



ADVOKATFORENINGEN

Advokatforeningens veileder om advokatvirksomheters etterlevelse av GDPR

Thomas Olsen, Rune Opdahl, Christopher Sparre-Enger Clausen

Innhold

1	Introduksjon om personvern i advokatvirksomheter - GDPR	3
2	Dokumentasjon for å kunne påvise etterlevelse.....	5
3	Kartlegging av personopplysninger	7
4	Formålsbegrensninger	9
5	Behandlingsgrunnlag	10
6	Informasjon	14
7	De registrertes rettigheter	16
8	Sikkerhet.....	18
9	Databehandleravtaler.....	19
10	Sletting av personopplysninger	21
11	Personvernrådgiver	22
12	Vurdering av personvernkonsekvenser (DPIA).....	23
13	Markedsføring	25
14	Innsyn i ansattes e-postkasse mv.	26

1 INTRODUKSJON OM PERSONVERN I ADVOKATVIRKSOMHETER - GDPR

Den 25. mai 2018 får EUs personvernforordning, [General Data Protection Regulation 2016/679](#) (GDPR), virkning. Forordningen vil bli innført i norsk rett gjennom henvisning i ny personopplysningslov, som vil erstatte dagens lov. Det er antatt at dette skjer samtidig. I tillegg til å gjøre personvernforordningen til norsk lov, vil den nye personopplysningsloven inneholde utfyllende særnorske regler, blant annet regler om behandling av personopplysninger i arbeidslivet. Den 6. juli 2017 ble slik ny personopplysningslov sendt på [høring](#). Advokatforeningen innga høringsvar, som tok opp særlige problemstillinger ved behandling av personopplysninger i advokatvirksomhet.

Personvernforordningen er dels en videreføring, dels en modernisering, og dels en skjerping av eksisterende personvernregelverk. Selv om mange av reglene i personvernforordningen også finnes i dagens lovgivning, har det økte sanksjonsnivået medført økt bevissthet omkring etterlevelse av regelverket.

All advokatvirksomhet vil være underlagt personopplysningsloven – og dermed personvernforordningen fra og med 25. mai 2018. Dette gjelder uavhengig av størrelse og rettsområde. Kravet til personvernrutiner vil likevel kunne tilpasses virksomhetens art. 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.

Formålet med denne veilederen

Denne veilederen forklarer hvordan store og små advokatvirksomheter kan forberede seg til personvernforordningen frem mot 25. mai 2018 og – ikke minst – etterleve forordningen deretter. Selv om dette ikke er noen uttømmende oversikt over forordningens krav, vil det å følge disse rådene være et godt utgangspunkt for å etablere et personvern i samsvar med forordningen.

2 DOKUMENTASJON FOR Å KUNNE PÅVISE ETTERLEVELSE

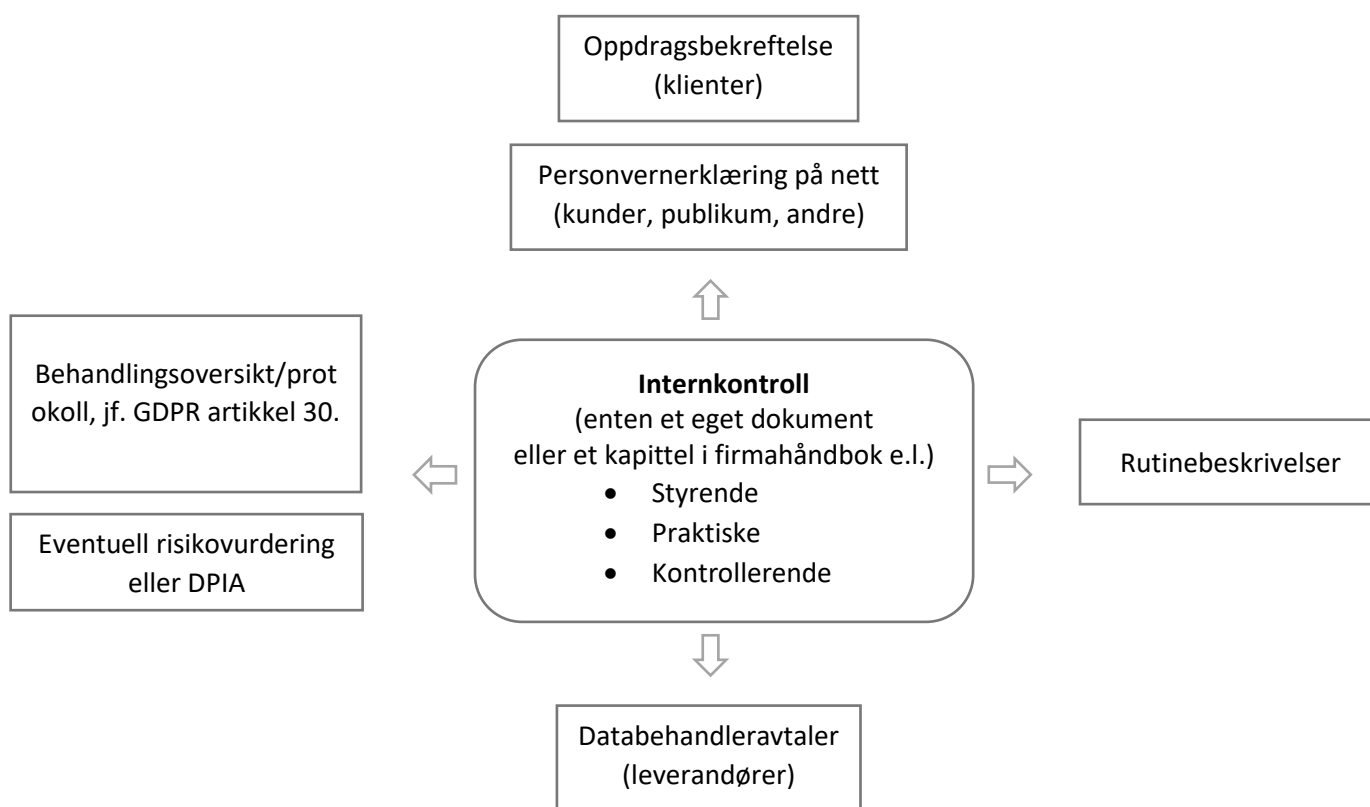
Personvernforordningen oppstiller i artikkel 5 nr. 2 et generelt prinsipp om at den behandlingsansvarlige skal kunne "påvise" at forordningens prinsipper etterleveres. Dette betyr i praksis at virksomheten må ha på plass intern dokumentasjon som viser at virksomheten har oversikt over egen behandling av personopplysninger og rutiner og systemer som sikrer at personvernreglene følges i praksis.

