

**Hensikt**

Sikre at vi behandler personopplysninger i samsvar med krav i regelverk  
Informere om hvordan vi håndterer personalopplysninger

**Omfang**

Personopplysninger som registreres i firmaet

**Ansvar**

Daglig leder er ansvarlig for at personopplysninger vi behandler, om egne ansatte, kontaktpersoner hos kunder og leverandører, privatkunder og andre forretningsforbindelser håndteres i henhold til krav i regelverk

**Utførelse****1. Kunnskap over reglene om personopplysninger**

Ledelse og alle ansatte som håndterer personopplysninger skal ha kunnskap om reglene for håndtering av personopplysninger – spesifikt utdypet i dette dokumentet om personvern. Kunnskapsnivået skal være tilpasset den enkelte ansattes behandling av personopplysninger.

**2. Kartlegging av behandling av personopplysninger**

All behandling av personopplysninger er kartlagt i eget skjema, der vi angir bl. annet kategorier av registrerte, formål med behandlingen, hvordan vi behandler opplysningene og hvilke grunnlag den har for behandlingen. Skjemaet bidrar til at vi etterlever reglene for behandling av personopplysninger. Skjemaet er kun tilgjengelig for ledelsen – men alle kan få innsynsrett i kartleggingsskjemaet.

**3. Grunnkrav for behandling av personopplysninger**

Det er seks grunnlag som gjelder for all behandling av alle personopplysninger:

- 1) Behandles på en lovlig, rettfærdig og gjennomiktig måte med hensyn til den registrerte («lovlighet, rettfærdighet og gjennomiktighet»). Ref. art. 5 a i personvernforordningen
- 2) Samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene («formålsbegrensning»). Ref. art. 5 b i personvernforordningen
- 3) Være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»). Ref. art. 5 c i personvernforordningen
- 4) Være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller korrigeres («riktighet»). Ref. art. 5 d i personvernforordningen
- 5) Lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for («lagringsbegrensning»). Ref. art. 5 e i personvernforordningen

## 11-7-0 Personverdokument for DEEP C

---

- 6) Behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og fortrolighet»). Ref. art. 5 f i personvernforordningen

### 4. Grunnlag/lovlighet for å behandle personopplysninger

#### 4.1 Behandlingsgrunnlag

Vi skal ha minst ett av følgende grunnlag for all behandling av personopplysninger:

- 1) Den registrerte har gitt **samtykke** til behandling av sine personopplysninger for ett eller flere spesifikke formål, **ref. art. 6 a** i personvernforordningen
- 2) Behandlingen er nødvendig for å **oppfylle en avtale** som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse, **ref. art. 6 b** i personvernforordningen
- 3) Behandlingen er nødvendig for å **oppfylle en rettslig forpliktelse** som påhviler den behandlingsansvarlige, **ref. art. 6 c** i personvernforordningen
- 4) Behandlingen er nødvendig for å **ivareta legitime interesser** – interesseavveining, dvs. formål knyttet til de **berettigede interessene** som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn, **ref. art. 6 f** i personvernforordningen

Det skal gå frem av kartleggingskjemaet hvilke(t) grunnlag vi har for å behandle opplysninger.

Hvis grunnlaget for behandling er samtykke fra den registrerte (se nr. 1), er det særlige regler som gjelder for slike samtykker, blant annet kravet om dokumentasjon.

Hvis grunnlaget for behandling er vår berettigede interesse (interesseavveining) (se nr. 4), skal vi konkret og skriftlig dokumentere avveiningen, se nærmere nedenfor.

#### 4.2 Ansatte

Behandling av opplysninger er i hovedsak rettslige forpliktelser. Noe av behandlingen er også basert på interesseavveining. Vi har behov for å dokumentere at vi har oppfylt forpliktelser etter lov og avtale etter at de er oppfylt. Vi har også behov for dokumentasjon for personaladministrasjon til bruk for fremtidig personaladministrasjon. Dette er berettigede interesser. Det er ikke mulig å ha tilgang til opplysningene på en annen måte enn å lagre opplysningene. Behandling er derfor nødvendig.

