Ny personvernlovgivning

Om ganske nøyaktig ett år erstattes den norske personvernloven av EUs nye personvernforordning, General Data Protection Regulation (GDPR). Den nye forordningen vil i større eller mindre grad påvirke alle virksomheter som behandler, lagrer og samler personopplysninger.

Advokat
Daniel Henriksen,
Head of Privacy and Data Protection i Intility

Til tross for at flere av dagens regler videreføres, vil også nye prinsipper og regler gjøre seg gjeldende og GDPR representerer på mange områder en innstramming i forhold til eksisterende lovverk. Den nye forordningen trer i kraft 25. mai 2018.

Et felles rammeverk

Hovedtanken bak GDPR-regelverket er at Europa skal få et mer moderne, ensartet og harmonisert personregelverk på tvers av hele EU/EØS. Forordningen har til hensikt å styrke personvernet ved behandling av personopplysninger, og skal bidra til at det blir enklere for virksomheter å etterleve reglene. Dermed styrkes individets posisjon i et marked hvor virksomheter samler inn personopplysninger over en lav sko. Informasjonssikkerhet knyttet til personopplysninger dreier seg om at virksomheten må håndtere risikoen for at personopplysningene de samler inn sikres på en tilfredsstillende måte og ikke gjøres tilgjengelig for uvedkommende. GDPR vil dermed ha stor betydning for norske IT-kunder og tjenesteleverandører.

Digitalisering og økt omfang av persondata

Gjennom digitalisering og teknologiutvikling genereres det stadig mer persondata. Ny teknologi åpner opp for nye muligheter for innsamling, deling, lagring, sammenstilling og videreforedling av personopplysninger. Utbredelsen av Internet of Things (IoT) gjør at ustrukturerte data kan hentes gjennom ting koblet til internett for å spore brukerens atferd. Verdien og innsikten i dette resulterer i at fremoverlente virksomheter innhenter og analyserer persondata (ofte ved hjelp av Big Data Analytics-verktøy) for å skape bedre og mer tilpassede produkter og tjenester.

Innsamlingen av stadig mer persondata utvider mengden og typen personopplysninger virksomhetene etter hvert besitter. Data hentet fra beacons (nettvarder – små radiosendere), fingeravtrykk, ansiktsgjenkjenning, loggdata og IP-adresser skal i de fleste tilfellene regnes som personopplysninger. Virksomheten må derfor skaffe seg et helhetlig bilde over hvilke av de innsamlede dataene som utgjør personopplysninger, og hvilke av disse den besitter. For å håndtere de innsamlede persondataene, kan virksomheter benytte Big Data-verktøy som kan håndtere store mengder med data og som har funksjonalitet som identifiserer og sikrer «skjulte» personopplysninger i ustrukturerte data. En virksomhet må ha et aktivt forhold til å verne om de personopplysningene de behandler og sørge for at persondata ikke kommer på avveie.

Individet i sentrum

Når forbrukere i stor grad deler personlig informasjon gjennom digitale tjenester, er det utfordrende å ha oversikt over hvem som vet hva og hvorfor. Den nye personvernforordningen har til hensikt å gi forbrukerne større rettigheter og styrke deres tillit til digitale tjenester gjennom en rekke nye regler. Forbrukere skal få større innsikt i hvordan virksomhetene benytter informasjonen de henter inn, i tillegg til hvordan den blir lagret. Forbrukere får også rett til å kreve at personlig informasjon blir «glemt» eller slettet. Videre får forbrukere rett til å ta med seg eller kreve flytting av data til andre tjenesteleverandører, såkalt dataportabilitet. I tillegg skal virksomhetene ha strengere og klarere samtykke fra de som det samles inn personopplysninger fra, og personer kan til enhver tid trekke tilbake samtykket til bruk av persondata. Personopplysninger skal kun, i likhet med dagens regelverk, brukes i samsvar med det formålet som ble oppgitt ved innsamlingen. Alle bedrifter bør allerede nå starte arbeidet med å tilpasse rutiner og løsninger for å møte de nye kravene.

Nye krav – gjensidig ansvar

Virksomhetene som blir omfattet av GDPR, er alt fra et lokalt tannlegekontor til store, internasjonale skyleverandører. Virksomhetene som besitter personopplysninger, er enten definert som *behandlingsansvarlig* eller *databehandler*. En databehandler er en virksomhet som behandler personopplysninger på vegne av en annen virksomhet, den behandlingsansvarlige. En IT-tjenesteleverandør er typisk en databehandler, mens en virksomhet som setter ut tjenesten er

– påvirker «alle»

behandlingsansvarlig. Den nye personvernforordningen stiller flere krav til databehandler i form av dokumentasjon og rutiner rundt informasjonssikkerhet, som bevis for etterlevelse av reglene. Dersom persondata kommer på avveie, skal dette varsles både til Datatilsynet og den som er rammet av datatapet innen 72 timer. Husk at databehandler og behandleransvarlig sammen har et ansvar for at reglene i GDPR overholdes.