I tillegg til det generelle prinsippet i artikkel 5, oppstiller forordningen 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).

Personvernforordningen gir lite veiledning i hvor detaljert dokumentasjon virksomheten må ha på plass for å etterleve kravet til å påvise etterlevelse. Mens det etter personopplysningsloven av 2001 og Datatilsynets praksis har vært krav om nokså omfattende dokumentasjon, antas det at personvernforordningen gir større rom for å tilpasse dokumentasjonen avhengig av behandlingens art og omfang. Det er, som nevnt ovenfor, forskjell på større advokatvirksomheter som driver med strafferett eller pasientskaderett og mindre advokatvirksomheter som driver med forretningsjus. Etter artikkel 24 skal tiltakene stå i forhold til personvernrisikoen. Forordningen åpner for at det i noen tilfeller ikke kreves særskilte rutiner og retningslinjer for personvern (jf. artikkel 24 nr. 2).

Advokatforeningen anbefaler imidlertid at alle advokatvirksomheter etablerer personverndokumentasjon.

For de fleste advokatvirksomheter vil det være hensiktsmessig å operere med to hovedkategorier av personverndokumentasjon som angitt nedenfor.



A. Intern dokumentasjon ("internkontroll")

I Datatilsynet veiledning og praksis etter tidligere regelverk 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 mange virksomheter 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 personvern. Dersom virksomheten er av en viss størrelse bør det også vurderes å utpeke ansvarlige for 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:

- Personverngjennomgang før endring eller iverksetting av nye behandlingsaktiviteter.
- Rutiner knyttet til håndtering av klient og ansattopplysninger.
- 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. Ekstern dokumentasjon

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 KARTLEGGING AV PERSONOPPLYSNINGER

Formålet med kartleggingen

Ett første skritt for å sikre etterlevelse av personvernregelverket er å kartlegge virksomhetens behandlinger. Formålet med kartleggingen vil ofte være tredelt:

- 1) Gjennom kartleggingen får virksomheten en oversikt over behandlingsaktiviteter og et grunnlag for å vurdere evt. avvik fra regelverket og relevante oppfølgingstiltak. Med «behandlingsaktivitet» menes ikke *hver ny sak* en advokat jobber med, men hver arbeidsprosess, for eksempel klientadministrasjon, sakshåndtering generelt, markedsføring mv.
- 2) Resultatene fra kartleggingen vil gi grunnlag for å vedlikeholde protokoll over behandlingsaktiviteter etter artikkel 30 som er sentral dokumentasjon som Datatilsynet kan kreve utlevert
- 3) Mange virksomheter anser det også hensiktsmessig å vedlikeholde en oversikt over behandlinger med informasjon utover det som er påkrevet etter artikkel 30. Oversikten kan da tjene som støtte for virksomhetens interne arbeid, men også som dokumentasjon overfor Datatilsynet for å kunne påvise etterlevelse av personvernreglene. Disse ekstra kolonnene kan evt. fjernes dersom det kun er informasjonen etter artikkel 30 det er ønskelig å dele med tilsynsmyndigheten eller andre.

Gjennomføring av kartleggingen

Kartleggingen av virksomhetens behandling kan gjennomføres på flere måter. For mange kan det være hensiktsmessig å benytte en tabell i word, [excel](#) eller annet støtteverktøy som tar utgangspunkt i de elementene som er påkrevet etter artikkel 30.

For å få presise svar, fordrer kartleggingen at de personer som kjenner virksomhetens ulike prosesser knyttet til behandlingen involveres. Med litt veiledning kan man forsøke å få relevante miljøer som behandler personopplysninger til å svare på spørsmålene på egen hånd. Erfaringsmessig får man imidlertid best resultat dersom noen med kjennskap til personvernregelverket gjennomfører møter/intervjuer med relevante nøkkelpersoner.

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

- Navn og kontaktinformasjon (og navn og kontaktinformasjon 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).

For advokatvirksomheter vil det som regel være relevant å sondre mellom følgende sentrale behandlinger av personopplysninger. Hver virksomhet må vurdere om kategoriene nedenfor må deles opp enda mer. Det avgjørende er at svarene kommer godt nok frem:

- Sakshåndtering.
- Kunnskapsforvaltning (f.eks. gjenbruk av dokumenter i senere saker).
- Lagring av saksdokumenter.
- Klientadministrasjon.
- Markedsføring.
- Fakturering.
- Sikkerhetsformål (f.eks. logger på servere, avdekking, oppklaring og oppfølging av sikkerhetshendelser).