Ansatte har et løpende avtaleforhold med oss. Personopplysningene vi behandler er knyttet til dette avtaleforholdet. Det er i stor grad snakk om opplysninger ansatte har gitt oss. Opplysningene gjelder forhold det er nærliggende at en arbeidsgiver behandler.

Vi mener at den berettigede interessen går foran den ansattes interesser.

### **4.3 Tidligere ansatte**

Behandlingen av de fleste av personopplysningene er basert på interesseavveining. Det kan oppstå behov (for oss) for å dokumentere personalforhold også etter at arbeidsforholdet er avsluttet, f.eks. en tvist med en tidligere ansatt, eller en skade (yrkesskadesak). Dette kan gjelde f.eks. dokumentasjon for at vi som arbeidsgiver har oppfylt våre forpliktelser etter lovgivning eller arbeidsavtalen. Dette er berettiget interesse. Det er ikke mulig å ha tilgang til opplysningene på en annen måte. Behandling er derfor nødvendig.

Behandlingen går ut på å lagre opplysningene i inntil 2 år. Opplysninger om at den ansatte har vært ansatt, varighet av arbeidsforholdet og arbeidsoppgaver kan vi lagre lengre. Opplysningene vil ikke bli utlevert til andre uten at den tidligere ansatte ber om det, f.eks. i forbindelse med vurdering av ansettelse hos ny arbeidsgiver.

Vi mener at den berettigede interessen går foran den ansattes interesser.

### **4.4 Jobbsøkere**

Behandlingen av personopplysninger er basert på interesseavveining. Vi har behov for å bruke opplysninger for å vurdere jobbsøknader som blir tilsendt. Dette er berettiget interesse. Det er ikke mulig å vurdere en søknad uten å behandle personopplysninger. Behandling er derfor nødvendig.

Vi ber de som vil søke jobb hos oss om å sende minimum opplysninger om navn, utdanning, arbeidserfaring, referanser, m.v. (CV). Jobbsøkere vil ofte, i tillegg, gi ytterligere personopplysninger de anser som relevante for vurdering av søknaden, som f.eks. kontaklinformasjon, familieforhold og interesser. I intervjuprosessen stiller vi spørsmål for å avgjøre om jobbsøkeren passer til stillingen. I noen tilfeller kan vi bruke tester eller spørsmålsskjemaer for dette formålet. Hvis det blir aktuelt å ansette jobbsøkeren vil vi kunne be om ytterligere informasjon, samt om dokumentasjon for opplysninger vi allerede har mottatt. Det er frivillig å gi oss opplysninger.

Vi bruker ikke opplysningene til noe annet enn å vurdere søknaden. Vi gir ikke opplysningene til noen andre. Vi kan beholde opplysninger fra jobbsøkere i 6 mnd., i tilfelle jobbsøkere skulle mene at deres rettigheter ikke er oppfylt.

Vi mener at den berettigede interessen går foran den jobbsøkendes interesser.

### **4.5 Kontaktpersoner hos leverandører**

Behandlingen av personopplysninger er basert på interesseavveining. Vi har behov for å holde kontakt med våre leverandører for å følge opp blant annet tilbud, bestillinger og leveranser. Dette er en berettiget interesse. Denne kontakten blir bare effektiv ved å kontakte enkeltpersoner direkte. Behandling er derfor nødvendig.

## **11-7-0 Personverndokument for DEEP C**

---

Behandlingen skjer overfor kontaktpersonens arbeidsgiver, som ønsker å være leverandør hos oss. I tillegg til navn behandler vi kontaktopplysninger som telefonnummer, mailadresse og arbeidsgiver, som alle er knyttet, først og fremst, til kontaktpersonens arbeidsforhold, og ikke til kontaktpersonens privatliv. Omfanget av opplysningene er svært begrenset. Behandlingen av opplysningene er knyttet til leverandørens næringsvirksomhet og ikke til kontaktpersonens privatliv. Vår behandling av personopplysningene er klart påregnelig for kontaktpersonen.

