Versjon 2, 24. oktober 2024

Advokatforeningens veileder om advokatvirksomheters etterlevelse av GDPR

Thomas Olsen, Rune Opdahl, Christopher Sparre-Enger Clausen

Innhold

1 Introduksjon om personvern i advokatvirksomheter

EUs personvernforordning, General Data Protection Regulation 2016/679 (GDPR) trådte i kraft 20. juli 2018. Forordningen ble innført i norsk rett gjennom henvisning i ny personopplysningslov I tillegg til å gjøre personvernforordningen til norsk lov, inneholder personopplysningsloven utfyllende særnorske regler, blant annet regler om behandling av personopplysninger i arbeidslivet og om straffedommer og lovovertredelser mv.

I utgangspunktet vil advokatvirksomhet være underlagt personopplysningsloven – og dermed personvernforordningen. Dette gjelder uavhengig av størrelse og rettsområde.

Denne veilederen er ikke en uttømmende oversikt over forordningens krav. Å følge disse rådene vil imidlertid være et godt utgangspunkt for å etablere tiltak i samsvar med forordningen.

Hvilke tiltak og dokumentasjon som må være på plass for å sikre etterlevelse vil være avhengig av virksomhetens art og omfang. Eksempelvis vil større advokatvirksomheter som driver med strafferett eller pasientskaderett måtte ha mer utførlige personvernrutiner enn mindre advokatvirksomheter som driver med forretningsjus.

Sentrale konsepter i personvernforordningen

Personvernforordningens pliktsubjekter er behandlingsansvarlige og databehandlere. "Behandlingsansvarlig" er den som bestemmer formålet med behandling av personopplysninger og hvilke midler som skal benyttes. "Databehandler" er den som behandler personopplysninger på vegne av den behandlingsansvarlige. Advokatvirksomheter fungerer i all hovedsak som behandlingsansvarlige.

"Personopplysninger" er enhver opplysning om en identifisert eller identifiserbar person. "Behandling" er all innsamling, lagring, utlevering og annen bruk av personopplysninger. Advokatvirksomheter behandler typisk personopplysninger om klienter som er privatpersoner, kontaktpersoner hos klienter som ikke er privatpersoner, personer som er involvert i saken eller omtalt i saksdokumenter (f.eks. motparter, sakkyndige, vitner, og ansatte i selskap, organisasjoner og offentlige organer), kontaktpersoner hos leverandører og samarbeidspartnere samt egne ansatte.

Personvernforordningen får anvendelse for behandling av personopplysninger som helt eller delvis gjøres "automatisert", samt behandling av personopplysninger som inngår eller skal inngå i et "register". All behandling av personopplysninger som skjer med elektroniske hjelpemidler anses som automatisert. All behandling av personopplysninger i papirform som er strukturert slik at personopplysninger er tilgjengelig etter særlige kriterier, f.eks. alfabetisk, inngår i et register.

Forholdet til advokaters taushetsplikt

Advokater er underlagt taushetsplikt. Dette gjelder uavhengig av om opplysningene utgjør personopplysninger. Også i personvernforordningen finnes konfidensialitetsplikt. Uautorisert tilgang til eller utlevering av opplysninger vil derfor kunne utgjøre brudd på både lovbestemt taushetsplikt og – dersom det gjelder personopplysninger – brudd på personvernforordningen.

Personvernforordningen rammer imidlertid videre enn taushetsplikten. Blant annet setter den begrensninger for hvilke formål personopplysninger kan brukes for, hvor lenge personopplysninger kan oppbevares, og hvilke rettigheter personene har til blant annet å få informasjon og innsyn. Fortrolig håndtering av opplysninger er derfor ikke nok for å etterleve personvernforordningen.

Forholdet til rettspleielovunntaket

I personopplysningsloven § 2 bokstav b fremgår det såkalte rettspleielovunntaket, altså at loven ikke

gjelder «for saker som behandles eller avgjøres i medhold av rettspleielovene (domstolloven, straffeprosessloven, tvisteloven og tvangsfullbyrdelsesloven mv.)». Unntaket er begrunnet i hensynet til en uavhengig rettspleie, samt at personvernet anses ivaretatt gjennom de alminnelige rettssikkerhetsgarantiene som rettspleielovene gir, jf. PVN-2022-16. Dette unntaket omfatter også advokaters behandling av personopplysninger når de yter bistand i saker som behandles eller avgjøres i medhold av rettspleielovene. Rekkevidden av unntaket fremgår ikke tydelig av lovtekst eller forarbeider, men tilsynspraksis og avgjørelser fra Personvernnemda gir visse føringer.

Advokatforeningen tolker unntaket slik at all behandling av personopplysninger som finner sted fra det tidspunkt en sak anses å være til behandling eller avgjørelse etter rettspleielovene, og frem til saken er endelig avsluttet, vil være unntatt. Dette vil eksempelvis omfatte innhenting av saksopplysninger, fremleggelse av bevis, korrespondanse mellom partene og de ulike aktørene etc. Både advokatene, deres parter/klienter, sakkyndige, vitner og andre involverte i behandling av saken må anses omfattet av unntaket.

Når en sak anses å være til behandling eller avgjørelse vil variere mellom de ulike rettspleielovene. I saker som behandles etter tvisteloven vil unntaket eksempelvis komme til anvendelse i alle fall fra tidspunktet forliksklage eller stevning tas ut.

2 Dokumentasjon for å kunne påvise etterlevelse

Personvernforordningen oppstiller i artikkel 5 nr. 2 et generelt prinsipp om at den behandlingsansvarlige skal kunne "påvise" at forordningens prinsipper etterleves. I henhold til artikkel 24 skal virksomheten ha på plass tekniske og organisatoriske tiltak som står i forhold til risikoen. Dersom det står i et rimelig forhold til behandlingsaktivitetene, skal tiltakene omfatte egnede retningslinjer for vern av personopplysninger.

Forordningen oppstiller også mer spesifikke dokumentasjonskrav. I henhold til artikkel 30 skal virksomheten vedlikeholde en protokoll med oversikt over behandlingsaktiviteter og ved høy risiko for personvernet er det krav om gjennomføring av en personvernkonsekvensutredning (artikkel 35).

For de fleste advokatvirksomheter vil det være hensiktsmessig å ha på plass to hovedkategorier av personverndokumentasjon som angitt nedenfor.

A. Interne retningslinjer

I Datatilsynets veiledning og praksis har det vært vanlig å skille mellom tre hovedelementer i den interne dokumentasjonen ("internkontrollen"): *styrende*, *gjennomførende* og *kontrollerende*. Denne tredelingen vil være et godt utgangspunkt for intern dokumentasjon også etter forordningen.

