

DEN NORSKE KIRKE
Postboks 799 Sentrum
0106 OSLO

Deres referanse

Vår referanse
20/01772-14

Dato
23.06.2021

Påpeking av plikt - Behandling av personopplysninger i Den norske kirke

Vi viser til tidligere korrespondanse i saken, senest ved redegjørelse fra Kirkerådet (heretter DNK) datert 11. mai 2021.

Vi viser videre til vårt varsel om vedtak om irettesettelse til DNK av samme dato som dette brevet for brudd på personvernforordningen artikkel 6 nr. 1 og artikkel 14 nr. 1 bokstav d og nr. 2 bokstav f, jf. artikkel 12 nr. 1.

Vi viser for øvrig til gjengivelsen av sakens bakgrunn i punkt 3 i varselet, og at Human-Etisk Forbund (HEF) har klaget inn eller påpekt øvrige deler av DNKs behandling av personopplysninger enn det som er behandlet i Datatilsynets varsel om irettesettelse.

Vi har ikke konkludert eller gjort ytterligere undersøkelser for disse delene av saken, men basert på saken vi behov for å påpeke hvilke krav personopplysningsloven og personvernforordningen (GDPR) stiller til dere som behandlingsansvarlig.

Ansvarlighet og internkontroll

Det følger av artikkel 5 nr. 2 at den behandlingsansvarlige ansvarlig for å påse og dokumentere at deres behandling av personopplysninger skjer i tråd med prinsippene i artikkel 5 nr. 1. Den behandlingsansvarlige har plikt til å gjennomføre egnede tekniske og organiske tiltak for å sikre og påvise at behandling av personopplysninger skjer samsvar med personvernforordningen, jf. artikkel 24.

Dere kan lese mer om ansvarlighet, internkontroll og informasjonssikkerhet her:

<https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonsikkerhet-internkontroll/etablere-internkontroll/>

De registrertes rettigheter

Den behandlingsansvarlige må legge til rette for at den registrerte kan utøve sine rettigheter etter personvernforordningen, jf. artikkel 12 nr. 2.

Dette innebærer at virksomheter må sette av ressurser og ha systemer for å vurdere forespørsler fra privatpersoner. For eksempel må virksomhetene ha ressurser og rutiner for å håndtere begjæringer om sletting av personopplysninger i tråd med personvernforordningen artikkel 17.

Dere kan lese mer om å legge til rette for de registrertes rettigheter her:

<https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/legge-til-rette-for-rettigheter/>

Brudd på personopplysningssikkerheten

Brudd på personopplysningssikkerheten er et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet, jf. artikkel 4 nr. 12.

Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til Datatilsynet, jf. artikkel 33 nr. 1. Meldeplikten gjelder ikke dersom bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Dere kan lese mer om hvilke brudd på personopplysningssikkerheten som må meldes til Datatilsynet her:

<https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/nar-skal-jeg-melde-avvik/>

Uavhengig av om et brudd på personopplysningssikkerheten skal meldes til Datatilsynet, må den behandlingsansvarlige dokumentere ethvert brudd på personopplysningssikkerheten, herunder de faktiske forhold rundt nevnte brudd, virkningene av det og hvilke tiltak som er truffet for å utbedre det, jf. artikkel 33 nr. 5. Denne dokumentasjonen skal gjøre det mulig for Datatilsynet å kontrollere etterlevelsen av regelverket.

Dersom det er sannsynlig at et brudd på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige uten ugrunnet opphold underrette den registrerte om bruddet i tråd med artikkel 34. Dere kan lese mer om krav til informasjon til de berørte her: <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/ma-si-fra-til-berorte/>.

Vurdering av personvernkonsekvenser

Dersom det er sannsynlig at en behandling, særlig ved bruk av ny teknologi, vil medføre høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige foreta en vurdering før behandlingen av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet i tråd med artikkel 35. I vurderingen av om behandlingen medfører høy risiko, skal det tas hensyn til behandlingens art, omfang, formål og

sammenhengen den utføres i. Dere kan lese mer om kravene til vurdering av personvernkonsekvenser her: <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/>.

Avsluttende merknader

Basert på pliktene nevnt ovenfor forventer vi at dere sørger for etterlevelse av personvernreglene. Vi har imidlertid myndighet til å undersøke flere deler av saken på et senere tidspunkt, og eventuelt beslutte tiltak dersom dere ikke overholder personvernregelverket.

Med vennlig hilsen

Ida Småge Breidablikk
seksjonssjef

Anders Sæve Obrestad
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

Kopi til: BULL & CO ADVOKATFIRMA AS