Fastställd av:	Senast uppdaterad:	Fastställs	Tillgänglighet:	Version:
Styrelsen	2018-04-24 2019-05-07	Årligen samt vid behov	Intern	1.1
Ägare:	**Tillämpningsområde:**	**Rättslig grund:**		**Sidor:**
Corporate Compliance Officer	Personuppgiftsbehandling	• Dataskyddsförordningen GDPR (General Data Protection Regulation) samt nationell dataskyddslagstiftning i Sverige och Danmark • Dataskyddsmyndigheterna i Sverige och Danmarks föreskrifter och allmänna råd		15

Integritetspolicy

OKQ8 Scandinavia

Antagen av styrelsen för OK-Q8 AB den 7 maj 2019

Innehållsförteckning

1 Inledning

1.1 Bakgrund och syfte

OK-Q8 AB och dess dotterbolag (”OKQ8 Scandinavia”) hanterar i sin verksamhet en stor mängd personuppgifter. Personuppgifterna behandlas bland annat för att OKQ8 Scandinavia ska kunna fullgöra ingångna avtal med kunder, leverantörer och anställda, kunna ge god service till kunder samt på grund av skyldigheter enligt andra lagar och regelverk.

Insamlingen av personuppgifter sker exempelvis när en kund lämnar sina uppgifter till OKQ8 Scandinavia i samband med köp av tjänster eller när en anställd påbörjar sin anställning i OKQ8 Scandinavia. Personuppgifter kan också samlas in utan en aktiv handling från kundens sida, t.ex. genom cookies på hemsidan eller samkörning med externa adressregister.

Mer information om vilka personuppgifter som OKQ8 Scandinavia behandlar och för vilka syften finns på intranätet samt hos Legal/Compliance. Det finns även extern information om personuppgiftsbehandling på OKQ8 Scandinavias externa webbsidor.

Denna policy innehåller övergripande krav och riktlinjer för att säkerställa att insamling och behandling av personuppgifter inom OKQ8 Scandinavia sker i enlighet med gällande Dataskyddslagstiftning och andra tillämpliga externa lagar och regelverk. Denna policy börjar gälla den 25 maj 2018.

För OK-Q8 Bank AB finns en separat Integritetspolicy som även beaktar andra lagar och regelverk tillämpliga för banker och finansiella institut.

1.2 Definitioner

Behandling av personuppgift

Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig de sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning, ändring, begränsning, justering, radering eller förstöring, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning.

Dataskyddslagstiftning

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och varje annan nationell eller internationell lag, förordning, direktiv, myndighetsföreskrift eller allmänna råd som från tid till annan gäller för OKQ8 Scandinavias behandling av personuppgifter.

Ett tvärfunktionellt forum inom OKQ8 Scandinavia för att säkerställa hög regelefterlevnad i styrning och utförande av personuppgiftshanteringen**.**

Datadelningsavtal

Ett avtal mellan samtliga bolag och föreningar inom OK/OKQ8-sfären som syftar till att uppfylla de legala kraven för nödvändig och laglig delning, utbyte och behandling av personuppgifter inom OK/OKQ8-sfären.

Dataskyddsforum

Ett forum bestående av dataskyddskontakter från samtliga bolag och föreningar inom OK/OKQ8-sfären**.** På Dataskyddsforum hanteras och diskuteras frågor som avser ändringar i Datadelningsavtalet, specifikationer samt dataskyddskontakternas mandat och arbetsuppgifter.

Interna regelverk

OKQ8 Scandinavias interna styrdokument bestående av policyer, instruktioner, rutiner och checklistor avseende behandling av personuppgifter.

OK/OKQ8-sfären

Samtliga bolag inom OKQ8 Scandinavia, OK Detaljhandel AB, samtliga OK-föreningar samt franchisetagare som bedriver verksamhet under något av OKQ8 Scandinavias varumärken.

Personuppgift

Varje upplysning som avser en identifierad eller identifierbar fysisk person som är i livet. Med identifierbar fysisk person menas en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Personuppgiftsansvarig

Den juridiska person som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträde

En juridisk person som behandlar personuppgifter för den personuppgiftsansvariges räkning, t.ex. OKQ8 Scandinavias IT-leverantörer.