Forordningen oppstiller ikke noe formkrav til dokumentasjonen, og den nærmere utformingen må tilpasses den enkelte virksomhet. For virksomheter av en viss størrelse vil det imidlertid være hensiktsmessig å ha ett sentralt dokument (for eksempel kapittel i firmahåndbok e.l.) som inneholder de tre elementene, med henvisning til protokoll over behandlingsaktiviteter og praktiske rutiner.

- Styrende
  Virksomheten bør utpeke en person som er ansvarlig for å følge opp virksomhetens arbeid med personvern. Dersom virksomheten er av en viss størrelse, kan det være aktuelt å fordele oppgaver knyttet til personvern på flere personer, f.eks. ved å skille mellom klientrelaterte opplysninger, HR, IT mv. Det overordnede ansvaret for virksomhetens etterlevelse bør forankres hos virksomhetens styre.

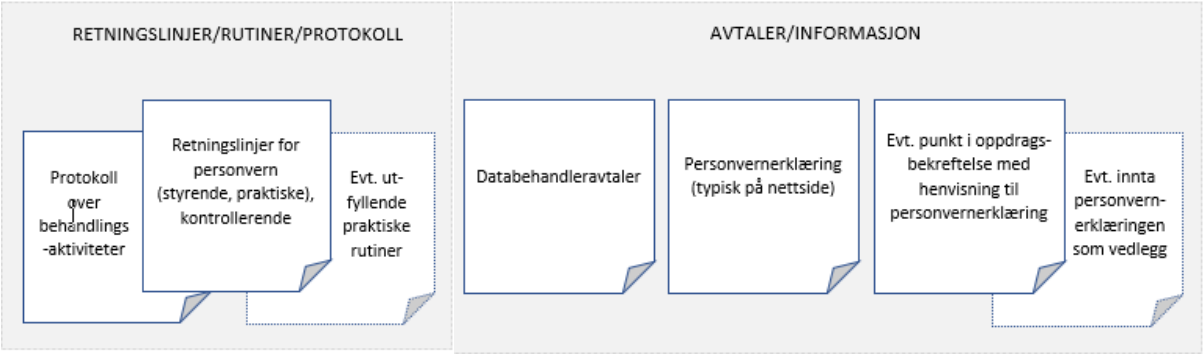
- Praktiske rutiner
  Virksomhetens daglige praktiske rutiner. Eksempelvis kan det her tas inn bestemmelser eller referanser til:
- Vurdering av hvordan personopplysninger håndteres før virksomheten setter i gang med nye behandlingsaktiviteter eller systemer.
- Rutiner for håndtering av opplysninger om klienter.
- Rutiner for håndtering av ansattopplysninger.
- Rutiner for håndtering av opplysninger om jobbsøkere.
- Krav til vurdering av databehandleravtaler og risikovurdering knyttet til bruk av eksterne leverandører.
- Rutiner for å etterleve de registrertes rettigheter (bl.a. innsyn, retting og sletting).
- Rutiner for innsyn i ansattes e-post og avvikling av e-post.
- Sletterutiner.

- Kontrollerende
  Bestemmelser som sørger for vedlikehold og stadig forbedring av internkontrollen, typisk:
- Håndtering av avvik fra virksomhetens rutiner.
- Ledelsens årlige gjennomgang av virksomhetens etterlevelse av personvernreglene.

B. Avtaler og informasjon

I tillegg til den interne personverndokumentasjonen, må virksomheten ha følgende dokumentasjon:

- Personvernerklæring som oppfyller forordningens krav til informasjonsplikt.
- Oppdragsbekreftelse kan gjerne henvise til full personvernerklæring, og regulere enkelte aspekter ved håndteringen av klient- og saksdokumenter.
- Databehandleravtaler med leverandører som håndterer personopplysninger på vegne av virksomheten.



3 Oversikt over behandlinger og vedlikehold av protokoll

For å sikre etterlevelse av personvernregelverket er det viktig med oversikt over virksomhetens behandling av personopplysninger. Som det fremgår nedenfor anbefaler Advokatforeningen at advokatvirksomheter etablerer en protokoll i henhold til personvernforordningen artikkel 30. Protokollen gir oversikt over behandling av personopplysninger og er sentral dokumentasjon som Datatilsynet kan kreve utlevert.

Krav til protokoll

Det kan reises spørsmål ved om advokatvirksomheter må føre protokoll over behandlingsaktiviteter, som beskrevet nedenfor, ettersom det gjelder et unntak for virksomheter med færre enn 250 ansatte, jf. GDPR artikkel 30 nr. 5. Det gjelder mange unntak fra unntaket for virksomheter med færre

enn 250 ansatte, som gjør at de aller fleste likevel må føre protokoll. Kravet til protokoll gjelder neppe for mindre advokatvirksomheter som ikke retter seg mot privatklienter. Vi anbefaler likevel at de fleste advokatvirksomheter fører slik protokoll.

Gjennomføring av kartlegging og utarbeidelse av protokoll

Utarbeidelse og vedlikehold av protokoll fordrer at det gjennomføres en kartlegging av virksomhetens behandlinger. De personer som kjenner virksomhetens ulike prosesser knyttet til behandlingen bør involveres i kartleggingen. Kartleggingen kan gjennomføres på flere måter. For mange kan det være hensiktsmessig å benytte en tabell i Word, eller annet støtteverktøy som tar utgangspunkt i de elementene som er påkrevet etter artikkel 30. Eksempel på protokoll er tilgjengelig på Advokatforeningens sider.

Kartleggingen bør i alle tilfeller omfatte de opplysninger som kreves etter artikkel 30:6

- Navn og kontaktinformasjon (og navn og kontaktperson på evt. personvernrådgiver)
- Formålet med behandlingen
- Kategorier av registrerte (f.eks. ansatte, kontaktpersoner hos klienter, leverandører mv.)
- Kategorier av personopplysninger (f.eks. kontaktinformasjon, saksopplysninger, finansiell informasjon, helseopplysninger mv.)
- Kategorier av mottakere som personopplysningene er eller vil bli utlevert til (f.eks. databehandlere, eksterne samarbeidspartnere, parter i tvister, domstoler mv.)
- Hvorvidt det skjer overføring eller tilgjengeliggjøring av personopplysninger til mottaker utenfor EØS, og i så fall det rettslige grunnlaget for overføringen
- Dersom det er mulig, de planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger
- Dersom det er mulig, en generell beskrivelse av tekniske og organiske sikkerhetstiltak (f.eks. tilgangskontroll, totrinnsautentisering, kryptering, innlåsing av dokumenter, sikringstiltak i bygg og/eller datasenter, evt. henvisning til sikkerhetsregime hos leverandør mv.)

