De viktigste reglene i ny personvernforordning

Artikkelen tar for seg et utvalg av de viktigste reglene i den nye personvernforordningen. Den ser på hvilken betydning de nye reglene vil få for organisasjoner og identifiserer enkelte tiltak som bør iverksettes for å overholde kravene i forordningen.

Advokat
Jane Wesenberg
Partner EY Tax & Law

Advokatfullmektig
Ida Kristine Hjorteset
EY Tax & Law

Innføringen i norsk rett

EUs nye personvernforordning trer i kraft 25. mai 2018 og bringer med seg omfattende endringer i personvernlovgivningen slik vi kjenner den i dag.[1] Den styrker eksisterende rettigheter og innfører nye rettigheter for individer hvis personopplysninger behandles («den registrerte»), og pålegger nye og omfattende forpliktelser for den som bestemmer formålet med behandlingen («behandlingsansvarlig») eller behandler personopplysninger på vegne av denne («databehandler»). Ansvaret for å oppfylle forordningens krav er tydelig plassert hos den behandlingsansvarlige, eventuelt også databehandleren, og dette ansvaret er gjort reelt gjennom trussel om potensielt betydelige administrative gebyrer ved overtredelse.

Forordningen vil erstatte og oppheve EUs gjeldende personverndirektiv.[2] Den gjelder direkte i alle EUs medlemsstater fra ikrafttredelsen, og vil i stor grad harmonisere personvernregelverket innen EU. Forordningen gjelder ikke direkte i Norge, men må gjennomføres i norsk rett. Det er foreslått at dette skal skje ved inkorporasjon,[3] dvs. at det vedtas en ny personopplysningslov med en bestemmelse som henviser til forordningen og stadfester at denne gjelder som lov. Forordningens regler vil da i hovedsak anvendes slik de står. Någjeldende regelverk blir opphevet.

Økt flyt av personopplysninger

Omfanget av utveksling av personopplysninger har økt betraktelig de siste årene, både mellom offentlige og private aktører, sammenslutninger og foretak som følge av digitaliseringen av kommunikasjon og tjenester. Globaliseringen og økt økonomisk og sosial integrasjon har ført til betydelig økt flyt av personopplysninger over landegrensene. Den teknologiske utviklingen gjør utveksling av personopplysninger enkel, rask og effektiv. Den gjør det også mulig for mottakerne å benytte seg av personopplysninger i et helt nytt omfang. Denne utviklingen bringer med seg behov for kontroll og store utfordringer ved å beskytte personopplysninger mot urettmessig bruk.

Styrker borgernes rettsvern

Forordningen har til formål å styrke borgernes grunnleggende rett til vern ved behandling av personopplysninger, og i avveiningen mot de økonomiske og praktiske interessene til de som behandler personopplysninger, har borgernes interesser fått gjennomslag. Forordningen erkjenner imidlertid at retten til personvern ikke er en absolutt rettighet, og den enkeltes interesse i å verne opplysninger om seg selv, er veid opp mot andre grunnleggende rettigheter.

Ikke alt i den nye forordningen er nytt. Forordningen bygger videre på de grunnleggende personvernprinsippene i personverndirektivet, og grunntrekkene er kjent. Alle virksomheter bør imidlertid forberede seg på de endringene som kommer ved å gjennomgå egen organisasjon, rutiner og teknologi og sette i gang de tiltakene som er nødvendige for at virksomhetens håndtering av personopplysninger blir i samsvar med de nye kravene innen 25. mai 2018. Tiden begynner å bli knapp.

