BEHANDLING AV PERSONOPPLYSNINGER I DEKK OG FELG AS

Disse rutinene for behandling av personopplysninger («Rutinene») er besluttet av ledelsen i Dekk og Felg AS («Selskapet») og gjelder all behandling av personopplysninger i Selskapet, herunder for ansatte og andre som utfører arbeid eller tjenester for Selskapet.

Ansatte og andre som er involvert i Selskapets behandling av personopplysninger plikter å sette seg inn i og følge Rutinene. Dersom det er bestemmelser eller prosedyrer i Rutinene som ikke kan følges, eller som ikke stemmer med hvordan personopplysninger behandles i Selskapet, skal det gis beskjed om dette til leder for Selskapet.

Innhold

1. PRINSIPPER FOR BEHANDLING AV PERSONOPPLYSNINGER I SELSKAPET

Følgende prinsipper skal være styrende for behandling av personopplysninger i Selskapet:

1) **Lovlig behandling.** All behandling av personopplysninger i Selskapet skal skje på en lovlig, rettferdig og transparent måte. Transparens skal allikevel vike dersom dette prinsippet kommer i strid med prinsippene om konfidensialitet eller hvis det kan være en risiko for personvernet til den enkelte registrerte.
2) **Formålsbegrensning**. Det skal kun behandles personopplysninger med et klart formål og behandlingen skal kun skje innenfor det formålet. Det skal ikke viderebehandles personopplysninger utenfor formålet.
3) **Registrertes rettigheter**. Det skal sørges for at de registrertes, herunder de ansatte, kan håndheve og benytte seg av sine rettigheter etter personvernregelverket.
4) **Dataminimering**. De personopplysninger som behandles skal være adekvate, relevante og begrenset til det som er nødvendig for formålene personopplysningene behandles for.
5) **Krav til it-systemer**. De it-systemer og -løsninger som Selskapet benytter seg av skal understøtte pliktene etter personvernregelverket, og skal ikke forhindre etterlevelse av lovverket eller de registrertes rettigheter.
6) **Riktighet.** Opplysningene skal sikres riktighet, og skal rettes på oppfordring eller når det avdekkes at opplysningene ikke er korrekte eller oppdaterte.
7) **Begrensning i behandlingstid.** Personopplysninger skal slettes når formålet for behandlingen er opphørt, eller når de kreves slettes av de registrerte.
8) **Integritet og fortrolighet.** Det skal iverksettes tilstrekkelige tiltak for å sikre personopplysninger mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak.
9) **Ansvarlighet.** Selskapet skal opptre ansvarlig for behandling av personopplysninger når Selskapet er behandlingsansvarlig, og skal påse at databehandlere Selskapet benytter gir de tilstrekkelige garantier og sørger for lovlig og sikker behandling.

2. STYRENDE REGELVERK

Personopplysningsloven stiller krav til at det skal gjennomføres egnede tekniske og organisatoriske tiltak for å sikre at og påvise at behandlingen av personopplysninger utføres i samsvar med personopplysningsloven og personvernforordningen. Det må tas hensyn til behandlingens art, omfang, formål og sammenhengen behandlingen utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for de registrertes rettigheter og friheter. Rutinene skal sikre gjennomføring av de nevnte tiltakene, herunder for:

- Oppfyllelse av Selskapets plikter og de registrertes rettigheter, og
- organisatoriske og tekniske tiltak for å sikre informasjonssikkerhet

Tiltakene, og derved Rutinene, skal gjennomgås regelmessig og oppdateres ved behov.

Med «personopplysningsloven» menes også personvernforordningen (Europaparlaments- og rådsforordning 2016/679 - GDPR) som er implementert i norsk rett gjennom personopplysningsloven. Dersom personopplysningsloven endres eller erstattes av annen lovgivning, skal denne lovgivningen være styrende for behandling av personopplysninger i Selskapet. Tilsvarende gjelder om det tilkommer ytterligere lovgivning og regelverk som er av betydning for behandling av personopplysninger for Selskapet.