I tillegg vil det ofte være hensiktsmessig at kartleggingen omfatter:

- Rettslig grunnlag for de ulike behandlingsformålene
- System for lagring og behandling
- Angivelse av databehandler og hvorvidt det foreligger tilfredsstillende databehandleravtale
- Hvorvidt det er gjennomført risikovurdering av informasjonssystemet
- Hvorvidt det foreligger nærmere rutiner for behandlingen
- Angivelse av hvem i virksomheten som er internt ansvarlig for den aktuelle behandlingen/systemet
- Vurdering av hvorvidt behandlingen innebære høy personvernrisiko, som kan kreve gjennomføring av konsekvensutredning (DPIA)

Hvert av formålene, se pkt. 4 nedenfor, bør få en linje i behandlingsprotokollen.

4 Formålsbegrensninger

All behandling av personopplysninger skal ha et spesifikt, uttrykkelig angitt formål som er saklig begrunnet i virksomheten, jf. GDPR art. 5 nr. 1 bokstav b. Formålet må komme til uttrykk i virksomhetens behandlingsoversikt og i personvernerklæringen på nett.

Typiske formål for advokatvirksomhet er:

- Etablering av klientforhold herunder lovpålagt identitets- og hvitvaskingskontroll samt kredittvurdering ved saklig behov
- Sakshåndtering
- Arkivhold
- Kunnskapsforvaltning (f.eks. gjenbruk av dokumenter i senere saker)
- Klientadministrasjon
- Markedsføring (utsendelse nyhetsbrev, arrangementsinvitasjoner o.l.)
- Fakturering
- Sikkerhet (f.eks. logger på servere, avdekking, oppklaring og oppfølgning av sikkerhetshendelser)

En advokatvirksomhet kan benytte personopplysninger til sekundære formål som ikke er uforenlig med formålet de opprinnelig ble samlet inn for, jf. GDPR art. 6 nr. 4. Mulige eksempler på forenlige formål er: bruk av saksdokumentasjon for å forsvare seg mot klager og krav fra klient eller tredjepart og anonymisering av saksdokumentasjon for å bruke det til å utvikle AI-modeller.

Dersom personopplysninger ellers skal brukes til et annet formål enn det de er blitt samlet inn for, må dette ha ett av følgende grunnlag:

- Samtykke
- Hjemmel i EU-retten
- Nasjonal lovhjemmel

5 Behandlingsgrunnlag

Advokatvirksomheter må ha behandlingsgrunnlag for all sin behandling av personopplysninger. Dette gjelder imidlertid ikke dersom rettspleielovunntaket får anvendelse, jf. kapittel 1.

Behandlingsgrunnlagene fremgår av GDPR artikkel 6 nr. 1 bokstav a - f. For å behandle særlige kategorier personopplysninger må i tillegg et av unntakene i GDPR artikkel 9 nr. 22 bokstav a - j være oppfylt. For å behandle opplysninger om straffedommer og lovovertredelser må i tillegg et av unntakene i GDPR artikkel 9 nr. 2 bokstav a - f være oppfylt, jf. personopplysingsloven § 11.

<u>Kommentarer til aktuelle behandlingsgrunnlag</u>
Samtykke (GDPR art. 6 nr. 1 bokstav a) er et dårlig egnet behandlingsgrunnlag for advokatvirksomhet, blant annet fordi samtykke må innhentes direkte fra den registrerte og når som helst kan trekkes tilbake og fordi samtykket må være helt frivillig å avgi (altså: det må være mulig å få advokatbistand uten å samtykke).

Avtale som behandlingsgrunnlag er aktuelt når det er nødvendig å behandle personopplysninger for å inngå eller oppfylle en avtale (herunder oppdragsbekreftelse) med et individ. Altså vil dette behandlingsgrunnlaget i praksis være begrenset til advokatvirksomhet som har privatklienter. For advokatvirksomhet med virksomhetsklienter vil *berettiget interesse* i å oppfylle avtalen (herunder oppdragsbekreftelse) fungere tilsvarende.

Berettiget interesse som behandlingsgrunnlag er aktuelt når behandling av personopplysninger er nødvendig for å oppfylle en berettiget interesse for advokatvirksomheten eller tredjepart (herunder klienten), og denne interessen overstiger berørte individers rettigheter og interesser. Det forutsetter altså en interesseavveining, som bør dokumenteres.

Rettslig forpliktelse som behandlingsgrunnlag er aktuelt når det er nødvendig å behandle personopplysninger for å oppfylle en lov- eller forskriftsbestemt plikt. Eksempelvis stiller advokatloven § 36 krav til at advokater holder forsvarlig arkiv over fysiske og elektroniske dokumenter som de har mottatt eller produsert i anledning advokatoppdrag.

Fastsette, gjøre gjeldende eller forsvare rettskrav er for eksempel aktuelt når behandling av personopplysninger er nødvendig i tilknytning til et krav eller en klage som gjøres gjeldende fra en klient eller tredjepart mot en advokatvirksomhet, eller vice versa. Det kan i prinsippet diskuteres om advokaten som sådan kan påberope seg *rettskrav* som den gjør gjeldende eller forsvarer på vegne av klient. I praksis er det uansett ukontroversielt at advokater behandler opplysninger i den grad det er nødvendig for å utøve sin advokatvirksomhet.

Behandlingsgrunnlag for aktuelle behandlingsaktiviteter

I tabellen nedenfor gis en oversikt over hvilke behandlingsgrunnlag som er mest aktuelle for noen typiske behandlingsaktiviteter for advokatvirksomhet. Hva som er det mest egnede behandlingsgrunnlaget, må vurderes av den enkelte advokatvirksomhet.

Behandlingsaktivitet	**Behandlingsgrunnlag for alminnelige personopplysninger**	**Behandlingsgrunnlag for særlige kategorier personopplysninger og personopplysninger om straffedommer og lovovertredelser**
Etablering av klientforhold	GDPR artikkel 6 nr. 1 bokstav b (avtale med privatklienten) GDPR artikkel 6 nr. 1 bokstav c (rettslig forpliktelse, f.eks. hvitvaskingsloven §§ 4 (2) nr. 3, jf. 17 og 18) GDPR artikkel 6 nr. 1 bokstav f (berettiget interesse)	GDPR artikkel. 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav)
Sakshåndtering	GDPR artikkel 6 nr. 1 bokstav b (avtale med privatklienten) GDPR artikkel 6 nr. 1 bokstav f (berettiget interesse)	GDPR artikkel. 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav)
Arkivhold (lagring/oppbevaring av saksdokumenter)	GDPR artikkel 6 nr. 1 bokstav c (rettslig forpliktelse, jf. advokatloven § 36) GDPR artikkel 6 nr. 1 bokstav e (oppgave i allmenhetens interesse, jf. advokatloven § 36) GDPR artikkel 6 nr. 1 bokstav b (avtale med privatklienten) GDPR artikkel 6 nr. 1 bokstav f (berettiget interesse)	GDPR artikkel 9 nr. 2 bokstav g (viktige allmenne interesser), jf. advokatloven § 36) GDPR artikkel 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav)
Kunnskapsforvaltning (f.eks. gjenbruk av dokumenter i senere saker)	GDPR artikkel 6 nr. 1 bokstav f (berettiget interesse)	Kunnskapsforvaltning bør som hovedregel ikke skje med særlige kategorier personopplysninger eller opplysninger om straffedommer eller lovovertredelser. Dersom det likevel er nødvendig, vil GDPR artikkel. 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav) etter omstendighetene kunne være aktuelt.
Klientadministrasjon	GDPR artikkel 6 nr. 1 bokstav b (avtale med privatklienten) GDPR artikkel 6 nr. 1 bokstav f (berettiget interesse)	GDPR artikkel 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav)

