Del 2 Fagdag GDPR - Arkiv Troms

Fokus på ny personopplysningslov og personvern

Ole Mikalsen, GDPR-konsulent, IT Partner Tromsø AS

INNHOLD, ANDRE SESJON

- Lovlig grunnlag
- De registrertes rettigheter
- Varslingsplikter
- Roller innen GDPR
- Personvernombud
- Databehandleravtale

NB: Innholdet i denne presentajonen er nedjustert og forenklet fra vår vanlige presentasjon i forbindelse med opplæring innen GDPR. Noen unøyaktigheter vil derfor forekomme.

Innsamling av persondata - Lovlig grunnlag

Behandlingsgrunnlag

Lovlig grunnlag (basis)

All registrering og bruk av persondata skal ha lovlig grunnlag

- Det må finnes et lovlig grunnlag for behandlingen (artikkel 6.1)
- Hver behandling må ha et selvstendig formål (artikkel 5.1)
- Grunnlag for behandling av persondata må identifiseres og dokumenteres
- Behandlingsprosesser må avstemmes i forhold til grunnlaget
- Lovlig basis innebærer også begrensning av databehandling
- Behandling skal bare skje i henhold hva som er definert i grunnlaget.

- De ulike rettslige grunnlagene kan falle bort på ulike måter:
  - Lovhjemmel kan falle bort fordi loven endres eller oppheves
  - Samtykke kan når som helst trekkes tilbake
  - Nødvendig grunn kan opphøre fordi situasjonen forandrer seg
- Dersom det rettslige grunnlaget faller bort, og det ikke finnes et alternativt rettslig grunnlag, mister den behandlingsansvarlige retten til å behandle opplysningene, og opplysningene skal slettes

Lovlig grunnlag for innsamling av personopplysninger

- a Samtykke
- b Avtale / Kontrakt
- c Juridisk forpliktelse
- d Vital interesse
- e Allmennhetens interesse/offentlig myndighet
- f Berettiget interesse

Lovlig grunnlag for innsamling av sensitive personopplysninger

Artikkel 9.1 Generelt forbudt, artikkel 9.2 med noen unntak:
(a) Samtykke
(b) Juridisk forpliktelse (arbeid og sosiale tjenester)
(c) Vital interesse
(d) Legitim aktivitet til ideell organisasjon
(e) Info personer aktivt selv har offentliggjort
(f) Juridisk prosess
(g) Vesentlig offentlig interesse
(h) Helse og sosialtjenester
(i) Offentlig helse
(j) Arkivering i offentlig interesse

Samtykke som grunnlag

Samtykke defineres som en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv

- Personer skal aktivt gi sitt samtykke for registrering
- Samtykke kan typisk være et skjema i forbindelse med en bestilling eller web registrering
- Samtykke skal spesifikt beskrive hvilke data som samles inn, hvordan data skal brukes og hvor lenge data vil lagres
- Samtykke skal kunne dokumenteres i ettertid og den registrerte skal kunne trekke sitt samtykke. Det skal være like lett å trekke tilbake et samtykke som å gi det

Samtykke anses som det “sterkeste” grunnlag

Den registertes rettigheter

Detaljer rundt håndtering av individets rettigheter

GDPR – oppsummering enkeltpersoner rettigheter:

- rett til innsyn (artikkel 15)
- rett til korrigering av informasjon (artikkel 16)
- rett til å bli glemt (artikkel 17)
- rett til begrenset behandling (artikkel 18)
- rett til dataportabilitet (artikkel 20)
- Rett til å motsette seg behandling (artikkel 21)
- rett til å motsette seg profilering og automatisk beslutningstaking (artikkel 22)

- rett til å bli informert
- rett til å bli varslet ved databrudd
- personer må aktivt gi sitt samtykke