Det kan reises spørsmål ved om advokatvirksomheter må føre slik protokoll over kartleggingen som beskrevet ovenfor, ettersom det gjelder et unntak for virksomheter med færre enn 250 ansatte, jf. GDPR artikkel 30 nr. 5. Vi anbefaler likevel at alle advokatvirksomheter fører slik protokoll. Det gjelder nemlig så mange unntak fra unntaket for virksomheter med færre enn 250 ansatte, som gjør at de aller fleste likevel må føre protokoll. Det gjelder for eksempel hvis virksomheten behandler personopplysninger som kan medføre risiko for de registrertes rettigheter og denne behandlingen ikke kun skjer leilighetsvis, eller hvis behandlingen omfatter særlige kategorier av personopplysninger, eller hvis man behandler personopplysninger om straffedømme og straffbare forhold.

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 kategorier av formål for advokatvirksomhet kan være:

- Sakshåndtering
- Kunnskapsforvaltning (f.eks. gjenbruk av dokumenter i senere saker)
- Etablering av klientforhold
- Klientadministrasjon
- Informasjon om motparter og andre tredjeparter
- Potensielle kunder/klienter
- Markedsføring
- Administrasjon av ansatte, herunder HR, personal og informasjon om ansatte etter opphør av arbeidsforholdet
- Fakturering
- Sikkerhet (f.eks. logger på servere, avdekking, oppklaring og oppfølging av sikkerhetshendelser)

Listen er ikke uttømmende. Vi ønsker ikke å forsøke å utarbeide en standardformulering for disse formålene. Det er viktig at man selv gjør denne øvelsen og på den måten har et bevisst forhold til hva som er formålet med behandlingen.

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

- Samtykke
- Hjemmel i unionsretten
- Nasjonal lovhjemmel
- Forenlighetsvurdering

Det er særlig viderebehandling på grunnlag av *samtykke* eller en *forenlighetsvurdering* som er relevant for advokatvirksomhet. GDPR stiller opp en rekke momenter som skal tas hensyn til ved en slik forenlighetsvurdering, jf. GDPR art. 6 nr. 4:

- Enhver forbindelse mellom formålene som personopplysningene er blitt samlet inn for, og formålene med den tiltenkte viderebehandlingen.
- I hvilken sammenheng personopplysningene har blitt samlet inn, særlig med hensyn til forholdet mellom de registrerte og den behandlingsansvarlige.
- Personopplysningenes art, særlig om særlige kategorier personopplysninger («sensitive personopplysninger») behandles, eller om personopplysninger om straffedømmer og straffbare forhold behandles.
- De mulige konsekvensene av den tiltenkte viderebehandlingen for den registrerte.
- Om det foreligger nødvendige garantier, for eksempel kryptering, anonymisering eller pseudonymisering

Et eksempel på et uforenlig formål, er saksforholdet i Rt. 2013 s. 143. En sjåfør hadde blitt sagt opp på grunn av avvik mellom timelistene han hadde levert og bilens elektroniske logg. Formålet med den elektroniske loggen av bilen, var flåtestyring. Det var uforenlig å bruke denne informasjonen til personalmessig oppfølging/kontroll av ansatte. Dette skyldtes at de ansatte ikke var informert om muligheten for slik etterfølgende bruk.

5 BEHANDLINGSGRUNNLAG

Innledning

All behandling personopplysninger må ha et behandlingsgrunnlag. GDPR viderefører i stor grad reglene som gjelder i dag.

Det alminnelige kravet til rettslig grunnlag følger av GDPR artikkel 6. I tillegg er det et krav til særlig rettslig grunnlag for behandling av sensitive personopplysninger i GDPR artikkel 9.

Det rettslige grunnlaget må være oppfylt *før* behandlingen av personopplysninger begynner.

Advokatvirksomheter vil som den klare hovedregel være behandlingsansvarlig ved behandling av personopplysninger i tilknytning til advokatvirksomheten, og må da påse at det foreligger et behandlingsgrunnlag. I tilfeller hvor det er avklart at advokatvirksomheten skal opptre som databehandler, vil det være databehandleravtalen med behandlingsansvarlig oppdragsgiver som gir grunnlaget for behandlingen.

Rettslig grunnlag for advokaters behandling av personopplysninger

I tabellen nedenfor har vi gitt en oversikt over hvilke behandlingsgrunnlag som er mest aktuelle for noen typiske behandlingsaktiviteter for advokatvirksomhet:

Behandlingsaktivitet	Behandlingsgrunnlag alminnelige personopplysninger	Behandlingsgrunnlag sensitive personopplysninger
Etablering av klientforhold	GDPR artikkel. 6 nr. 1 bokstav a (samtykke fra den registrerte) GDPR artikkel. 6 nr. 1 bokstav b (avtale med privatklienten) GDPR artikkel. 6 nr. 1 bokstav c (oppfylle rettslig forpliktelse, f.eks: <ul style="list-style-type: none"> • hvitvaskingsloven §§ 4 (2) nr. 3, jf. 17 og 18) GDPR artikkel. 6 nr. 1 bokstav e (allmennhetens interesse)	GDPR artikkel. 9 nr. 2 bokstav a (samtykke fra den registrerte) GDPR artikkel. 9 nr. 2 bokstav b (avtale med privatklienten) GDPR artikkel. 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav)
Sakshåndtering	GDPR artikkel. 6 nr. 1 bokstav f (interesseavveining) GDPR artikkel. 6 nr. 1 bokstav a (samtykke fra den registrerte)	GDPR artikkel. 9 nr. 2 bokstav a (samtykke fra den registrerte) GDPR artikkel. 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav) GDPR artikkel. 9 nr. 2 bokstav e (opplysninger offentliggjort av den registrerte)
Kunnskapsforvaltning (f.eks. gjenbruk av dokumenter i senere saker)	GDPR artikkel. 6 nr. 1 bokstav f (interesseavveining)	Bør ikke inneholde sensitive personopplysninger. GDPR artikkel. 9 nr. 2 bokstav a (samtykke fra den registrerte)