Vi mener at den berettigede interessen går foran kontaktpersonens interesser.

### **4.6 Kontaktpersoner hos bedriftskunder**

Behandlingen av personopplysninger er basert på interesseavveining. Vi har behov for å holde kontakt med våre bedriftskunder for å følge opp blant annet tilbud, bestillinger og leveranser. Dette er en berettiget interesse. Denne kontakten blir bare effektiv ved å kontakte enkeltpersoner direkte. Behandling er derfor nødvendig.

Behandlingen skjer overfor kontaktpersonens arbeidsgiver, som er kunde hos oss. I tillegg til navn behandler vi alminnelige opplysninger som telefonnummer, mailadresse og arbeidsgiver, som alle er knyttet, først og fremst, til kontaktpersonens arbeidsforhold, og ikke til kontaktpersonens privatliv. Omfanget av opplysningene er svært begrenset. Behandlingen av opplysningene er knyttet til kundens næringsvirksomhet og ikke til kontaktpersonens privatliv. Når det er nødvendig med samtykke etter markedsføringsloven, vil kontaktpersonen dessuten ha gitt samtykke før vi sender eposter med markedsføring. Vår behandling av personopplysningene er klart påregnelig for kontaktpersonen.

Vi mener at den berettigede interessen går foran kontaktpersonens interesser.

### **4.7 Andre kontaktpersoner**

Behandling av personopplysninger er basert på interesseavveining. Vi har behov for å ha kontakt med offentlige myndigheter, f.eks. NAV og tilsynsmyndigheter i forbindelse med offentligrettslige forhold der vi kan ha forpliktelser og rettigheter. Dette er en berettiget interesse. I en del tilfeller vil denne kommunikasjonen bare kunne være effektiv hvis vi kan kontakte enkeltpersoner direkte. Behandling er derfor nødvendig.

Vi lagrer navn og kontaktdetaljer og vår behandling av personopplysningene er klart påregnelig for kontaktpersonen.

Vi mener at den berettigede interessen går foran kontaktpersonens interesser.

## **5. Grunnlag for behandling av sensitive personopplysninger**

Behandling av sensitive personopplysninger krever behandlingsgrunnlag i tillegg til de som er nevnt i pkt. 6.

Sensitive personopplysninger er: opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, samt genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person,

## **11-7-0 Personverdokument for DEEP C**

---

helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, ref. art. 9 i personvernforordningen.

Skal vi behandle slike opplysninger, skal vi sørge for å ha behandlingsgrunnlag. For ansatte hos oss vil opplysninger om helse og evt. fagforeningsmedlemskap være særlig aktuelle. Helse omfatter f.eks. sykdom og skader og fravær begrunnet i dette. Særlig aktuelt behandlingsgrunnlag vil være at behandling er nødvendig i egenskap av arbeidsgiver, f.eks. ved oppfølging og rapportering til offentlige myndigheter eller ved tilrettelegging av arbeidsforhold.

Behandling av opplysninger om straffbare forhold og lovovertridelser, o.l. er underlagt særlige regler som vi skal sette oss inn i hvis vi skal behandle slike opplysninger.

### **6. Informasjon til de registrerte (personvernerklæring)**, ref. art. 12, nr. 1

Vi skal gi lovbestemt informasjon til de registrerte. Vi skal gi slik informasjon i en personvernerklæring. Alle registrerte skal ha tilgang til den informasjonen som gjelder dem. Informasjon til ansatte gir vi i *(personalhåndbok, ansettelsesavtale, intranett eller lignende)*

Informasjonen skal inneholde blant annet navn på bedriften og kontaktinformasjon, formålet med behandlingen, kategoriene av personopplysninger, mottakere av personopplysninger (dersom de utleveres), informasjon om evt. utlevering av personopplysninger til andre land, hvor lenge personopplysningene vil bli lagret, de registrertes rett til å kreve innsyn, rette eller kreve slettet personopplysningene, hvordan virksomheten fikk tilgang til personopplysningene og muligheten til å klage virksomheten inn til Datatilsynet. Ref. art. 13 - 15 i personvernforordningen.

