GDPR: EN OVERSIKT OVER DE DE NYE REGLENE

I denne oversikten gis en enkel oversikt over de viktigste kravene som GDPR stiller til virksomheter. Oversikten er utarbeidet av Bing Hodneland advokatselskap (kun for deltagere). Den bygger på boken «Personvern – publisering og behandling av personopplysninger» som utgis sommeren 2018.

INNHOLD:

1. DEFINISJONER

1.1 Hva er en personopplysning?

GDPR artikkel 4(1) & artikkel 9(1) & artikkel 10

Personopplysning: En personopplysning er enhver opplysning om en identifisert eller identifiserbar fysisk person. Denne personen kalles den registrerte.

Identifiserbar betyr at det må være mulig å finne ut hvem som er den registrerte som personopplysningene tilhører. Epostadressen post@binghodneland.no er ikke en personopplysning.

Eksempler: Navn, adresse, fødselsnummer, epostadresse, mobilnummer, IP-adresse, GPS-koordinater/lokasjonsdata, bilskilt, fotografi/bilde, betalingsoverføring/bankinformasjon, brukernavn på sosiale medier.

Personopplysning er et vidt begrep, det gjelder alle elementer som er spesifikke for en persons identitet.

Eksempler: Adferdsmønstre, hvilke butikker personen handler i og når, hvilken musikk de hører på, hvordan de bruker en app, hvilke lenker de trykker på, hvilke konserter de har vært på, hvilke videoer de ser på etc.

Sensitive personopplysninger: Det som tidligere het sensitive personopplysninger heter nå **særlige kategorier personopplysninger**. Dette er opplysninger av mer privat karakter og det gjelder strengere krav i form av ekstra behandlingsgrunnlag. Artikkel 9 nr. 1 angir disse: Rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person (eksempel: skann av iris i øyet eller fingeravtrykk), helseopplysninger (eksempel: opplysning om et persons brukket fot, medisiner de bruker eller at de går til psykolog) eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Opplysninger om straffbare forhold: Personopplysninger om straffedommer og straffbare forhold er også særskilt regulert i GDPR, se artikkel 10. Eksempler: Opplysninger om at en fysisk person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling.

1.2 Hva er behandling?

GDPR artikkel 4(2)

Behandling: Enhver operasjon eller rekke operasjon som utføres på personopplysninger.

Eksempel: Lagre, sende, slette, organisere personopplysninger, men også å laste opp på en internett side eller sosiale medier.

Unntak: Behandling for helt private formål er unntatt fra GDPR.

Eksempel: Hvis man setter opp kameraer på egen eiendom som kun viser innvendige rom/sin egen hage, vil dette være behandling med privat formål og ikke være omfattet av GDPR. Men hvis kameraene også viser veien som går forbi huset ved siden av hagen, så vil det ikke lenger falle inn under unntaket i GDPR.

1.3 Hvem er aktørene?

GDPR artikkel 4(1), (7) & (8)

Den registrerte: Den fysiske personen som er identifisert eller identifiserbar og som personopplysningene gjelder.

Behandlingsansvarlig: Den som bestemmer formålet med og midlene for behandlingen. Det kan være hvem som helst, fysisk person, selskap, offentlig myndighet.

Eksempel: En arbeidsgiver er behandlingsansvarlig for sine ansatte. En virksomhet vil også være behandlingsansvarlig når de behandler kunders personopplysninger. En konsertarrangør vil være behandlingsansvarlig både som arbeidsgiver overfor ansatte eller innleide personer og som arrangør overfor både kunder og artister.

Databehandler: Den som utfører behandlingsaktivitetene på vegne av den behandlingsansvarlige.

Eksempel: Revisor, billettleverandør, outsourcet IT-drift, skylagrinsleverandør.

2. OVERSIKT OVER NOEN VIKTIGE ANSVARSOMRÅDER FOR VIRKSOMHETEN

2.1 Prinsipper

GDPR artikkel 5

Behandling av personopplysninger må følge visse prinsipper. Disse prinsippene kan egentlig anses som de overordnede kravene til behandlingen. Resten av GDPRs spesifikke krav har sitt opphav i disse prinsippene som dermed må følges for behandling av personopplysninger.

Eksempel: Behandlingsansvarlig har en informasjonsplikt overfor de registrerte. Denne vil vanligvis oppfylles med en personvernerklæring. Informasjonsplikten er et spesifikt krav som har sitt utsprang fra prinsippet om åpenhet (også kalt gjennomsiktighetsprinsippet).

