedsføringstiltag uden samtykke og på grundlag af en afvejning af interesser. Dette gælder under den forudsætning, at OKQ8 Scandinavias legitime interesse går forud i forhold til den registreredes interesse i ikke at være underlagt en sådan behandling/markedsføring.

Hvis der er andre regler, der kræver eksplicit samtykke, f.eks. markedsføring via e-mail i henhold til markedsføringsloven i Danmark, går disse regler forud for databeskyttelseslovgivningen.

Under alle omstændigheder kræver markedsføringstiltag, der baserer sig på en afvejning af interesser, nøje overvejelse, herunder om den registrerede på tidspunktet for indhentning af personoplysningerne og i forbindelse med dette med rimelighed kan forvente, at en behandling af personoplysninger til dette formål kan forekomme. Når der foretages en afvejning af interesser, skal dette dokumenteres, og det anføres i informationsteksten til de registrerede (se punkt 5), hvilken legitim interesse OKQ8 Scandinavia lægger til grund herfor. I tilfælde af eventuel tvivl kontaktes

Corporate Compliance Officer eller selskabsjuristerne altid. Såfremt der skal indhentes samtykke, skal dette ske frivilligt og specifikt, dvs. i forbindelse med en særskilt behandling med et bestemt formål.

Samtykke skal også kunne dokumenteres med tilbagevirkende kraft. Der skal indhentes et nyt samtykke ved nye behandlinger, hvis den nye behandling ikke er omfattet af et tidligere givet samtykke.

Den registrerede kan til enhver tid trække sit samtykke til en specifik behandling tilbage. En tilbagekaldelse skal ske skriftligt i henhold til gældende procedurer. En tilbagekaldelse betyder, at den specifikke behandling, der er givet samtykke til, skal ophøre.

4.3 Retsgrundlag for behandling af personoplysninger om medarbejdere

I forbindelse med behandling af personoplysninger om medarbejdere gælder som hovedregel, at der skal anvendes et andet retsgrundlag end samtykke. Samtykke fra medarbejdere anses nemlig typisk for at være ugyldigt, eftersom medarbejderen befinder sig i en afhængighedsposition i forhold til sin arbejdsgiver og derfor ikke kan give et fuldstændig frivilligt samtykke.

I forbindelse med behandling af personoplysninger om medarbejdere har OKQ8 Scandinavia normalt et andet retsgrundlag end samtykke, eftersom en sådan behandling for eksempel er nødvendig for at administrere ansættelsesforholdet, opfylde forpligtelserne i ansættelseskontrakten og/eller overholde retlige forpligtelser (f.eks. indberetning til myndigheder).

4.4 Overførsel af personoplysninger til tredjeland

Såfremt og i det omfang OKQ8 Scandinavias behandling af personoplysninger betyder, at personoplysninger overføres til, opbevares eller på anden måde behandles uden for EU/EØS-området, skal der træffes yderligere foranstaltninger for at sikre, at behandlingen er lovlig. Det er tilstrækkeligt, at personoplysningerne er tilgængelige fra et sted uden for EU/EØS, eller at visse infrastrukturer eller ressourcer befinder sig uden for EU/EØS, for, at der kræves yderligere foranstaltninger.

De foranstaltninger, OKQ8 Scandinavia træffer for at sikre, at behandling af personoplysninger uden for EU/EØS er lovlig, skal altid dokumenteres og godkendes af Corporate Compliance Officer eller selskabsjuristerne.

5 Den registreredes rettigheder

Når OKQ8 Scandinavia indsamler personoplysninger, skal de personer, der indsamles personoplysninger om, informeres. Denne information skal indeholde de oplysninger, der kræves i henhold til databeskyttelseslovgivningen, og i hvert fald:

- Den dataansvarliges identitet, dvs. hvilken juridisk enhed der er dataansvarlig, og kontaktoplysninger

- Formål og retsgrundlag for behandlingen (hvis behandlingen er baseret på en afvejning af interesser, skal de interesser, som behandlingen er baseret på, angives)
- Kategorier af modtagere
- Angivelse af eventuel overførsel til et tredjeland
- Opbevaringstid eller kriterier for sortering
- Retten til at gøre indsigelse mod behandlingen eller (i givet fald) tilbagekalde af samtykke
- Retten til at indgive klage til tilsynsmyndigheden
- Eventuel forekomst af automatisk behandling, profilering
- Retten til at blive informeret om de personoplysninger, der behandles

Alle personer har ret til gratis at modtage de personoplysninger, som OKQ8 Scandinavia har registreret om dem. Hvis en person ønsker at vide, hvilke oplysninger der er registreret om den pågældende,

skal vedkommende indsende en skriftlig og personligt underskrevet anmodning herom. Svaret sendes til den registreredes folkeregisteradresse.