### **7. Registrertes rettigheter**

Vi skal besvare henvendelser fra registrerte uten ugrunnet opphold, og senest innen 1 mnd. Mottar vi slike henvendelser, skal de sendes til daglig leder, ref. art. 12, nr. 3 i personvernforordningen.

Vi skal sørge for at registrerte får gjennomført sine rettigheter hos oss. Ref. art. 12 - 22 i personvernforordningen.

### **8. Sletting av personopplysninger** ref. art. 17 i personvernforordningen

Vi skal slette personopplysninger uten ugrunnet opphold når de ikke lenger er «nødvendig» for formålet som de ble samlet inn eller behandlet for. Minst 1 gang i året skal vi gjennomgå dette. Våre retningslinjer for sletting følger nedenfor eller av kartleggingsskjemaet.

### **9. Ansatte**

Vi beholder som hovedregel alle opplysninger i hele ansettelsestiden. Ansatte kan be om at opplysninger blir slettet. Dette vil bli vurdert konkret. Lovgivningen kan stille krav til lengre oppbevaringstid.

## **11-7-0 Personverdokument for DEEP C**

---

### **10. Tidligere ansatte og jobbsøkere**

Se ovenfor om behandlingsgrunnlaget for disse kategoriene. Lovgivningen kan stille krav til lengre oppbevaringstid enn det som fremgår der.

### **11. Kontaktpersoner hos leverandører og kunder**

Vi skal slette opplysningene når vi blir kjent med at kontaktpersonen har sluttet hos leverandøren eller kunden, eller at leverandøren eller kunden har utpekt ny kontaktperson. Det samme gjelder når leverandør- eller kundeforholdet er opphørt.

Vi kan likevel lagre opplysningene for en lengre periode hvis vi mener det kan bli nødvendig med dokumentasjon av den kontakten vi har hatt med leverandøren eller kunden. Det kan f.eks. gjelde spørsmål om rettigheter eller forpliktelser i avtaleforholdet mellom leverandøren eller kunden. Også lovgivningen kan stille krav til lengre oppbevaringstid.

### **12. Andre kontaktpersoner**

Vi skal slette opplysningene når vi blir kjent med at personen ikke lenger er relevant for våre behov, f.eks. hvis den personen slutter hos den bedriften, offentlige etaten, osv.

Vi kan likevel lagre opplysningene for en lengre periode hvis vi mener det kan bli nødvendig med dokumentasjon/kontakt med personen eller personens arbeidsgiver. Det kan gjelde f.eks. spørsmål og rettigheter eller forpliktelser i avtale-, offentligrettslige- eller andre forhold.

### **13. Personvernombud**

Vi har vurdert om personvernforordningen krever at vår bedrift skal ha personvernombud.

Vi har ingen eller svært få fysiske personer som kunder. Vi driver ikke regelmessig og systematisk monitorering i stor skala av registrerte. For de fleste kategorier av registrerte behandler vi stort sett alminnelige personopplysninger som navn, adresse, arbeidsgiver, mailadresse, telefonnummer, o.l. Vi behandler enkelte sensitive opplysninger om ansatte.

Vi har konkludert med at vår bedrift ikke er underlagt krav om å ha personvernombud. Ref. art. 37 i personvernforordningen.

### **14. Alminnelig risikovurdering**

Vi skal risikovurdere behandlingen av personopplysninger. Denne vurderingen skal gjøre at vi er i stand til å identifisere og definere hvilke sikkerhetstiltak vi skal gjennomføre. Ref. art. 24 (og 35)

Vurderingene skal gjelde sannsynlighet og alvorlighetsgrad (risiko) for personers «rettigheter og friheter», som fysisk skade, skade på ting eller formue og medisinsk skade. Eksempler på skader er diskriminering, identitetstyveri, omdømmeskade, tap av sosial aktelse, at konfidensielle opplysninger blir kjent for uvedkommende og uakseptable inngrep i privatlivets fred.