Markedsføring	GDPR artikkel 6 nr. 1 bokstav f (berettiget interesse) GDPR artikkel 6 nr. 1 bokstav a (samtykke fra den registrerte)	Markedsføring kan ikke skje med særlige kategorier personopplysninger eller opplysninger om straffedommer eller lovovertredelser.
Fakturering	GDPR artikkel 6 nr. 1 bokstav b (avtale med privatklienten) GDPR artikkel 6 nr. 1 bokstav c (rettslig forpliktelse) GDPR artikkel 6 nr. 1 bokstav f (berettiget interesse)	GDPR artikkel 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav)
Sikkerhet (f.eks. logger på servere, avdekking, oppklaring og oppfølgning av sikkerhetshendelser)	GDPR artikkel 6 nr. 1 bokstav c (rettslig forpliktelse) GDPR artikkel 6 nr. 1 bokstav f (berettiget interesse)	GDPR artikkel 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav)

6 Informasjon

Gjennomsiktighet (åpenhet/transparens) er et av de grunnleggende personvernprinsippene som er nedfelt i personvernforordningens artikkel 5. Et utslag av gjennomsiktighets-prinsippet er kravet om å gi personverninformasjon til de registrerte. Slik personverninformasjon omtales gjerne som "personvernerklæring".

Artikkel 13 stiller krav til å gi informasjon når personopplysningene innhentes fra den registrerte selv, mens artikkel 14 stiller informasjonskrav når personopplysningene innhentes fra andre kilder, f.eks. fra offentlige kilder eller motparter. Vi anbefaler at informasjonen gis samlet. Artikkel 12 inneholder enkelte fellesregler for hvordan informasjonen skal gis. Artikkel 23 åpner for visse unntak fra informasjonsplikten.

<u>Hvordan informasjon kan gis og hvem den skal gis til</u>
Personverninformasjonen skal gis uoppfordret og være lett tilgjengelig for de registrerte. Dette betyr at informasjonen skal presenteres for dem, eller at det skal gjøres klart for dem hvor de kan finne informasjonen. Informasjonen kan både gis elektronisk eller i papirform.

Overfor *ansatte* kan personverninformasjon gjerne gis på et intranett, i en personalhåndbok, i papirform, eller kommuniseres internt på annen egnet måte.

Overfor *privatklienter* kan informasjon gis som et vedlegg til en oppdragsbekreftelse, eller på en nettside (med henvisning til nettsiden fra oppdragsbekreftelsen).

Overfor *klienter i straffesaker* vil advokaten sjeldent utstede en oppdragsbekreftelse til sin klient. Vanligvis vil det i slike saker heller ikke være særlig praktisk å gi skriftlig informasjon som henviser til advokatens nettside. Det bør etter Advokatforeningens syn derfor være tilstrekkelig at informasjonen finnes tilgjengelig via advokatens nettside, slik at informasjonen er enkelt tilgjengelig for klienten. Når advokaten ikke selv har samlet inn opplysningene fra den registrerte, men eksempelvis mottatt disse fra påtalemyndigheten, kriminalomsorgen eller domstolen som en del av saksdokumentene, vil advokaten kunne være unntatt fra plikten til å gi informasjon, jf. artikkel 14 (5) (d) og/eller rettspleielovunntaket.

Overfor *kontaktpersoner hos virksomhetsklienter* vil en nettside normalt være den mest egnede måten å kommunisere personverninformasjonen på, men gjerne slik at oppdragsbekreftelsen henviser til nettsiden.

Overfor *kontaktpersoner hos leverandører og eventuelle samarbeidspartnere* vil også en nettside

normalt være den mest egnede måten å kommunisere personverninformasjonen på, men gjerne slik at avtaler e.l. med leverandører og samarbeidspartnere henviser til nettsiden.

Overfor *personer som for øvrig er involvert i saken eller som omtales i saksdokumenter* (f.eks. motparter, sakkyndige, vitner, og ansatte i selskap, organisasjoner og offentlige organer) vil det være en tilnærmet umulig oppgave å kommunisere personverninformasjon. Personvernforordningen artikkel 14 nr. 5 (b) oppstiller et unntak fra informasjonsplikten der det å gi informasjon er umulig eller vil innebære uforholdsmessig stor innsats. Dette unntaket vil kunne få anvendelse overfor nevnte kategorier av personer.

Oppsummert anbefaler vi følgende kanaler for *ekstern* kommunikasjon av personverninformasjonen:
- Personvernerklæring på virksomhetens nettside
- Hvis klientene i hovedsak er næringsdrivende, organisasjoner eller offentlige organer, kan man ha et punkt i oppdragsbekreftelsen som henviser til personvernerklæringen på nettsiden.
- Hvis klientene i hovedsak er privatpersoner, kan man vurdere å ha personvernerklæringen som vedlegg til oppdragsbekreftelsen.

Hva informasjonen skal inneholde
Personvernerklæringen skal minst svare til listen i personvernforordningens artikkel 13 og 14. Advokatforeningen har utarbeidet en mal for personvernerklæring, som gir veiledning på hvilket innhold og overskrifter som typisk bør inntas. Malen er tilgjengelig på Advokatforeningens nettsider.

7 De registrertes rettigheter

GDPR kapittel 3 gir de registrerte en rekke rettigheter. Oppfyllelse av disse påhviler først og fremst den behandlingsansvarlige. Imidlertid vil databehandlerens bistand ofte være påkrevet. Derfor følger det av GDPR artikkel 28 at enhver databehandleravtale skal regulere databehandlers plikt til å yte bistand slik at den behandlingsansvarlige skal kunne oppfylle de registrertes rettigheter.