Flere virksomheter som behandler personopplysninger, vil også bli pålagt å opprette et personvernombud etter de nye reglene. Se egen artikkel om dette.

Et annet viktig krav er såkalt *innebygd personvern*, som går ut på at virksomheter skal bygge personvern inn i alle løsninger, f.eks. i utvikling av informasjonssystemer. Virksomhetene skal også forfatte en forståelig personvernerklæring, tilpasset leseren.

Store konsekvenser

En av hovedårsakene til all oppmerksomheten rundt GDPR er muligheten for store bøter ved ikke å etterleve regelverket. Virksomheter som bryter regelverket, kan i ytterste konsekvens bli ilagt bøter på opptil 4 % av samlet årlig omsetning eller 20 millioner euro – avhengig av hvilket beløp som er størst. Størrelsen på disse bøtene har til hensikt å sørge for at bedriftene i større grad opptrer proaktivt fremfor reaktivt, og at ansvaret blir løftet opp på ledelsesnivå. Brudd på regelverket vil også kunne gi virksomheten omdømmetap, samt potensielt svekket konkurranseevne som følge av manglende evne til å etterleve reglene og tilby den graden av personvern som markedet krever.

Kom i gang med forberedelsene nå

Til tross for at mye fortsatt er usikkert rundt forståelsen av det nye regelverket, bør virksomheter allerede nå starte forberedelsene til det nye regelverket. Gjør man dette, vil man ha et godt utgangspunkt for 2018.

a) Avklare og få oversikt over personopplysninger som behandles i dag
   - Hvilke?
   - Hvor kommer de fra?
   - Hvem har tilgang?
   - Hvor lenge lagres de? Ligger de i skytjenester?
   - Kan opplysningene aksesseres av personer utenfor EU?

b) Sørge for å oppfylle dagens lovkrav (dokumentasjon og compliance)
   - Risikovurderinger
   - Compliance
   - Handlingsplaner ved databrudd
   - Katastrofeberedskap
   - Retningslinjer for innebygget personvern

c) Sette seg godt inn i det nye regelverket

d) Starte arbeidet med å utføre nye rutiner for å følge de nye reglene.

Utbredelse av Internet of Things (IoT) gjør at ustrukturerte data kan hentes gjennom ting koblet til internett for å spore brukerens atferd.

Flere må ha personvernombud

EUs personvernforordning trer i kraft i mai 2018, og dette innebærer blant annet at flere virksomheter får krav om å ha personvernombud. For mange er dette helt nytt og ukjent.

Jurist
Kai Runar Bang,
Personvernombud i Sticos

Et personvernombud er etter dagens regler en frivillig ordning administrert av Datatilsynet. Tilsynet omtaler personvernombudet som en «ressursperson som styrker virksomhetens kunnskap og kompetanse om personvern». Ombudet pekes ut av virksomheten selv og godkjennes av Datatilsynet.

Hvem må ha ombud?

Den største endringen i reglene om personvernombud er at det ikke lenger vil være en rent frivillig ordning. De som ikke har plikt til å ha ombud, kan likevel velge å ha det, og for mange virksomheter vil det være en positiv ressurs å ha med på laget for å forsikre seg om at man overholder regelverket.

De nye reglene bestemmer at følgende virksomheter må utnevne et personvernombud:

- Offentlige virksomheter, bortsett fra domstoler
- Virksomheter som har en kjerneaktivitet som består i regelmessig og systematisk overvåking av personer i stort omfang
- Virksomheter som behandler sensitive personopplysninger i stort omfang

Offentlige virksomheter

Forordningen beskriver ikke hva som skal anses å være «offentlig virksomhet». Dette vil i stor grad måtte defineres av norske myndigheter selv. Det vil være uproblematisk for de klart offentlige virksomhetene, som f.eks. kommuner, men på privatiserte eller delprivatiserte områder vil det kunne bli en vanskeligere vurdering. EUs arbeidsgruppe som jobber med tolkning av reglene, den såkalte Artikkel 29-gruppen, anbefaler som god praksis at alle virksomheter som behandler data for en gruppe som, på lik linje som hos offentlig myndighet, har lite eller intet valg om hvordan personopplysningene behandles, bør ha personvernombud.