3. PERSONOPPLYSNINGSDOKUMENTASJON

All dokumentasjon knyttet til personopplysninger og som skal foreligge etter Rutinene skal være tilgjengelig for alle ansatte, med unntak av informasjon som av sikkerhetsmessige eller andre grunner ikke bør være tilgjengelig for flere, som lagres på område med begrenset tilgang.

4. ORGANISERING OG ANSVAR

Ledelsen i Selskapet har det øverste ansvar for at Selskapet behandler personopplysninger i henhold til det til enhver tid gjeldende regelverk.

Leder av Selskapet har ansvar for at det faktisk gjennomføres egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med det til enhver tid gjeldende regelverk.

Den som er oppgitt som ansvarlig for behandling i Behandlingsoversikten, se punkt 6.2, har et spesielt ansvar for behandling som denne er ansvarlig for. Dette ansvaret er angitt knyttet til konkrete plikter i Rutinene.

Enhver som er ansatt eller håndterer personopplysninger hos Selskapet har et individuelt ansvar og plikter til at personopplysninger behandles etter disse Rutinene og etter det til enhver tid gjeldende regelverk for behandling av personopplysninger. Er det usikkerhet om hvordan personopplysninger skal behandles, skal behandling avventes til det er bragt klarhet ved at leder eller personvernekspertise konfereres. Det skal uansett alltid velges den behandlingsmåte som medfører minst risiko for de registrerte dersom det er alternative behandlingsmåter.

5. LEDELSENS GJENNOMGANG

5.1 Regelmessig gjennomgang

Ledelsen i Selskapet skal gjennomføre regelmessige gjennomganger for å sikre:

- At de mål som er satt for behandling av personopplysninger oppnås
- At det gjøres korrigerende tiltak for å sikre at behandlingen av personopplysninger skjer innenfor lov- og regelverk, herunder Rutinene, samt vurdere oppfølging av korrigerende tiltak
- At det sørges for at internkontroll og styringssystem for informasjonssikkerhet er hensiktsmessige, tilstrekkelig og effektive og at det tilfredsstiller relevante krav i lover og regler

Selskapets leder har ansvar for at gjennomgangen gjennomføres.

De elementer som er styrende for internkontroll og informasjonssikkerhet bør gjennomgås med regelmessige intervaller - avhengig av Selskapets virksomhet og omfanget av behandling av personopplysninger - med følgende vurderinger:

- Internkontroll: Vurdere endringer i omfang av dagens internkontroll.
- Sikkerhetsmål og -strategi: Vurdere eventuelle forslag til endringer i sikkerhetsmål og sikkerhetsstrategi, dersom endringene i vesentlig grad har økonomiske eller andre virksomhetsmessige konsekvenser.
- Risiko- og sårbarhetsanalyse: Vurdering av risiko og sårbarhet ved ønske om ny funksjonalitet eller nye systemer/løsninger som medfører vesentlige investeringer eller endringer i eksisterende sikkerhetsnivå.
- Virksomhetskritisk informasjon og/eller system: Vurdering av endringer i hvilken informasjon eller hvilke systemer som er virksomhetskritisk for Selskapet.

5.2 Sikkerhetsmål

Selskapet har definert en rekke prinsipper for behandling av personopplysninger i Selskapet, se punkt 1. I tillegg er sikkerhetsmålene nedenfor definert for Selskapet. Sikkerhetsmålene skal understøtte og sikre Selskapets drift, allmenne tillit og omdømme i det offentlige rom, ved å forebygge og begrense konsekvensene av uønskede hendelser. Sikkerhetsmålene beskriver Selskapets overordnete mål for beskyttelse av Selskapets informasjonsbehandling mot interne og eksterne trusler av tilsiktet og utilsiktet art.

Opplysningene i Selskapet skal sikres med hensyn til:

- **Konfidensialitet** - uvedkommende får ikke tilgang på opplysningene,
- **Integritet** - opplysningene endres ikke uautorisert eller utilsiktet, og
- **Tilgjengelighet** - opplysningene er tilgjengelige når det er behov for dem.

