Sjekkliste GDPR

Nye personvernregler

Hvordan jobbe med utgangspunkt i sjekklisten

- Sjekklisten gir en oversikt over hovedtemaer og spørsmål.
- Den gir ikke svaret på vurderingene, men er en huskeliste for hva som bør gjøres.
- Mange av punktene innebærer en form for gap-analyse, dvs:
  - Hva er status i dag?
  - Hva følger av det nye regelverket?
  - Hva er «gapet»?
  - Hva må gjøres for å «lukke gapet»?

10 punkts sjekkliste for forberedelse til GDPR

(se mer om hvert punkt i egne foiler)

1. Interninformasjon. Kjenner organisasjonen til det nye regelverket?
2. Kartlegging. Hvilken type personopplysninger lagres og i hvilke prosesser brukes dataene?
3. Rettslig grunnlag. Hvilket formelt grunnlag har dere for å kunne lagre personopplysninger?
4. Informasjon. Utarbeid en personvernerklæring.
5. Registrertes utvidede rettigheter. Hvordan ivaretas de?
6. Samtykke. Hvordan innhentes samtykke?
7. Avvik/sikkerhetsbrudd. Hvilke rutiner er etablert?
8. Vurdering av risiko og personvernkonsekvenser. Lagres det opplysninger som medfører behov for ytterligere konsekvensvurdering?
9. Personvernombud. Vurder om det må opprettes.
10. Informasjonssikkerhet. Ansvar og rutiner?

1. Interninformasjon

- Informer beslutningstakere og nøkkelpersoner om endringene som kommer, og hva det innebærer for virksomheten.
- Nøkkelpersoner kan være alle som har ansvar for løsninger og produkter som inneholder personopplysninger, dvs. løsninger innen marked, salg, HR, IKT, arkiv, innkjøp/leverandører mv.
- Informasjonen kan f.eks. baseres på Datatilsynets punktliste.
- Se også en nærmere beskrivelse av begrepet personopplysning.
- Tydeliggjør at dette er et lederansvar, ikke noe som alene kan overlates til IKT eller HR.

2. Kartlegging

- Hvilken type personopplysninger lagres?
- Hva er formålet med opplysningene?
- Hvilke prosesser inngår de i?
- Hvordan hentes de inn?
- Hvilke systemer lagres de i?
- Hvem har tilgang til opplysningene?
- Hvor behandles og lagres personopplysningene (lokalt, sentralt, hos en driftsleverandør).
- Hvilke databehandleravtaler er inngått?

(Kartleggingen kan gjerne gjøres i form av en tabell).

Eksempel kartleggingstabell)

Type opplysning	Formål med innhenting/lagring	Hvilke prosesser inngår de i?	Hvilke systemer lagres de i?	Hvem har tilgang til opplysningene?	Hvilke sikringstiltak og sletterutiner finnes?	Hvor behandles og lagres opp-lysningene? (fysisk/geo-grafisk)	Hvilke data-behandlere og avtaler er berørt?
Personal-opplysninger	Nødvendig for ansettelsesforholdet, lønnsutbetaling osb.	Ansettelses-prosesser, personalsaker, utbetalinger osb	Lønnssystem, personalmapper	Personalansvarlig	Innlogging med passord, sletting ved fratreden av stilling, sky-systemer, kryptering, etablerte varslings-rutiner	Lokalt og hos driftsleverandør (Norge)	Xledger, Intility, Office
Offentlige personopplysninger (kunstnerprofiler, arkiv)	Informasjon og PR, arkivering, historisk, vitenskapelig, journalistisk o.a. samfunnsmessig interesse	Arkivering, forskning, informasjons- og pressearbeid m.m.	Nettsider, fysiske og digitale arkiv osb	Informasjons- og arkivansvarlige m.fl., offentligheten	Digitale kopier, arkivskap, luftkamre, evt. mangler sletterutiner og sikringstiltak	Lokalt og hos driftsleverandør (Norge, Litauen), samt eksternt (Norge)	Nettleverandør, registerleverandør, databaseleverandører m.m.
Kundedata (publikum)	Publikumsutvikling, markedsføring, informasjons-utveksling	Salg, målrettet markedsføring, invitasjoner, informasjon om avlyste forestillinger osb.	Billettsystem, nyhetsbrev osb.	Kommunikasjonsavdeling, billettluke, salg	Innlogging med passord, rutiner for sletting, back-up	Lokalt og hos driftsleverandør (Norge)	Ticketmaster, Campaign monitor, Questback

3. Rettslig grunnlag

- Hva er det rettslige grunnlaget for å innhente de kartlagte opplysningene:
  - Egen lov?
  - Avtale?
  - Samtykke? (Husk ett samtykke pr. formål).
- Med de nye reglene følger det krav om å informere om det rettslige grunnlaget allerede når opplysningene innhentes.
- Er det eventuelt motstrid mellom forskjellige regelverk?