		GDPR artikkel. 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav)
Lagring/oppbevaring av saksdokumenter	<p>GDPR artikkel. 6 nr. 1 bokstav b (avtale med privatklienten)</p> <p>GDPR artikkel. 6 nr. 1 bokstav f (interesseavveining)</p> <p>GDPR artikkel. 6 nr. 1 bokstav c (oppfylle rettslig forpliktelse, f.eks: <ul style="list-style-type: none"> • hvitvaskingsloven §§ 4 (2) nr. 3, jf. 17 og 18) </p>	<p>GDPR artikkel. 9 nr. 2 bokstav a (samtykke fra den registrerte)</p> <p>GDPR artikkel. 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav)</p> <p>GDPR artikkel. 9 nr. 2 bokstav e (opplysninger offentliggjort av den registrerte)</p>
Klientadministrasjon	<p>GDPR artikkel. 6 nr. 1 bokstav b (avtale med privatklienten)</p> <p>GDPR artikkel. 6 nr. 1 bokstav f (interesseavveining)</p>	GDPR artikkel. 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav)
Markedsføring	<p>GDPR artikkel. 6 nr. 1 bokstav a (samtykke fra den registrerte)</p> <p>GDPR artikkel. 6 nr. 1 bokstav f (interesseavveining)</p>	
Administrasjon av ansatte	<p>GDPR artikkel. 6 nr. 1 bokstav b (avtale med den ansatte)</p> <p>GDPR artikkel. 6 nr. 1 bokstav c (oppfylle rettslig forpliktelse)</p> <p>GDPR artikkel. 6 nr. 1 bokstav f (interesseavveining)</p> <p>GDPR artikkel. 6 nr. 1 bokstav a (samtykke fra den registrerte, forutsatt reell frivillighet)</p>	GDPR artikkel. 9 nr. 2 bokstav b
Fakturering	<p>GDPR artikkel. 6 nr. 1 bokstav b (avtale med privatklienten)</p> <p>GDPR artikkel. 6 nr. 1 bokstav c (oppfylle rettslig forpliktelse)</p> <p>GDPR artikkel. 6 nr. 1 bokstav f (interesseavveining)</p>	GDPR artikkel. 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav)
Sikkerhet (f.eks. logger på servere, avdekking, oppklaring og oppfølging av sikkerhetshendelser)	<p>GDPR artikkel. 6 nr. 1 bokstav c (oppfylle rettslig forpliktelse)</p> <p>GDPR artikkel. 6 nr. 1 bokstav f (interesseavveining)</p>	GDPR artikkel. 9 nr. 2 bokstav f (fastsette, gjøre gjeldende eller forsvare rettskrav)

Tabellen over viser at det kan være flere behandlingsgrunnlag som kan være aktuelle for en og samme behandling. Hva som er det mest egnede behandlingsgrunnlaget må vurderes konkret, og i enkelte tilfeller vil man se at grunnlagene ikke passer så godt for advokatvirksomhet. Foreløpig er dette ikke blitt problematisert av Datatilsynet.

I Advokatforeningens høringsuttalelse til ny personopplysningslov er det etterspurt lovgivning som gir et klarere rettslig grunnlag for advokaters behandling av personopplysninger:

«I tillegg til behandling av opplysninger om klient i medhold av avtale eller samtykke, anser Advokatforeningen at det er grunnlagene i artikkel 6 nr. 1 c) ("nødvendig for å oppfylle rettslig forpliktelse") og e) ("utføre en oppgave i allmenhetens interesse") samt artikkel 9 nr. 2 f) ("fastsette, gjøre gjeldende og forsvare rettskrav") og g) "viktige samfunnsinteresser", som de mest relevante for advokatvirksomhet.

Etter Advokatforeningens syn vil utfyllende regler inntatt i ny advokatlov innenfor rammene artikkel 9 nr. 2 g), være den foretrukne løsningen med størst klarhet og forutsigbarhet for advokatstanden og de berørte registrerte. Slike regler må ifølge bestemmelsen stå i forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger, og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettighet og interesser.»

Nedenfor knytter vi noen særlige bemerkninger til de mest relevante behandlingsgrunnlagene.

Samtykke (GDPR art. 6 nr. 1 bokstav a) som behandlingsgrunnlag vil være dårlig egnet for advokatvirksomhet, blant annet fordi samtykke må innhentes direkte fra den registrerte og når som helst kan trekkes tilbake. Det stilles også strenge krav til at samtykket er reelt frivillig. Det betyr at dersom avtaleforholdet ikke kommer i stand uten den aktuelle behandlingen av personopplysninger, kan ikke samtykke være grunnlaget, men avtale.

Avtale kan være et viktig behandlingsgrunnlag for advokaters behandling av personopplysninger, men dette vil i praksis være begrenset til behandling som er nødvendig for å oppfylle avtale med privatklienter, jf. GDPR artikkel 6 nr. 1 bokstav b.

Dersom *lov* skal benyttes som rettslig grunnlag må loven gi direkte hjemmel til å behandle opplysninger eller klart forutsette dette. Det er nok ikke aktuelt å bruke lov som behandlingsgrunnlag før det eventuelt vedtas en egen advokatlov som regulerer dette. For advokater med rapporteringsplikt etter hvitvaskingsloven, er imidlertid behandlingsgrunnlaget lov når det gjelder behandling i denne sammenhengen, jf. hvitvaskingsloven § 4 annet ledd nr. 3.

For å benytte behandlingsgrunnlaget i GDPR artikkel 6 nr. 1 bokstav c og e – altså om oppfyllelse av *rettslig forpliktelser* og oppgaver i *allmenhetens interesse* – krever GDPR eksplisitt hjemmel i nasjonal lovgivning, og det finnes i liten grad slike rettslige grunnlag i dag. Reglene om hvitvasking er et eksempel.