Grunnleggende prinsipper – ansvar

De grunnleggende personvernprinsippene som vi kjenner til fra dagens personverndirektiv og personopplysningslov, er i stor grad uendret i forordningen.[4] Personopplysninger skal behandles på en lovlig, rettferdig og gjennomsiktig måte overfor den registrerte («lovlighet, rettferdighet og gjennomsiktighet»). Personopplysninger skal kun samles inn for spesifikke, uttrykkelig angitte og berettigede formål og skal ikke viderebehandles på en måte som er uforenlig med disse formålene («formålsbegrensning»). Personopplysninger må være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»). Personopplysninger må være korrekte og, om nødvendig, holdes oppdatert. Det skal treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige, under hensyn til de formålene de behandles for, slettes eller korrigeres uten opphold («riktighet»). Personopplysninger skal som hovedregel lagres i et format som gjør at det ikke er mulig å identifisere de registrerte for en lengre periode enn det som er nødvendig for formålene som personopplysningene behandles for («lagringsbegrensning»). Personopplysninger skal også behandles på en måte som sikrer til-

1 Forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning).

2 Direktiv 95/46 EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

3 Justisdepartementet sendte utkast til ny personopplysningslov og forslag til gjennomføring av personvernforordningen i norsk rett på høring 6. juli 2017.

4 Forordningen artikkel 5 nr. 1.

La oss effektivisere din hverdag

Xledger er et ekte skybasert ERP-system som gir deg en mer effektiv hverdag gjennom automatiserte regnskapsprosesser.

Les mer på xledger.no

xledger

Samtykke fra den registrerte må til for å behandle personopplysninger. Forordningen stiller strengere krav til samtykkeerklæring fra den registrerte enn etter dagens regler.

strekkelig sikkerhet for personopplysninger; egnede tekniske eller organisatoriske tiltak skal iverksettes for å verne personopplysninger mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade («integritet og fortrolighet»).

Rettigheter for registrerte – plikter for behandlingsansvarlige

De grunnleggende prinsippene er konkretiserte gjennom en rekke individuelle rettigheter for den registrerte, med tilhørende plikter for den behandlingsansvarlige, samt generelle forpliktelser som pålegger den behandlingsansvarlige å innføre tiltak for å redusere risikoen for brudd og påvise at behandlingen utføres i samsvar med forordningen (ansvarstiltak). Dessuten inneholder forordningen en uttrykkelig bestemmelse om ansvar: Den behandlingsansvarlige er ansvarlig for *og skal kunne påvise* at prinsippene for behandling av personopplysninger overholdes.[5] Sammen med de andre pliktbestemmelsene innebærer dette at den behandlingsansvarlige skal være i stand til når som helst å dokumentere at behandlingen av personopplysningene oppfyller kravene i forordningen, herunder at de tiltakene som er truffet for å fremme og sikre ivaretakelse av personvern, er gjennomført og hensiktsmessige.

Større og tydeligere ansvar

Prinsippet om ansvar og kravene til iverksettelse av tiltak for å fremme og sikre ivaretakelse av personvern, representerer en prinsipiell endring sammenlignet med dagens personvernlovgivning. Den behandlingsansvarlige – herunder de aller fleste virksomheter – får et langt større og tydeligere ansvar for personvernet enn tidligere. Forordningens bestemmelser krever at personvern løftes frem som et sentralt vurderingstema ved alle beslutninger som kan ha betydning for prosesser, systemer og verktøy for behandling av personopplysninger, og virksomheter skal til enhver tid kunne dokumentere at de overholder forordningens krav.

Skjerpede krav til samtykke

Prinsippet om samtykke

Samtykke fra den registrerte er fortsatt ett av flere grunnlag for å behandle personopplysninger.[6] Forordningen stiller imidlertid strengere krav til samtykkeerklæring fra den registrerte enn dagens regler. Dessuten er det inntatt særlige regler om samtykke fra barn ved innhenting av personopplysninger gjennom informasjonssamfunnstjenester.[7] Etter forordningen kan barn over 16 år gi samtykke til slik behandling, men medlemsstatene er gitt adgang til å fastsette en lavere aldersgrense, forutsatt at den ikke er lavere enn 13 år. Justisdepartementet foreslår i et høringsutkast til ny lov at aldersgrensen i Norge blir 13 år. Er barnet under 13 år, kreves det samtykke fra foreldrene for at behandlingen er lovlig.