## 11-7-0 Personverndokument for DEEP C

---

Kartleggingskjemaet viser at vi:

- i stor grad behandler bare alminnelige kontaktopplysninger som navn, adresse, arbeidsgiver, mailadresse, telefonnummer, o.l.
- behandler opplysninger om ansatte som er vanlige for å administrere personalforhold, herunder etterlevelse av lovpålagte forpliktelser.
- Har få eller ingen privatkunder
- Har få eller ingen opplysninger om barn
- Behandler opplysninger som er en del av det å drive alminnelig næringsvirksomhet

Vi har aldri vært utsatt for datainnbrudd. Vi er heller ikke kjent med at utenforstående har vist interesse for de personopplysningene vi behandler. Vi mener derfor at det er liten sannsynlighet for at opplysningene er utsatt for regelbrudd.

Basert på arten og omfanget av de opplysningene vi behandler, mener vi at konsekvensene ved regelbrudd ikke vil være alvorlige.

Når det gjelder en del av opplysningene om ansatte, er både sannsynlighet og alvorret ved regelbrudd en del større. Vi har derfor egne rutiner for behandling av slike opplysninger, herunder begrensning av tilgang til dem.

Vi skal risikovurdere endringer som kan påvirke informasjonssikkerheten, f.eks. når vi kjøper nye IT-tjenester.

Resultatene av risikovurderinger skal godkjennes av den som har det daglige behandlingsansvaret i bedriften.

### 15. Informasjonssikkerhet

Vi skal etter loven treffe passende tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som svarer til risikoen knyttet til vår behandling av personopplysninger. Vi skal ta hensyn til teknikkens stand, gjennomføringskostnadene og behandlingens karakter, omfang og formål, samt sammenhengene den utføres i. Ref. art. 32 i personvernforordningen.

Risikoene våre er vurdert overordnet i punktet overfor.

På denne bakgrunn har vi gjennomført disse tiltakene:

- Det er utpekt en person hos oss med særlig oppgave å påse sikkerheten:
  - **Tittel / Navn: Daglig leder Odd Gustav Kvalvåg**
- Uvedkommende skal hindres tilgang til personopplysningene eller utstyr disse er lagret på.
- Det skal sikres at virksomhetens nettverk er beskyttet mot inntrenging fra eksterne nettverk med brannmur som kun slipper gjennom nødvendig datatrafikk.
- Det skal sikres at virksomhetens nettverk er beskyttet mot uvedkommendes bruk, eksempelvis ved sikring av trådløst nettverk.
- Ekstra tiltak skal iverksettes for spesielt beskyttelsesverdige opplysninger, som for eksempel sykemeldinger, vurderinger av den ansatte, merknader og advarsler.
- Ansatte skal gis opplæring i bruk av virksomhetens IT-system.

**16. Kjøp av IT-tjenester - databehandleravtaler**

Vanligvis vil vi opptre som behandlingsansvarlig når virksomheten kjøper IT-tjenester fra en tjenesteleverandør. Vi har da fortsatt ansvaret for et personvernlovgivningen blir etterlevd ved kjøp av IT-tjenester, for eksempelvis HR-løsninger eller kundedatabaser/CRM.

Før vi kjøper IT-tjenester skal vi derfor, blant annet, vurdere om leverandøren tilfredsstillere kravene til sikkerhet som personvernloven krever (ref. artikkel 32). Seriøse leverandører vil ofte kunne dokumentere at de oppfyller kravene. Vi må også sørge for å inngå en databehandleravtale som regulerer hvordan databehandleren skal håndtere personopplysningene den mottar fra og behandler på vegne av oss. Leverandører vil ofte ha egne avtaler som oppfyller kravene i regelverket.

Dersom tjenesteleverandøren skal overføre personopplysninger til land utenfor EU/EØS, må det foreligge et lovlig grunnlag for dette (ref. art. 44 – 50 i personvernforordningen).