Sikkerhetsmålene for Selskapet er som følger:

1) Selskapet skal sikre at informasjon behandles kun i henhold til relevante lover og forskrifter og etter adferdsnormer og sertifiseringer som gjelder for Selskapet.
2) Sikkerheten ved Selskapet skal ha forankring i ledelsen ved Selskapet og skal ivaretas som en integrert del av hele Selskapets organisasjon.
3) Den fysiske sikkerheten ved Selskapet skal hindre at uautoriserte får adgang til lokaler der personopplysninger og andre opplysninger kan være lagret og behandles.
4) Tilgang til systemer og informasjon gis kun til medarbeidere etter behov («need to know») og tilgang til systemer og informasjon for uvedkommende skal forhindres.
5) Selskapet skal sikre at informasjonsbehandling er korrekt og at informasjon ikke endres uten lovlig tilgang.
6) Selskapet skal sikre tilgjengelighet til systemer, tjenester og informasjon til rett tid for de personer som er autorisert.
7) Det skal være tatt i bruk rutiner for å håndtere uønskede hendelser, inkludert virksomhetskritiske sådan, og det skal være mulig å spore slike uønskede hendelser.
8) Det skal være tatt i bruk systematiske læreprosesser ved uønskede hendelser slik at sannsynligheten for tilsvarende eller gjentatte hendelser reduseres.
9) Det skal forhindres at personer eller systemer hos Selskapet bevisst eller ubevisst er årsak til sikkerhetsmessig uønskede hendelser mot egen eller andre virksomheter eller fysiske personer.
10) Selskapet skal sikre at medarbeidere som bruker Selskapets informasjonssystemer og behandler personopplysninger har tilstrekkelig kompetanse til å ivareta Selskapets sikkerhetsbehov/krav.

Sikkerhetsmål skal regelmessig gjennomgås og endres etter Selskapets virksomhet, rammevilkår og trusselbilde. Bakgrunnsmateriale for gjennomgangen vil være:

- Resultater og hovedkonklusjoner fra risikoanalyser og egenkontroll
- Endringer i offentlige sikkerhetskrav, som kan medføre vesentlig endringer for Selskapet
- Vurderinger om tilstrekkelige ressurser er tilgjengelige for å ivareta internkontroll og informasjonssikkerhet

5.3 Gjennomgang av avvik og hendelser

Det skal gjennomføres en detaljert gjennomgang av de alvorligste hendelsene og avvikene som har vært gjennom året - dersom det har vært slike hendelser eller avvik - og kun summarisk gjennomgang av de mindre alvorlige. Årsaker til hendelser og avvik i

vid forstand og hvordan hendelser og avvik er håndtert skal gjennomgås og diskuteres.

Slik gjennomgang skal gjennomføres årlig. Selskapets leder skal sørge for å innkalle og organisere gjennomgangen, og gjennomgangen skal dokumenteres i Personopplysningsdokumentasjonen (se punkt 3). I dokumentasjonen skal det tydelig fremgå de avgjørelser og aksjoner som er bestemt og med hvilken begrunnelse.

5.4 Oppfølging

Oppfølging av sikkerhetsmål for å vurdere om de nås og om forbedringstiltak og korrigerende tiltak virker, gjøres blant annet gjennom egenkontroll.

Oppfølging av at forbedringstiltakene virker, gjøres i forbindelse med den regelmessige gjennomgangen etter punkt 5.1.

6. BEHANDLING AV PERSONOPPLYSNINGER I SELSKAPET

Selskapet behandler personopplysninger for å administrere forholdet til sine ansatte, kunder, kandidater, leverandører og andre som Selskapet har kontakt med, samt annen behandling dersom dette fremkommer nedenfor.

6.1 Sentrale begreper

Med «behandlingsansvarlig» menes den som bestemmer formålet med behandling av personopplysninger og hvilke midler som skal benyttes.

«Databehandler» er den som behandler personopplysninger på vegne av den behandlingsansvarlige.

«Personopplysninger» er enhver opplysning om en identifisert eller identifiserbar person.

«Behandling» er all innsamling, lagring, utlevering og annen bruk av personopplysninger. Selskapet behandler typisk personopplysninger om kandidater som er i rekrutteringsprosesser, kontaktpersoner hos våre kunder og oppdragsgivere og ansatte i selskaper som vi gjennomfører treningsoppdrag for.

