Personvernforordningen

Bransje-/atferdsnormer og sertifisering

Advokat Nils Henrik Heen

Finans Norge

FORMÅLET MED EN BRANSJENORM

Art. 40 nr. 1;

«Medlemsstatene, tilsynsmyndighetene, Personvernrådet og Kommisjonen skal oppmuntre til at det utarbeides atferdsnormer som skal bidra til riktig anvendelse av denne forordningen…»

HVEM KAN UTARBEIDE ATFERDSNORMER?

Art. 40 nr. 2;

«Sammenslutninger og andre organer som representerer kategorier av behandlingsansvarlige eller databehandlere…»

Høringsnotatet s. 72;

Bransjene nevnt over har sterke bransjeorganisasjoner, og etter departementets syn ligger det derfor godt til rette for at det utarbeides atferdsnormer for behandling av personopplysninger på dette feltet.

HVORDAN UTARBEIDE ATFERDSNORM

Samarbeid med Datatilsynet

Datatilsynet godkjenner og publiserer nasjonale atferdsnormer

Grensekryssende atferdsnormer forelegges og godkjennes av Eus Databeskyttelsesråd.

HVA BØR EN ATFERDSNORM REGULERE?

Art. 40 nr. 2 bokstav a) til k), for eksempel med hensyn til:

rettferdig og gjennomsiktig behandling,

de berettigede interessene som forfølges av behandlingsansvarlige i bestemte sammenhenger,

innsamling av personopplysninger,

psedonymisering av personopplysninger,

informasjon som gis allmennheten og de registrerte,

utøvelse av registrertes rettigheter,

informasjonen som gis til barn, og vern av barn, samt måten samtykke fra de personer som har foreldreansvar for barn, innhentes på,

tiltakene og fremgangsmåtene som nevnt i artikkel 24 og 25 og tiltakene for å ivareta sikkerheten ved behandlingen nevnt i artikkel 32,

melding av brudd på personopplysningssikkerheten til tilsynsmyndigheter og underretning av registrerte om nevnte brud,

overføring av personopplysninger til tredjestater eller internasjonale organisasjoner, eller

utenrettslige prosesser og andre mekanismer for tvisteløsning mellom behandlingsansvarlige og databehandlere med hensyn til behandling, uten at det berører de registrertes rettigheter i henhold til artikkel 77 og 79.

KONTROLL AV ETTERLEVELSE

Datatilsynet skal akkreditere et privat organ som har «passende ekspertise-nivå».

SERTIFISERING

Artikkel 42 og 43 i personvernforordningen.

Skal være en frivillig og gjennomsiktig prosess.

Innskrenker ikke behandlingsansvarlige eller databehandlers plikt til å overholde forordningen.

Sertifisering gis for tre år, kan forlenges og trekkes tilbake.

Utstedes mv. av Datatilsynet og nasjonalt akkrediteringsorgan

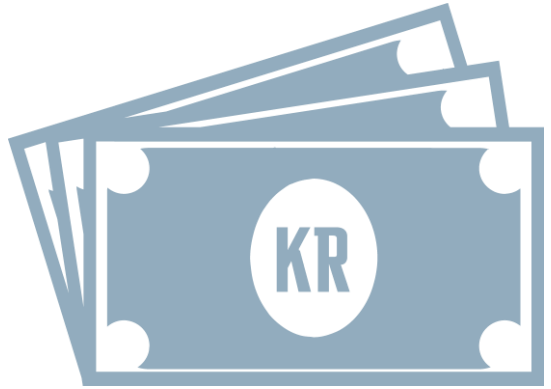
HVILKE FORDELER VIL OVERHOLDELSE GI

Kan være et element for å påvise overholdelses av forordningens krav/garantier,

Overholdelse av bransjenormer i DPIA kan være relevant (måling/evaluering av risiko),

En godkjent sertifiseringsmekanisme kan brukes som element til å påvise databeskyttelse gjennom design og standardinnstillinger, og

Kan ha innvirkning på nivået for en eventuell sanksjon.



UTFORDRINGER

Tidsperspektivet

Nivå på atferdsnormen

Internasjonalisering


Finans Norge