Retten til innsyn
- skal fås fra den behandlingsansvarlige

1. Informasjon om
   a) Formålet med behandlingen
   b) Kategorier av personopplysninger som behandles
   c) Mottakere eller kategorier av mottakere som har/skal få tilgang til personopplysningene
   d) Hvor lenge personopplysningene lagres eller hvilke kriterier som brukes for å avgjøre lagringstiden
   e) Retten til retting, bli glemt, begrenset behandling eller å motsette seg behandling
   f) Retten til å klage hos Datatilsynet
   g) Kilden til personopplysningene dersom disse ikke er samlet inn fra den registrerte
   h) Automatiserte beslutningsprosesser, logikken bak disse samt konsekvenser for den registrerte
2. Informasjon om sikkerhetsmekanismer etter artikkel 46, der data overføres til tredjeland eller internasjonale organisasjoner
3. Kopi av personopplysningene som behandles

Artikkel 33

Varslingsplikter ved sikkerhetsbrudd

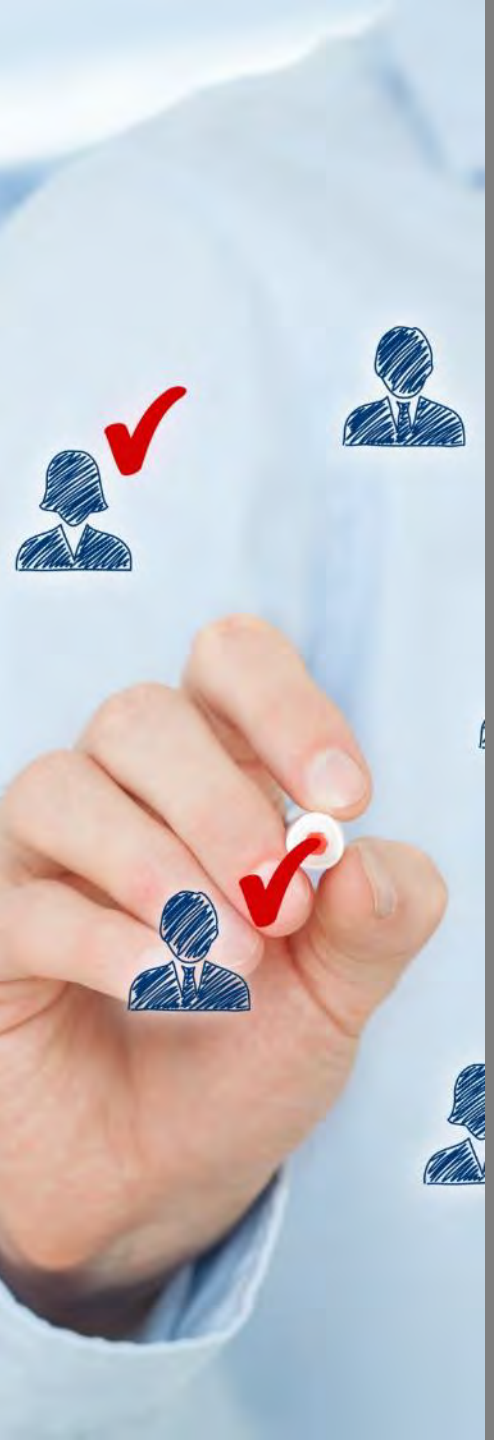
Datatilsynet og de registrerte skal oftest varsles uten unødig opphold

Varsling til Datatilsynet

Ved sikkerhetsbrudd, der persondata kan være kompromittert, skal det varsles.

- Behandlingsansvarlig skal varsle tilsynsmyndighet, dvs Datatilsynet
- Varsling skal skje uten unødvendig forsinkelse og ikke senere enn 72 timer etter at man er blitt kjent med bruddet
- Dersom ikke all informasjon er tilgjengelig på varslingstidspunktet så kan informasjon gis i faser uten unødig forsinkelse

NB: Databehandler skal varsle Behandlingsansvarlig umiddelbart ved sikkerhetsbrudd



Varsling til de registrerte

Der sikkerhetsbruddet sannsynligvis resulterer i høy risiko for rettigheter og frihet for personer, skal de registrerte varsles uten unødig forsinkelse

Unntak for varsling til de registrerte

- Det er gjennomført egnede tekniske og organisatoriske sikkerhetstiltak som gjør personopplysningene uleselige for de som ikke har autorisert tilgang til dem, f.eks. kryptering
- Det er truffet etterfølgende tiltak som sikrer at det er lite trolig at den høye risikoen for de registrertes rettigheter og friheter inntrer
- det vil innebære en uforholdsmessig stor innsats

Roller innen GDPR

Gjennomgang av de ulike roller og deres ansvar (unntatt Personvernombud)

Den registrerte

Den person som personopplysningene relaterer seg til (ansatte, brukere, kunder, kontakter osv.)