6.2 Oversikt over behandling av personopplysninger

Det skal føres en oversikt over behandling av personopplysninger i Selskapet («Behandlingsoversikt» eller omtalt som «protokoll» i GDPR).

Behandlingsoversikten skal være tilgjengelig som en del av Personopplysningsdokumentasjonen, se punkt 3.

6.3 Behandling av personopplysninger

All behandling av personopplysninger skal kun skje etter det formål som opplysningene ble innsamlet for.

Det skal sikres at det ikke samles inn og behandles mer personopplysninger enn nødvendig (dataminimering) ved at enhver som er i befatning med personopplysninger skal vurdere om det er nødvendig å behandle personopplysningene.

Selskapet skal alltid kunne svare på spørsmål, både fra publikum og de som er registrert, om behandlingene av personopplysninger. Henvendelser fra ansatte om behandling av personopplysninger skal håndteres av Selskapets leder eller den som har ansvar for ansatte. Henvendelser fra kunder om behandling av personopplysninger skal håndteres av den enkelte som er ansvarlig for kunden.

Ekstra tiltak, utover tiltak med utgangspunkt i sikkerhetsstrategiene ovenfor, skal iverksettes for spesielt beskyttelsesverdige opplysninger som:

- sykmeldinger
- opplysninger rundt tilrettelegging av arbeidsplassen

- vurderinger av den ansatte
- merknader og advarsler
- lønnstrekk

Det skal vurderes å pseudonymisere eller anonymisere personopplysninger i den grad dette kan gjøres uten at det går utover kvaliteten på behandlingen av personopplysningene. Dersom tilfredsstillende anonymisering ikke er mulig, og det ikke er grunnlag for å fortsette behandling, herunder ved at formålet for behandlingen ikke foreligger fremdeles, skal opplysningene slettes.

6.4 Behandling av særlige kategorier (sensitive) personopplysninger

Med særlige kategorier personopplysninger regnes følgende etter personvernforordningen:

- Rasemessig/etnisk opprinnelse
- Politisk oppfatning
- Religion og overbevisning
- Fagforeningsmedlemskap
- Helseopplysninger
- Seksuelle forhold eller orientering
- Genetiske og biometriske opplysninger for identifikasjonsformål

Det behandles ikke slike opplysninger i Selskapet.

6.5 Behandling av personopplysninger om mindreårige

Det behandles ikke personopplysninger om mindreårige.

6.6 Grunnlag for behandling

Det skal foreligge et lovmessig grunnlag for all behandling i Selskapet.

Benyttes det *samtykke* som grunnlag, skal det kontrolleres om samtykket er dekkende for behandlingen som skal gjennomføres

Selskapet skal kun behandle nødvendige personopplysninger om ansatte og kunder. De som registreres hos Selskapet skal om mulig informeres og være klar over behandlingen, se nærmere om informasjonsplikten i punkt 9.4.

6.7 Ny behandling

Ved ny behandling av personopplysninger skal følgende rutine gjelde:

- Den nye behandlingen skal føres inn i Behandlingsoversikten (se punkt 6.2).
- Det skal vurderes om det foreligger gyldig behandlingsgrunnlag, og behandling skal ikke påstartes uten at det er sikkert at det foreligger et gyldig behandlingsgrunnlag. For kontroll av behandlingsgrunnlag, se punkt 6.6 ovenfor.
- Det skal sikres at all behandling skjer innenfor det formål som opplysningene ble innsamlet for. Det er den som er ansvarlig for behandlingen av opplysningene etter Behandlingsoversikten som har ansvar for å kontrollere at alle former for behandling som skjer med personopplysningene er dekket av det opprinnelige formål for innsamling av personopplysningene. Er den ansvarlige usikker på om behandlingen er innfor det opprinnelige formålet, skal Selskapets leder beslutte om behandling skal gjøres.
- Vil behandlingen kunne påvirke informasjonssikkerheten, eller vil behandlingen

kunne medføre en risiko for de registrerte, skal det gjennomføres en risikovurdering, se punkt **Error! Reference source not found.**, før behandlingen iverksettes.