I mangel av andre rettslige grunnlag vil det nok være mest naturlig å falle tilbake på GDPR artikkel 6 nr. 1 bokstav f, altså at behandlingen er nødvendig for formål knyttet til de berettigede interessene som den behandlingsansvarlige forfølger.

Når det gjelder sensitive personopplysninger er det sentrale behandlingsgrunnlaget GDPR artikkel 9 nr. 2 bokstav f "fastsette, gjøre gjeldende og forsvare rettskrav" og bokstav g "viktige samfunnsinteresser". Som det fremgår av tabellen ovenfor vil også andre grunnlag være aktuelle.

Særlig om behandling av personopplysninger om straffedommer og lovovertridelser

En særlig problemstilling er hvilket behandlingsgrunnlag som gjelder for behandling av personopplysninger om straffedommer og lovovertridelser. I gjeldende regelverk er dette kategorisert som sensitive personopplysninger (personopplysningsloven § 2 nr. 8, mens etter GDPR reguleres dette særskilt i artikkel 10).

Artikkel 10 lyder:

Behandling av personopplysninger om straffedommer og lovovertridelser eller tilknyttede sikkerhetstiltak på grunnlag av artikkel 6 nr. 1 skal bare utføres under en offentlig myndighets kontroll eller dersom behandlingen er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett som sikrer egnet vern av de registrertes rettigheter og friheter. Alle omfattende registre over straffedommer må bare føres under en offentlig myndighets kontroll.

Det er ikke klart etter bestemmelsen eller forordningen for øvrig hvilke opplysninger som omfattes av ordlyden i bestemmelsen, men det omfatter i alle fall behandling av personopplysninger om fellende straffedommer (dvs. informasjon om at en person er straffedømt). Dette er opplysninger som strafferettsadvokater vil behandle i stor utstrekning.

Som det følger av bestemmelsen, kan slike personopplysninger kun behandles av en offentlig myndighet eller "dersom behandlingen er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett som sikrer egnet vern av de registrertes rettigheter og friheter". Advokater vil ikke være under offentlig myndighet. Det må altså foreligge en klar lovhjemmel for behandling av personopplysninger om straffedommer, og som gir tilstrekkelig sikkerhet for at personopplysningene behandles på en måte som ivaretar interessene og rettighetene til de registrerte.

Det kan ikke være noen tvil om at strafferettsadvokater skal kunne behandle slike personopplysninger – det følger av vårt rettssystem og av straffeprosesslovens system. I tillegg sikrer reglene om straff for brudd på taushetsplikt i straffeloven § 211 og reglene for god advokatskikk punkt 2.3 om fortrolighet noe sikkerhet for at opplysningene behandles på en måte som ivaretar de registrerte. Det er imidlertid tvilsomt om disse reglene er tilstrekkelige etter GDPR, ettersom de ikke regulerer rettighetene til de registrerte, men kun pliktene til advokater. Det mangler altså en klar hjemmel som gir advokater rett til å behandle personopplysninger om straffedommer. Vi mener at dette er en lovteknisk utfordring som lovgiver må løse. Frem til det gjøres må advokatvirksomheter kunne fortsette å behandle slike personopplysninger ut fra en systembetragtning.

6 INFORMASJON

Generelt

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 artikkel 13- og artikkel 14-informasjon gis samlet. Artikkel 12 inneholder enkelte fellesregler for hvordan informasjonen skal gis. Artikkel 23 åpner for visse unntak fra informasjonsplikten.

Hvordan informasjon kan gis og hvem den skal gis til

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).

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 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. Imidlertid anbefaler vi at personvernerklæringen på en nettside inneholder informasjon som også er adressert til disse kategoriene.

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. Dette kan f.eks. gjøres med innhold etter følgende innhold/overskrifter:

- Virksomhetens fulle navn og kontaktinformasjon.
- Hva slags personopplysninger virksomheten behandler.
- Hvilke formål virksomheten bruker personopplysningene.
- Hva er det [rettslige grunnlaget](#) for virksomhetens behandling av personopplysninger. Hvis behandlingen er basert på *interesseavveiningen* iht. forordningens artikkel 6 nr. 1 bokstav f), hva er vår berettigede interesse.
- Hvem utleverer virksomheten eventuelt personopplysninger til (f.eks. leverandører, motparter, domstoler, offentlige organer)
- Hvorvidt personopplysninger blir [overført til tredjestater](#) (f.eks. til leverandør i USA eller India) og hva som er overføringsgrunnlaget (f.eks. EUs standardavtale for overføring)
- Hvor lenge lagres personopplysningene, eller dersom dette ikke er mulig, kriteriene for å fastsette lagringstid.
- Hvilke [rettigheter](#) har den registrerte (innsyn, korrigering, sletting, begrensning, protestere, rett til å klage til Datatilsynet).

Personvernerklæringen bør også oppgi datoen den sist ble endret/oppdatert og hva denne oppdateringen gjaldt.

Måten informasjonen skal formuleres på

Personverninformasjonen skal gis på en kortfattet, åpen og forståelig måte, med et klart og enkelt språk. Her er tre tips:

- Unngår juridiske ord og uttrykk som ikke er dagligtale. Skriv for eksempel "som" istedenfor "herunder".
- Unngå bruk av betingende/modifiserende. Skriv for eksempel "vi utleverer personopplysninger til ..." istedenfor "vi vil kunne utlevere personopplysninger til ...".
- Bruke aktivt istedenfor passivt språk. Skriv for eksempel "vi vil samle inn navn og kontaktinformasjon" istedenfor "det vil samles inn navn og kontaktinformasjon".
- Unngå nominalisering. Skriv "Vi gjennomgår..." istedenfor "vi gjør en gjennomgang...".