2 Organisation och ansvar

För varje behandling av personuppgifter kan någon aktör inom OK/OKQ8-sfären vara ensamt personuppgiftsansvarig, gemensamt personuppgiftsansvarig eller personuppgiftsbiträde. Mot bakgrund av gällande Dataskyddslagstiftning måste det vara klarlagt och dokumenterat vem/vilka inom OK/OKQ8-sfären som är personuppgiftsansvarig för varje personuppgiftsbehandling.

För OK/OKQ8-sfären dokumenteras ansvarsfördelningen i Datadelningsavtalet samt i respektive bolags/förenings förteckning över personuppgiftsbehandlingar.

2.1 Logiska register för fastställande av personuppgiftsansvar

Inom OKQ8 Scandinavia är personuppgiftsansvaret fördelat utifrån ”logiska register”. De logiska registren är en logisk gruppering av de personuppgifter som behandlas för ett specifikt ändamål, oavsett vilket eller vilka IT-system som används för behandlingen.

Varje logiskt register är kopplat till ett eller flera bolag i OKQ8 Scandinavia med personuppgiftsansvar.

2.2 Ansvar, roller och samverkansformer

2.2.1 Roller och ansvar

Ansvaret för att personuppgifter behandlas enligt gällande Dataskyddslagstiftning, denna policy och andra interna och externa regelverk omfattar alla nivåer inom OKQ8 Scandinavias organisation från styrelsen till operativa utförande funktioner. Ansvaret för behandlingen av personuppgifter inom OKQ8 Scandinavia är fördelat enligt vad som framgår av denna policy.

Styrelsen

Styrelsen är ansvarig för att fastställa denna policy samt andra policyer som behöver finnas för att säkerställa efterlevnad av gällande Dataskyddslagstiftning.

VD

VD är ansvarig för att denna policy upprättas och uppdateras och för att samtliga anställda och uppdragstagare har tillgång till policyn. VD ansvarar för att det finns en fungerande organisation och möjligheter för Dataskyddsombudet att bedriva sitt arbete i enlighet med Dataskyddslagstiftningen.

Dataskyddsombud / Corporate Compliance Officer

OKQ8 Scandinavias Corporate Compliance Officer har utsetts till Dataskyddsombud för samtliga bolag inom OKQ8 Scandinavia. Corporate Compliance Officer har det övergripande ansvaret för att utarbeta, implementera och säkerställa uppföljning av interna regelverk som möjliggör för OKQ8 Scandinavia att hantera personuppgifter i enlighet med gällande Dataskyddslagstiftning och denna policy.

Corporate Compliance Officer ansvarar för att utbilda och stödja OKQ8 Scandinavias anställda i frågor och ärenden som rör behandling av personuppgifter samt för kontakten med behöriga dataskyddsmyndigheter.

Avtalstecknare och Personuppgiftsbiträden

Personuppgiftsbiträden behandlar personuppgifter på uppdrag av OKQ8 Scandinavia och för OKQ8 Scandinavias räkning. Mellan personuppgiftsansvarig och varje personuppgiftsbiträde krävs ett skriftligt avtal med visst innehåll (biträdesavtal) enligt Dataskyddslagstiftningen. Sådant biträdesavtal ska utformas enligt Corporate Compliance Officers instruktioner och OKQ8 Scandinavias avtalsmall. Avtalstecknare ansvarar för att ett korrekt personuppgiftsbiträdesavtal finns för alla personuppgiftsbiträden. Avvikelser från avtalsmallen ska godkännas i förväg av Corporate Compliance Officer eller Legal. Avtalstecknaren ansvarar vidare för att biträdesavtalet innehåller specifikationer och tillräckliga instruktioner i anledning av uppdraget. Avtalstecknare ansvarar för att rådfråga Corporate Compliance Officer eller Legal vid behov.

Personuppgiftskoordinatorer

OKQ8 Scandinavias personuppgiftskoordinatorer ansvarar för att den operativa behandlingen av personuppgifter uppfyller gällande Dataskyddslagstiftning, denna policy och övriga interna regelverk. Varje personuppgiftskoordinator har ansvar för ett eller flera logiska register av personuppgifter, tillåtna behandlingar, regler för gallring, etc. I ansvaret ingår även att implementera och löpande uppdatera processer, rutiner och checklistor som säkerställer korrekt hantering av personuppgifter samt att rapportera frågor som rör personuppgifter till Corporate Compliance Officer.