Den registrerede har også ret til at få:

- Ukorrekte persondata **rettet** eller suppleret.
- Få deres personoplysninger **slettet ('blive glemt')**, hvis samtykket tilbagekaldes, og der ikke findes nogen anden lovlig grund for behandlingen af personoplysningerne, eller de ikke længere er nødvendige til det formål, hvortil de blev indsamlet.
- Den registrerede har ret til at **gøre indsigelse** mod behandlingen, hvis OKQ8 Scandinavia ikke kan påvise, at der er en lovlig forpligtelse eller en legitim grund, der vejer tungere end den registreredes rettigheder. Eksempler på behandling kan være segmentering eller målrettet markedsføring.
- Den registrerede har ret til at få behandlingen af sine personoplysninger **begrænset**, for eksempel mens en undersøgelse af en bestemt behandling eller rigtigheden af de personlige oplysninger er i gang. Begrænsninger og indsigelser håndteres ved at markere, blokere og/eller slette i de relevante registre.
- Den registrerede har på visse betingelser ret til **at anmode om, at de oplysninger, vedkommende selv har givet, overføres til en anden part** (dataportabilitet).

6 Sortering i personoplysninger

I henhold til databeskyttelseslovgivningen må personoplysninger ikke opbevares i længere tid end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. Hovedreglen i OKQ8 Scandinavia er derfor, at personoplysninger, som OKQ8 Scandinavia ikke længere behøver for at opfylde formålet med behandlingen, skal tilintetgøres (sortering).

Hvis der findes andre love og regler, der kræver opbevaring af personlige oplysninger i en vis periode, som f.eks. i skatte- og regnskabslovgivning eller i lovgivningen om bekæmpelse af hvidvaskning af penge, går sådanne bestemmelser forud for databeskyttelseslovgivningen. Det fremgår f.eks. af regnskabsloven, at regnskabsoplysningerne skal opbevares i syv år fra det år, hvor regnskabsåret blev afsluttet. Det betyder dog ikke, at personoplysningerne kan anvendes til andre formål, f.eks. til direkte markedsføring.

7 Persondatasikkerhed

7.1 Generelt

OKQ8 Scandinavia skal træffe passende tekniske og organisatoriske foranstaltninger for at forhindre, at personoplysningerne tilintetgøres, ændres eller forvanskes. Det betyder, at der skal foretages en sikkerhedsvurdering fra sag til sag, og at forskellige behandlinger/tjenester/systemer kræver forskellige niveauer af sikkerhedsforanstaltninger afhængigt af oplysningernes følsomhed, risikoen for ulovlig indtrængen (og andre risici) samt sårbarhed.

Ved al behandling af personoplysninger skal OKQ8 Scandinavias instruktioner vedrørende informationssikkerhed tages i betragtning. Du kan finde yderligere information om OKQ8 Scandinavias procedurer for personoplysningssikkerhed i OKQ8 Scandinavias informationssikkerhedspolitik.

Før OKQ8 Scandinavia indleder behandling af personoplysningerne, skal der foretages en indledende risikoanalyse, der tager stilling til:

- De tekniske og organisatoriske sikkerhedsforanstaltninger, der er relevante for den pågældende behandling, baseret på en vurdering af oplysningernes følsomhed, relevante risici og sårbarhed.
- Om behandlingen er tilpasset ud fra og opfylder OKQ8 Scandinavias krav til indbygget databeskyttelse (privacy by design).
- Om behandlingen sandsynligvis vil indebære en høj risiko for den registreredes rettigheder og frihedsrettigheder, f.eks. ved brug af ny teknik, eller fordi den registrerede ikke kan forventes at vide, at denne underkastes behandlingen. Hvis der identificeres en sådan høj risiko, skal Corporate Compliance Officer underrettes og træffer derefter beslutning om, hvorvidt der er behov for yderligere analyse i form af konsekvensanalyse.

Persondatakoordinatorerne er ansvarlige for gennemførelse af risikoanalyser med støtte fra Corporate Compliance Officer og, om nødvendigt, Head of Information & IT Security.

8 Videregivelse af personoplysninger

Personoplysninger kan overføres til eksterne parter med eller uden en databehandlingsaftale afhængigt af, om modtageren behandler oplysningerne på OKQ8 Scandinavias vegne eller på egne vegne. I alle tilfælde skal der være en lovlige grund til overførslen, og kun de oplysninger, som modtageren behøver, må overføres.

8.1 Videregivelse til eksterne databehandlere

OKQ8 Scandinavia kan overføre personoplysninger til en ekstern part, der behandler personoplysninger på vegne af OKQ8 Scandinavia og i henhold til instruktioner fra OKQ8 Scandinavia. En sådan ekstern part er databehandler for OKQ8 Scandinavia og skal altid indgå en databehandlingsaftale med det relevante selskab i OKQ8 Scandinavia.