Må kunne påvise samtykke

Når behandlingen av personopplysninger bygger på samtykke, skal den behandlingsansvarlige kunne påvise at den registrerte har gitt samtykke.[8] Samtykke er definert som «enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte, der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende».[9] Dette vil f.eks. kunne være i form av en skriftlig, herunder elektronisk, eller en muntlig erklæring. At samtykket skal være «frivillig», innebærer at den registrerte må ha en reell valgfrihet, og være i stand til å nekte å gi eller trekke tilbake et samtykke uten risiko for skade. At samtykket skal være «spesifikt», innebærer at det må være knyttet til en klart definert behandlingsaktivitet. Dersom det er flere formål med behandlingen, kreves samtykke til samtlige formål. Kravet om at samtykke må være utvetydig, er ikke nytt. Fortalen til forordningen viser til at samtykke vil kunne gis «ved å krysse av i en boks under et besøk på et nettsted, velge tekniske innstillinger (…) eller en annen erklæring eller handling som (…) tydelig viser at den registrerte godtar den foreslåtte behandlingen (...) Taushet, forhåndsavkryssede bokser eller inaktivitet bør derfor ikke utgjøre et samtykke.»

I enkelte tilfeller stilles det krav til at samtykket er «uttrykkelig». Dette gjelder ved behandling av sensitive personopplysninger og i enkelte tilfeller ved overføring av personopplysninger utenfor EU.

Hvis samtykke skal gis i en skriftlig erklæring som også gjelder andre forhold, må anmodningen om samtykke fremlegges i en forståelig og lett tilgjengelig form som er atskilt fra slike andre forhold og på et klart og enkelt språk.[10] I praksis innebærer dette at anmodninger om samtykke til behandlinger av personopplysninger i forbindelse med avtaler og kontrakter, må fremlegges atskilt fra selve avtalen eller kontrakten.

Retten til å trekke tilbake samtykke

Den som har gitt sitt samtykke, skal kunne trekke det tilbake når som helst.[11] Det skal dessuten være like enkelt å trekke samtykke tilbake som å gi det. Alle behandlingsansvarlige og databehandlere må derfor ha systemer og rutiner som muliggjør en slik tilbaketrekking. Den behandlingsansvarlige skal informere den

5 Forordningen artikkel 5 nr. 2.

6 Forordningen artikkel 6 nr. 1 a).
7 Forordningen artikkel 8.

8 Forordningen artikkel 7 nr. 1.
9 Forordningen artikkel 4 nr. 11.
10 Forordningen artikkel 7 nr. 2.
11 Forordningen artikkel 7 nr. 3.

registrerte om retten til å trekke tilbake samtykke på tidspunktet for innsamlingen.[12] Fra det tidspunktet den registrerte har trukket tilbake sitt samtykke, kan disse opplysningene ikke lenger benyttes.

Cookies

Bruk av cookies – eller informasjonskapsler – er et praktisk viktig eksempel der samtykke er nødvendig for at behandling av personopplysninger skal være lovlig. Når man samtykker til bruk av cookies, lagrer nettsiden handlingene eller preferansene til den registrerte over tid, samt opplysninger om hvor ofte nettsiden blir besøkt. De skjerpede kravene til samtykke innebærer at det ved samtykkeerklæringen til bruk av cookies også skal være mulig å nekte slikt samtykke og ha mulighet til å trekke tilbake samtykket til enhver tid. Utgangspunktet er at nektelse av å gi slikt samtykke ikke skal medføre at brukeren avskjæres fra å bruke siden eller tjenesten, selv om enkelte tjenester eller opplevelser på nettsiden ikke vil være tilgjengelige. Leverandører vil derfor måtte gjøre tilgjengelig parallelle systemer som kan brukes med og uten å akseptere cookies.