Prinsippene er:

- **Lovlighet, rimelighet og åpenhet**: Personopplysninger skal behandles lovlig, rimelig og på en åpen måte.
- **Formålsbegrensning**: Personopplysninger skal innsamles til uttrykkelig angitte og legitime formål og må ikke behandles videre på en måte som er uforenlig med disse formål.
- **Dataminimering**: Personopplysninger skal være relevante og begrenset til det som er nødvendig for det formål som gjør at de behandles.
- **Riktighet**: Personopplysninger skal være korrekte og om nødvendig ajourførte, det skal tas ethvert rimelig skritt for å sikre at uriktige personopplysninger straks rettes eller slettes.
- **Lagringsbegrensning**: Personopplysninger skal oppbevares på en slik måte at det ikke er mulig å identifisere den registrerte i et lengre tidsrom enn det som er nødvendig for formålet.
- **Integritet og fortrolighet**: Personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet, herunder beskyttelse mot uautorisert eller ulovlig behandling og mot hendelig tap, tilintetgjørelse eler beskadigelse, under anvendelse av passende tekniske eller organisatoriske foranstaltninger.
- **Ansvarlighet**: Den behandlingsansvarlige er ansvarlig for å kunne påvise at disse personvernsprinsippene overholdes.

2.2 De registrertes rettigheter

GDPR kapittel III

Behandlingsansvarlig har et ansvar om å **informere** de registrerte om sine rettigheter, om å **tilrettelegge** for at de registrerte kan utøve sine rettigheter, å gjennomføre tiltak på de registrertes anmodning om å utøve sine rettigheter og å underrette dersom de gjennomfører visse tiltak.

De registrerte har rett til:

- Den registrerte skal ha rett til å få den behandlingsansvarliges bekreftelse på om personopplysninger om dem behandles, og, dersom dette er tilfellet, **innsyn** i personopplysningene om seg selv,

- Den registrerte skal ha rett til å få uriktige personopplysninger om seg selv **korrigert** av den behandlingsansvarlige uten ugrunnet opphold,

- Den registrerte skal ha rett til å få personopplysninger om seg selv **slettet** av den behandlingsansvarlige uten ugrunnet opphold, og den behandlingsansvarlige skal ha plikt til å slette personopplysninger uten ugrunnet opphold dersom ett av seks forskjellige forholdene gjør seg gjeldende.

    - Mest aktuelt: sletteplikten utløses når personopplysningene **ikke lenger er nødvendige for formålet** som de ble samlet inn eller behandlet for. Eller alternativt, når den registrerte **trekker tilbake sitt samtykke**.

    - Nytt med sletteplikten: hvis behandlingsansvarlig tidligere har offentliggjort slike personopplysninger som kreves og skal slettes, må den behandlingsansvarlige sørge for

at andre behandlingsansvarlige sletter alle lenker til, kopier av eller reproduksjoner av nevnte personopplysninger,

- Den registrerte skal ha rett til å kreve av den behandlingsansvarlige at behandlingen **begrenses** dersom ett av flere forhold er angitt, for eksempel opplysningenes riktighet et omtvistet.
- Retten til **dataportabilitet er nytt** med GDPR. Behandlingsansvarlige må gi tilbake personopplysningene til den registrerte når den registrerte krever sine personopplysninger flyttet – den behandlingsansvarlige kan ikke behandle disse personopplysningene lenger etter de er overført.
    - Vilkår: Behandlingsgrunnlaget må være **samtykke**, behandlingen må ha vært utført **automatisk**, personopplysningene må være gitt til den behandlingsansvarlige av den registrerte selv og gjelde den registrerte selv.
    - Eksempel: Hjemmeside med elektronisk skjema som den registrerte kan sende inn sine personopplysninger via.
- Den registrerte kan fremme innsigelser - **protestere** mot behandling av personopplysninger om seg selv, i visse situasjoner.
    - Eksempel: den registrerte kan alltid protestere mot behandling av personopplysninger om seg selv til direkte markedsføring.
- Den registrerte skal ha rett til **ikke å være gjenstand for** en avgjørelse som **utelukkende** er basert på **automatisert behandling**, herunder **profilering**, som har rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker vedkommende. For eksempel at den registrerte automatisk blir frakoblet fra sin mobiltjenesteleverandør for kontraktsbrudd siden han glemte å betale fakturaen innen han dro på ferie.
- **Utelukkende** betyr at et menneske må være en reel del av beslutningsprosessen og kunne ta en selvstendig avgjørelse. Mennesket må faktisk kunne påvirke resultatet, det er ikke nok at en ansatt rutinemessig går gjennom de automatiske beslutningene og stempler OK på alt.