7 DE REGISTRERTES RETTIGHETER

GDPR kapittel 3 gir de registrerte en rekke rettigheter. Flere av disse rettighetene finnes også i eksisterende personopplysningslov, men noen er nye.

Oppfyllelse av disse påhviler først og fremst den behandlingsansvarlige. Imidlertid vil databehandlerens bistand ofte være påkrevd. 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. I departementets forslag til ny personopplysningslov er visse unntak foreslått. Vi legger i denne veiledningen til grunn at de unntakene blir vedtatt som lov.

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 behandlingens ansvarliges 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. forslag til ny personopplysningslov § 13. 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 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 korrigerings (artikkel 16)

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

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 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 aktuelt.

Øvrige tilfeller

Den registrerte har også rett til 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 sensitive 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 gjennom kryptert VPN-tunnel eller lignende sikkerhetstiltak.
- Mobilt utstyr med jobb-epost har automatisk tastelås etter kort tid.

Se også Advokatforeningens tidligere rådgivning om sikkerhet og advokaters bruk av IKT-verktøy: <https://www.advokatforeningen.no/radgivning/oppstart-drift-og-avvikling/advokaters-bruk-av-moderne-teknologi/>

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. dersom klienten engasjerer advokat for å utføre konkrete dataprosesserings-oppdrag, f.eks. å loggføre rettighetskrenkelsers på Internett.

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 å kunne dokumentere at man har gjort et forsvarlig valg av leverandør bør det fremgå at følgende forhold er kartlagt/vurdert: Dokumentasjon om hvordan tjenesten fungerer, leverandørens sikkerhetsdokumentasjon, revisjonsrapporter, om leverandøren bruker underleverandører og om leverandøren overfører opplysninger ut av EU. I mange tilfeller vil det være nødvendig å stille oppfølgingsspørsmål til leverandøren for å få avklaring på disse spørsmålene.

Forordningen oppstiller ikke uttrykkelige krav til risikovurdering. Krav til risikovurdering følger imidlertid indirekte av artikkel 28 om at behandlingsansvarlig bare kan benytte databehandlere som sikrer etterlevelse av forordningen samt artikkel 32 om at sikkerhetsnivået må være tilpasset risikoen ved behandlingen. Hvor omfattende en risikovurdering skal være, må vurderes konkret. Det er grunn til å være særlig oppmerksom dersom man behandler sensitive personopplysninger, andre særlig fortrolige opplysninger, eller har privatklienter. Risikovurderingen bør angi akseptabel risiko mht. konfidensialitet (hindre uvedkommende tilgang), integritet (hindre uautorisert endring) og tilgjengelighet (robusthet, oppetid, backup-løsning mv.). Videre bør vurderingen inneholde en kartlegging av sannsynlighet og risiko for uønskede hendelser samt tiltak for å sikre at risikoen er innenfor det akseptable.

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. Dette kan f.eks. gjøres med innhold etter følgende innhold/overskrifter:

- Bakgrunn/formål (bl.a. forholdet til hovedavtalen)
- Formålet med og arten av behandlingen, og typer personopplysninger og typer registrerte behandlingen gjelder (dette inntas gjerne som vedlegg til databehandleravtalen)
- Databehandlerens plikter (bl.a. at personopplysninger ikke skal brukes til andre formål enn for å utføre tjenesten)
- Bistand til den behandlingsansvarlige (bl.a. at databehandleren skal bistå den behandlingsansvarlige i å overholde sine forpliktelser etter forordningens artikkel 32-36)
- Informasjonssikkerhet (bl.a. at databehandleren skal gjennomføre sikkerhetstiltak i henhold til forordningens artikkel 32, som tiltak for å sikre opplysningens konfidensialitet)

- Bruk av underleverandører (enten at hver og en underleverandør skal forhåndsgodkjennes, eller at bruk av underleverandører generelt aksepteres mot at databehandleren orienterer om endringer og gir den behandlingsansvarlige rett til å motsette seg endringen).
- Overføring av personopplysninger til tredjestater (for eksempel at dette ikke skal forekomme, eller at det kun skal skje på den behandlingsansvarliges instruksjoner).
- Brudd på personopplysningsikkerheten (bl.a. databehandlerens plikt til å varsle den behandlingsansvarlige ved eventuelle brudd).
- Revisjon (bl.a. den behandlingsansvarliges rett til å få nødvendig informasjon fra databehandleren og til gjøre revisjon/inspeksjon av databehandlerens virksomhet).
- Varighet og oppsigelse (f.eks. at databehandleravtalen opphører når tjenesteavtalen opphører, og at databehandleren da skal levere tilbake eller slette personopplysningene).

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. Det normale tiltaket er at den behandlingsansvarlige inngår en EU-kommisjonens standardavtale for dataoverføring (Model Clauses) med mottakerselskapet i tredjestaten. Slik avtale finnes [her](#). For overføring til USA vil det at mottakerselskapet er Privacy Shield-sertifisert gi et rettslig grunnlag for overføringen.

10 SLETNING AV PERSONOPPLYSNINGER

Som behandlingsansvarlig har en advokat plikt til å slette personopplysninger uten ugrunnet opphold i visse tilfeller, herunder når behandlingen ikke lenger er "nødvendig" for formålet som de ble samlet inn eller behandlet for, jf. GDPR artikkel 17 nr 1 bokstav a. Dette betyr i praksis at virksomheten må utarbeide oppbevarings- og sletterutiner for alle sine behandlingsaktiviteter, samt ved jevne mellomrom vurdere om det er nødvendig at den oppbevarer og behandler de aktuelle personopplysningene. Virksomheten bør i rutinene innta hvem i virksomheten som er ansvarlig for at sletterutinene følges og revideres.