- får et styrket personvern gjennom GDPR

Bør sørge for å lese personvernerklæringer og samtykkeskjema for å sikre sin rett, være kritisk til hva man svarer JA/OK til

Roller i selskapet

- Følge policyer, rutiner og prosedyrer som selskapet har i forhold til personvern
- Være bevist sin egen og andres behandling av persondata, korrigere ved behov

Behandlingsansvarlig

Er vedkommende virksomhet eller enkeltperson som bestemmer hva personopplysningene skal brukes til (formål) og hvilke elektroniske hjelpemidler (IT-systemer, -tjenester, -utstyr eller -infrastruktur) som skal anvendes til å behandle opplysningene.

Behandlingsansvarlig er ansvarlig for at personopplysninger håndteres i tråd med reglene i forordningen og i den nye personopplysningsloven.

Dersom dette ikke er tilfelle, kan den behandlingsansvarlige bli gjenstand for ulike typer sanksjoner, for eksempel overtredelsesgebyr eller tvangsmulkt.

BEHANDLINGSANSVARLIGS PLIKTER

Generelt:

- Sørge for at loven om GDPR blir fulgt i egen organisasjon og hos databehandler
- Vurdere ved valg av nye systemer og leverandører om disse kan vise til GDPR-samsvar
- Vurdere/dokumentere om man trenger personvernombud
- Vurdere risiko ved behandling av persondata, og evt kjøre en konsekvensanalyse
- Ha på plass rutiner og prosedyrer for å sikre persondata, dokumentere disse
- Sørge for at hele organisasjonen har nødvendig kunnskap og fokus på personvern
- Føre protokoll over behandlingsaktiviteter som utføres under deres ansvar
- Dokumentere samsvar. Ha logg over hvor persondata finnes, grunnlag for behandlingen og hvordan/når de behandles og slettes.
- Dokumentere rutiner og prosesser for behandling og sletting, samt utlevering av informasjon til de registrerte.
- Dokumentere rutiner og prosesser for håndtering av databrudd.
- Informere alle som har fått tilgang på persondata, og følge opp tilsvarende som forrige punkt

- Overfor myndighet (Datatilsyn)
  - Kontaktpunkt og samarbeidspartner med Datatilsynet
  - Rapportere databrudd uten unødig opphold (frist 72 timer)

- Overfor de registrerte:
  - Kontaktpunkt overfor de registrerte
  - Informere om datainnsamling (formål og grunnlag)
  - Informere om kontaktdata for organisasjonen
  - Lage Personvernerklæring og samtykkeskjema
  - Kontaktpunkt (enkeltperson eller personvernombud) for forespørsler og korrigeringer fra de registrerte
  - Sletting av persondata som ikke lenger finnes grunnlag for via rutiner og revisjoner
  - Ha på plass sikkerhetsrutiner for å forhindre datatap
  - Rapportere databrudd uten unødig opphold

- Overfor databehandler
  - Utferdige databehandleravtale
  - Gi skriftlig beskjed om utførelse av all databehandling
  - Kontrollere/inspisere databehandlers håndteringer og rutiner

Databehandler

Er den virksomhet eller enkeltperson som behandler personopplysninger på vegne av den behandlings-ansvarlige.

Databehandleren skal bare behandle personopplysninger i henhold til avtale med den behandlingsansvarlige.

Databehandleren har et selvstendig ansvar for at person-opplysninger som tilhører den behandlingsansvarlige håndteres i tråd med reglene i forordningen og i den nye person-opplysningsloven.

Dersom dette ikke er tilfelle, kan databehandleren bli gjenstand for ulike typer sanksjoner, for eksempel overtredelsesgebyr eller tvangsmulkt.