GDPR artikkel 23 gir nasjonal lovgiver anledning til å oppstille unntak fra de registrertes rettigheter. Flere slike unntak er inntatt i personopplysningsloven kapittel 4.

Nedenfor adresserer vi de rettighetene som vi anser som mest relevant for advokatvirksomheter å være oppmerksom på.

Rett til informasjon (artikkel 13 og 14)
De registrerte har rett til uoppfordret å motta informasjon om hvordan deres personopplysninger behandles.

Rett til innsyn (artikkel 15)
De registrertes rett til innsyn er todelt.

For det første gis den registrerte, på forespørsel, rett til *informasjon* om hvordan deres personopplysninger behandles. Dette er langt på vei et speilbilde av den behandlingsansvarliges plikt til å gi informasjon etter artikkel 13 og 14.

For det andre gis den registrerte, på forespørsel, rett til å få *kopi* av de personopplysninger som en behandlingsansvarlig har om vedkommende. Dersom forespørselen skjer elektronisk, skal opplysningene gis elektronisk.

Et unntak oppstilles for opplysninger som "i lov eller i medhold av lov er underlagt taushetsplikt", jf. personopplysningsloven § 16 (d). Straffeloven § 111 pålegger advokater taushetsplikt for opplysninger betrodd dem i anledning stillingen eller oppdraget. Advokatforskriftens kapittel 12

(regler for god advokatskikk) pålegger dessuten advokater taushetsplikt også for opplysninger advokaten blir kjent med i sitt virke som advokat, selv om de ikke er omfattet av lovbestemt taushetsplikt. Begge disse taushetspliktene gir derfor unntak fra de registrertes rett til innsyn etter GDPR artikkel 15.

Det betyr i praksis at en advokatvirksomhet ikke kan gi innsyn i kopi av personopplysninger som advokaten er betrodd eller blitt kjent med i sitt virke. Altså vil GDPR artikkel 15 ikke gi en person innsynsrett i opplysninger i saksdokumenter (med mindre den registrerte er klient som privatperson).

Et annet unntak oppstilles "der det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger". Unntaket kan tenkes å være relevant for advokatvirksomhet som driver med strafferett. I slike tilfeller følger eventuelle rettigheter isteden reglene i straffeprosessloven, slik som rett til innsyn i sakens dokumenter etter straffeprosessloven § 242.

Ovennevnte innebærer at innsynsretten for advokatvirksomheter først og fremst er relevant dersom en av virksomhetens ansatte anmoder om innsyn.

Rett til korrigering (artikkel 16)

De registrerte har, på forespørsel, rett til å få uriktige personopplysninger om seg selv korrigert.

Rett til sletting (artikkel 17)

De registrerte har, på forespørsel, rett til å få personopplysninger om seg selv slettet. Denne retten gjelder kun i visse tilfeller.

Tilfelle 1
En registrert har rett til å få personopplysninger om seg slettet der hvor *opplysningene ikke lenger er nødvendige for formålet de ble samlet inn for.*

Dette er langt på vei et speilbilde av den generelle sletteplikten. Den behandlingsansvarlige skal uansett ikke lagre personopplysninger lenger enn nødvendig for formålet (uavhengig av de registrertes sletteforespørsel).

Dette betyr i praksis at det ikke er noe plikt til å etterkomme en sletteanmodning hvis virksomheten fortsatt har behov for opplysningene for det formålet de behandles for, jf. GDPR art. 17 nr. 1 (virksomhetens generelle behov for oppbevaring skal fremgå av dokumenterte sletterutiner). Tilsvarende gjelder dersom advokatvirksomheten fortsatt trenger personopplysningene for å oppfylle en rettslig forpliktelse eller for å fastsette, gjøre gjeldende eller forsvare et rettskrav, jf. GDPR art. 17 nr. 3. Altså går advokatvirksomhetens plikt eller behov for å oppbevare personopplysningene generelt foran den registrertes ønske om å få opplysningene slettet.

Tilfelle 2 (sjelden relevant)
En registrert har rett til å få personopplysninger om seg slettet der hvor opplysningene *behandles basert på et samtykke og samtykket trekkes tilbake,* med mindre advokatvirksomheten fortsatt har behov for opplysningene, typisk fordi opplysningene fortsatt er nødvendig (i) for å oppfylle en avtale med den registrerte (som personklient), (ii) for å oppfylle en rettslig forpliktelse eller (iii) for å ivareta en berettiget interesse som veier tyngre enn den registrertes personverninteresse.

Fordi samtykke sjelden vil være et aktuelt rettslig grunnlag for en advokatvirksomhet, se punkt 5, er denne retten til sletting neppe særlig aktuell.

Øvrige tilfeller
Den registrerte har også rett til å kreve sletting i enkelte andre tilfeller, som i all hovedsak ikke vil være relevante for typiske advokatvirksomheter.

8 Sikkerhet

Personvernforordningens artikkel 32 stiller krav til at egnede sikkerhetstiltak er gjennomført for å sikre personopplysninger mot blant annet uautorisert utlevering eller innsyn. Dette gjelder ikke bare personopplysninger som er *lagret* hos den behandlingsansvarlige, men også når personopplysninger *kommuniseres*.

Advokatvirksomheter bruker i stadig økende grad elektroniske virkemidler for kommunikasjon, f.eks. epost, opplasting av filer på nettbaserte portaler (som Aktørportalen) og ekstern tilkobling til arbeidsplassen.

Vi anbefaler særlig følgende tre tiltak for sikker kommunikasjon:

- Kommunikasjon av særlige kategorier personopplysninger krypteres. Kryptering kan f.eks. oppnås gjennom å bruke funksjonalitet i Outlook, eller ved isteden å gi tilgang til informasjonen ved hjelp av en nettportal som krever brukernavn og passord.
- Ekstern tilkobling til arbeidsplassen skjer ved flerfaktorautentisering ved pålogging og gjennom kryptert VPN-tunnel eller lignende sikkerhetstiltak.
- Mobilt utstyr med tilgang til virksomhetsdata slik som e-post mv. sikres særskilt og at PC, mobil, nettbrett mv. har automatisk tastelås etter kort tid.

9 Databehandleravtaler

Forholdet mellom advokatvirksomhet og klient
Personvernforordningens artikkel 28 gjelder forholdet mellom en behandlingsansvarlig og en databehandler.

Som nevnt i punkt 1 er advokatvirksomheter generelt behandlingsansvarlige. Personopplysninger behandles ikke på vegne av klienten, men på egne vegne, som ledd i utførelsen av advokatoppdraget. Det betyr at forordningens artikkel 28 generelt ikke er relevant i relasjon advokat-klient. Derfor er det normalt verken nødvendig eller riktig å inngå databehandleravtale med klient. Det kan unntaksvis tenkes situasjoner hvor dette er annerledes, f.eks. der klienten engasjerer advokatvirksomheten til å lagre informasjon (for eksempel datarom) helt uten noen tilknytning til juridisk rådgivning.