6.8 Endring av behandling

Ved endret behandling av personopplysninger skal følgende rutine gjelde:

- Endring i behandlingen skal hensyntas i Behandlingsoversikten (se punkt 6.2).
- Det skal kontrolleres at behandlingen skjer etter det formål som personopplysningene opprinnelig ble innsamlet for. Er ikke behandlingen innenfor det opprinnelige formålet, skal det undersøkes om behandlingen kan gjennomføres til tross for at denne ikke er dekket av det opprinnelige formålet. Vurderingen av om behandling skal kunne endres, skal dokumenteres.
- Medfører endret behandling at personopplysninger blir overflødige eller ikke trengs etter formålet, skal personopplysningene tilbørlig slettes, se nærmere i punkt 6.11 om sletting av personopplysninger.
- Vil endringen i behandlingen kunne påvirke informasjonssikkerheten, eller vil kunne medføre en risiko for de registrerte, skal det gjennomføres en risikovurdering, se punkt **Error! Reference source not found.**, før endringen gjennomføres.

6.9 Opphør av behandling

Ved opphør av behandling av personopplysninger skal følgende rutine gjelde:

- Behandlingen skal merkes som opphørt i Behandlingsoversikten (se punkt 6.2).
- Det skal vurderes å informere de registrerte om opphør av behandlingen, og de registrerte skal informeres dersom dette er påkrevet.
- Det skal sørges for at personopplysninger blir tilbørlig slettet etter rimelig tid, og når det er klart at det ikke lenger er nødvendig å oppbevare opplysningene eller den registrerte ber om å bli slettet, jf. pkt. 6.11.

6.10 Overføring av personopplysninger til andre, som behandlingsansvarlige og tredjeparter

Skal personopplysninger overføres til andre, herunder andre behandlingsansvarlige og tredjeparter, skal det undersøkes om mottaker av opplysningene har lovlig behandlingsgrunnlag for personopplysningene. Personopplysninger skal ikke overføres dersom mottakeren ikke har behandlingsgrunnlag eller om det er uklart om det foreligger behandlingsgrunnlag, eller om det er usikkert om mottakeren kan behandle personopplysningene på lovlig og sikker måte.

Overføring av personopplysningene skal skje på sikker måte, som sikrer personopplysningenes konfidensialitet og integritet.

6.11 Sletting av personopplysninger

Personopplysninger skal ikke beholdes og skal slettes sikkert når det ikke lenger er saklig behov for å oppbevare dem i Selskapet, som at det ikke foreligger formål for fortsatt behandling, eller når den registrerte ber om sletting (dersom det er grunnlag for sletting). Den som er angitt som ansvarlig for behandlingen i Behandlingsoversikten er ansvarlig for dette hvis det er endringer ved Selskapet som tilsier at opplysningene skal slettes.

Det vil angis sletteplikter for konkret behandling i Behandlingsoversikten.

6.12 Tilgang til personopplysninger og sikring av konfidensialitet

Personopplysninger om kunder, ansatte og andre skal:

- Ikke være tilgjengelige for personer som ikke har behov for opplysningene i arbeidet

sitt («need to know»).

- Være tilgjengelige og oppdaterte i henhold til behov.

Personopplysningene om ansatte skal kun være tilgjengelige internt i Selskapet for medarbeidere med tjenstlig behov, som leder, ansvarlig for ansatte og Selskapets leder.

6.13 Utlevering og overføring av personopplysninger til andre

Utlevering betyr at personopplysninger overlates til annen behandlingsansvarlig (utlevering til databehandler er behandlet i punkt 7). Dette er en ny behandling, og det kreves et eget behandlingsgrunnlag. Foreligger det ikke annet behandlingsgrunnlag, må det innhentes samtykke fra den registrerte.

Opplysninger om ansatte ved Selskapet kan utleveres til offentlige myndigheter i overensstemmelse med lovpålagte krav. Ved tvil om hjemmel for utlevering, bør det anmodes om at myndighetsorganet beskriver hjemmelen for å kreve opplysningene.

6.14 Overføring av personopplysninger til tredjeland

Dersom personopplysninger skal overføres til tredjeland, dvs. land utenfor EU/EØS, skal det foreligge et lovlig grunnlag for overføringen etter personvernregelverket. Overføring skal også være godkjent av Selskapets leder.