DATABEHANDLERS PLIKTER

- Generelt:
  - Dokumentere samsvar for å være aktuell databehandler
  - Sørge for at loven om GDPR blir fulgt i egen organisasjon
  - Vurdere risiko ved behandling av persondata
  - Ha på plass rutiner og prosedyrer for å sikre persondata, dokumentere disse, (ha en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene)
  - Ha logg over hvor persondata finnes, hvordan/når de behandles og slettes. Dokumentere rutiner og prosesser for behandling og sletting. Dette skal være spesifisert i databehandleravtaler.
  - Vurdere/dokumentere om man trenger personvern-ombud (i samsvar med behandlingsansvarlig)
  - Føre protokoll over behandlingsaktiviteter som utføres på vegne av en behandlingsansvarlig
- Overfor myndighet (Datatilsyn)
  - Kontaktpunkt og samarbeidspartner med Datatilsynet
  - Indirekte - Rapportere databrudd uten unødig opphold til Behandlingsansvarlig som igjen er ansvarlig for å varsle Datatilsynet
- Overfor Behandlingsansvarlig
  - Vurdere/godkjenne databehandleravtale
  - Kun utførelse av databehandling etter skriftlig beskjed fra behandlingsansvarlig
  - Vurdere ønske om databehandling opp mot GDPR, og informere databehandler hvis regelverk ikke er fulgt
  - Rapportere databrudd uten unødig opphold
  - Behandle/sikre data etter loven (se generelt)
  - Bistå behandlingsansvarlig ….
- Overfor de registrerte:
  - Ha på plass sikkerhetsrutiner for å forhindre datatap
  - Indirekte - Rapportere databrudd uten unødig opphold til Behandlingsansvarlig som igjen er ansvarlig for å varsle den registrerte

serit
IT Partner Tromsø

DATATILSYNET

Nasjonalt uavhengig tilsynsorgan for GDPR

I forordningen heter det Independent Supervisory authority

Artikkel 51-59 og føring 117-129 omhandler tilsynsorganet

Datatilsynet – Tilsyn og ombud
Opprettet 1. januar 1980

Oppgaven er å føre kontroll med personvernregelverket og medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem.

Datatilsynet er et uavhengig forvaltningsorgan administrativ underordnet Kongen og Kommunal- og moderniserings-departementet (KMD). Det at vi er uavhengige betyr at de ikke kan instruere eller omgjøre våre vedtak eller avgjørelser.

- kontrollere at lover og forskrifter for behandling av person-opplysninger blir fulgt, og at feil og mangler blir rettet. Dette gjøres blant annet gjennom tilsyn og saksbehandling
- holde oss orientert om nasjonal og internasjonal utvikling når det gjelder behandling av personopplysninger
- identifisere farer for personvernet, og gi råd for hvordan farene kan unngås eller begrenses

Datatilsynet – Tilsyn og ombud
Opprettet 1. januar 1980

- være høringsinstans i saker som berører personvern
- delta i råd og utvalg
- bistå bransjeorganisasjoner med å gi råd og utarbeide atferdsnormer for å sikre personopplysninger i virksomhetene
- stimulere til opprettelse av personvernombud og bygge kompetanse hos ombudene
- ha en ombudsrolle overfor publikum, og gi råd og informasjon. Dette gjøres blant annet ved hjelp av våre nettsider, blogg og veiledere
- få viktige saker på dagsorden i media og bidra til samfunnsdebatt om personvern
- føre en offentlig fortegnelse over alle behandlinger av personopplysninger som er meldt inn til oss, og behandle søknader om konsesjon
- følge med på etterlevelsen av en rekke lover og forskrifter

Artikkel 37

Personvernombud

Personvernombudet er en ressurs innen personvern og et kontaktpunkt i organisasjonen

Vurdering om man skal ha personvernombud skal dokumenteres

Virksomheter skal vurdere om de trenger personvernombud

- Med mindre det er helt opplagt at en virksomhet ikke er pålagt å ha ombud anbefaler Datatilsynet at virksomheten dokumenterer de vurderingene som har blitt gjort dersom personvern-ombud *ikke* blir opprettet.