Forholdet mellom advokatvirksomhet og leverandører
Forordningens artikkel 28 er først og fremst relevant for advokatvirksomheter der de bruker leverandører, f.eks. leverandører av IT-driftstjenester. I slike tilfeller har advokatvirksomheten særlig to oppgaver:

For det første må det påses at leverandøren sikrer et vern av personopplysninger i samsvar med forordningen. Dette innebærer å vurdere om leverandørens IT-løsning gjør det mulig å etterleve forordningens regler og om informasjonssikkerheten er tilfredsstillende.

For det andre må det inngås databehandleravtale med leverandøren. Som regel vil databehandleravtalen være et vedlegg til avtalen som regulerer tjenestene.

Databehandleravtalens/databehandlervedleggets innhold skal minst svare til listen som fremgår av artikkel 28 nr. 3.

For advokatvirksomheter er det viktig at en leverandør håndterer alle opplysninger forsvarlig, uavhengig av om de er personopplysninger eller ikke. Det kan derfor være fornuftig å regulere at databehandleravtalen også skal gjelde for opplysninger som ikke er personopplysninger.

Internasjonal overføring av personopplysninger

Personvernforordningen tillater overføring av personopplysninger mellom EØS-land (forutsatt at forordningens generelle krav er oppfylt). Derimot oppstiller den som utgangspunkt et forbud mot å overføre personopplysninger ut av EØS. "Overføring" er både der informasjon blir *sendt og lagret* i et land utenfor EØS, eller der hvor personer i slike land gis *tilgang* til personopplysninger som er lagret i EØS.

I praksis betyr dette at en advokatvirksomhet som utgangspunkt ikke kan bruke leverandører i f.eks. USA eller India, eller bruke leverandører i Norge som har underleverandører i f.eks. USA eller India, med mindre det foreligger et gyldig overføringsgrunnlag. Hvis virksomheten man planlegger å overføre personopplysninger til omfattes av en av EU-kommisjonens såkalte adekvansbeslutninger, kan personopplysningene overføres uten ytterligere vurderinger knyttet til overføringsgrunnlaget. Et eksempel på en slik adekvansbeslutning er EU-US Data Privacy Framework (DPF), som innebærer at det foreligger overføringsgrunnlag for overføring til amerikanske virksomheter som er selvsertifisert i henhold til DPF. Nærmere informasjon om hvilke selskaper som er omfattet av dette programmet finnes her: https://www.dataprivacyframework.gov/list.

Dersom virksomheten man skal overføre personopplysninger til ikke omfattes av en adekvansbeslutning, er det vanlig å bruke EU-kommisjonens standardavtale for dataoverføring (EU SCC). EU SCC kan inngås mellom advokatvirksomheten i Norge og virksomheten utenfor EØS, men EU SCC har også kontraktsmoduler som kan inngås mellom f.eks. en databehandler i EØS og dennes underleverandører utenfor EØS. Et ytterligere alternativ er at virksomheten som overfører personopplysninger har etablert bindende virksomhetsregler (Binding Corporate Rules – BCR).

10 Arkivhold, tilgangsbegrensning og sletting av personopplysninger

Som behandlingsansvarlig har en advokatvirksomhet plikt til å slette personopplysninger når behandlingen ikke lenger er nødvendig for formålet som de ble samlet inn eller behandlet for, jf. GDPR artikkel 5 nr. 1 bokstav e, jf. artikkel 17 nr. 1 bokstav a. Dette betyr i praksis at virksomheten må utarbeide oppbevarings- og sletterutiner for sine behandlingsaktiviteter.

Ved praktiseringen av rutinene, er det gjerne praktisk å ta utgangspunkt i kalenderår, ikke eksakt dato. For eksempel kan man gjennomføre sletting én gang i året. Rutinene bør også angi kriteriene for tilgangsstyring, slik at personopplysningene bare er tilgjengelig for personer i virksomheten som har saklig behov for å behandle personopplysningene, noe som endre seg underveis i lagringsperioden. Virksomheten bør i rutinene innta hvem i virksomheten som er ansvarlig for at sletterutinene følges og revideres.

Sletteplikten omfatter i utgangspunktet kun "personopplysningen" og ikke dokumentet i seg selv. Dette innebærer blant annet at dersom dokumentet fullt ut er anonymisert vil virksomheten kunne oppbevare det så lenge det er ønskelig. Når det gjelder opplysninger om selskaper som klienter, som ikke inneholder personopplysninger, kan opplysningene lagres og behandles uten hensyn til GDPR. For advokatvirksomheter vil det ved praktisering av arkivhold og sletting likevel være utfordrende å

skille personopplysninger fra andre opplysninger. Det vil normalt være hensiktsmessig å praktisere dette for alle opplysninger i en sak, uten å identifisere enkeltdokumenter som inneholder personopplysninger og bare slette dem.

Dersom behandlingen er nødvendig for å oppfylle en rettslig forpliktelse i medhold av lov eller for å fastsette, gjøre gjeldende eller forsvare et rettskrav, gjelder ikke sletteplikten, jf. GDPR artikkel 5 nr. 1 bokstav e og artikkel 17 nr. 3 bokstav b. Sletteplikten må derfor ses i sammenheng med lovpålagte plikter til å oppbevare visse opplysninger, herunder eksempelvis lovpålagte oppbevaringsplikter i advokatlovgivningen, bokføringslovgivningen, hvitvaskingslovgivingen og skattelovgivningen.

Nedenfor listes det opp sentrale formål og veiledning om hvor lenge personopplysningene vil være nødvendige for de ulike formålene:

Etablering av klientforhold

Personopplysninger som er nødvendig for å etablere klientforholdet, slik som passkopi og fødsels- og personnummer innhentet for anti-hvitvaskingskontroll, bør lagres separat og slettes når virksomheten ikke lenger har plikt til å oppbevare slik dokumentasjon, jf. personopplysningsloven § 12 og hvitvaskingsloven § 30, samt hvitvaskingsforskriften § 6-3, hvor det fremgår at rapporteringspliktige advokatvirksomheter i alle fall kan lagre opplysninger og dokumenter omfattet av hvitvaskingsloven § 30 så lenge klientforholdet består.

Klientadministrasjon

På samme måte som med informasjon om hvem som har vært ansatt i virksomheten, i hvilken stilling og i hvilken periode er det naturlig av historiske og administrative årsaker at en advokatvirksomhet aldri sletter overordnede opplysninger om hvem som har vært klienter av virksomheten, i hvilket tidsrom og hva saken gjaldt.