2.3 Sikkerhet

GDPR artikkel 32

Både databehandler og behandlingsansvarlige plikter å følge krav om informasjonssikkerhet. Begge har selvstendig plikt til gjennomføre **egnede tekniske og organisatoriske tiltak** for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen

2.3.1 Tiltak

Dette kravet til egnede tekniske og organisatoriske tiltak kan kalles **sikkerhetsprinsippet** i GDPR.

Eksempler på slike tiltak fremgår av artikkel 32:

a) pseudonymisering og kryptering av personopplysninger,
b) evne til å sikre vedvarende fortrolighet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,
c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,
d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

Det siste nevnte tiltaket innebærer at behandlingens sikkerhet må verifiseres. Sikkerheten må testes ved jevne mellomrom.

Hvilke sikkerhetstiltak en bedrift skal ha på sine systemer må baseres på virksomhetens **risikovurdering**, se punkt 8.

Eksempel: Virksomheten bør sørge for at kun de som har behov for tilgang til sensitive personopplysninger, har faktisk tilgang.

2.3.2 Brudd

GDPR artikler 33-34

Ved brudd på personopplysningssikkerheten skal behandlingsansvarlig **melde ifra** til **Datatilsynet** uten ugrunnet opphold og seneste **72 timer** etter at de fikk kjennskap til sikkerhetsbruddet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter.

Meldingen må **beskrive sikkerhetsbruddet** med blant kategorier av berørte registrerte og omtrentlig annet antall berørte registrerte, kategorier personopplysninger og omtrentlig mengde personopplysninger, kontaktpunkt for mer informasjon, sannsynlige konsekvenser av bruddet og beskrivelse av iverksatte eller planlagte tiltak for å håndtere situasjonen.

For å bidra til informasjonsflyten skal databehandleren melde ifra til behandlingsansvarlig på samme vis uten ugrunnet opphold.

Hvis det er sannsynlig at bruddet vil medføre **høy risiko** for fysiske personer rettigheter og friheter, skal de registrerte underrettes om bruddet.

2.4 Innebygd personvern

GDPR artikkel 25

Innebygd personvern består av både **privacy by design** og **privacy by default**.

Formålet med disse nye prinsippene er å forhindre at personvern kun blir en ettertanke, fremfor et styrende prinsipp i utviklingen av nye IT-systemer. Man skal tenke på personvern **lenge før** behandlingen finner sted.

Privacy by design forplikter virksomheten til å implementere grunnleggende personvernprinsipper (eksempel: minimalisme) inn i sine tekniske systemer, både når de først designes og senere i tid. Formålet med bestemmelsen er å bevisstgjøre utviklere og IT-ansvarlige til å tenke over hvilke konsekvenser tekniske designvalg har for juridiske rettigheter.

Privacy by default innebærer at den mest personvernvennlige praksisen alltid skal være standardinnstillingen i IT-systemet.

Eksempel: ved publisering av bilder på Facebook, skal standardinnstillingen være at bildet kun deles med brukerens venner. Offentlig deling, altså et mer personverninngripende alternativ, må brukeren selv aktivere.

2.5 Sanksjoner

GDPR artikkel 83

Samme vurdering: Den eksisterende skjønnsmessige vurderingen av om det skal ilegges overtredelsesgebyr er videreført i den nye personvernforordningen. I vurderingen skal det blant annet legges vekt på hvor alvorlig krenkelsen er, graden av skyld, om det kunne vært iverksatt tiltak for å forebygge overtredelsen, om det foreligger gjentakelse og overtrederens økonomiske evne.

Bøtenivået heves: Etter dagens regler kan Datatilsynet maksimalt ilegge bøter på 10 ganger grunnbeløp i folketrygden, dvs. like under 1 million kroner. Den nye personvernforordningen åpner for at bøtenivået for de mest alvorlige overtredelsene kan settes til **4 % av årlig, global omsetning** eller **20 millioner Euro**, alt ettersom hva som er høyest.

3. BEHANDLINGSGRUNNLAG

GDPR artikkel 6

Behandlingsgrunnlag: det grunnleggende vilkåret for at lovlig behandling av personopplysninger kan finne sted.

Behandlingsansvarlig må alltid ha et behandlingsgrunnlag **før** behandlingen kan påbegynnes. Når en behandling er påbegynt kan ikke behandlingsansvarlig bytte behandlingsgrunnlag. Behandlingsansvarlig må **selv vurdere konkret** hvilket behandlingsgrunnlag som **passer best** for de ulike behandlingssituasjonene av personopplysninger som virksomheten er ansvarlig for.

3.1 Samtykke

I noen tilfeller er samtykke fra den registrerte eneste mulige behandlingsgrunnlag. Se punkt. 4 om hvordan innhente gyldig samtykke.