8.2 Videregivelse til parter med eget dataansvar

OKQ8 Scandinavia kan overføre personoplysninger til en anden ekstern part, der har sit eget dataansvar, forudsat at OKQ8 Scandinavia har lovlige grund til en sådan overførsel. En sådan lovlige grund kan for eksempel være, at overførslen udgør en juridisk forpligtelse for OKQ8 Scandinavia eller en kundeaftale, der giver OKQ8 Scandinavia ret til at overføre oplysningerne.

Denne form for videregivelse kræver ikke en databehandlingsaftale, men skal altid afstemmes med Corporate Compliance Officer.

8.3 Videregivelse af oplysninger til tredjeland

Ved videregivelse af personoplysninger til lande uden for EU og EØS (såkaldt overførsel til tredjeland) gælder særlige bestemmelser, se punkt 4.4.

8.4 Anmodning fra myndigheder om oplysninger

OKQ8 Scandinavia og dets medarbejdere er forpligtede til at give oplysninger om OKQ8 Scandinavias aktiviteter og dertil relaterede forhold, hvis den kompetente databeskyttelsesmyndighed anmoder herom. Der kan også være en forpligtelse til at give oplysninger til politiet eller anklageren ved en strafferetlig efterforskning af en forbrydelse. I sådanne tilfælde skal oplysningerne kun videregives på anmodning fra lederen af den strafferetlige efterforskning og efter samråd med Corporate Compliance Officer eller selskabsjuristerne. Andre myndigheder kan også have ret til at modtage oplysninger, der indeholder persondata fra OKQ8 Scandinavia, såsom fogedretten, skattemyndighederne eller myndighederne for økonomisk kriminalitet.

Corporate Compliance Officer har ansvar for OKQ8 Scandinavias kontakt til de kompetente databeskyttelsesmyndigheder. Al kontakt med databeskyttelsesmyndigheder eller andre myndigheder vedrørende behandling af personoplysninger på OKQ8 Scandinavias vegne skal henvises til Corporate Compliance Officer eller selskabsjuristerne.

9 Brud på persondatasikkerheden

Et brud på persondatasikkerheden er dataindtrængen eller anden sikkerhedshændelse, der involverer hændelig eller ulovlig tilintetgørelse, tab eller ændring af personoplysninger eller uautoriseret videregivelse eller adgang til personoplysninger.

I henhold til gældende databeskyttelseslovgivning er OKQ8 Scandinavia forpligtet til straks at indberette hændelsen til den kompetente databeskyttelsesmyndighed og senest 72 timer efter, at OKQ8 Scandinavia er blevet opmærksom på hændelsen. Hvis hændelsen ikke indberettes til databeskyttelsesmyndigheden inden for 72 timer, skal der anføres en begrundelse for forsinkelsen. Hvis hændelsen kan føre til, at personer udsættes for alvorlige risici, f.eks. forskelsbehandling, identitetstyveri, bedrageri eller økonomisk tyveri, skal den registrerede også informeres.

Brud på persondatasikkerheden skal straks, når det opdages, indberettes til Corporate Compliance Officer i henhold til gældende procedure. De gældende procedurer er tilgængelige på intranettet eller udleveres af selskabsjuristerne.

10 Indberetning

Corporate Compliance Officer skal hvert år eller efter behov foretage indberetning til OKQ8 Scandinavias bestyrelse vedrørende OKQ8 Scandinavias behandling af personoplysninger.

Derudover skal Corporate Compliance Officer straks informere bestyrelsen om væsentlige mangler, integritetsrisici eller brud på persondatasikkerheden, der måtte opstå.

Indberetningen skal indeholde resultatet af den opfølgning og kontrol af personoplysningerne, der foretages i henhold til denne politik, herunder:

- Antal indtrufne brud på persondatasikkerheden
- OKQ8 Scandinavias overholdelse af gældende databeskyttelseslovgivning og denne politik
- Eventuel kontakt til databeskyttelsesmyndigheder
- Væsentlige ændringer i gældende databeskyttelseslovgivning og tilsynspraksis vedrørende behandling af personoplysninger, der påvirker OKQ8 Scandinavia

11 Opfølgning og kontrol

Bestyrelsen har ansvar for at sikre, at der følges op på og foretages kontrol af overholdelsen af denne politik.

12 Vedtagelse og opdatering

Denne politik vedtages af bestyrelsen og opdateres efter behov.

Corporate Compliance Officer har ansvar for at sikre, at politikken gennemgås én gang om året og opdateres efter behov inden bestyrelsens vedtagelse.