Head of Information & IT Security

Head of Information & IT Security verkställer samordningen av informationssäkerhetsarbetet inom OKQ8 Scandinavia och förvaltar policy, de tillhörande riktlinjerna och instruktionerna, samt den övergripande handlingsplanen inom informationssäkerhetsområdet. Ansvaret omfattar även att kravställa på IT- och informationssäkerhet i OKQ8 Scandinavias IT-miljöer, samt att bemanna och arbetsleda de specialistroller som behövs för kravställandet. Hantering av incidenter inom IT-säkerhetsområdet, rapportering till Informationssäkerhetsgruppen samt uppföljning av leverantörer är andra ansvar inom IT- och informationssäkerhetsområdet. Vid behov ska Head of Information & IT Security assistera Corporate Compliance Officer med riskanalyser och konsekvensbedömningar avseende säkerställande av principen om inbyggt dataskydd (privacy by design).

Samtliga anställda

Samtliga anställda och i förkommande fall uppdragstagare som arbetar under OKQ8 Scandinavias ledning har ett eget ansvar för att hantera personuppgifter i enlighet med gällande Dataskyddslagstiftning, denna policy samt interna regelverk. Vid osäkerhet om en behandling av personuppgifter är tillåten ska Corporate Compliance Officer eller Legal alltid tillfrågas.

Samtliga kontorsanställda och i förekommande fall uppdragstagare under OKQ8 Scandinavias ledning ska genomgå en obligatorisk GDPR utbildning som OKQ8 Scandinavia har tagit fram.

2.2.2 Samverkansformer

Interna regelverk, OKQ8 Scandinavias GDPR-forum, Dataskyddsforum och tydlig funktionell rapportering mellan styrande och utförande funktioner för behandling av personuppgifter har etablerats i syfte att säkerställa hög regelefterlevnad och hög medvetandegrad i personuppgiftsbehandlingen inom hela OKQ8 Scandinavia.

Interna styrdokument

Utifrån denna integritetspolicy, som fastställts av OKQ8 Scandinavias styrelse, finns detaljerade och specifika instruktioner för att säkerställa och tydliggöra vilket ansvar olika enheter och medarbetare har såvitt avser behandling av personuppgifter. Sådana instruktioner finns tillgängliga på intranätet och hos Legal/Compliance. Corporate Compliance Officer är ansvarig för att se till att personuppgiftskoordinatorerna hålls uppdaterade om gällande instruktioner och rutiner.

OKQ8 Scandinavia GDPR-forum

OKQ8 Scandinavias GDPR-forum är ett tvärfunktionellt forum för att säkerställa efterlevnad av gällande Dataskyddslagstiftning i OKQ8 Scandinavias operativa verksamhet. GDPR-forum har det övergripande ansvaret för att säkerställa regelefterlevnad för personuppgiftshanteringen. Ansvaret utövas utifrån de krav som ställs i Dataskyddslagstiftningen.

Corporate Compliance Officer ansvarar för att organisera och leda arbetet i GDPR-forum. Personuppgiftskoordinatorerna deltar och rapporterar utfall, status och planerade aktiviteter från eget ansvarsområde och ansvarar för att beslutade aktiviteter kommuniceras och att förutsättningar för att genomföra beslut fattas. Därutöver deltar relevanta personer från IT, affärsverksamheten samt utförandefunktioner vid behov. Corporate Compliance Officer är sammankallande. Alla möten protokollförs och protokollen arkiveras av Corporate Compliance Officer.

2.3 Förteckning över personuppgiftsbehandling

Corporate Compliance Officer ansvarar för att förteckningen över personuppgiftsbehandlingar uppfyller kraven i gällande Dataskyddslagstiftning. Samtliga behandlingar som bolag inom OKQ8 Scandinavia utför ska föras in i en förteckning. Varje personuppgiftskoordinator ansvarar i sin tur för att säkra innehållet är komplett och korrekt över tid både avseende behandlingar av personuppgifter och personuppgiftsbiträden

