GDPR i EVRY – Informasjon og forespørsel rundt den nye personvernforordningen

Den nye personvernforordningen fra EU, kalt GDPR – General Data Protection Regulation, trer i kraft 25. mai 2018. Vi legger til grunn at dere er kjent med forordningen, og vil derfor kun gi et kortfattet sammendrag av det EVRY anser som de mest sentrale kravene i forordningen for både dere som kunde og EVRY som leverandør. Dernest ønsker vi så raskt som mulig å få klarhet i de konkrete neste stegene hvor begge parter må samarbeide for å imøtekomme GDPR krav på en koordinert måte. Endringer som vil måtte utføres på eksisterende kundeleveranser, vil bli prioritert i rekkefølgen endringsordrene blir mottatt på. Det forventes at et større antall endringsordre vil komme nærme mai 2018, og at det derfor kan oppstå kapasitetsproblemer med å få utført de endringsordre som blir levert mot slutten. I det tilfellet kunden har et dedikert GDPR prosjekt, ber vi dere videreformidle dette brevet til de ansvarlige for dette prosjektet.

Det er flere viktige krav for behandlingsansvarlige i GDPR, noen er uendret fra tidligere, mens andre er nye. Under er det EVRY anser som de mest sentrale kravene for våre kunder.

- **Behandlingsansvarlig (art. 24, 5)** – er primæransvarlig for behandlingen av personopplysninger og at denne skjer i henhold til lovverket.
- **Behandlingsaktiviteter (art. 30)** – må være regulert i en databehandleravtale med leverandører, og skriftlig dokumentasjon om blant annet typer behandlinger må vedlikeholdes.
- **Databehandleravtale (art. 28)** – må blant annet dekke varigheten av lagring og sikkerhetstiltak som skal implementeres.
- **Data Protection Impact Assessment (DPIA) (art. 35)** – skal utføres for risikofylte behandlinger av personopplysninger (DPIA er også kalt «Vurdering av personvernkonsekvenser» på norsk).
- **Data Protection by Design and Default (art. 25) –** passende personvern- og sikkerhetsfremmende tiltak skal reguleres via databehandleravtalen slik at løsninger som behandlingsansvarlig benytter er i overensstemmelse med prinsipper rundt innebygd personvern.
- **Registrertes rettigheter (art. 12-23)** – sikre at rettighetene til de registrerte, slik som innsyn og retten til sletting, blir ivaretatt.

EVRY anser følgende krav under GDPR som de mest sentrale i forhold til vårt leverandøransvar til våre kunder:

- **Ansvarlig for dokumentasjon om behandlinger (art. 30)** – EVRY og kunde må vedlikeholde skriftlig dokumentasjon om typer behandlinger av personopplysninger som gjøres på vegne av kundeselskapene.
- **Samarbeid og konsultasjon (art. 31)** – EVRY må samarbeide med Datatilsynet og andre myndigheter på forespørsel og etter eget initiativ der dette er nødvendig.
- **Følge instruks fra behandlingsansvarlig (art. 28)** – EVRY skal følge avtale og instrukser fra behandlingsansvarlig og må for eksempel ha autorisasjon for å benytte /erstatte underleverandør som behandler personopplysninger.
- **Sikkerhet (art. 32)** – EVRY skal påse tilstrekkelige tekniske og organisatoriske tiltak for å sikre sikkerhet i henhold til risikonivå. Dette kravet gjelder også for kunden.
- **Informasjonssikkerhetsbrudd og varslingsplikt (art. 33)** – EVRY må varsle kunden så raskt som mulig ved oppdagelse av et brudd på informasjonssikkerheten.
- **Data Protection Officer (art. 37)** – EVRY må ha en Data Protection Officer siden selskapets kjernevirksomhet består av behandling av personopplysninger på vegne av kunder.

For å oppfylle krav som gjelder begge parter, ber vi deg som kunde av EVRY om å:

- Fylle ut og signere på oppdatert mal av EVRYs databehandleravtale som er vedlagt dette skrivet og er revidert i henhold til GDPR krav (art. 28)
    - Denne avtalen vil blant annet sørge for at kravet om skriftlig dokumentasjon på behandlinger blir oppfylt for både EVRY og for kunde (art. 30).
- Dokumentere i en endringsordre hvilke eventuelle tekniske og organisatoriske sikkerhetstiltak som ønskes i tillegg til det som leveres per i dag (art. 32), samt hvilke tekniske og organisatoriske tiltak som eventuelt ønskes implementert for å innfri Privacy by Design krav i leveransene (art. 25)
    - EVRY vil på sin side gjennomgå eksisterende dokumentasjon på sikkerhetstiltak (art. 32) for å sikre at denne er tilfredsstillende og eventuelt vurdere tilleggstiltak. Kunden har et lignende dokumentasjon- og evalueringsansvar på sin side (art. 32), i tillegg til å sørge for at Privacy by Design er implementert i leveransene sine (art. 25).
- EVRY kan bistå med konsulenttjenester inn i kundens eget GDPR prosjekt med å evaluere hvilke tekniske og organisatoriske tiltak er mest hensiktsmessige i deres tilfelle for å imøtekomme GDPR krav. Tjenestene innebærer blant annet en modenhetsanalyse og workshop som bistår med avdekking og retting av svakheter i både prosesser og systemer med hensyn til GDPR krav. Dersom dette er av interesse, så ta kontakt for en uforpliktende samtale om dette.

Har dere behov for veiledning eller ytterligere informasjon, vennligst kontakt deres Key Account Manager eller responder via avsender e-postadressen. Vi ønsker deres svar med signert databehandleravtale og eventuell endringsordre innen 09.05.2018. Dette vil sørge for at databehandleravtalen og registerføring er i henhold til GDPR krav, og at det er nok tid til å prioritere de endringsordre som skal gjennomføres på vegne av våre kunder.

Vennlig hilsen,

EVRY