Virksomheter som benytter samtykke som grunnlag for å behandle personopplysninger, bør forsikre seg om at samtykke fortsatt vil være et lovlig grunnlag for behandlingen. De bør også sørge for at de nye kravene til samtykke er oppfylt, f.eks. at samtykke omfatter alle formål med behandlingen, at det er frivillig og at det ikke er basert på taushet, forhåndsavkryssede bokser eller inaktivitet. De må sørge for at det er mulig og lettvint å trekke samtykke tilbake, og informere om denne retten ved tidspunktet for innsamlingen. Det må sørges for at anmodning om samtykke fremlegges atskilt fra andre dokumenter.

Rettigheter for den registrerte

Forordningen gir som nevnt en rekke individuelle rettigheter for den registrerte, med tilhørende plikter for den behandlingsansvarlige. Disse behandles nedenfor.

Rett til informasjon – opplysningsplikt

Databehandleren plikter å gi den registrerte informasjon om behandlingen av dennes personopplysninger, med mindre den registrerte har denne informasjonen fra før. Informasjonen kan eksempelvis gis i en personvernerklæring der det fremgår hvordan virksomheten behandler personopplysninger. Forordningen inneholder en omfattende liste over informasjonen som må gis,[13] men behandleren kan ha plikt til å gi ytterligere opplysninger dersom dette etter forholdene er nødvendig for å sikre en rettferdig og transparent behandling.

Den registrerte har rett til å få innsyn i personopplysninger som er samlet inn om vedkommende, samt en kopi av opplysningene og utfyllende informasjon om behandlingen.

Frister

Det er frister for når informasjonen skal gis. Fristene varierer avhengig av om opplysningene er samlet inn direkte fra den registrerte eller fra andre. Fristene er korte. For eksempel, hvis personopplysninger samles inn direkte fra en registrert, plikter den behandlingsansvarlige å gi den registrerte informasjonen *på tidspunktet for innsamlingen*. Hvis de ikke samles inn direkte fra den registrerte, er hovedregelen at informasjonen skal gis innen rimelig tid etter at personopplysningene er samlet inn, men senest innen én måned.

Informasjonen må gis på en kortfattet, åpen, forståelig og lett tilgjengelig måte, og på et klart og enkelt språk. Dette gjelder særlig når den registrerte er et barn. Informasjonen skal som regel gis skriftlig, og kan gis i elektronisk format.

Alle virksomheter bør gjennomgå og revidere sine personvernerklæringer for å bringe dem i samsvar med de nye kravene. De må også ha rutiner som sikrer at informasjonen gis innenfor de fastsatte fristene.

Rett til innsyn

Forordningen gir den registrerte rett til å få innsyn i personopplysninger som er samlet inn om vedkommende, samt en kopi av opplysningene og utfyllende informasjon om behandlingen.[14] Det skal være enkelt å utøve innsynsretten for å forvisse seg om og kontrollere at behandlingen er lovlig.

Den behandlingsansvarlige plikter som regel å svare på anmodninger om innsyn uten ugrunnet opphold og senest innen én måned. Retten til innsyn kan oppfylles ved å tilby direkte tilgang til egne personopplysninger gjennom et sikkert elektronisk system (f.eks. «min side»). Kopi av personopplysningene og informasjonen skal som regel gis gratis og i en vanlig elektronisk form.

Alle virksomheter bør vurdere om de har prosedyrer som gjør dem i stand til å besvare innsynsanmodninger i det formatet og innenfor de fristene som forordningen krever.

Korrigering

Den registrerte kan kreve at den behandlingsansvarlige korrigerer uriktige personopplysninger om vedkommende. I enkelte tilfeller kan den registrerte kreve at den behandlingsansvarlige utfyller ufullstendige personopplysninger eller lagrer en supplerende erklæring.