3 Utgångspunkter för behandling av personuppgifter inom OKQ8 Scandinavia

3.1 Allmänt om behandling av personuppgifter

OKQ8 Scandinavia ska följa vid var tid gällande Dataskyddslagstiftning vid behandling av personuppgifter som helt eller delvis företas på automatisk väg och, i vissa fall, även vid behandling av personuppgifter i manuella register. Vid osäkerhet om Dataskyddslagstiftningen är tillämplig för viss behandling ska Corporate Compliance Officer eller Legal tillfrågas. Utöver Dataskyddslagstiftningen finns det regler om hantering av personuppgifter i andra lagar och regelverk som har företräde framför Dataskyddslagstiftningen. När andra lagar och regelverk ges företräde ska detta dokumenteras i förteckningen över personuppgiftsbehandlingar. Corporate Compliance Officer ansvarar för att följa förändringar i Dataskyddslagstiftningen och relaterade lagar och regelverk. Personuppgiftkoordinatorer ansvarar för att löpande uppdatera förteckningen över personuppgiftsbehandlingar och kravställa på förändringar i rutiner och IT-stöd.

3.2 Grundläggande principer för OKQ8 Scandinavias personuppgiftsbehandling

OKQ8 Scandinavia ska endast behandla personuppgifter på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Den personuppgiftsansvarige ska kunna bevisa att nedanstående punkter efterlevs, exempelvis vid en revision från behörig dataskyddsmyndighet. Detta innebär bl.a. att OKQ8 Scandinavias personuppgiftsbehandling ska följa följande grundläggande principer:

- **Laglig grund:** Varje behandling av personuppgifter ska utföras med stöd av en dokumenterad laglig grund, se vidare punkt 4.
- **Ändamålsbegränsning**: Uppgifterna ska samlas in för särskilt, uttryckligen angivna och dokumenterade ändamål och får inte senare behandlas på ett oförenligt sätt.
- **Uppgiftsminimering**: Endast personuppgifter som är adekvata, relevanta och inte för omfattande i förhållande till ändamålet ska samlas in.
- **Korrekthet:** Uppgifterna ska vara korrekta och uppdaterade och det ska vara möjligt att spåra ändringar.
- **Lagringsminimering**: Uppgifterna får inte förvaras längre än vad som krävs i förhållande till ändamålet, se vidare punkt 6.
- **Konfidentialitet**: Personuppgifter ska skyddas av lämpliga tekniska och organisatoriska säkerhetsåtgärder för att förhindra obehörig eller otillåten behandling och förlust, förstöring eller förvanskning av uppgifterna. Se vidare punkt 7.

4 När är behandling av personuppgifter laglig?

4.1 Allmänt om laglig grund

Behandlingen av personuppgifter är endast laglig om minst ett av följande sex villkor är uppfyllda:

- Den registrerade har **lämnat sitt samtycke** till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
- Behandlingen är **nödvändig för att fullgöra ett avta**l i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
- Behandlingen är **nödvändig för att fullgöra en rättslig förpliktelse** som åvilar den personuppgiftsansvarige.
- Behandlingen är nödvändig för att **skydda intressen som är av grundläggande betydelse** för den registrerade eller för en annan fysisk person.
- Behandlingen **är nödvändig för att utföra en uppgift av allmänt intresse** eller som ett led i den personuppgiftsansvariges myndighetsutövning.
- Behandlingen är **nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen**, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Laglig grund för OKQ8 Scandinavias behandlingar av personuppgifter ska säkerställas och dokumenteras i den personuppgiftsansvariges förteckning. Vid osäkerhet ska samråd ske med Corporate Compliance Officer eller Legal.

4.2 Laglig grund vid direktmarknadsföring

Vid riktad marknadsföring eller profilering ska samtycke endast inhämtas om annan laglig grund saknas. OKQ8 Scandinavia har ett generellt berättigat intresse av att marknadsföra sina tjänster. Detta innebär att OKQ8 Scandinavia, beroende på omständigheterna, kan vidta vissa marknadsföringsåtgärder utan samtycke och med stöd av en intresseavvägning. Detta gäller under förutsättning att OKQ8 Scandinavias berättigade intresse väger tyngre än de registrerades intresse av att inte bli föremål för sådan behandling/marknadsföring.

Om det finns andra regelverk som kräver uttryckligt samtycke, t.ex. för e-postmarknadsföring enligt marknadsföringslagen i Danmark, har dessa regler företräde framför Dataskyddslagstiftningen.