Sakshåndtering

Formålet sakshåndtering opphører når saken er avsluttet. Dette må vurderes konkret, men i mange tilfeller kan en sak regnes som avsluttet når det har gått ett år uten aktivitet. For å sikre etterlevelse av plikten til forsvarlig arkiv, bør arkivverdige dokumenter og materiale lagres fortløpende på den aktuelle saken under sakshåndteringen. Hvorvidt dokumenter og annet materiale er arkivverdig, må vurderes ut fra f.eks. klientens behov for å kunne finne frem til bakgrunnen for en sak, og både klientens og advokatens behov for å finne ut av faktum i et erstatningskrav mot advokaten.

Kunnskapsforvaltning

Dokumentasjonen i saksarkiv bør normalt kunne være tilgjengelig for advokater som har saklig behov for å kunne gjenbruke dokumentasjonen som grunnlag for kunnskap i 10-15 år. Maldokumenter osv. som ev. er basert på tidligere saker bør ikke inneholde klientopplysninger eller personopplysninger.

Arkivhold

I henhold til advokatloven § 36 (i kraft 1. januar 2025) har advokater plikt til å holde forsvarlig arkiv over fysiske og elektroniske dokumenter som de har mottatt eller produsert i anledning advokatoppdrag. Dokumentene skal oppbevares i ti år eller lenger dersom oppdragets karakter eller dokumentenes innhold tilsier det. I utkast til ny advokatforskrift § 15 er det foreslått at kravet til oppbevaringstid ikke gjelder for dokumenter som overleveres til klienten eller som oppbevares av det offentlige.

Hensynet bak arkivplikten er å ivareta klienters og andres krav på fortrolighet, integritet og deres behov for at dokumenter i saken er tilgjengelige, samt å ivareta advokatens interesser (jf. Prop. 214 L (2020-2021), merknader til § 36). Advokatens interesser vil bl.a. være å forsvare seg mot rettskrav fra

klienten. I forslaget til ny advokatforskrift § 15 er det presisert at advokater kan oppbevare kopier dersom oppbevaringen er nødvendig for å ivareta advokatens interesser (til tross for at kravet til oppbevaringstid ikke lenger gjelder fordi dokumentene enten er overlevert klient eller oppbevart av det offentlig). Ifølge forarbeidene kan dokumentene oppbevares så lenge et av formålene bak arkivplikten gjør det nødvendig.

Klientens interesse i lagring lengre enn ti år kan f.eks. være aktuelt for dokumenter knyttet til rettslige disposisjoner som antas å få betydning utover ti år, slik som testamenter, ektepakter og langvarige kontrakter. Dessuten har klienter generelt en forventning om at advokater oppbevarer saksdokumenter i lengre tid, som et arkiv dersom det skulle vise seg relevante senere. Advokatens interesse i lagring lengre enn ti år kan særlig være aktuelt for å forsvare seg mot rettskrav eller at dokumentene kan ha betydning som bevis i rettssaker.

Ut ifra nevnte hensyn kan en nærliggende lagringstid generelt være tretti år, men kortere eller lenger avhengig av omstendighetene. En omstendighet som kan tilsi lengre oppbevaring er hvis saken gjelder rent virksomhetsmessige forhold, hvor det presumptivt ikke er opplysninger i saken som vedrører personer (utover som kontaktpersoner i korrespondanse).

Når oppbevaringen av dokumentene *kun* er begrunnet i arkivhold, og ikke de øvrige formålene som forutsetter løpende tilgang til dokumentene, bør dokumentene underlegges snever tilgangsbegrensning, som et digitalt fjernarkiv.

Illustrasjon (eksempel)

Klientopplysninger	
Formål	**Varighet**
Etablering av klientforhold (som opplysninger innhentet for anti-hvitvaskingskontroll)	I alle fall så lenge klientforholdet vedvarer
Klientadministrasjon (som klientnavn, samt navn, type og periode for saker)	Til "evig tid"

Saksopplysninger	
Formål	**Varighet**
Sakshåndtering	Så lenge saken vedvarer
Kunnskapsforvaltning	Ti år etter sak er avsluttet
Arkivhold (med snever tilgangskontroll, som et digitalt fjernarkiv)	Tretti år etter sak er avsluttet

Håndtering av personopplysninger ved opphør av ansettelsesforhold

Når en arbeidstaker/partner slutter må man være oppmerksom på at forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk materiale § 4 oppstiller enkelte særlige krav til sletting av opplysninger lagret i e-postkasse og personlige filområder på virksomhetens datanettverk, PC-er og annet elektronisk utstyr som arbeidsgiver har stilt til disposisjon til bruk i arbeidet. Sjekklisten nedenfor bør følges:

- Den ansatte bør pålegges å arkivere eller overføre virksomhetsrelaterte e-poster og filer samt slette privat innhold i e-postkassen og på personlige filområder før vedkommende slutter;
- E-postkonto og tilgang til systemer skal i utgangspunktet avsluttes straks arbeidsforholdet opphører; og

- Det bør benyttes fraværsmelding med beskjed om at arbeidsforholdet er avsluttet samt informasjon om hvem som kan kontaktes.

Dersom virksomhetsrelatert innhold i e-postkassen har blitt sortert ut før arbeidsforholdet opphørte, skal e-postkassen og sikkerhetskopier av denne slettes innen rimelig tid etter at arbeidsforholdet opphørte.

11 Personvernombud

Etter personvernforordningen har visse typer av private virksomheter plikt til å ut utpeke et personvernombud. Ombudet skal være en person med dybdekunnskap om personvernlovgivning og -praksis som skal bistå virksomheten med å føre tilsyn med den interne overholdelsen av forordningen. Etter personvernforordningen artikkel 37 skal private virksomheter utpeke personvernombud hvis:

- virksomhetens hovedvirksomhet består i å behandle personopplysninger på en måte som innebærer regelmessig og systematisk overvåkning av personer i stor skala, eller
- virksomhetens hovedvirksomhet består i å behandle særlige kategorier personopplysninger eller personopplysninger knyttet til straffedommer og straffbare forhold i stor skala.

Advokatvirksomheter som driver ordinær advokatvirksomhet faller i utgangspunktet utenfor kretsen av virksomheter som må utpeke personvernombud. Dette har særlig sammenheng med at advokatvirksomheters hovedvirksomhet normalt ikke består i verken å overvåke personer eller behandle særlige kategorier personopplysninger. Enkelte typer advokatvirksomheter vil imidlertid kunne omfattes av kravet etter artikkel 37, eksempelvis større advokatvirksomheter som hovedsakelig driver innenfor strafferetten, personskaderetten eller på annen måte driver virksomhet som faller inn under vilkårene ovenfor. Advokatvirksomheter bør derfor uansett vurdere hvorvidt et personvernombud bør utpekes eller ikke (og vurderingen bør være skriftlig og grunngitt).