Hvis den behandlingsansvarlige plikter å korrigere opplysninger, plikter han også å underrette enhver mottaker som har fått utlevert personopplysningene, med mindre dette er umulig eller uforholdsmessig tyngende.[15]

12 Forordningen artikkel 13 nr. 2 c).

13 Forordningen artikkel 12-14.

14 Forordningen artikkel 15.

15 Forordningen artikkel 19.

Rett til dataportabilitet
Retten til innsyn gir som nevnt den registrerte rett til å få utlevert en kopi av sine personopplysninger i vanlig elektronisk form. Retten til dataportabilitet går et stykke lenger og stiller krav til at den behandlingsansvarlige etter nærmere bestemte vilkår utleverer personopplysningene i et format som gjør det mulig for den registrerte å overføre dem til en annen behandlingsansvarlig, eventuelt kreve at de overføres direkte.[16]

Retten til dataportabilitet er snevrere enn den generelle retten til innsyn. Den gjelder kun når behandlingen skjer automatisk (ikke ved manuell behandling av personopplysninger på papir) og kun personopplysninger som den registrerte har gitt til den behandlingsansvarlige selv. Videre gjelder den kun i tilfeller hvor behandlingen skjer på grunnlag av samtykke fra den registrerte eller i forbindelse med en avtale som den registrerte er part i.

Vid definisjon av «har gitt»
Personopplysninger som den registrerte «har gitt til den behandlingsansvarlige selv», må forstås vidt. I en veiledning til bestemmelsen om dataportabilitet, er det nevnt at slike opplysninger omfatter både opplysninger gitt av den registrerte i utfylte skjemaer o.l., og opplysninger som databehandleren innhenter i løpet av sin befatning med den registrerte eller genererer gjennom kartlegging av vedkommendes aktivitet. Retten til dataportabilitet vil således gjelde for data hos en streamingtjeneste for musikk, beskrivelse av varer kjøpt fra en nettbutikk, data fra en smartmåler eller lignende, aktivitetslogger, søkeaktiviteter, m.v. Retten til dataportabilitet omfatter imidlertid ikke personopplysninger som databehandleren avleder eller utleder fra slike data, f.eks. resultatene av en algoritmisk analyse av den registrertes aktivitet eller handlingsmønster.

Alle virksomheter bør vurdere hvorvidt de behandler personopplysninger hvor retten til dataportabilitet kan komme til anvendelse, og i så fall om de er stand til å eksportere personopplysningene i et format som oppfyller forordningens krav.

Innsigelsesrett
Det er ingen generell rett for den registerte til å motsette seg behandling av personopplysninger, men forordningen gir den registrerte rett til å motsette seg behandling i enkelte nærmere bestemte tilfeller. Et viktig tilfelle er at den registrerte når som helst kan motsette seg behandling med henblikk på direkte markedsføring.[17] Denne retten er absolutt. Så snart den registrerte protesterer, skal all behandling med henblikk på direkte markedsføring opphøre.

Den registrerte kan også, under nærmere bestemte vilkår, motsette seg behandling for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål[18] og behandling som påstås å være nødvendig for å beskytte den behandlingsansvarliges berettigede interesser, allmennhetens interesse eller for å utøve offentlig myndighet.[19]

Den behandlingsansvarlige plikter å informere den registrerte om innsigelsesretten «senest på tidspunktet for den første kommunikasjon» med den registrerte.[20] Informasjonen skal fremlegges på en klar måte og atskilt fra annen informasjon.

Alle virksomheter bør gjennomgå sine personvernerklæringer og prosedyrer, og forsikre seg om at de registrerte får klar og separat informasjon om innsigelsesretten på tidspunktet for den første kommunikasjonen. Dersom virksomheten tilbyr onlinetjenester, bør innsigelsesretten også kunne gjøres gjeldende online. Alle markedsføringsaktiviteter, også de som utøves av tjenesteleverandører, bør gjennomgås for å sikre at de vil kunne gjennomføres i tråd med kravene i forordningen.

Retten til å bli glemt
Hvis behandlingen ikke oppfyller forordningens krav, har den registrerte, med enkelte unntak, rett til å få opplysninger om seg selv slettet.[21] En anmodning om sletting må etterkommes uten ugrunnet opphold. Retten til å få slettet personopplysninger oppstår bl.a. når personopplysningene ikke lenger er nødvendige for det formålet som de ble samlet inn eller behandlet for, eller når den registrerte trekker tilbake et samtykke hvor dette er det eneste rettslige grunnlaget for behandlingen.