Hvem må ha personvernombud?

Behandlingsansvarlige og/eller databehandlere skal utpeke et personvernombud dersom:

- behandlingen utføres av en offentlig myndighet eller et offentlig organ, bortsett fra domstoler
- selskapets hovedvirksomhet består av regelmessig og systematisk monitorering i stor skala av registrerte
- selskapets hovedvirksomhet består av behandling i stor skala av særlige kategorier av opplysninger (sensitive data) eller opplysninger knyttet til straffedommer og straffbare forhold

Hvem kan ha personvernombud?

Datatilsynet sier:

«Styrkingen av personvernombudets rolle er godt nytt for personvernet.

Erfaringsmessig har Datatilsynet sett at det å ha en person med kunnskap om og fokus på personvern i en virksomhet kan gjøre en stor forskjell.

Vi oppfordrer derfor alle virksomheter til å opprette *personvernombud*, uavhengig om de er pålagt å ha det eller ikke»

Hva slags kvalifikasjoner må personvernombudet ha?

Regelverket stiller ingen spesifikke krav når det kommer til utdanningsbakgrunn eller sertifiseringer, men det stilles tydelige krav til kompetanse og egnethet for de oppgaver ombudet skal gjøre for virksomheten.

Ombudet skal utpekes på grunnlag av:

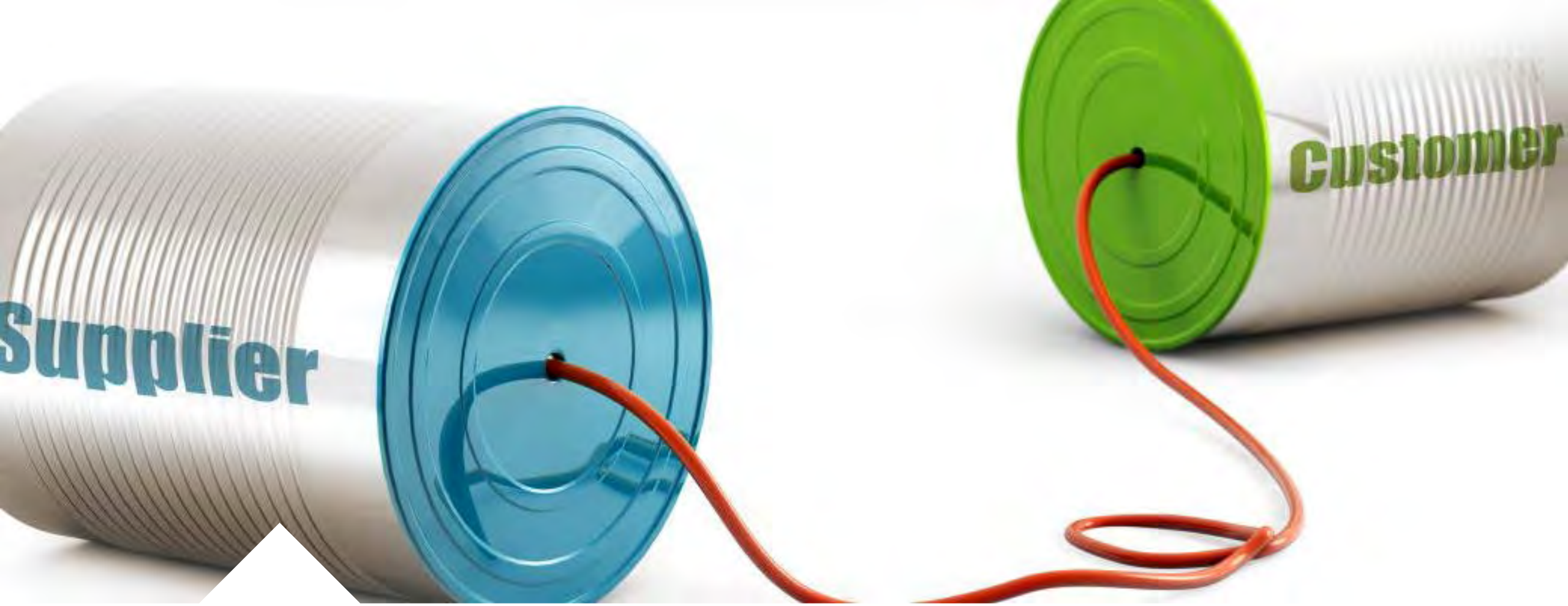
- Ombudets faglige kvalifikasjoner bør stå i forhold til hvor omfattende behandling av personopplysninger virksomheten har
- Dybdekunnskap om personvernlovgivning og praksis på området
- Ombudet bør også ha en god forståelse av behandlingsaktivitetene, IT-systemene, informasjonssikkerhet og personvernbehovene i virksomheten
- Evne til å utføre oppgavene sine. Dette referer både til personlige kvaliteter og kunnskap, men også til ombudets posisjon i virksomheten

