

SJEKKLISTE INFORMASJONSPLIKT/PERSONVERNERKLÆRING

Informasjon som gis til de personopplysningene gjelder (de registrerte) – som kan tas inn i personvernerklæring eller informeres om på annen måte – skal være følgende (en oversikt):

- Identiteten og kontaktopplysninger til behandlingsansvarlig mv.** Det må opplyses om hvem som er behandlingsansvarlig og kontaktopplysningene til denne/dennes representant og til eventuelt personvernombud.
- De enkelte behandlinger.** Det må informeres om de enkelte behandlinger av personopplysninger som gjøres. Bruk gjerne behandlingsprotokollen som skal lages etter GDPR artikkel 30 for å sjekke at alle behandlinger er med. Merk at det skal ikke tas med opplysninger som man «kan eventuelt» behandle – informasjonen skal være konkret. Følgende informasjon må tas med for hver enkelt behandling:
 - *Formålet* med behandlingen, gjerne supplert med at det tas inn en beskrivelse av behandlingen (men sistnevnte er ikke et krav).
 - De berørte *kategorier personopplysninger* (gjelder kun om opplysningene ikke samles inn fra den registrerte selv, men kan være hensiktsmessig å ta med også i andre tilfelle).
 - *Opphavet til opplysningene*, dvs. fra hvilken kilde personopplysningene stammer fra, og, dersom det er relevant, om de stammer fra offentlig tilgjengelige kilder (gjelder kun om opplysningene ikke samles inn fra den registrerte selv).
 - *Rettslige grunnlag* for behandlingen etter GDPR artikkel 6, og eventuelle unntak for behandling av særlige kategorier personopplysning etter GDPR artikkel 9. Her bør man ikke bare liste grunnlagene, men være klar på grunnlagets forhold til den enkelte behandling, ref. krav om klarhet nedenfor.
 - ◆ Ved behandling basert på berettigede interessene, ta med disse interessene.
 - ◆ Ved behandling basert på samtykke, ta med den registrertes rett til å trekke tilbake samtykket uten at det påvirker lovligheten av en behandlingen før samtykket trekkes tilbake.
 - Det tidsrom personopplysningene vil bli lagret, eller dersom dette ikke er mulig, kriteriene som brukes for å fastsette dette tidsrommet (herunder sletting).
- Utlevering/mottakere.** Eventuelle mottakere eller kategorier av mottakere av personopplysningene.
- Overføring ut av EØS.** Om personopplysningene skal overføres til en tredjestat og om det skjer til et land med tilstrekkelig beskyttelsesnivå eller ikke, eller henvisning til annet overføringsgrunnlag (som EU-kommisjonens standard kontraktsbestemmelser), hvordan man får tak i et eksemplar av dem, eller hvor de er gjort tilgjengelig.
- Lov-/avtalefestet krav om å avgi personopplysning.** Om det foreligger et lov- eller avtalefestet krav om å gi personopplysninger eller et krav som er nødvendig for å inngå en avtale, samt om den registrerte har plikt til å gi personopplysningene og om mulige konsekvenser dersom vedkommende ikke gjør det (kun et krav for opplysninger som samles inn fra den registrerte).
- Viderebehandling.** Om personopplysningene skal viderebehandles for et annet formål enn det opplysningene ble samlet inn for: Gi informasjon om nevnte andre formål og annen nødvendig informasjon.

Rettighetene til de registrerte, se GDPR artikkel 15 til 22, herunder retten til:

- Innsyn
- Retting
- Sletting
- Begrensning av behandlingen som gjelder den registrerte
- Rett til å bli varslet ved retting, sletting eller begrensning i behandling. Samt rett til å bli varslet ved personvernbrudd.
- Protestere mot behandlingen
- Dataportabilitet
- (Rett til å trekke tilbake samtykke, se ovenfor).
- (Rett til å klage, se nedenfor).

Det bør også tas med hvordan de registrerte kan bruke sine rettigheter.

Retten til å klage til en tilsynsmyndighet (som Datatilsynet).

Automatiserte avgjørelser/profilering. Forekomsten av automatiserte avgjørelser, herunder profilering, og, i det minste i nevnte tilfeller, relevant informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte.

Sikkerhet for behandlingen (ikke krav, men mange inkluderer dette).

Endringer i personvernerklæringen (ikke krav, men kan være hensiktsmessig hvordan det gis informasjon ved endringer).

Det er noe ulike krav til informasjon om personopplysningene er mottatt fra den registrerte eller ikke. Ovenfor er alle kravene tatt samlet, men det er angitt når informasjon kreves henholdsvis når informasjonen er mottatt fra den registrerte eller fra andre.

I tillegg skal informasjonen ovenfor gis på en *«kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk»*, se GDPR artikkel 12. Dette stiller krav til hvordan personvernerklæringen skrives, og det kan bli en vanskelig avveining om erklæringen skal være dekkende og samtidig kortfattet.

Husk at en personvernerklæring skal være et levende dokument som skal dekke behandlingen til enhver tid. Denne må derfor oppdateres ved endring i behandlingen, og gjennomgås ved jevne mellomrom for å kontrollere at den er dekkende.

Denne oversikten er kortfattet og gir bare en oversikt. Se artikkel 12 til 15 i GDPR for mer informasjon, samt [veileder fra Datatilsynet](#).