Hvis den behandlingsansvarlige plikter å slette opplysninger, plikter han også å underrette enhver mottaker som har fått utlevert personopplysningene, med mindre dette er umulig eller uforholdsmessig tyngende.[22] Hvis personopplysningene er offentliggjort, plikter han også å underrette andre behandlingsansvarlige som behandler personopplysningene, om anmodningen om sletting. Den behandlingsansvarlige må «treffe rimelige tiltak» under hensyn til tilgjengelig teknologi og gjennomføringskostnadene. Rekkevidden av forpliktelsen er likevel potensielt vid og den kan være vanskelig å etterleve. Blant annet kan det være vanskelig å få oversikt over og identifisere andre behandlingsansvarlige som behandler personopplysninger som er blitt offentliggjort.

Alle virksomheter bør sørge for at de har prosedyrer for å håndtere krav om sletting. Hvis sletting fremstår som uforholdsmessig byrdefullt, må virksomheter vurdere om noen av unntakene kan være aktuelle.

Retten til å motsette seg profilering m.m.
I likhet med dagens personverndirektiv, gir forordningen den registrerte rett til ikke å være gjenstand for «en avgjørelse som utelukkende er basert på automatisert behandling», herunder profilering, som har rettsvirkning for eller i betydelig grad påvirker den registrerte. Et eksempel på en slik avgjørelse er avslag på en søknad om kreditt på internett uten menneskelig inngripen. I disse tilfellene har den registrerte rett til å kreve at mennesker er involvert i avgjørelsesprosessen. Det er enkelte unntak. Retten gjelder ikke hvis automatisert behandling er nødvendig for å gjennomføre en avtale mellom den registrerte og den behandlingsansvarlige, eller når slik behandling er basert på den registrertes samtykke. Retten gjelder heller ikke hvis automatisert behandling er tillatt etter lov, forutsatt at det er fastsatt egnede tiltak for å verne den registrertes interesser. Strengere regler gjelder for adgangen til å treffe avgjørelser basert på automatisert behandling av sensitive personopplysninger.

Virksomheter som treffer avgjørelser basert på automatisert behandling, må sørge for at grunnlaget for slik behandling er i samsvar med forordningen.

Krav til interne rutiner og håndtering av personopplysninger
Forordningen avvikler systemet om melde- og konsesjonsplikt og av den grunn er kravene til interne rutiner og virksomhetens håndtering av personopplysninger i større grad utdypet. Når det stilles strengere krav til virksomhetenes behandling av

16 Forordningen artikkel 20.

17 Forordningen artikkel 21 nr. 2.
18 Forordningen artikkel 21 nr. 3.
19 Forordningen artikkel 21 nr. 1.
20 Forordningen artikkel 21 nr. 4.
21 Forordningen artikkel 17.
22 Forordningen artikkel 19.

Det er foreløpig uklart hva som ligger i «stor skala», men det antas at eksempelvis banker, forsikringsselskaper, finansforetak og vaktselskaper, samt private forskningsinstitusjoner, vil omfattes.

personopplysninger, er det nødvendig at kravene til virksomhetenes systemer og rutiner for behandling av personopplysninger også skjerpes. Prinsippene og reglene er likevel ikke nye: Enkelte av reglene har vi allerede (f.eks. reglene om dataminimering og personvernombud). Andre regler og prinsipper har til nå vært uttalt som beste praksis (f.eks. prinsippene om innebygget personvern og personvern som standardinnstilling) og er nå inntatt i forordningen.