Eksempel: et selskapet som skal verve nye medlemmer til sin kundeklubb eller medlemsklubb, trenger samtykke fra hvert medlem for å kunne behandle medlemmets personopplysninger.

Hvis personopplysninger blir innsamlet og behandlet for et formål, og behandlingsansvarlig i etterkant finner ut at de vil behandle personopplysningene for et **nytt formål**, så må det innhentes samtykke for å få lov til å bruke personopplysningene til det nye formålet.

Eksempel: den registrertes navn og kontaktopplysninger behandles av behandlingsansvarlig i forbindelse med den registrertes kjøp av billetter til en konsert over internett. Behandlingsansvarlig finner ut at de også ønsker å sende reklame til den registrerte så den kanskje kjøper andre billetter senere. Da må behandlingsansvarlig be om samtykke for å bruke kontaktopplysningene som allerede er lagre om den registrerte for en ny behandling med nytt formål.

Eksempel: dersom behandlingsansvarlig har en kundeliste som en samarbeidspartner ønsker å få innsyn i eller tilgang til, så må behandlingsansvarlig først be om samtykke fra de registrerte om å utlevere slik informasjon, med mindre de har et annet behandlingsgrunnlag.

Eksempel: dersom det tas bilder av frivillige eller deltagere på et arrangement som behandlingsansvarlig ønsker å laste opp på internett, kreves det samtykke fra de registrerte. Et unntak vil være bilder av større forsamlinger på offentlig sted der personene må regne med å kunne bli fotografert og der de spesifikke personene ikke er hovedfokuset, for eksempel et 17.mai tog.

3.2 Avtale

Behandlingen er lovlig hvis den er **nødvendig** for å oppfylle en avtale med den registrerte eller for å gjennomføre tiltak den registrerte ber om **før** avtaleinngåelse. Dette kan være et svært nyttig behandlingsgrunnlag å bruke, men det er kun den behandlingen og de personopplysningene som er nødvendig for å oppfylle avtalen som man da har gyldig behandlingsgrunnlag for å behandle.

Eksempel: den registrertes personopplysninger behandles i forbindelse med bestilling, betaling og levering av en vare.

3.3 Rettslig forpliktelse

Behandlingen er lovlig hvis den er nødvendig for å oppfylle en rettslig forpliktelse.

Eksempel: Selskap er lovpålagt å føre regnskap. De personopplysningene som er nødvendig for lovpålagt bokføring og regnskap vil behandlingsansvarlig kunne behandle lovlig, og slike opplysninger må lagres så lenge slik særlovgivning krever.

3.4 Vitale interesser

Behandlingen er lovlig hvis den er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser. Dette vil være en konkret vurdering.

Eksempel: ambulansen må vite hvor den skal kjøre og hvem den skal hente for å kunne verne den skadede/sykes vitale interesser.

3.5 Offentlig myndighet

Dersom behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som behandlingsansvarlig er pålagt, har man også lovlig behandlingsgrunnlag.

3.6 Berettiget interesse

Det siste lovlige behandlingsgrunnlaget er at behandlingen er nødvendig for å vareta behandlingsansvarliges berettiget interesse som veier tyngre enn hensynet til den enkeltes personvern. Dette krever en konkret vurdering som behandlingsansvarlig må kunne dokumentere at er foretatt. Her skal den registrertes personvernhensyn veies opp mot behandlingsansvarliges berettiget interesse.

Behandlingsansvarlig kan vurdere å implementere personvernsrisikoreduserende tiltak, og utfører til slutt en balansetest mellom interessene.

Eksempel: GDPR nevner at det kan tenkes at behandlingsansvarlig har en berettiget interesse av å sende ut markedsføring til eksisterende kunder.

I tillegg må behandlingsansvarlig, hvis konklusjonen er at den har en berettiget interesse, opplyse den registrerte om at vurderingen er foretatt. Den registrerte kan da reservere seg mot å bli behandlet for det formålet den behandlingsansvarlige mener den har berettiget interesse om å behandle personopplysningene for.

3.7 Behandlingsgrunnlag for behandling av sensitive personopplysninger

GDPR artikkel 9

Kravene til behandlingsgrunnlag for behandling av sensitive personopplysninger er strengere enn kravene for alminnelige personopplysninger. Utgangspunktet er at slik behandling er ulovlig, men vi har visse unntak.

Ett unntak er **eksplisitt samtykke**, med mindre nasjonal lov tilsier at den registrerte ikke kan samtykke til slik behandling.

