Vejledning
Advokatens behandling af personoplysninger

Revideret marts 2025

ADVOKAT SAMFUNDET

Indholdsfortegnelse

1. Indledning og anvendelsesområde

1.1 Om vejledningen

I denne vejledning finder du gode råd til, hvordan du som advokat kan forholde dig til databeskyttelsesreglerne i GDPR/databeskyttelsesforordningen[1] og databeskyttelsesloven[2] og til de problemstillinger, der kan opstå i krydsfeltet mellem databeskyttelsesreglerne og advokatpligterne.

GDPR og databeskyttelsesloven indeholder ikke særlige regler for advokater, som det for eksempel er tilfældet på hvidvaskområdet. Det er derfor et væsentligt formål med vejledningen at beskrive de regler, der er særligt relevante for advokater og sætte databeskyttelsesreglerne ind i en advokatretlig sammenhæng. Vejledningen er således målrettet mod advokater med fokus på deres virksomhed som advokater, og den klientrettede virksomhed vil være i centrum.[3]

Man skal som advokat udvise en adfærd, der stemmer overens med god advokatskik – også når man behandler personoplysninger. Vejledningen indeholder derfor også en beskrivelse af de regler i de advokatetiske regler (AER), som kan have betydning for advokatens håndtering af personoplysninger. Vejledningen tilstræber at have fokus på de udfordringer af advokatetisk og databeskyttelsesretlig karakter, som advokaten i sin hverdag kan stå overfor.

Vejledningen er ikke udtømmende og beskæftiger sig som udgangspunkt ikke med de mere driftsmæssige sider af advokatvirksomhed og intern håndtering af for eksempel personaleoplysninger, markedsføring[4], cookies mv. Datatilsynet har som tilsynsmyndighed offentliggjort en lang række vejledninger bl.a. også om disse emner, hvortil der henvises.

Da det som nævnt er Datatilsynet, som er tilsynsmyndighed i forhold til overholdelse af databeskyttelsesreglerne, herunder også advokaters overholdelse. Vejledningen er alene udtryk for Advokatsamfundets bud på, hvordan advokater kan arbejde med håndteringen af GDPR. Forslag til udarbejdelse af dokumenter er alene forslag, som der kan tages udgangspunkt i, og som den enkelte advokatvirksomhed kan arbejde videre med. Anvendelse af forslagene i vejledningen forudsætter i alle tilfælde, at der i den enkelte advokatvirksomhed foretages en vurdering af de konkrete forhold i virksomheden.

Vejledningen er en opdatering og udvidelse af den eksisterende vejledning om Advokatens behandling af personoplysninger[5] og er udarbejdet af Advokatsamfundets sekretariat med bistand fra advokaterne Andreas Leidesdorff (Advokatrådet), Susanne Stougaard, Max Gersvang Sørensen, Birgitte Toxværd, Anna de Vos-Zehngraff, Johan Leonhard, Sanne Dahl Fredslund, Stefanie Lynge Eriksen, Martin Juul Christensen, Anton Gramstrup og Tim Løvschal (chefkonsulent i sekretariatet).

Det er Advokatsamfundets håb, at vejledningen vil være med til skabe større klarhed over og lette advokaters arbejde med databeskyttelsesreglerne. Vejledningen er et dynamisk dokument og vil blive løbende opdateret.

1 Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger mv. omtales i vejledningen som GDRP. Henvisninger til artikler er henvisninger til artikler i GDPR, medmindre andet fremgår.

2 Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. Omtaltes i vejledningen som databeskyttelsesloven eller loven.

3 Bemærk, at pligtsubjektet efter databeskyttelsesreglerne er advokatfirmaet eller -virksomheden og ikke den enkelte advokat i firmaet/virksomheden. Når der i vejledningen bruges terminologi som for eksempel "når du som advokat behandler personoplysninger" er dette ikke udtryk for, at den enkelte advokat er pligtsubjekt og ansvarlig for overholdelsen af GDPR – det er den juridiske person, som er det. Det er således advokatfirmaet eller -virksomheden, der som selvstændig juridisk person er dataansvarlig. I nogle situationer kan advokatfirmaet eller -virksomheden også blive databehandler. I forhold til konkursbehandling er konkursboet en selvstændig juridisk person, og kurator bliver ved sin overtagelse af konkursboet dataansvarlig.