Selskapet skal søke å begrense overføring av personopplysninger til tredjeland, og det skal ikke benyttes databehandler eller tjenester i tredjeland dersom det foreligger like bra alternativer innenfor EU/EØS eller om behandlingen kan skje på måte som gjør at det ikke er nødvendig med overføring til tredjeland.

7. BRUK AV DATABEHANDLER OG BEHANDLING AV ANDRE

Fysiske eller juridiske personer som behandler personopplysninger på vegne av Selskapet, er Selskapets databehandlere. Det skal alltid inngås avtale med databehandlere, hvor Selskapets standard databehandleravtale skal benyttes.

Oversikt over alle databehandlere skal inntas i Behandlingsoversikten (se punkt 6.2).

Det skal sikres at databehandlere og enhver person som handler for Selskapet eller Selskapets databehandlere, og som har tilgang til personopplysninger, skal behandle opplysninger bare etter instruks fra Selskapet.

8. PERSONVERNOMBUD

Selskapet har vurdert at det ikke er pålagt å ha personvernombud etter GDPR artikkel 37, og det er ikke nødvendig for Selskapet å ha personvernombud av andre grunner, siden Selskapet ikke behandler personopplysninger i omfattende grad.

9. FORHOLD TIL DE REGISTRERTE

9.1 Innsyn fra de registrerte i behandling av personopplysninger

Alle registrerte skal få vite hva slags behandling av personopplysninger som foretas i Selskapet og få utlevert de personopplysninger som behandles dersom vedkommende ber om dette.

Henvendelser fra ansatte om innsyn i sine personopplysninger skal håndteres av Selskapets leder eller den som har ansvar for ansatte. Henvendelser fra kunder, kandidater og andre om behandling av personopplysninger skal håndteres av den enkelte som er ansvarlig for vedkommende eller av Selskapets leder.

Forespørsel kan være muntlig, men de ansvarlige for å etterkomme forespørsler om innsyn kan be om skriftlig forespørsel dersom de ønsker det, for å bl.a. kunne dokumentere svartid. Det skal føres logg om innsynsforespørsler.

Innsyn og/eller utskrift skal gis uten unødig opphold og senest innen én måned fra forespørsel er mottatt.

Det skal sikres at opplysninger kun utleveres til den som opplysningene vedrører, ved at det gjøres ID-kontroll. Dersom det er tvil om det er den registrerte som foretar innsynsforespørsel, skal opplysninger ikke utleveres. Det skal også sikres at utlevering av personopplysninger ikke gis på en måte som kan medføre risiko for opplysningenes konfidensialitet og integritet. Opplysninger som anses som sensitive eller for å være ømtålige for den registrerte samt alle spesielle kategorier personopplysninger, skal ikke sendes på e-post eller på måte som ikke sikrer opplysningene tilstrekkelig. Det skal videre sikres at det ikke utleveres personopplysninger om andre ved utlevering av personopplysninger til den registrerte. Eksempelvis skal det ikke utleveres personopplysninger til ansatte som kan inneholde vurdering fra ledere eller andre ansatte.

Henvendelser om innsyn skal behandles på følgende måte:

1. Henvendelse fra den registrerte skal formidles til kundeansvarlige, ansvarlige for ansatte eller Selskapets ledelse for at henvendelser besvares fortløpende, og senest innen én måned.
2. Dersom det behandles personopplysninger om den registrerte, skal det gis følgende informasjon til den registrerte:
    a. Formålene med behandlingen,
    b. de berørte kategoriene av personopplysninger,
    c. mottakerne eller kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, særlig mottakere i tredjestater (dvs. utenfor EU/EØS), samt om de nødvendige garantiene i henhold til GDPR artikkel 46 i forbindelse med overføringen.
    d. dersom det er mulig, hvor lenge det forventes at personopplysningene vil bli lagret, eller, dersom dette ikke er mulig, kriteriene som brukes for å fastsette denne perioden,
    e. retten til å anmode Selskapet om korrigering eller sletting av personopplysninger eller begrensning av behandlingen av personopplysninger som gjelder den registrerte, eller til å protestere mot nevnte behandling,
    f. retten til å klage til Datatilsynet,
    g. dersom personopplysningene ikke er samlet inn fra den registrerte, all tilgjengelig informasjon om hvor personopplysningene stammer fra,
3. Dersom den registrerte ber om det, skal det gjøres tilgjengelig en kopi av de personopplysninger som behandles om den registrerte. I slike tilfelle skal det påses at innsyn i og utlevering av personopplysninger ikke medfører at den som ber om innsyn får innsyn i andre fysiske personers personopplysninger. Det skal foretas en verifikasjon av den registrertes identitet før personopplysninger utleveres. Det skal sikres at det ikke utleveres personopplysninger om andre fysiske personer eller at andre fysiske personers personvern krenkes på noen måte ved utleveringen eller innsynet i personopplysningene.