Innebygget personvern og personvern som standardinnstilling

Forordningen pålegger behandlingsansvarlige virksomheter å sørge for at systemene de bruker til behandling av personopplysninger «tenker» personvern, og standardinnstillinger skal i alle systemer beskytte personopplysninger i størst mulig grad.[23] Virksomheter er pålagt å gjennomføre «egnede tekniske tiltak» for å sørge for at de grunnleggende personvernprinsippene er gjennomført og for å verne registrerte rettigheter. Dette gjelder på alle stadier, både ved valg og implementering av systemer som skal brukes til å behandle personopplysninger, og ved tidspunktet for selve behandlingen. Vurderingen av hvilke tiltak som skal brukes, skal være risikobasert. Det vil si at virksomheten ved valg av tiltak skal ta hensyn til sannsynligheten for brudd på de grunnleggende personvernprinsippene og individuelle rettigheter, samt alvorlighetsgrad ved et eventuelt brudd.

Personvernombud – nå personvernrådgiver

Ordningen med personvernombud er i dag frivillig, men ordningen vil med forordningen pålegges en rekke virksomheter. Justisdepartementet har i sitt lovutkast foreslått at «data privacy officer» skal over-

23 Forordningen artikkel 25. Datatilsynet har nylig utgitt en omfattende veileder om innebygget personvern.

settes til «personvernrådgiver», som erstatning for betegnelsen personvernombud.

Regelmessig og systematisk monitorering i stor skala
Plikten til å oppnevne en personvernrådgiver omfatter alle offentlige organer, samt private virksomheter der *hovedvirksomheten* er «behandlingsaktiviteter som på grunn av sin art, sitt omfang og/eller formål krever regelmessig og systematisk monitorering/overvåking i stor skala av registrerte» eller behandling av sensitive opplysninger «i stor skala».[24] «Regelmessig og systematisk monitorering» anses å omfatte alle former for online sporing og profilering, inkludert adferdsbasert annonsering og e-postutsendelser, profilering og scoring (f.eks. i forbindelse med kredittvurderinger, tiltak mot svindel eller fastsettelse av forsikringspremier), geografisk sporing, sporing av trenings- og helsedata, videoovervåkning, behandling gjennom tilkoblede enheter (smartmålere, smartbiler osv.) og datadrevne markedsføringsaktiviteter (big data). Hva som ligger i «stor skala» er foreløpig uklart, men det antas at eksempelvis banker, forsikringsselskaper, finansforetak og vaktselskaper, samt private forskningsinstitusjoner, vil omfattes.[25]

Det er i dag ingen formelle krav til personvernombudets kvalifikasjoner. Forordningen oppstiller imidlertid krav om at «personvernrådgiveren skal utpekes på grunnlag av faglige kvalifikasjoner, og særlig på grunnlag av dybdekunnskap om personvernlovgivning og praksis på området».

Vurdering av personvernkonsekvenser
Nytt i forordningen er også kravet om «Data Privacy Impact Assessment (DPIA)» – eller «vurdering av personvernkonsekvenser»[26] for behandling av personopplysninger som innebærer «høy risiko for fysiske personers rettigheter og friheter». Innføringen av denne plikten må ses i lys av at systemet med melde- og konsesjonsplikt avskaffes. Behandling av personopplysninger skal derfor ikke lenger forhåndsgodkjennes av tilsynsmyndigheten eller andre. For å sikre at personopplysninger (og særlig sensitive eller andre spesielle kategorier av personopplysninger) blir behandlet med tilstrekkelig aktsomhet, oppstilles det derfor krav om en slik vurdering. For enkelte typer høyrisikobehandling av personopplysninger kan behandlingsansvarlig virksomhet også ha en plikt til å gjennomføre forhåndsdrøftinger med tilsynsmyndigheten, før slik behandling av personopplysninger finner sted.

Alle virksomheter bør gjennomgå sine relevante datasystemer i lys av prinsippene om innebygget personvern og personvern som standardinnstilling. Virksomhetene bør også vurdere karakteren og omfanget av de opplysningene de behandler. Dersom vurderingene tilsier det, må virksomheten oppnevne en personvernrådgiver, og utarbeide vurderinger av personvernkonsekvensene.