4 https://www.datatilsynet.dk/Media/0/8/Vejledning%20om%20databeskyttelse%20i%20forbindelse%20med%20ans%c3%a6ttelsesforhold.pdf. https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/markedsfoering

5 Vejledningen er senest opdateret i februar 2019.

1.2 Hvornår finder GDPR anvendelse materielt og geografisk

Databeskyttelsesreglerne finder anvendelse, når der sker en *behandling* af personoplysninger, jf. nærmere herom nedenfor. GDPR gælder i alle EU-medlemsstater (umiddelbar virkning) og finder anvendelse på behandlinger, som foretages som led i aktiviteter, der udføres for en dataansvarlig eller databehandler, som er etableret i EU, uanset om behandlingen finder sted i EU eller ej. Ligeledes finder GDPR anvendelse på behandling af personoplysninger om registrerede, der er i EU, og som foretages af en dataansvarlig eller databehandler, der ikke er etableret i EU, hvis behandlingsaktiviteterne vedrører udbud af varer eller tjenester til sådanne registrerede i EU (uanset om der kræves betaling), jf. artikel 3 og databeskyttelseslovens § 4. En overførelse og eksport af personoplysninger ud af Danmark og EU er ligeledes omfattet.

For yderligere beskrivelse af GDPR's geografiske anvendelsesområde henvises til det Europæiske Databeskyttelsesråds (EPDB) retningslinje.[6]

GDPR og databeskyttelseslovens gælder ikke i Grønland og på Færøerne.

Som advokat kan du lægge til grund, at din behandling af personoplysninger er omfattet af GDPR og lovens geografiske anvendelsesområde.

1.2.1 Hvad er "behandling"?

Behandling sker ved for eksempel indsamling, modtagelse, videregivelse, opbevaring, sletning mv. Begrebet er så omfattende, at stort set enhver berøring med personoplysninger udgør en behandling. Den blotte adgang til personoplysninger er en behandling, også selvom der ikke gøres brug af adgangen. Som udgangspunkt kan det derfor lægges til grund, at hvis man har med en personoplysning at gøre, så sker der også en behandling.

For yderligere beskrivelse af begrebet behandling se databeskyttelseslovens vejledning herom.[7]

1.2.2 Hvad er en personoplysning?

En personoplysning er en oplysning, som kan henføres til og identificere et bestemt individ (og altså en fysisk person). Omvendt er oplysninger om selskaber og juridiske personer ikke personoplysninger, og databeskyttelsesreglerne finder således ikke anvendelse på dem.[8]

En personoplysning er enhver form for information, der kan henføres til en bestemt person – også selvom personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger. Selv oplysninger, der umiddelbart fremstår som oplysninger, der ikke i sig selv kan anses for personoplysninger, for eksempel oplysning om en MAC-adresse (en unik adresse) eller IMEI-nummer på en mobiltelefon, eller en IP-adresse, vil ved sammenstilling med andre oplysninger, som navn, adresse, telefonnummer, kundenummer eller oplysninger om betalingskort, kunne bruges til at gøre en bestemt fysisk person identificerbar.

6 https://www.datatilsynet.dk/media/7872/edpb-guideline-3-2018-territorial-scope.pdf
7 https://www.datatilsynet.dk/Media/637647832459647592/Personoplysninger%20-%20f%C3%A5%20et%20hurtigt%20overblik.pdf
8 Virksomhedsoplysninger, der kan identificere enkeltpersoner (for eksempel enkeltmandsvirksomheder), er derimod omfattet.

Personoplysninger kan inddeles i tre kategorier: almindelige, strafbare forhold og lovovertrædelser og følsomme personoplysninger. Dansk ret indeholder yderligere en kategori om fortrolige personoplysninger, som omfatter oplysninger, der efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab, jf. straffelovens § 152 og forvaltningslovens § 27. GDPR indeholder endvidere mulighed for nationale særregler om typer af oplysninger, og denne er udnyttet i loven, som bl.a. indeholder regler om CPR-nummer, som i dansk ret er en fortrolig oplysning.

De almindelige personoplysninger nyder mindst beskyttelse og de følsomme størst. Som udgangspunkt gælder der et forbud mod behandling af følsomme personoplysninger, som kun må behandles, hvis en af undtagelserne i GDPR eller loven finder anvendelse. Det er vigtigt i den sammenhæng at være opmærksom på, at personoplysninger som for eksempel navn eller adresse, der normalt er almindelige personoplysninger, i særlige tilfælde kan afdække følsomme personoplysninger om bestemte personer.