Marknadsföringsåtgärder med stöd av intresseavvägning kräver under alla omständigheter en noggrann bedömning, som inbegriper huruvida den registrerade vid tidpunkten för inhämtandet av personuppgifter och i samband med detta rimligen kan förvänta sig att en uppgiftsbehandling för detta ändamål kan komma att ske. När intresseavvägning tillämpas ska detta dokumenteras och det ska anges i informationstexten till de registrerade (se punkt 5) vilket berättigat intresse som OKQ8 Scandinavia stödjer sig på. Vid eventuell osäkerhet ska samråd alltid ske med Corporate Compliance Officer eller Legal. I de fall samtycke behöver inhämtas ska det vara frivilligt och specifikt, dvs. gälla en särskild behandling med ett specifikt ändamål.

Samtycke ska också kunna bevisas i efterhand. Vid nya behandlingar ska nytt samtycke inhämtas om den nya behandlingen inte täcks av tidigare lämnat samtycke.

Den registrerade kan när som helst återkalla ett samtycke för en specifik behandling. En återkallelse ska ske skriftligen, enligt gällande rutiner. En återkallelse innebär att den specifika behandling samtycket avsåg måste upphöra.

4.3 Laglig grund för personuppgiftsbehandling om anställda

För behandling av personuppgifter om anställda gäller som huvudregel att annan laglig grund än samtycke måste användas. Samtycke från anställda anses nämligen, typiskt sett, vara ogiltiga eftersom den anställde befinner sig i en beroendeställning gentemot sin arbetsgivare och därmed inte kan lämna ett fullständigt frivilligt samtycke.

För behandling av personuppgifter om anställda har OKQ8 Scandinavia normalt annan laglig grund än samtycke, eftersom sådan behandling exempelvis är nödvändig för att administrera anställningsförhållandet, uppfylla åtaganden i anställningsavtalet och/eller uppfylla rättsliga förpliktelser (t.ex. rapportering till myndigheter).

4.4 Överföring av personuppgifter till tredje land

Om och i den mån OKQ8 Scandinavias personuppgiftsbehandling innebär att personuppgifter överförs till, lagras eller annat sätt behandlas utanför EU/EES-området krävs ytterligare åtgärder för att behandlingen ska vara laglig. Det är tillräckligt att personuppgifterna är nåbara från plats utanför EU/EES, eller att viss infrastruktur eller resurs befinner sig utanför EU/EES, för att ytterligare åtgärder är nödvändiga.

De åtgärder som OKQ8 Scandinavia vidtar för att säkerställa att personuppgiftsbehandling utanför EU/EES är laglig ska alltid dokumenteras och godkännas av Corporate Compliance Officer eller Legal.

5 Den registrerades rättigheter

När OKQ8 Scandinavia samlar in personuppgifter ska information lämnas till de personer vars personuppgifter samlas in. Sådan information ska innehålla de uppgifter som krävs enligt Dataskyddslagstiftningen och åtminstone:

- Den personuppgiftsansvariges identitet, dvs vilken juridisk enhet som är personuppgiftsansvarig, samt kontaktuppgifter
- Ändamål och rättslig grund för behandlingen (om behandlingen baseras på intresseavvägning ska de intressen som behandlingen grundar sig på anges)
- Kategorier av mottagare
- Uppgift om eventuell överföring till tredje land
- Lagringstid alternativt kriterier för gallring
- Rätten att invända mot behandling eller (om aktuellt) återta samtycke
- Rätten att lämna klagomål till tillsynsmyndighet
- Om aktuellt - förekomst av automatiserade beslut, profilering
- Rätten att få information om vilka personuppgifter som behandlas

Alla individer har rätt att kostnadsfritt få ta del av de personuppgifter som OKQ8 Scandinavia har registrerat om hen. Om en person vill veta vilka uppgifter som finns registrerade om hen, ska personen inkomma med en skriftlig och egenhändigt undertecknad begäran. Svaret ska skickas till den registrerades folkbokföringsadress.

