GDPR-arbeidet er ikke over

Artikkelen gir en statusoppdatering etter at GDPR nå har vært i kraft i rundt halvannet år. Vi ønsker å gjøre det klart at det er nå arbeidet starter. Overtredelsesgebyrer, internasjonal påvirkning og ikke minst oppfølgingsarbeid ligger foran oss.

Advokatfullmektig
Carl Emil Bull-Berg
Wiersholm

Advokat
Line Helen Haukalid
Wiersholm

GDPR står for General Data Protection Regulation, og er EUs nye personvernforordning. GDPR er gjennomført i personopplysningsloven og i skrivende stund er det ett år, seks måneder og ni dager siden GDPR trådte i kraft i Norge. I tiden før og etter 20. juli 2018 har det vært et enormt fokus på betydningen av det nye regelverket, både for virksomheter og enkeltindivider.

Mye av interessen og ikke minst bekymringen kan nok tilskrives tilsynsmyndighetenes adgang til å ilegge historisk høye overtredelsesgebyrer.

Interessen rundt GDPR har vært enorm. Som illustrasjon kan det nevnes at GDPR i sommermånedene 2018 var mer søkt på gjennom Google enn Kim Kardashian. I etterkant har imidlertid interessen dalt.

Halvannet år etter ser vi at virksomheter som behandler personopplysninger, har fått på plass de grunnleggende strukturene for overholdelse av regelverket. Til tross for at mye er på plass, er det viktig å understreke at arbeidet ikke er over.

Etterlevelse av GDPR er et kontinuerlig arbeid

Å sørge for at virksomheten opptrer i samsvar med GDPR er ikke et engangsprosjekt, men et kontinuerlig oppfølgingsarbeid som først slutter når personopplysninger ikke lenger behandles.

Vi opplever at mange virksomheter har hatt fokus på å få på plass den nødvendige dokumentasjonen, som for eksempel rutiner for behandling av personopplysninger, databehandleravtaler og protokoller over behandlingsaktiviteter. Det er imidlertid først når dette er på plass at det virkelige arbeidet starter.

Mange virksomheter kan nok oppleve implementeringen av GDPR som utfordrende. Grunnen til dette er at behandling av personopplysninger foretas i alle ledd i en virksomhet, i alt fra anskaffelser til revisjon. Følgelig kan ikke virksomheten ha én avdeling som sørger for overholdelse av GDPR, alle må ta del i arbeidet. Alle ansatte som behandler personopplysninger, må ha et bevisst forhold til for eksempel sletting og oppbevaring, hvilke personopplysninger som skal samles inn og konfidensialitet. Virksomheten må derfor sørge for at de ansatte får tilstrekkelig opplæring.

Velg dine samarbeidspartnere med omhu

Når en virksomhet engasjerer en leverandør og oppdraget innebærer behandling av personopplysninger, må det også inngås databehandleravtale. Databehandleravtalen etablerer rammene for hva leverandøren kan og ikke kan gjøre med personopplysningene, og skal sikre at personopplysningene behandles i tråd med personvernregelverket. Det er imidlertid ikke tilstrekkelig kun å få avtalen signert og deretter tro at arbeidet er fullført. Databehandleravtalen må følges opp i praksis. Virksomheten er for eksempel pålagt å betinge seg en innsyns- og inspeksjonsrett hos databehandleren, og virksomheten bør etablere rutiner for når og hvordan denne retten skal gjennomføres.

Rent umiddelbart kan en slik oppfølgingsjobb fremstå tids- og ressurskre-

vende. Virksomheten kan imidlertid ta visse grep for å gjøre oppfølgingen mer håndterbar. Å engasjere databehandlere som forholder seg til sertifiseringsmekanismer, vil for eksempel gjøre denne oppfølgingsjobben langt lettere. Da vil virksomheten kunne utøve sin innsyns- og inspeksjonsrett gjennom å kreve at leverandøren legger frem sertifiseringsbevis. I en potensiell transaksjon vil også slik dokumentasjon være nyttig for å vise øvrige involverte at virksomheten tar de løpende forpliktelsene på alvor.

I valg av leverandører som skal behandle personopplysninger på virksomhetens vegne, er det derfor lurt å velge en samarbeidspartner som også viser villighet og evne til å etterleve og dokumentere dette i praksis.

Økning i antall rapporterte avvik

GDPR stiller krav om rapportering til Datatilsynet ved brudd på personopplysningssikkerheten. Et slikt brudd kan for eksempel være at beskyttelsesverdige personopplysninger er sendt til feil mottaker, at datavirksomheten har blitt utsatt for hacking eller datainnbrudd, eller det er mangelfull tilgangskontroll. Datatilsynet har opplevd en betydelig økning i antall avviksmeldinger etter at GDPR trådte i kraft. Statistikken viser en økning fra 206 avviksmeldinger i hele 2016 til rundt 1401 pr. september 2019. Denne økningen innebærer ikke nødvendigvis flere databrudd hos norske virksomheter, men er snarere et tegn på at virksomhetene er mer fokusert på etterlevelse av sine personvernforpliktelser. Denne tendensen ser vi også i øvrige europeiske land.

Flere og større overtredelsesgebyrer

GDPR introduserte en økning i taket på overtredelsesgebyret som kan ilegges av tilsynsmyndighetene ved brudd på personvernregelverket. Overtredelsesgebyret kan bli så høyt som 20 millioner euro eller fire prosent av virksomhetens samlede årsomsetning. Til sammenligning var den øvre grensen for overtredelsesgebyret etter den gamle personopplysningsloven ti ganger folketrygdens grunnbeløp.