4. Informasjon og personvernerklæring

- Hvordan informeres de registrerte i dag?
- Når dere behandler personopplysninger, plikter dere å informere de registrerte. Kravene til denne informasjonen blir strengere når forordningen trer i kraft.
- Det er blant annet krav om:
  - At informasjonen skal være lett tilgjengelig.
  - Klart språk som er tilpasset leserens «nivå».
  - Hvilke opplysninger som skal gis. Det er nærmere beskrevet her.
- Det anbefales også å utarbeide en personvernerklæring. Datatilsynets forslag til hovedpunkter.

5. Utvidede rettigheter

- Kartlegg hvilke utvidede rettigheter som kommer (retten til å bli glemt/slettet, retten til begrensning, retten til dataportabilitet mv.).
- Nærmere om utvidede rettigheter.
- Hvordan vil dere ivareta de utvidede rettighetene i dagens systemer?

6. Samtykke

- Der samtykke er det rettslige grunnlaget for innhenting av opplysninger:
  - Hvordan innhentes samtykke i dag?
  - Er det i tråd med de nye reglene? Samtykket må være frivillig, uttrykkelig og informert mv. Husk at det også må være ett samtykke pr. formål.
  - Hva må eventuelt gjøres av endringer?
  - Nærmere om samtykke .

7. Avvik/sikkerhetsbrudd

- Hvilke rutiner finnes i dag?
- Hva kreves iht. nytt regelverk?
  - Kravene til håndtering av sikkerhetsbrudd skjerpes.
  - Hovedregelen i forordningen er at alle *avvik* som skyldes brudd på datasikkerheten skal meldes til Datatilsynet.
  - Avviksmeldingen skal leveres innen 72 timer.
  - Nærmere om nye krav til avvikshåndtering.
- Hva må oppdateres/endres ift. dagens rutiner?

8. Risiko og konsekvensvurdering

- De nye reglene stiller krav om en vurdering av personvernkonsekvenser ved blant annet:
  - Automatiserte avgjørelser.
  - Behandling av sensitive personopplysninger i stort omfang.
  - Systematisk overvåking av offentlig område i stort omfang.
- Dette vil i hovedsak gjelde ved innføring av nye systemer, men det kan også gjelde systemer som er i drift.
- Datatilsynet har egne veiledninger for konsekvensvurderinger.

- I loven brukes det nye begrepet «personvernrådgiver». Datatilsynet bruker fortsatt begrepet «personvernombud».
- Vurder om det må opprettes personvernrådgiver i virksomheten.
- Det innføres plikt til å ha personvernrådgiver for offentlige myndigheter/organ og for visse private virksomheter.
- Private virksomheter som har som hovedvirksomhet å gjøre følgende i stor skala må opprette *personvernrådgiver*:
  - Regelmessig og systematisk monitorering av personer.
  - Behandling av sensitive personopplysninger, eller opplysninger om straffbare forhold.
- Nærmere om krav til personvernombud/personvernrådgiver.

10. Informasjonssikkerhet

- Definer hvem som har ansvaret for informasjonssikkerhet.
- Kartlegg hvilke rutiner som finnes i dag?
- Hvordan ivaretar disse rutinene kravene i de nye reglene? F.eks.
  - Pseudonymisering og *kryptering* av personopplysninger.
  - *Konfidensialitet*, *integritet* og *tilgjengelighet*.
  - At virksomheter plikter å kontinuerlig vurdere hvilken teknologi som er tilgjengelig for å sikre personopplysninger på en best mulig måte.
  - Nærmere om krav til informasjonssikkerhet.

Nærmere om HR-relaterte spørsmål

- Behandlingsgrunnlag -må være lovlig, tydelig formål.
- Begrenset bruk av samtykke.
- Informasjon til ansatte.
- Gå gjennom hva som kan og bør lagres i personalmappene:
  - Hva har vi og hva trenger vi?
  - Hvorfor?
  - Hvor lenge skal det oppbevares?
  - Hvordan?
  - Hvem har tilgang?
- Kontroll og overvåkning på arbeidsplassen, egne regler.
- Innsyn i epostkasse, egne regler.

Noen kilder

- Datatilsynet https://www.datatilsynet.no/regelverk-og-skjema/veiledere/

- Datatilsyn i Sverige, Danmark og UK
  - https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
  - https://www.datatilsynet.dk/vejledninger/vejledninger-databeskyttelsesforordningen/
  - https://www.datainspektionen.se/