Den registrerade har även rätt att få:

- Felaktiga personuppgifter **rättade** alternativt kompletterade.
- Få sina personuppgifter **raderade ("bli bortglömd** ") om samtycke återkallas och ingen annan rättslig grund finns för behandlingen av personuppgifterna eller de inte längre är nödvändiga för det ändamål de samlats in för.
- Den registrerade har rätt att **invända** mot behandling, om inte OKQ8 Scandinavia kan påvisa att det finns lagligt tvång eller berättigade skäl som väger tyngre än den registrerades rättigheter. Exempel på behandling kan vara segmentering eller riktad marknadsföring.
- Den registrerade har rätt att få behandlingarna av sina personuppgifter **begränsade,** exempelvis under tiden en utredning om en viss behandling eller personuppgifternas korrekthet pågår. Begränsning och invändning hanteras genom markering, blockering och/eller radering i berörda register.
- Den registrerade har rätt att, under vissa förutsättningar, **begära att de uppgifter man själv lämnat flyttas till en annan part** (dataportabilitet).

6 Gallring av personuppgifter

Enligt Dataskyddslagstiftningen får personuppgifter inte sparas längre än vad som är nödvändigt för de ändamål för vilka uppgifterna behandlas. Huvudregeln inom OKQ8 Scandinavia är därför att personuppgifter som OKQ8 Scandinavia inte längre är i behov av för att uppfylla ändamålet med behandlingen ska förstöras (gallring).

Om det finns andra lagar och regelverk som kräver lagring av personuppgifter under viss tid, såsom i t.ex. i skatte-, bokförings- eller penningtvättslagstiftningen gäller sådana bestämmelser före Dataskyddslagstiftningen. Av bokföringslagen framgår exempelvis att räkenskapsinformation ska sparas i sju år från det år då räkenskapsåret avslutades. Detta innebär dock inte att personuppgifterna får användas för något annat ändamål, t.ex. för direktmarknadsföring.

7 Säkerhet vid behandling av personuppgifter

7.1 Allmänt

OKQ8 Scandinavia ska vidta lämpliga tekniska och organisatoriska åtgärder för att förhindra att personuppgifter förstörs, ändras eller förvanskas. Detta innebär att en säkerhetsbedömning behöver göras från fall till fall och att olika behandlingar/tjänster/system kräver olika nivå av säkerhetsåtgärder beroende på informationens känslighet, intrångsrisk (och andra risker) samt sårbarhet.

Vid all behandling av personuppgifter ska OKQ8 Scandinavias instruktioner rörande informationssäkerhet beaktas. Mer detaljerad information om OKQ8 Scandinavias rutiner för säkerhet vid behandling av personuppgifter finns i Informationssäkerhetspolicy för OKQ8 Scandinavia.

Innan OKQ8 Scandinavia påbörjar behandling av personuppgifter ska en initial riskanalys genomföras för att ta ställning till:

- Vilka tekniska och organisatoriska säkerhetsåtgärder som är lämpliga för den aktuella behandlingen, baserat på en bedömning av informationskänslighet, relevanta risker och sårbarhet.
- Om behandlingen är anpassad utifrån och uppfyller OKQ8 Scandinavias krav avseende inbyggt dataskydd (privacy by design).
- Om behandlingen sannolikt medför en hög risk för de registrerades rättigheter och friheter, t.ex. genom användning av ny teknik eller genom att den registrerade inte kan förväntas känna till att de blir föremål för behandlingen. Om sådan hög risk identifieras ska Corporate Compliance Officer informeras och avgöra om vidare analys i form av konsekvensbedömning är nödvändig.

Personuppgiftskoordinatorerna ansvarar för att riskanalys genomförs med stöd av Corporate Compliance Officer och, vid behov, Head of Information & IT Security .

8 Utlämnande av personuppgifter

Personuppgifter kan överföras till externa parter med eller utan biträdesavtal, beroende på om mottagaren behandlar uppgifterna för OKQ8 Scandinavias räkning eller för sin egen räkning. I samtliga fall gäller att det ska finnas en laglig grund för överföringen och att endast de uppgifter som mottagaren behöver ska överföras.

8.1 Utlämning till externa personuppgiftsbiträden

OKQ8 Scandinavia kan komma att överföra personuppgifter till extern part, som behandlar personuppgifter för OKQ8 Scandinavias räkning och enligt instruktion från OKQ8 Scandinavia. Sådan

extern part är personuppgiftsbiträde till OKQ8 Scandinavia och ska alltid underteckna ett biträdesavtal med relevant bolag inom OKQ8 Scandinavia.