    Det skal ikke utleveres opplysninger som kan krenke andres rettigheter eller friheter, herunder kundekonfidensialitet, forretningshemmeligheter eller immaterialrett og opphavsrett. Disse hensynene bør imidlertid ikke føre til at den registrerte nektes innsyn i alle opplysninger. Behandles det en stor mengde opplysninger om den registrerte, kan det anmodes om at den registrerte presiserer hvilke opplysninger eller behandlingsaktiviteter anmodningen gjelder.

Det skal ikke kreves gebyr eller annen betaling for oppfyllelse av innsynet.

9.2 Anmodning om endring eller sletting fra registrerte

Anmodning om endring eller sletting fra registrerte skal håndteres av den ansvarlige for behandlingen etter Behandlingsoversikten. Sletting skal kun skje dersom det foreligger grunnlag for sletting og det ikke er et fortsatt formål for behandling av personopplysningene.

For regnskapsmateriale og arkivverdig materiale skal det vurderes om opplysninger kan slettes etter spesiell lovregulering.

9.3 Retting og supplering

Personopplysninger om ansatte og kunder skal være tilstrekkelige og relevante for formålet med behandlingen. Kravet til relevans trekker opp en ytre grense for hvilke personopplysninger som kan tas med i behandlingen, og kan ikke fravikes gjennom samtykke fra den registrerte. Kravet til tilstrekkelighet innebærer at man må ha nok opplysninger for å kunne ivareta formålet med behandlingen.

Følgende rutine skal gjelde for behandling av forespørsel om retting og supplering:

- Mottak av forespørsel om retting eller supplering for ansatt eller kunde.
- Verifisering at den som fremmer forespørselen er den registrerte eller har fullmakt til å fremme forespørsel om retting eller supplering.
- Formidling av forespørsel til rette ansvarlige. Er det ingen ansvarlig, skal forespørselen håndteres av Selskapets leder.
- Mottakeren av forespørselen skal verifisere korrekthet av forespurte endringer av opplysninger.
- Hvis endringene er verifisert, foreta endring eller supplering, herunder utstede arbeidsordre for oppdatering av system(er).
- Dokumentere endringen/suppleringen.
- Bekrefte skriftlig til den som har fremmet forespørselen (den registrerte).

9.4 Oppfyllelse av informasjonsplikt

Det skal sørges for at de registrerte får informasjon når det samles inn informasjon fra de registrerte (GDPR artikkel 13) og når det samles inn opplysninger fra andre enn de registrerte (GDPR artikkel 14).

Det skal søkes i størst mulig grad å gi informasjon direkte til den registrerte om behandling av personopplysninger i Selskapet. Dette kan gis ved e-post eller skriftlig informasjon på annen måte. Uansett skal Selskapet ha en dekkende informasjon om behandling av personopplysninger i Selskapet tilgjengelig på sine eksterne nettsider for kunder og andre som det behandles personopplysninger om, og informasjon på intranettet og/eller i personalhåndbok om behandling av personopplysninger om ansatte.

9.5 Dataportabilitet

Selskapet har ikke behandling som er underlagt reglene om dataportabilitet, men blir det behandlet personopplysninger på grunnlag av samtykke eller avtale, hvor behandlingen er kun automatisert og det er kun personopplysninger som de registrerte selv har avgitt, skal det tilrettelegges for dataportabilitet ved at det skal være mulig å eksportere personopplysningene på et maskinlesbart format som kan utleveres til den registrerte og/eller overføres til annen behandlingsansvarlig.