Datatilsynet har i skrivende stund ilagt tre overtredelsesgebyrer etter at GDPR trådte i kraft. Oslo kommune ble i oktober 2019 ilagt to overtredelsesgebyr på 1,2 millioner kr og 500 000 kroner. Gebyrene gjaldt henholdsvis manglende informasjonssikkerhet knyttet til en skoleapplikasjon og lagring av pasientopplysninger utenfor journalsystemet. Året før ble Bergen kommune ilagt et overtredelsesgebyr på 1,6 millioner kroner etter at brukernavn og passord til 35 000 grunnskoleelever og ansatte lå åpent tilgjengelig for andre brukere.

Det svenske og danske datatilsynet har også ilagt sine første bøter etter GDPR. Det største overtredelsesgebyret så langt er på 50 millioner euro, og er ilagt av det franske datatilsynet til Google.

At større overtredelsesgebyrer vil bli ilagt med tiden, ser vi allerede i sakene mot British Airways og Marriot International, som begge gjelder dataangrep/-innbrudd. Her har det britiske datatilsynet varslet om overtredelsesgebyr på henholdsvis 183,4 millioner britiske pund og 99 millioner britiske pund. Endelig vedtak er foreløpig ikke fattet.

Det er all grunn til å tro at europeiske datatilsyn vil ilegge stadig flere økonomiske sanksjoner i tiden som kommer.

Konkurransefortrinn for europeiske leverandører

Mange spådde nok at GDPR ville være en påkjenning for virksomheter som opererer i og mot EU. De omfattende forpliktelsene og frykten for overtredelsesgebyr førte til at enkelte virksomheter i tiden rundt ikrafttredelsen valgte å stenge nettsidene for europeiske brukere. For eksempel valgte flere større amerikanske nyhetsnettsider å stenge tilgangen for sine europeiske lesere. Andre kom med prognoser om at implementeringen av GDPR ville være en konkurransemessig ulempe for bedrifter i EU. Vårt inntrykk er imidlertid det motsatte. Vi ser nå at flere virksomheter foretrekker europeiske samarbeidspartnere som er direkte underlagt GDPR, fremfor aktører som opererer i tredjeland.

GDPR – ikke bare for europeiske virksomheter

Det er ikke bare europeiske virksomheter som må forholde seg til GDPR. Alle virksomheter som retter sine behandlingsaktiviteter mot europeiske borgere, er underlagt GDPR. Videre vil GDPR også beskytte borgere fra land utenfor EØS, ettersom GDPR gjelder for europeiske virksomheter uavhengig av nasjonaliteten til borgerne som får sine personopplysninger behandlet.

Europakommisjonen har mandat til å beslutte at en tredjestat eller en internasjonal organisasjon har et tilstrekke-

lig beskyttelsesnivå. Dette innebærer at lovverket i den aktuelle staten ivaretar den enkeltes personvern i like stor grad som i land underlagt GDPR.

Dersom en stat oppnår slik beslutning, vil personopplysninger kunne overføres på samme vilkår som ellers i EØS. Beslutningen vil dermed være meget praktisk for virksomheter etablert i tredjestaten, og vi har sett at stater er villige til å gjøre endringer i eget personvernregelverk for å oppfylle kravene til Europakommisjonen. Vi ser med andre ord at tredjestater motiveres til å oppdatere lovverket som følge av GDPR. Pr. desember 2019 har tretten land fått en slik status, mens Sør-Korea for tiden er under vurdering.

Videre ser vi at internasjonale virksomheter finner det enklere å behandle alle personopplysninger i samsvar med GDPR, uavhengig av om GDPR kommer direkte til anvendelse eller ei. Årsaken er kostnadene forbundet med å skulle etablere to ulike mekanismer for behandling av personopplysninger. Vi ser på den bakgrunn at effekten av GDPR strekker seg utover hva det geografiske virkeområdet skulle tilsi.

Også andre land har på eget initiativ arbeidet med lovgivning og håndheving på personvern. Selv USA, som mange nok anser som en av verstingene på behandling av personopplysninger, har tatt slike steg. For eksempel har California implementert sin egen personopplysningslov (California Consumer Privacy Act). Videre har vi sett en økt villighet hos amerikanske myndigheter til å forfølge brudd på føderale personvernregler.

Vi ser på den bakgrunn en utvikling mot sterkere personvernsbeskyttelse også utenfor Europa.

Mer aktivitet forventes fra EU

EU-domstolen gir stadig viktige tolkningsbidrag for hvordan GDPR skal tolkes. Det er derfor helt nødvendig for virksomheter å holde seg oppdatert på avgjørelser og utviklingstrekk.

EU er heller ikke ferdig med å gi relevant lovgivning på feltet. I skrivende stund arbeider EU aktivt med ny lovgivning som er tett knyttet opp mot personvernrettslige problemstillinger. Som eksempel nevnes arbeidet med den nye kommunikasjonsvernforordningen om elektroniske kommunikasjonstjenester, for eksempel bruk av cookies. Ytterligere aktivitet fra EU – og ikke minst EU-domstolen – må forventes.

Veien videre

I tiden fremover er det viktig at virksomhetene har et kontinuerlig fokus på etterlevelse av personvernregelverket. Til tross for at et formelt rammeverk er på plass hos den enkelte virksomhet, er tiden nå inne for å etterleve dette i praksis.

Arbeidet er ikke over, men begynner nå.