8.2 Utlämning till parter med eget personuppgiftsansvar

OKQ8 Scandinavia kan komma att överföra personuppgifter till annan extern part, som har eget personuppgiftsansvar, under förutsättning att OKQ8 Scandinavia har laglig grund för sådan överföring. Sådan laglig grund kan exempelvis vara att överföringen utgör en rättslig skyldighet för OKQ8 Scandinavia, eller ett kundavtal som ger OKQ8 Scandinavia rätt att överföra uppgifterna.

Denna typ av utlämning kräver inget personuppgiftsbiträdesavtal, men ska alltid stämmas av med Corporate Compliance Officer.

8.3 Utlämning av information till tredje land

För överföring av personuppgifter till länder utanför EU och EES (så kallad tredjelandsöverföring) gäller särskilda bestämmelser, se punkt 4.4.

8.4 Myndighets begäran om uppgifter

OKQ8 Scandinavia och dess anställda är skyldiga att lämna upplysningar om OKQ8 Scandinavias verksamhet och därmed sammanhängande omständigheter om behörig dataskyddsmyndighet begär det. Det kan också föreligga uppgiftsskyldighet till polis eller åklagare vid en förundersökning om brott. Uppgifterna ska i sådana fall lämnas ut endast på begäran av förundersökningsledaren och efter samråd med Corporate Compliance Officer eller Legal. Även andra myndigheter kan ha rätt att få upplysningar som innehåller personuppgifter från OKQ8 Scandinavia, exempelvis Kronofogdemyndigheten, Skatteverket eller Ekobrottsmyndigheten.

Corporate Compliance Officer ansvarar för OKQ8 Scandinavias kontakter med behöriga dataskyddsmyndigheter. Alla kontakter med dataskyddsmyndigheter eller andra myndigheter avseende frågor om personuppgiftsbehandling för OKQ8 Scandinavias räkning ska hänskjutas till Corporate Compliance Officer eller Legal.

9 Personuppgiftsincidenter

En personuppgiftsincident är ett dataintrång eller annan säkerhetsincident som innebär oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter, eller obehörigt röjande eller obehörig åtkomst till personuppgifter.

OKQ8 Scandinavia är enligt gällande Dataskyddslagstiftning skyldigt att rapportera incidenten till behörig dataskyddsmyndighet utan dröjsmål, dock inte senare än 72 timmar efter att OKQ8 Scandinavia fått vetskap om incidenten. Om anmälan till dataskyddsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen. Om incidenten kan leda till att personer

utsätts för allvarliga risker som t.ex. diskriminering, id-stöld, bedrägeri eller finansiella stölder måste även de registrerade informeras.

Personuppgiftsincidenter ska omedelbart när de upptäcks rapporteras till Corporate Compliance Officer enligt gällande rutin. Gällande rutiner finns på intranätet samt hos Legal/Compliance

10 Rapportering

Corporate Compliance Officer ska årligen eller vid behov rapportera till styrelsen i OKQ8 Scandinavia om OKQ8 Scandinavias behandling av personuppgifter.

Corporate Compliance Officer ska därutöver omedelbart rapportera till styrelsen om väsentliga brister, integritetsrisker eller personuppgiftsincidenter uppstår.

Rapporten ska innehålla resultatet av den uppföljning och kontroll av personuppgifter som görs enligt denna policy, inklusive:

- Antalet inträffade personuppgiftsincidenter
- OKQ8 Scandinavias efterlevnad av gällande Dataskyddslagstiftning och denna policy
- Eventuella kontakter med dataskyddsmyndigheter
- Väsentliga förändringar av gällande Dataskyddslagstiftning och tillsynspraxis rörande behandling av personuppgifter som påverkar OKQ8 Scandinavia

11 Uppföljning och kontroll

Styrelsen ansvarar för att säkerställa att uppföljning och kontroll av efterlevnaden av denna policy sker.

12 Fastställande och uppdatering

Denna policy ska fastställas av styrelsen och uppdateras vid behov.

Corporate Compliance Officer ansvarar för att policyn ses över årligen och vid behov uppdateras för styrelsens beslut.