Visse typer behandling er unntatt sletteplikten, jf GDPR artikkel 17 nr 3. Dette gjelder blant annet dersom behandlingen er nødvendig for å oppfylle en rettslig forpliktelse i medhold av lov eller for å fastsette, gjøre gjeldende eller forsvare et rettskrav.

Sletteplikten må således ses i sammenheng med lovpålagte plikter til å oppbevare visse opplysninger, herunder eksempelvis lovpålagte oppbevaringsplikter i bokføringslovgivningen og skattelovgivningen, og virksomhetens behov for å forfølge eller forsvare seg mot et rettskrav.

Utfordringen for en advokatvirksomhet vil ofte være å balansere sletteplikten mot ulike oppbevaringsplikter/-hensyn. En advokatvirksomhet vil for eksempel være underlagt visse lovpålagte krav knyttet til oppbevaring av regnskapsmateriale, dokumentasjon knyttet til hvitvaskingskontroll, etc. Et annet eksempel kan være informasjon om ansatte, herunder en ansatt som har mottatt en skriftlig advarsel. Dersom den skriftlige advarselen slettes vil virksomheten kunne få et dokumentasjonsproblem dersom den ansatte sies opp og går til sak for å få oppsigelsen kjent ugyldig.

NB! 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. Til syvende og sist er sletteplikten knyttet til en konkret vurdering i hvert enkelt tilfelle, og det vil på bakgrunn av slike vurderinger kunne være mulig å oppbevare personopplysninger i lengre perioder. En advokatvirksomhet vil også kunne innhente samtykke fra klienter til å oppbevare personopplysninger lenger enn det som følger av personvernreglene (se punkt 6 for nærmere informasjon om [samtykke som behandlingsgrunnlag](#)).

11 PERSONVERN RÅDGIVER

Etter personvernforordningen har visse typer av private virksomheter plikt til å utpeke en personvernrådgiver. Rådgiveren 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 personvernrådgiver hvis:

- virksomhetens hovedvirksomhet består i å behandle personopplysninger på en måte som innebærer regelmessig og systematisk overvåkning av personer i stor skala, eller
- virksomheten hovedvirksomhet består i å behandle sensitive 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 personvernrådgivere. Dette har særlig sammenheng med at advokatvirksomheters hovedvirksomhet normalt ikke består i verken å overvåke personer eller behandle sensitive 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 en personvernrådgiver bør utpekes eller ikke (og vurderingen bør være skriftlig og grunnlagt).

12 VURDERING AV PERSONVERNKONSEKVENSER (DPIA)

Personvernforordningen artikkel 35 oppstiller en plikt for behandlingsansvarlig til å gjennomføre en vurdering av personvernkonsekvenser (data protection impact assessment, 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 straffbare forhold 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 et 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.

I følge forordningens fortale nummer 91 nevnes at DPIA særlig bør få anvendelse på "behandlingsaktiviteter i stor skala der formålet er å behandle en betydelig mengde personopplysninger på regionalt, nasjonalt eller overnasjonalt plan, og som kan påvirke et stort antall registrerte og innebære en høy risiko, f.eks. fordi opplysningene er sensitive." Samme sted angis det også at "behandling av personopplysninger bør ikke anses for å være i stor skala dersom det er snakk om en leges, annet helsepersonells eller en advokats behandling av personopplysninger tilhørende pasienter eller klienter. I slike tilfeller bør en vurdering av personvernkonsekvenser ikke være obligatorisk".

Forordningens ordlyd og uttalelsene i fortalen trekker i retning av at advokatvirksomheters behandling av særlige kategorier av opplysninger, jf. over, som den klare hovedregel ikke krever gjennomføring av DPIA.

Relevant for tolkningen er også de europeiske tilsynsmyndighetenes ("Artikkel 29-gruppens") veiledning knyttet til DPIA.¹ I følge veiledningen vil behandlingsaktiviteter som omfattes av to eller flere av følgende kriterier som hovedregel innebære høy risiko for den registrerte og derfor kreve DPIA:

- Evaluation or scoring (including profiling and predicting)
- Automated decision-making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining data sets

¹ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01, sist oppdatert 4. oktober 2017, tilgjengelig på http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organizational solutions
- When the processing prevents data subjects from exercising a right or using a service or a contract

For advokatvirksomhet er det særlig kriteriene sensitive data og muligens opplysninger vedrørende sårbare registrerte som er mest aktuelle. Det skal imidlertid mye til for at behandlingen kan sies å være av stor skala.

Redegjørelsen viser at det må gjennomføres en konkret vurdering av hvorvidt én eller flere behandlinger krever gjennomføring av DPIA. Det klare utgangspunktet er at det ikke er påkrevet å gjennomføre DPIA for advokatvirksomheters behandlinger. Unntak kan tenkes ved behandling innenfor strafferett, personskade, forsikring eller arbeidsrett hvor det behandles særlige sensitive opplysninger og kategorier i stor skala, vedrørende sårbare registrerte, særlig dersom den registrertes rettigheter som f.eks. rett til innsyn og retting/sletting settes til side.

Vurderingen bør dokumenteres slik at virksomheten kan påvise at man har vurdert spørsmålet og de konkrete argumentene for ikke 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 tilfredsstillende forordningens innholdskrav. 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 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 kunne utvides til å tilfredsstillende 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

Dersom man vurderer å sende markedsføringshenvendelser til klienter er det viktig å huske på 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.

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.

På nærmere vilkår er det gjort unntak fra regelen om forhåndssamtykke i noen eksisterende kundeforhold. Slik markedsføring kan bare gjelde den næringsdrivendes egne varer, tjenester eller andre ytelser tilsvarende dem som kundeforholdet bygger på. Se ytterligere vilkår i markedsføringsloven § 15 tredje ledd.