Eksempel: Dersom behandlingsansvarlig ønsker å behandler både alminnelige og sensitive personopplysninger for ett formål, så ber den om ett samtykke for behandlingen av de alminnelige personopplysningene og ett samtykke for behandlingen av de sensitive personopplysningene.

Ett annet unntak er sensitive personopplysninger som er **nødvendig** å behandle for å gjennomføre **arbeidsrettslige plikter eller rettigheter**, se ny personopplysningslov § 6.

4. HVORDAN INNHENTE GYLDIG SAMTYKKE?

GDPR artikkel 4(11) & artikkel 7

Samtykke: En frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte.

4.1 Frivillig

Den registrerte må gi samtykket frivillig.

Eksempel: Samtykke vil sjelden kunne brukes som behandlingsgrunnlag i ansettelsesforhold, fordi den ansatte ofte vil føle at han/hun må si ja, ellers kan det få negative konsekvenser for jobben. Det vil si at dersom man vil benytte seg av samtykke, til for eksempel å laste opp et bilde av den ansatte på hjemmesiden, så må man si klart ifra til den ansatte at de ikke risikere noen negative konsekvenser i jobbsammenheng dersom de skulle velge å ikke samtykke til det.

Dersom det inngås en avtale med den registrere, må ikke avtalen være betinget av at den registrerte «samtykker» til behandling av personopplysninger som ikke er nødvendig for den avtalen.

Eksempel: Dersom den registrerte kjøper en vare i en butikk, kan ikke butikken kreve at den registrerte samtykker til at deres kontaktinformasjon sendes til produsenten av varen de ønsker å kjøpe, for at de skal få lov til å kjøpe varen.

4.2 Spesifikk

Behandlingsansvarlig må be om ett samtykke til hvert formål med behandlingen. Det vil si at samtykketeksten må deles opp mer enn det som har vært praksis for mange hittil.

Eksempel: Behandlingsansvarlig ønsker å benytte seg av epostadressen til den registrerte både som kontaktpunkt for et kundemedlemskap, og for å sende målrettet reklame til den registrerte. Da trenger behandlingsansvarlig to samtykker, ett for kontaktpunktet og ett for reklamen. De må skilles fra hverandre.

4.3 Informert

Personen må vite hva de samtykker til og få all nødvendig informasjon om behandlingen. Dette kan blant annet oppfylles gjennom en lett tilgjengelig og tydelig **personvernerklæring**, se punkt 5. For at den

registrerte faktisk skal være informert må informasjonen presentere på en måte som er forståelig for den registrerte. Språket må være enkelt, tydelig og klart.

Det kreves også at informasjonen om hva den registrerte samtykker til, tydelig skilles fra tekst som gjelder annet forhold. Det er ikke lov å «gjemme» et samtykke midt i en lengere tekst.

Det må blant annet tydelig fremgå at den registrerte kan trekke tilbake samtykket når som helst og hvordan gjøre dette. Å trekke tilbake samtykket skal være minst like enkelt som det var å gi samtykke, men det kreves ikke at samme metode brukes. En lenke nederst i eposten med nyhetsbrev er som regel en god løsning.

Dersom det er innhentet samtykker før 25. mai 2018 hvor alle krav nevnt i punkt 4 er oppfylt, kan slike samtykker fortsatt brukes etter 25. mai dersom behandlingsansvarlige senest 25. mai 2018 informerer om at den er mulig for den registrerte å trekke sitt samtykke like enkelt som det var å gi samtykke.

4.4 Utvetydig viljesytring

Det skal være tydelig at den registrerte faktisk ønsker å samtykke til det den samtykker til. Dette krever en aktiv handling.

Eksempel: Hvis behandlingsansvarlig ber om samtykke med bokser som hukes av på en nettside, så skal avkryssingsboksene være tomme slik at den registrerte selv kan huke av boksen. Men, det er lov å ha et paraplysamtykke øverst («jeg samtykker til alt»), slik at dersom den registrerte huker av den ene boksen så hukes alle de andre boksene av under.

4.5 Dokumentert

I tillegg kreves det at behandlingsansvarlig kan påvise at samtykket er gitt. Det vil si at det er behandlingsansvarlig som har bevisbyrden for å dokumentere samtykket.

5. PERSONVERNERKLÆRINGEN

GDPR artikler 12-14

Personvernerklæringen er ment å gi informasjon til den registrerte om hvordan den behandlingsansvarlige behandler personopplysningene til den registrerte. Denne informasjonen skal fremstilles på en kortfattet, åpen, forståelig og lett tilgjengelig måte og være på et klart og enkelt språk.