Dersom det ikke foreligger en plikt til å utpeke et personvernombud, vil det likevel være en fordel om virksomheten oppnevner en i virksomheten som gis et overordnet ansvar for oppfølging av personvern i advokatvirksomheten.

12 Vurdering av personvernkonsekvenser (DPIA)

Personvernforordningen artikkel 35 oppstiller en plikt for behandlingsansvarlig til å gjennomføre en vurdering av personvernkonsekvenser (data protection impact assessement, DPIA) dersom den aktuelle behandlingen vil medføre en "høy risiko for fysiske personers rettigheter" tatt i betraktning behandlingens "art, omfang, formål og sammenheng".

En vurdering av personvernkonsekvenser skal ifølge artikkel 35 nr. 3 særlig være nødvendig i følgende tilfeller:

a) "En systematisk og omfattende vurdering av personlige aspekter ved fysiske personer som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for den fysiske personen eller på lignende måte i betydelig grad påvirker den fysiske personen,
b) behandling i stor skala av særlige kategorier av opplysninger som nevnt i artikkel 9 nr. 1, eller av personopplysninger om straffedommer og lovovertredelser som nevnt i artikkel 10, eller
c) en systematisk overvåking i stor skala av et offentlig tilgjengelig område."

Alternativene a) og c) vil sjelden være aktuelle for advokatvirksomheters behandling av personopplysninger. Når det gjelder alternativ b) er det er spørsmål om advokatvirksomheter med omfattende praksis innen områder som strafferett, personskade, forsikring eller arbeidsrett hvor det behandles slike særlige kategorier av opplysninger omfattes av plikten til å gjennomføre DPIA.

Dersom virksomheten konkluderer med at det er krav om DPIA, eller det er ønskelig å gjøre dette av forsiktighetsgrunner, må DPIA-en tilfredsstille forordningens krav til innhold. En DPIA skal minst inneholde:

a) en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen, herunder, dersom det er relevant, den berettigede interessen som forfølges av den behandlingsansvarlige,
b) en vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene,
c) en vurdering av risikoene for de registrertes rettigheter og friheter, og
d) de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysninger og for å påvise forordning overholdes, idet det tas hensyn til de registrertes og andre berørte personers rettigheter og berettigede interesser.

Forordningen oppstiller ikke nærmere formkrav til DPIA. For en advokatvirksomhet vil det være nærliggende i en DPIA å legge stor vekt på krav til forsvarlig informasjonshåndtering, informasjonssikkerhet og overholdelse av taushetsplikt. Dette er aspekter som vil være sentrale i en risikovurdering av informasjonssikkerhet. I praksis vil en tradisjonell informasjonssikkerhetsvurdering i mange tilfeller kunne utvides til å tilfredsstille krav til DPIA. Hovedforskjellen er at en DPIA ikke utelukkende fokuserer på aspekter knyttet til informasjonssikkerhet, men har som mål å identifisere hvordan behandlingen griper inn i personvernet og hvilke tiltak som bør på plass for å bøte på personvernulempene.

13 Markedsføring

Markedsføring innebærer ofte behandling av personopplysninger, for eksempel ved utsendelse av nyhetsbrev (e-postadresse). Dette er en egen behandling, som forutsetter at advokatvirksomheten har et behandlingsgrunnlag.

Det er kun nødvendig med samtykke, dersom advokatvirksomheten ikke har et annet behandlingsgrunnlag. I veilederens kapittel 5 fremgår det at GDPR artikkel 6 nr. 1 bokstav f «interesseavveining» er et aktuelt behandlingsgrunnlag for markedsføring av advokatvirksomhetens varer og tjenester.

I tillegg til å ha behandlingsgrunnlag etter GDPR, er det imidlertid viktig å også huske på de praktisk viktige begrensningene som følger av markedsføringsloven.

I markedsføringsloven § 15 er hovedregelen at det er forbudt å sende markedsføringshenvendelser per e-post eller andre elektroniske kommunikasjonsmetoder til fysiske personer uten forutgående samtykke. Henvendelse per brev eller telefon er ikke omfattet av kravet til forhåndssamtykke i § 15.

En markedsføringshenvendelse omfatter alle henvendelser som tar sikte på å fremme salget av advokatfirmaets varer eller tjenester, direkte eller indirekte, for eksempel også deltakelse i konkurranser eller utsendelse av nyhetsbrev.

At forbudet gjelder fysiske personer betyr at henvendelser ikke kan sendes til for eksempel fornavn.etternavn@firma.no. Forbudet gjelder imidlertid ikke juridiske personer, og dermed ikke adresser som post@firma.no.

Dersom forhåndssamtykke ikke er innhentet, kan man likevel, på nærmere vilkår, sende markedsføringshenvendelser i eksisterende kundeforhold. Slik markedsføring kan bare gjelde den næringsdrivendes egne varer, tjenester eller andre ytelser (ytelser er en fellesbetegnelse på varer, tjenester, fast eiendom, rettigheter og forpliktelser, jf. legaldefinisjonen i mfl. § 5(1)c) tilsvarende dem som kundeforholdet bygger på.

Det er altså fire kumulative vilkår: For det første må det være et *eksisterende kundeforhold*. For det andre må markedsføringen gjelde *egne* varer og tjenester eller andre ytelser. For det tredje må disse være *tilsvarende* dem som kundeforholdet bygger på. For det fjerde må man gi kunden mulighet til å *reservere seg* både ved innsamlingen av e-postadressen og ved hver enkelt utsendelse.

Dersom man ønsker å rette en markedsføringshenvendelse til fysiske personer hos en selskapsklient (eksisterende kundeforhold), må man for eksempel foreta en vurdering av om markedsføringen gjelder varer, tjenester eller andre ytelser som er tilsvarende dem klientens kundeforhold allerede bygger på.

Advokatvirksomheter bør sørge for at oppdragsbekreftelsen dekker det behovet man har for kommunikasjon med klienten utover selve rådgivningen, herunder forhåndssamtykke til eventuell markedsføring. Det må i så fall gå klart frem hvilke ytelser samtykket omfatter, hvor ofte det vil rettes markedsføringshenvendelser til kunden, samt at det er frivillig å avgi samtykke. Samtykket må være en aktiv handling og kan ikke avgis passivt. Det er ikke anledning til å gjøre samtykke til markedsføring til et kontraheringsvilkår. Dette vil antakelig være urimelig og i strid med markedsføringsloven, jf. Ot.prp. nr. 62 (1999-2000), s. 24.