**17. Brudd på personopplysningssikkerheten**

Ved brudd på personopplysningssikkerheten (hackerangrep, tap av personopplysninger), skal vi straks kontakte Datatilsynet for å finne ut hva vi bør gjøre.

«Brudd på personopplysningssikkerheten» betyr brudd som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som vi behandler.

Ved visse brudd på personopplysningssikkerheten skal vi varsle Datatilsynet, og av til også den registrerte. Varsling til Datatilsynet skal skje med en gang, og senest 72 timer etter at vi ble kjent med bruddet. Det er ikke nødvendig å varsle Datatilsynet hvis det er lite trolig at bruddet på personopplysningssikkerheten vil føre med seg risiko for enkeltpersoners rettigheter. For eksempel der et sikkerhetsbrudd har ført til at uvedkommende har fått tilgang til personopplysninger som allerede er offentlig tilgjengelige.

Vi har plikt til å varsle den registrerte dersom det er trolig at bruddet på personopplysningssikkerheten vil medføre høy risiko for enkeltpersonenes rettigheter og friheter. Vi mener at vår behandling av personopplysninger bare helt unntaksvis kan føre til slik risiko.

Vi skal dokumentere eventuelle brudd på personopplysningssikkerheten. Dette gjør vi ved å beskrive de faktiske forholdene rundt bruddet (hva har skjedd?). I tillegg skal vi beskrive virkningene av bruddet og hvilke tiltak som er truffet for å avhjelpe bruddet. Denne dokumentasjonen skal gjøre det mulig for Datatilsynet å kontrollere at virksomheten har etterlevd kravene i loven. Ref. art. 33 og 34 i personvernforordningen.

**18. Vurdering av personvernkonsekvenser og forhåndskonsultering med Datatilsynet**

Vi skal utrede personvernkonsekvensene når vi planlegger en behandling av personopplysninger som sannsynligvis vil utgjøre en høy risiko for personers rettigheter, som retten til personvern. I vurderingen av om det er nødvendig med en slik utredning skal vi ta

## **11-7-0 Personverndokument for DEEP C**

---

hensyn til arten, omfanget, sammenhengen og formålet med behandlingen. Den skal også ta hensyn til om den benytter ny teknologi.

Det er flere typetilfeller der det er nødvendig å utrede personvernkonsekvenser: Systematisk og omfattende vurdering av personlige forhold når opplysningene brukes til automatiserte avgjørelser, behandling av sensitive personopplysninger i stort omfang eller systematisk overvåking av offentlig område i stort omfang. Ref. art. 35 og 36 i personvernforordningen.

I tilfellene overfor skal vi sette oss inn i de særlige reglene som gjelder, blant annet om at Datatilsynet av og til skal involveres i forhåndsdrøftelser.

### **19. Kontroll, oppdatering og revisjon av dokument**

Vi skal oppdatere og revidere dette dokumentet jevnlig. Dette fordi at, blant annet, reglene i lov og forskrift kan bli endret, vår behandling av personopplysninger kan bli endret eller erfaringer kan tilsa at vi bør endre rutinene våre. Av de samme grunnene skal vi også jevnlig gjennomgå og oppdatere skjema for kartlegging av personopplysninger.

Det er daglig leder som har ansvaret for at behov for endringer og revisjoner blir identifisert og innarbeidet i dokumentet og skjemaet. Dette skal gjøres ved behov.

Vi har egne rutiner som gjelder intern revisjon og evaluering av system og dokumenter.

#### **19.1 Avvik, årsaksanalyse og tiltak for å rette opp i dem**

Vi må finne ut om behandlingen av personopplysninger følger reglene i personopplysningsloven og rutinene i dette dokumentet. Er det ikke tilfellet, må vi finne ut hvordan vi kan øke etterlevelsen. Vi skal dokumentere skriftlig både hvilke avvik vi har funnet og hva vi har gjort for å rette dem opp.

Viser det seg at rutinene ikke er godt nok tilpasset vår bedrift, bør vi vurdere å endre rutinene, ref. pkt. 19.