Hvordan sikre ombudets uavhengighet?

- Virksomheten skal sikre at personvernombudet ikke mottar instrukser om utførelsen av oppgavene sine.
- Som hovedregel kan en person ikke være personvernombud og samtidig ha en rolle der hun skal bestemme formålet og måten personopplysninger skal behandles på.
- I mange tilfeller vil det føre til interessekonflikter å være personvernombud samtidig som man har en høy lederstilling (administrerende direktør, HR-sjef, IT-sjef osv.), eller hvis rollen i situasjonen innebærer å bestemme formålet eller måten behandlingen skal skje på.

Hva er ombudets plikter?

- Informere og gi råd om forpliktelsene virksomheten har
- Kontrollere overholdelsen av forordningen og andre regelverk
- Gi råd om vurdering av personvernkonsekvenser
- Være kontaktpunkt mot Datatilsynet og de registrerte
- Bidra til å få oversikt over behandlingene i selskapet
- Bidra til etterlevelse av forordningen og virksomhetens personvernpolitikk



Databehandleravtale

Databehandleravtalen beskriver forholdet mellom Behandlingsansvarlige og de Databehandlere som behandler data på vegne av dem

Databehandleravtale

Det er behandlingsansvarlig som er ansvarlig for å ha databehandleravtale med alle sine databehandlere

Behandlingsansvarlig bare kan bruke databehandler som kan dokumentere at tilstrekkelige tekniske og organisatoriske tiltak er/vil bli gjennomført på en slik måte at kravene i forordningen vil bli imøtekommet og kan sikre de registrertes beskyttelse og rettigheter.

Overføring av data kan kreve databehandleravtale

1) Mellom to bedrifter i samme land
   - Krever databehandleravtale
2) Mellom to bedrifter innen EU/EØS
   - Krever databehandleravtale
3) Mellom avdelinger i samme bedrift i samme land
   - Krever ikke databehandleravtale
4) Mellom avdelinger i samme bedrift i forskjellige EU/EØS land
   - Krever ikke databehandleravtale
5) Mellom avdelinger i samme bedrift innen EU/EØS og 3.land eller internasjonal organisasjon
   - Krever ikke databehandleravtale, men kever utredning i hht. Artikkel 44-50
6) Mellom bedrifter innen EU/EØS og bedrift i 3.land eller internasjonal organisasjon
   - Krever databehandleravtale i hht artikkel 44-50