Minimum innhold i slik Personvernerklæring som også kan kalles Privacy Policy:

5.1 Behandlingsansvarlig

Hvem som er behandlingsansvarlig: Sett inn navn og org.nr. til virksomheten som er behandlingsansvarlig og få tydelig frem at det er rollen virksomheten har.

5.2 Kontaktinfo

Sett inn et kontaktpunkt for behandlingsansvarlig der personen kan utøve sine rettigheter hvis de skulle ønske det.

Eksempel: En generisk epostadresse som privacy@virksomheten.no kan brukes om virksomheten ikke har utpekt en person til å være kontaktpunkt. Hvis virksomheten har utpekt et **personvernombud**, må kontaktinformasjonen til ham/henne settes inn.

5.3 Behandlingen

Fortell hvilke personopplysninger som behandles, til hvilket formål, med hvilket grunnlag og hvem andre som evt. får tilgang til personopplysningene.

Eksempel: Hvis virksomheten lagrer personopplysningene i en nettsky levert av en tredjepart, opplys om det og helst fortell hvilken nettsky (også hvilke land data lagres eller overføres til).

5.4 Rettigheter

Fortell hvilke rettigheter personen har. Se punkt 2.2 om de registrertes rettigheter.

5.5 Klageadgang

Fortell den registrerte at det er mulig å klage til Datatilsynet hvis han/hun mener behandlingen er i strid med personvernlovgivningen.

6. PERSONVERNOMBUD

GDPR artikler 37-39

6.1 Hvem plikter å utpeke?

Både behandlingsansvarlig og databehandler kan plikte å utpeke et personvernombud. Det er i all hovedsak tre vilkår for når man plikter å utpeke et personvernombud:

a) Behandlingen utføres av en offentlig myndighet eller et offentlig organ,
b) Behandlingsaktiviteten krever regelmessig og systematisk monitorering i stor skala av registrerte, eller
c) Kjernevirksomheten består av behandling i stor skala av sensitive personopplysninger eller opplysninger om straffbare forhold.

6.2 Rett til å utpeke

Uansett har behandlingsansvarlig eller databehandler alltid en rett til å utpeke et personvernombud. Det kan være en praktisk måte å håndtere den pålagte egenkontrollen på og en nyttig kilde for bistand om personvernspørsmål. Personvernombudet kan utpekes internt, eller det kan engasjeres ekstern kompetanse.

6.3 Hvilke plikter har ombudet?

Personvernombudet skal blant annet bidra med informasjon, oppfølging av interne retningslinjer, dokumentering av internkontrollen og oppfylle eventuelle rapporteringsplikter. Ombudet vil fungere som bindeleddet til Datatilsynet.

7. INTERNKONTROLL

GDPR artikkel 24

Internkontrollsystemet har tre typer dokument – styrende, gjennomførende og kontrollerende. Den **styrende delen** med **Protokoll over behandlingsaktiviteter** er viktigst – sammen med **risikovurderingene**.

7.1 De tre delene

Den styrende delen gir en oversikt over virksomheten og hva slags behandling av personopplysninger de foretar, hvilke sikkerhetsmål og strategier de har satt seg og hvordan de er organisert innad (Eksempel: Roller må angis, bl.a. utpekt Sikkerhetsansvarlig og om virksomheten har utpekt et personvernombud).

De gjennomførende og kontrollerende dokumentene består stort sett av rutiner, instrukser, mal databehandleravtale og beskrivelse av virksomhetens fysiske og elektroniske løsning (informasjonssikkerheten må beskrives). Gjennomførende dokumenter skal brukes i det daglige, mens kontrollerende dokumenter (mest skjemaer som skal fylles ut ved brudd på personopplysningssikkerheten) skal brukes ved avvik eller etterkontroll.

I tillegg må slik dokumentasjon implementeres i virksomheten og jevnlig oppdateres (årlig eller når det skjer en viktig endring).

7.2 Protokoll over behandlingsaktiviteter

GDPR artikkel 30

Protokollen er en oversikt over alle behandlingsaktivitetene som behandlingsansvarlig foretar. Dette kan for eksempel fremstilles i et Excel dokument, og skal oppdateres hver gang det skjer noe nytt, f.eks. ny behandlingsaktivitet eller ny databehandler.