Bruk av databehandlere
De aller fleste virksomheter behandler ikke bare opplysninger de selv er ansvarlige for, men benytter seg av, eller samarbeider med, andre virksomheter om dette. Slike virksomheter som «behandler personopplysninger på vegne av den behandlingsansvarlige»[27] (kalt «databehandler»), skal i dag ha en databehandleravtale som formaliserer denne tjenesten eller dette samarbeidet.

Forordningen stiller krav om at en behandlingsansvarlig bare kan benytte seg av databehandlere «som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning og vern av den registrertes rettigheter». Kravene til innholdet i databehandleravtalene skjerpes, og det presiseres at databehandleren ikke kan delegere behandlingen av personopplysninger videre, uten at dette på forhånd er godkjent av den behandlingsansvarlige.

Alle virksomheter bør vurdere hvorvidt andre behandler opplysninger på deres vegne, eller om de selv behandler personopplysninger på vegne av andre. Videre bør virksomhetene i tilfelle undersøke hvordan slike avtaleforhold er regulert.

Avvikende behandling av personopplysninger
Når ansvaret for behandling av personopplysninger i større grad er skjøvet over på virksomhetene, og tilsynsmyndighetene ikke skal godkjenne behandlingen, er det også behov for strengere sanksjoner dersom tilsynsmyndighetene oppdager avvik. Tilsynsmyndighetene – Datatilsynet i Norge – vil gis kompetanse til å føre tilsyn med alle sider av virksomheten av betydning for personvernet, og kan pålegge behandlingsansvarlig en rekke tiltak. I tillegg vil myndighetene kunne ilegge virksomhetene administrative gebyrer som følge av avvik. Samtidig er det inntatt et eget grunnlag for de registrerte til å kreve erstatning fra behandlingsansvarlig og databehandler, dersom deres rettigheter er krenket. For en spesiell type avvik, kalt «brudd på personopplysningssikkerheten», inntrer det i tillegg spesifikke varslingsplikter.

Høyere nivå på administrative gebyrer
Forordningen gir adgang til å ilegge administrative gebyrer for overtredelse av forordningens regler, i tillegg til andre tiltak som tilsynsmyndighetene måtte pålegge. De nasjonale tilsynsmyndighetene (Datatilsynet) skal sikre at de administrative gebyrene i den enkelte sak er virkningsfulle, står i forhold til overtredelsen og virker avskrekkende.[28] I vurderingen av gebyrets størrelse skal momenter som karakteren, alvorlighetsgraden og varigheten av overtredelsen, graden av forsett eller uaktsomhet ved overtredelsen, eventuelle preventive eller reparerende tiltak som er forsøkt utført, eventuelle tidligere overtredelser m.m., tillegges vekt.

Et eventuelt gebyr avhenger av hvilken overtredelse som er begått. For alvorlige overtredelser av de mest sentrale forpliktelsene kan gebyrer på opptil 20 millioner euro ilegges, eller hvis det er tale om et foretak, opptil fire prosent av den samlede globale årsomsetningen i forutgående regnskapsår dersom dette er høyere enn 20 millioner euro. Til sammenligning kan Datatilsynet i dag ilegge gebyrer på inntil 10G (i dag 936 340 kroner). Målet er at virksomheter i større grad enn før skal sette personvern på dagsordenen, og ta sikkerheten på alvor.

Avslutning
Endringene som kommer med den nye personvernforordningen er omfattende og inngripende. Denne artikkelen dekker ikke alle sider ved forordningen, men tar for seg et utvalg av de viktigste reglene. Alle virksomheter bør imidlertid sette seg inn i forordningen og analysere hvilken betydning den vil få for organisasjonen, identifisere hvilke tiltak som må iverksettes for å overholde kravene i forordningen og sette i gang arbeidet med å implementere disse. Tiden begynner som nevnt å bli knapp.

24 Forordningen artikkel 37.
25 Se nærmere Guidelines on Data Protection Officers («DPOs»), vedtatt av Article 29 Data Protection Working Party 13. desember 2016.
26 Forordningen artikkel 35.
27 Forordningen artikkel 4 nr. 8.
28 Forordningen artikkel 83 nr. 1.