Virksomheter der kjerneaktiviteten er å overvåke i stort omfang

Med «kjerneaktivitet» menes at overvåkningen er uløselig knyttet til aktiviteten i selskapet. Dette vil være særlig relevant for regnskapsbransjen. Regnskapsførere har svært ofte som oppdrag å ha ansvar for den praktiske behandlingen av lønn for en stor mengde personer, og kan ikke levere en tjeneste uten å behandle disse opplysningene. Dette vil dermed anses for å være uløselig knyttet til aktiviteten, og er da en kjerneaktivitet.

Arbeidet utføres også regelmessig og systematisk, men det er mer tvilsomt om regnskapsfører faller inn under begrepet «overvåkning». Regnskapsfører har gjerne oversikt over opplysninger som timelister, tidspunkt og omfang av fravær, tidspunkt og omfang av ferier og avspasering, og lignende. Disse opplysningene blir også jevnlig behandlet over lang tid, noe som kan tale for at det er å anse som overvåkning. Like fullt så er nok dette i beste tilfelle i yttergrensen av hva som kan kalles overvåkning.

De samme vurderingene må gjøres for andre bransjer. Et helseforetak vil ha som hovedaktivitet å tilby helsetjenester. Dette lar seg ikke gjøre uten å kartlegge store mengder helseopplysninger og følge utviklingen hos pasienter. Behandlingen blir dermed en kjerneaktivitet. Det samme gjelder f.eks. et sikkerhetsselskap som har kameraovervåkning på et kjøpesenter. Oppgaven er sikkerhet, men overvåkningen er knyttet til å sikre kjøpesenteret.

EUs arbeidsgruppe opplyser at det gjelder et unntak for behandlinger som alle gjør i forbindelse med f.eks. lønn og alminnelige IT-verktøy. Dette kan da tale for at slik behandling ellers ville vært ansett for «overvåkning» etter forordningens betydning, og da at en regnskapsfører som gjør dette for flere virksomheter, vil falle inn under bestemmelsen.

Uansett har dette sannsynligvis begrenset praktisk betydning, da regnskapsførere gjerne behandler sensitive opplysninger som omtalt nedenfor.

Behandling av sensitive opplysninger i stort omfang

Sensitive personopplysninger er opplysninger om rase, etnisitet, politisk tilknytning, filosofisk eller religiøs oppfatning, helseforhold, seksuelle forhold og medlemskap i fagforeninger. Også opplysninger om kriminelle forhold er inkludert i vurderingen av om man må ha ombud, selv om dette ikke anses for å være sensitivt i den nye forordningen. Bestemmelsen vil gjerne gjelde for bedriftshelsetjenester, forsikringsselskap, og lignende virksomheter, men her vil det også for regnskapsførere raskt komme til at man faller innenfor reglene. Regnskapsførere behandler i stor grad informasjon om sykefravær og sykepenger, og utfører fagforeningstrekk, noe som fører til krav om ombud.