Den skal inneholde dette for hver type behandlingsaktivitet:

- Navn og kontaktinfo til behandlingsansvarlig
- Behandlingens formål (eksempel: å sende målrettet reklame på epost)
- Kategoriene av registrerte (eksempel: ansatte og private kunder)
- Kategoriene av personopplysninger (eksempel: navn, fødselsdato, epost osv.)
- Kategorier av mottakere som personopplysningene blir utlevert til (eksempel: skytjenesteleverandør, IT drift leverandør, regnskapsfører)
- Om personopplysningene blir overfør til et land utenfor EU/EØS
- Planlagt tidsfrist for sletting av personopplysningene
- Tekniske og organisatoriske sikkerhetstiltak

I utgangspunktet skal alle behandlingsansvarlige og databehandlere føre protokoll over behandlingsaktivitetene sine. Hvis de har **færre enn 250 ansatte** trenger de kun føre protokoll hvis behandlingen de utfører:

- Sannsynligvis vil medføre en **risiko** for de registrertes rettigheter og friheter,
- Ikke skjer leilighetsvis, eller
- Omfatter sensitive personopplysninger eller opplysninger om straffbare forhold.

8. RISIKOVURDERINGER

Det er to risikovurderinger alle behandlingsansvarlige må dokumentere å ha foretatt:

8.1 Vurdere informasjonssikkerheten

GDPR artikkel 32

Ulike systemer har **ulikt skadepotensial**, og **konsekvensene** for personopplysningssikkerheten vil også være ulik for ulike systemer.

Vurderingen: Behandlingsansvarlig må holde potensialet for skade opp mot konsekvensene for personopplysningssikkerheten for å foreta en overordnet vurdering av hvilket beskyttelsesbehov som er nødvendig.

Hvilke sikkerhetstiltak en bedrift skal ha på sine systemer må baseres på virksomhetens risikovurdering. Sikkerhetstiltakene vil typisk variere for en virksomhets ulike systemer.

Eksempel: For den delen som gjelder ansattes lønn og personalmapper, er det typisk sterkere behov for sikkerhetstiltak enn for bedriftens system som ikke inneholder sensitive personopplysninger. Det betyr at virksomheten må sørge for strengere sikkerhetstiltak for å beskytte de ansattes personopplysninger og andre deler av bedriftens systemer som behandler sensitive personopplysninger enn de deler som bare behandler alminnelige personopplysninger.

Systemer hvor **katastrofale** hendelser kan inntreffe vil ha behov for en bedre beskyttelse enn systemer hvor slike hendelser ikke kan inntreffe.

Behandlingsansvarlig må også vurdere informasjonssikkerheten til sine databehandlere før de tar dem i bruk. Virksomheten bør ha en sjekkliste for databehandlere som fylles ut per leverandør for å dokumentere at behandlingsansvarlig har sjekket at informasjonssikkerheten og avtalevilkårene fra slik databehandler er gode nok.

8.2 Vurdere personvernkonsekvenser

GDPR artikkel 35

Virksomheten bør ha en sjekkliste som fylles ut hver gang personvernkonsekvenser vurderes, og slik vurdering må gjennomføres årlig og oftere om virksomheten innfører ny innovativ teknologi el.l. Som minimum må forhåndsvurdering være dokumentert utført.

8.2.1 Forhåndsvurdering

Den første vurderingen kalles en **forhåndsvurdering** fordi det er en vurdering som skal konkludere om den behandlingsansvarlige plikter å foreta en **konsekvensanalyse** (på engelsk heter dette en Data Protection

Impact Assessment som forkortes **DPIA**). Denne vurderingen skal foretas *før* behandlingsaktivitetene igangsettes. Én vurdering kan omfatte flere lignende behandlingsaktiviteter.

Hvis det er **trolig** at en type behandling, idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en **høy risiko** for fysiske personers **rettigheter og friheter**, plikter den behandlingsansvarlige å foreta en konsekvensanalyse. På engelsk kalles slik **DPIA**.

GDPR oppramser tre behandlingsaktiviteter som krever at behandlingsansvarlig utfører en DPIA.

1. En **systematisk og omfattende vurdering** av **personlige aspekter** ved fysiske personer som er basert på **automatisert behandling**, herunder **profilering**, og som danner grunnlag for avgjørelser som har **rettsvirkning** for den fysiske personen eller på lignende måte i betydelig grad påvirker den fysiske personen.
2. Behandling i **stor skala** av **sensitive personopplysninger**.
3. En **systematisk overvåking** i **stor skala** av et **offentlig tilgjengelig område**.

For det andre kan den behandlingsansvarlige plikte å gjennomføre en DPIA fordi behandlingen omfattes av en **liste utarbeidet og publisert av Datatilsynet** over hvilke typer behandlingsaktiviteter som omfattes av kravet om å foreta en konsekvensanalyse. Vi venter fortsatt på listen per april 2018.

For det tredje kan det være flere momenter som tilsier at den behandlingsansvarlige også i andre tilfeller plikter å foreta en konsekvensanalyse. Eksempler på momenter: De registrerte er særlig sårbare (yngre enn 18 år, ansatte mv.), behandlingen gjelder sensitive personopplysninger, det foretas profilering, data fra flere kilder sammenstilles.