Dersom man ønsker å rette en markedsføringshenvendelse til fysiske personer hos en selskapsklient må man foreta en vurdering av hvor grensen for hvem man kan sende til går etter markedsføringsloven § 15 tredje ledd.

Hvis man har personklienter kan det være lurt å sørge for at oppdragsbekreftelsen dekker det behovet man har for kommunikasjon med klienten utover selve rådgivningen, herunder eventuell markedsføring.

Hvis man ønsker å reklamere for tredjeparters produkter kan man ikke basere seg på eksisterende kundeforhold, jf. ordlyden i markedsføringsloven § 15 tredje ledd.

I tilfeller hvor man ønsker å benytte klienter som referanse i forbindelse med nye klientforhold er det viktig å huske på at klientforholdet i seg selv er underlagt taushetsplikt, og at man dermed må ha samtykke for å åpenbare det for andre.

Når det gjelder å sende informasjon til eksisterende kunder er det ulike tolkninger av GDPR, og flere vil hevde at grunnlaget kan være «legitimate interests» jf. art. 6, 1 (f). Ved å benytte seg av dette behandlingsgrunnlaget unngår man samtidig å omfattes av reglene om dataportabilitet.

14 INNSYN I ANSATTES E-POSTKASSE MV.

Innledning

[Personopplysningsforskriftens regler om arbeidsgivers innsyn i ansattes e-postkasse mv.](#) er i hovedsak foreslått videreført i Justis- og beredskapsdepartementets utkast til ny personopplysningslov. Dette innebærer at det fortsatt vil gjelde særnorske regler for når arbeidsgiver kan kreve innsyn i den ansattes e-postkasse mv. og hvilke prosedyrer som må følges.

Bestemmelsene som fremgår av § 1 i høringsnotatets utkast til bestemmelser om arbeidsgivers innsyn i e-postkasse mv. innebærer at en arbeidsgiver har rett til innsyn i opplysninger lagret i (i) den ansattes e-postkasse, (ii) personlige område i virksomhets datanettverk eller annet elektronisk utstyr som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet, og (iii) aktivitetslogger i virksomhetens datanettverk. Bestemmelsen omfatter også opplysninger som finnes på sikkerhetskopier eller tilsvarende.

Retten til innsyn krever at visse vilkår er oppfylt, jf. § 2 i høringsnotatets utkast til bestemmelser om arbeidsgivers innsyn i e-postkasse mv. Dersom slik rett foreligger, skal innsyn skje i henhold til de prosedyrer som fremgår av § 3 i høringsnotatets utkast til bestemmelser om arbeidsgivers innsyn i e-postkasse mv.

Retten til innsyn gjelder både eksisterende og tidligere ansatte, samt andre som utfører eller har utført arbeid for virksomheten.

Rutiner for innsyn

Advokatvirksomheter som har ansatte bør etablere rutiner for arbeidsgivers rett til å foreta innsyn i en nåværende eller tidligere ansattes e-postkasse mv. Formålet med en slik rutine er å sikre at innsyn i ansattes e-postkasse mv. kun gjennomføres når det er lovlig, og at de lovbestemte prosedyrene følges ved et eventuelt innsyn.

Ansvarlig person i virksomheten skal vurdere om det er grunnlag for å gjennomføre innsyn, jf § 2 i høringsnotatets utkast til bestemmelser om arbeidsgivers innsyn i e-postkasse mv. Innsyn kan kun gjennomføres:

- Når det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten, eller
- Ved begrunnet mistanke om at arbeidstakers bruk av e-postkassen medfører grovt brudd på de plikter som følger av arbeidsforholdet, eller kan gi grunnlag for oppsigelse eller avskjed.

Dersom det etter dette kan gjennomføres innsyn, skal innsyn gjennomføres i tråd med prosedyrene i § 3 i høringsnotatets utkast til bestemmelser om arbeidsgivers innsyn i e-postkasse mv. Dette innebærer at virksomheten bør etablere rutiner som sikrer at ansvarlig person i virksomheten, i tilfeller der det er hjemmel for innsyn etter § 2, skal:

- Sørge for at arbeidstaker så langt som mulig varsles og gis mulighet til å uttale seg på forhånd. I varselet skal det begrunnes hvorfor vilkårene for innsyn anses å være oppfylt. Varselet skal også orientere om arbeidstakers rett til å være til stede under gjennomgangen, og om å la seg bistå av tillitsvalgt eller annen representant.
- Sørge for at arbeidstaker så langt som mulig gis anledning til å være til stede under gjennomføringen av innsynet. Arbeidstaker har rett til å la seg bistå av tillitsvalgt eller annen representant.
- Dersom innsyn er foretatt uten forutgående varsel, gi arbeidstaker skriftlig underretning om innsynet så snart det er gjennomført. Underretningen skal, i tillegg til begrunnelsen for hvorfor vilkårene for innsyn anses å være oppfylt og orienteringen om arbeidstakers

rettigheter, inneholde opplysninger om hvilken metode som ble benyttet ved innsynet, hvilke e-poster eller andre dokumenter som ble åpnet samt resultatet av innsynet.

- Dersom innsynet viser at det ikke foreligger dokumentasjon som arbeidsgiver har rett til innsyn i, sørge for at e-postkassen og dokumenter i denne straks lukkes, samt at eventuelle kopier slettes.
- Sørge for at innsyn gjennomføres på en slik måte at opplysningene så langt som mulig ikke endres og at frembrakte opplysninger kan etterprøves.
- Sørge for at det blir skrevet protokoll fra innsynet.

Det understrekes at advokaters lovpålagte taushetsplikt går foran den ansattes rett til informasjon ved innsyn, jf. § 3, fjerde ledd i høringsnotatets utkast til bestemmelser om arbeidsgivers innsyn i e-postkasse mv.