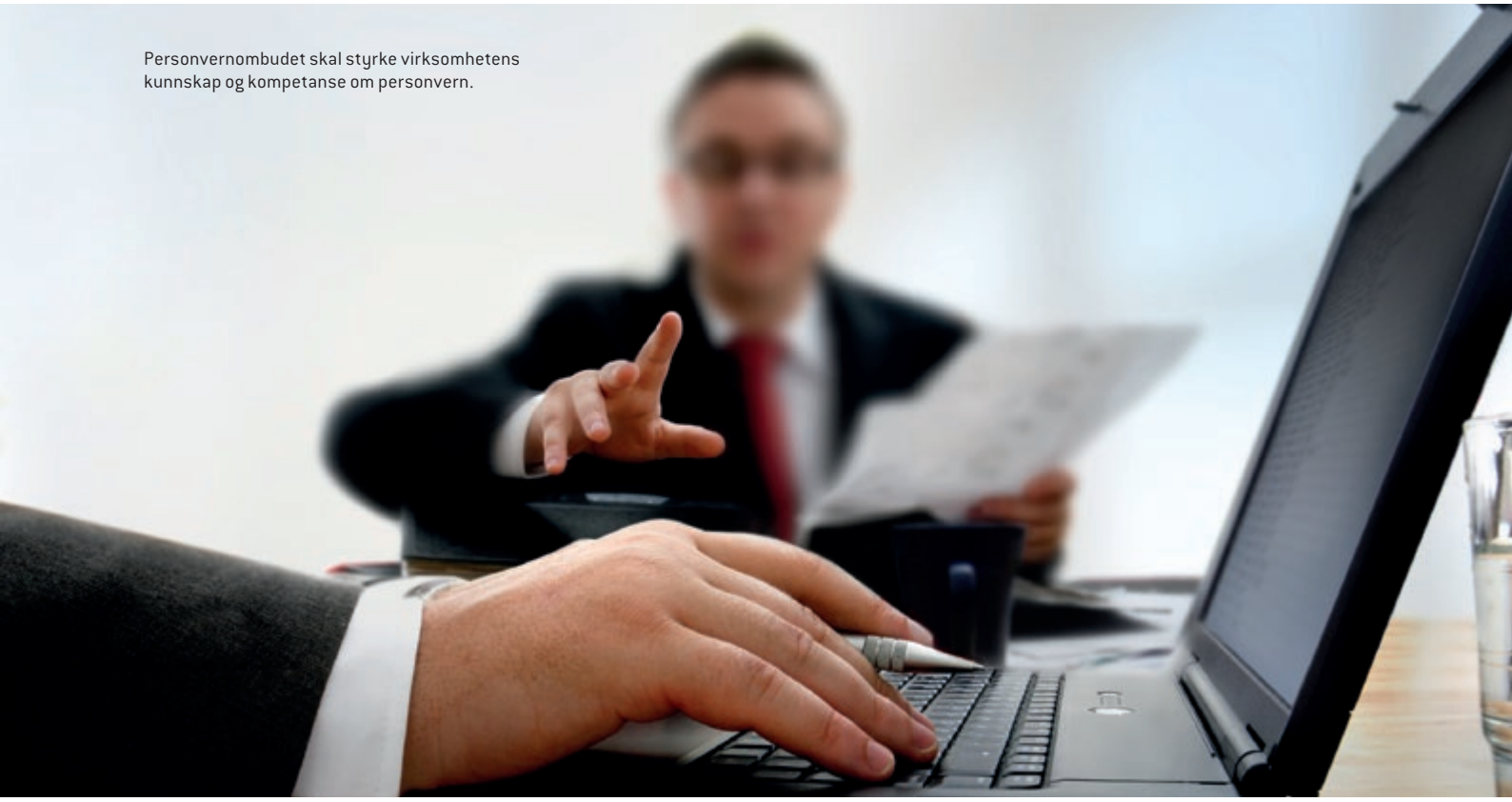
«Stort omfang»

Hva som anses som «stort omfang» er vanskelig å tallfeste. Direktivet sier ikke noe om det, så her må det utarbeides en praksis over tid. Man må vurdere hvor mange individer som behandles, hvor mye informasjon man har, og hvor ofte man behandler opplysningene. EUs arbeidsgruppe antyder at en enkeltstående advokat som kun behandler opplysninger om egne klienter, faller utenfor betegnelsen «stort omfang». Dette vil også kunne være sammenlignbart med revisor. Man kan tenke seg at det er naturlig å utlede at en enkeltstående regnskapsfører med begrenset oppdragsmengde også vil falle utenfor kravet om personvernombud på grunn av at omfanget ikke er stort. Men, dette er ikke selvsagt. Også en enkeltstående regnskapsfører eller revisor kan være i regelmessig befatning med store mengder ansattopplysninger, så her må man vurdere egen situasjon helt konkret. Inntil videre er det dessverre noe uklart hvor grensene går.

Regnskapsførers krav til ombud

Samlet sett fremstår de nye reglene slik at regnskapsfører som hovedregel vil ha krav om personvernombud. Det er tenkelig at man gjennom en konkret skjønnsmessig vurdering av egne forhold kommer til en konklusjon om at man ikke har behov. Dette kan være aktuelt for eksempel for en enkeltstående regnskapsfører med begrenset behandling av ansattopplysninger. Dersom man kommer til dette, er det viktig at man kan vise til at man har tatt en grundig vurdering før man har konkludert, og det er nok også en god idé å ta en samtale med en rådgiver på området eller kontakte Datatilsynet for å drøfte konklusjonen.

Forordningen åpner for at man har eksterne personvernombud. For mindre selskaper vil dette være en god løsning. For de større virksomhetene er det å anbefale å ha et eget ombud. Dette gir nødvendig kompetanse i selskapet, er ressurssparende da et internt ombud kjenner aktiviteten i virksomheten godt, og man kan lettere få raske avklaringer på personvernspørsmål. For kunder vil det også fremstå som betryggende at man har en intern ressurs.



Personvernombudet skal styrke virksomhetens kunnskap og kompetanse om personvern.