Konsekvens av manglende databehandleravtale

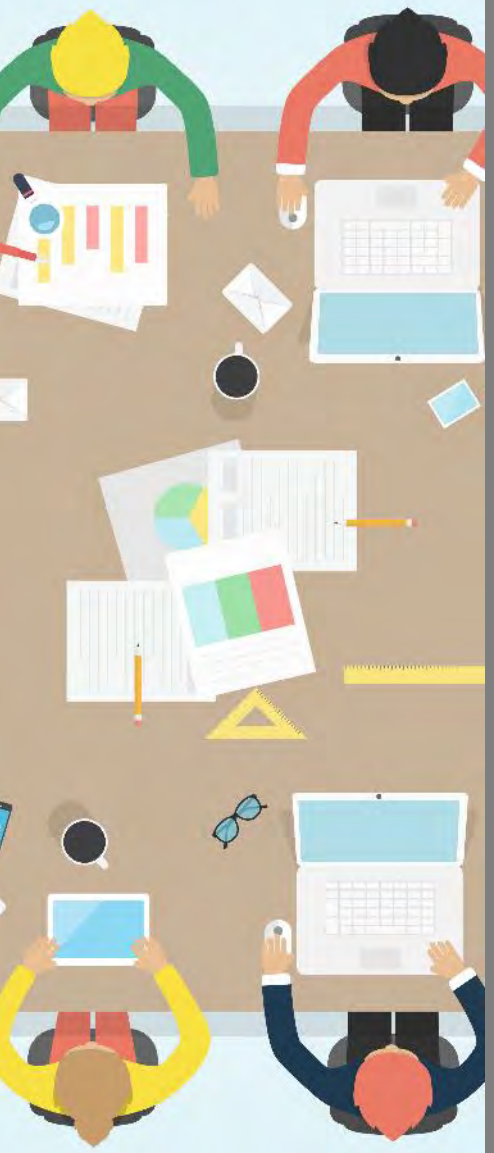
- Foreligger det ikke databehandleravtale vil utlevering av person-opplysninger fra den behandlingsansvarlige til databehandleren kunne være ulovlig.
- Hvis det ikke foreligger databehandleravtale vil det i seg selv være et brudd på loven
- Konsekvensene av at det ikke foreligger databehandleravtale, eller at avtalen ikke oppfyller lovens krav, er at databehandleren kan bli ansett å være behandlingsansvarlig og må ha grunnlag for behandling av personopplysninger

Innhold databehandleravtale

Etter GDPR blir det nå flere og klarere krav til innholdet i databehandleravtalen.

Blant annet skal databehandleravtalen inneholde angivelse eller beskrivelse av:

- Omfang og varigheten av behandlingen
- Behandlingens formål/hensikt og art
- Type personopplysninger og kategorier av registrerte som skal behandles
- Den behandlingsansvarliges rettigheter og plikter
- Bruksbegrensning – kun rett til bruk på dokumenterte instruksjoner
- Revisjon – plikt til å gi informasjon og tillate inspeksjoner
- Underleverandører



Databehandler skal (del 1):

- kun behandle personopplysningene på instruks fra den behandlingsansvarlige (som kan dokumenteres i ettertid)
- omgående underrette den behandlingsansvarlige dersom en instruks oppfattes å være i strid med GDPR eller andre bestemmelser om vern av personopplysninger

- Beskrivelse om hvilken behandling databehandler skal utføre, samt beskrivelser av overføringer, må være med i Databehandleravtalen.
- Databehandler skal «kvalitetssikre» instruksene.

serit
IT Partner Tromsø

Databehandler skal (del 2):

- Sikre at personer som er autorisert til å behandle personopplysningene har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt
- treffe alle tiltak som er nødvendig for sikkerhet ved behandlingen
- gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som tar hensyn til relevant risiko ved behandlingen

Databehandler skal (del 3):

Kun engasjere en annen databehandler ("underdatabehandler") dersom det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra den behandlingsansvarlige.

Beskrivelse om bruk av underleverandører må være med i Databehandleravtalen, og de ulike underdatabehandlere må være spesifisert i avtalen.

Databehandleren skal bistå

Databehandleren skal bistå den behandlingsansvarlige med oppfyllelse av plikter, som skal reguleres i databehandleravtalen. Dette omfatter å bistå den behandlingsansvarlige med å:

- oppfylle pliktene til å svare på anmodninger som de registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i kapittel III i GDPR hensyntatt til behandlingens art og i den grad det er mulig ved hjelp av egnede tekniske og organisatoriske tiltak
- sikre overholdelse av forpliktelser etter artikkel 32–36, som er krav til sikkerhet ved behandlingen, melding til tilsynsmyndigheten (Datatilsynet) og eventuelt de registrerte om brudd på personopplysningssikkerheten, vurdering av personvern-konsekvenser (såkalte DPIAs) og ved forhåndsdrøftinger med Datatilsynet før behandling med høy risiko.