Dersom den behandlingsansvarlige konkluderer med at det ikke foreligger høy risiko slik at DPIA anses unødvendig, må dette begrunnes og dokumenteres. Behandlingsansvarlig skal ta med kommentarer fra bedriftens personvernombud dersom slik person er utpekt

8.2.2 DPIA – selve personvernkonsekvensanalysen

En DPIA skal gjennomføres **før** behandlingen av personopplysninger starter dersom konklusjonen er «høy risiko» i en forhåndsvurdering. Dersom behandlingsansvarlig benytter seg av databehandlere, skal disse hjelpe behandlingsansvarlig med DPIA'en. Noen ganger skal også den behandlingsansvarlige innhente de registrertes synspunkter og innspill.

DPIA skal som et minimum inneholde dette om behandlingen av personopplysningene:

1. En systematisk beskrivelse av behandlingen, dens formål og eventuelt hvilken berettiget interesse den ivaretar.
2. En vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene behandlingen er nødvendig og forholdsmessig, sett opp mot formålet.
3. En vurdering av risikoen behandlingen har for personers rettigheter, herunder retten til personvern.
4. Hvilke tiltak som skal settes i verk mot risikoen som er identifisert.

Tiltakene nevnt til slutt er viktige. Vurderingen skal omfatte de planlagte tiltakene den behandlingsansvarlige kan sette i gang for å håndtere risikoene. Tiltak kan være garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysninger og for å påvise at GDPR overholdes, og den behandlingsansvarlige skal ta hensyn til de registrertes og andre berørte personers rettigheter og berettigede interesser.

Det skal også tas hensyn til behandlingsansvarliges eller databehandleres overholdelse av godkjente atferdsnormer.

DPIA er en **risikostyring** som skal håndtere risikoen for de registrerte. Den behandlingsansvarlige kan velge ulik metoder for å gjennomføre en slik analyse.

8.2.3 Forhåndsdrøftelse

GDPR artikkel 36

Dersom gjennomført konsekvensanalyse/DPIA viser **fortsatt høy risiko** for behandlingen den behandlingsansvarlige planlegger å starte, skal den behandlingsansvarlige ha **forhåndsdrøftelse** med

Datatilsynet. Dette skal fortsatt finne sted før behandling av personopplysninger eventuelt starter. Datatilsynet kan konkludere med at behandlingen kan fortsette som planlagt, eller ikke kan gjennomføres. Eventuelt kan de pålegge behandlingsansvarlig å gjennomføre tiltak først.

8.3 Til hjelp: Bransjenormer, atferdsnormer og sertifiseringsmekanismer

Dersom det kommer bransjenormer, atferdsnormer eller sertifiseringsmekanismer innenfor behandlingsansvarliges bransje som vil gjøre arbeidet med slike risikovurderinger enklere å overholde, skal behandlingsansvarlig bruke slike normer eller mekanismer. Datatilsynet har en veileder for hvordan få utarbeidet slik bransjenorm etter GDPR.

Eksempel: FEDMA har utarbeidet en bransjenorm for direkte markedsføring.
Eksempel: Norm for inkassobransjens bruk av personopplysninger utarbeidet av Norske Inkassobyråers Forening.

9. DATABEHANDLERAVTALE

GDPR artikkel 28

Når en tredjepart (leverandør) skal behandle personopplysninger på vegne av bedriften (kunden) – når en behandlingsansvarlig (kunden) tar i bruk en databehandler (leverandøren) – er det påbudt med databehandleravtale mellom kunden og leverandøren.

Databehandleravtalen utgjør behandlingsgrunnlaget for databehandlere. Behandlingen kan ikke gå ut over det databehandleravtalen angir.

GDPR ramser opp minstekrav til innhold i en databehandleravtale, se artikkel 28 (3). Avtalen skal blant annet inneholde formålet med behandlingen, hvilke personopplysninger som behandles, at alle som er autorisert til å behandle personopplysninger for databehandler er forpliktet av en taushetserklæring osv.

Dersom leverandøren lagrer eller behandler personopplysningene utenfor EU/EØS, gjelder det tilleggskrav. EU har lagd EU Model Contract som kan brukes som mal for avtale med slike leverandører, og husk også å ta med det som står i GDPR artikkel 28 (3) siden slik standardkontrakt ble lagd før EU startet arbeidet med GDPR. Dersom leverandør kun behandler personopplysninger i USA, trengs ikke slik EU Model Contract om leverandøren står på listen som sertifisert etter Privacy Shield. Avtalen mellom EU og USA.