Alle advokater behandler almindelige personoplysninger. Det sker for eksempel i forbindelse med etableringen af klientforholdet i form af for eksempel navn, adresse, e-mail mv., men også under den løbende varetagelse af klientens interesser og sag(er). Alle advokater behandler også fortrolige personoplysninger som for eksempel CPR-nummer og kørekort- eller pasnummer som en del af hvidvaskdokumentationen. Mange advokater behandler også følsomme personoplysninger i forbindelse med deres sager. Nogle advokater behandler også oplysninger om lovovertrædelser og strafbare forhold.

For yderligere beskrivelse af personoplysninger og de forskellige kategorier henvises til Datatilsynets vejledning.[9]

1.3 Hvornår må advokaten behandle personoplysninger?

Advokater må behandle personoplysninger, hvis 1) de grundlæggende principper for behandlingen er iagttaget, og hvis 2) der er et lovligt grundlag for behandlingen.

1.3.1 Grundlæggende behandlingsprincipper

De grundlæggende principper for behandlingen, jf. artikel 5, stk. 1, er:

1.3.1.1 Lovlighed, rimelighed, og gennemsigtighed

Principperne om lovlighed og rimelighed er udtryk for et grundprincip, som skal sikre, at behandlingen af personoplysninger altid er lovlig og rimelig. Princippet om lovlighed fastslår, at behandlinger skal være lovlige, dvs. være hjemlet i databeskyttelsesreglerne eller i særlovgivning som for eksempel whistleblowerloven og ikke må være ulovlig, jf. for eksempel en videregivelse af oplysninger om en whistleblowers identitet mv. i strid med whistleblowerloven § 26. Rimelighed i behandlingen kan bl.a. forstås som et krav om proportionalitet, og at behandlingen af personoplysninger for eksempel ikke må gå videre end, hvad der er nødvendigt i forhold til formålet.

Gennemsigtighed indebærer bl.a., at den person, der behandles oplysninger om, som udgangspunkt skal have oplyst, hvem der er ansvarlig for behandlingen af oplysninger, og hvad der er formålet med behandlingen. Behandlingen af personoplysninger skal ske på en gennemsigtig måde, hvor den registrerede på letforståelig vis bliver informeret om behandlingens vilkår.

9 https://www.datatilsynet.dk/Media/637647832459647592/Personoplysninger%20-%20f%C3%A5%20et%20hurtigt%20overblik.pdf. Her betegnes de tre kategorier som: personoplysninger (ikke-følsomme oplysninger), oplysninger om strafbare forhold og lovovertrædelser og personoplysninger (følsomme oplysninger).

Kravet om gennemsigtighed pålægger dig som advokat og dataansvarlig en oplysningspligt til at give let tilgængelig information om din behandling af personoplysninger til de personer, som du behandler oplysninger om, jf. artikel 13 og 14. Dette gælder ikke kun i forhold til hovedpersonen, som der behandles personoplysninger om (for eksempel din klient), men også i forhold til bipersoner (dvs. andre personer som indgår eller omtales i en sag som for eksempel part eller vidne).

Læs nærmere herom i afsnit 6.2.

1.3.1.2 Formålsbegrænsning
Når der indsamles oplysninger, skal den dataansvarlige gøre sig klart, hvilke formål oplysningerne indsamles til, og om formålene er databeskyttelsesretligt saglige. Man må ikke indsamle oplysninger med den begrundelse, at det måske senere kan vise sig nyttigt at være i besiddelse af oplysningerne, eller fordi det er ressourcebesparende, jf. også nedenfor om dataminimering. Det er i første omgang den, der indsamler oplysninger, som skal vurdere, om en bestemt indsamling af oplysninger er saglig. Det kan bl.a. vurderes ud fra, om indsamlingen sker i forbindelse med løsningen af en opgave, som det er naturligt at løse.

Kravet om formålsbegrænsning betyder, at du som advokat skal vurdere, om der er et **arbejds-/sagsbetinget behov** for at indsamle en oplysning. Det kan for eksempel være tilfældet, hvis oplysningen er relevant for varetagelsen af en klients interesser, en sag eller drift af advokatvirksomheden.

Du skal også være opmærksom på, om en eventuel, efterfølgende behandling sker til det samme, oprindelige formål, eller om der er tale om et nyt og andet formål. Hvis der er tale om et nyt formål, skal du også have et behandlingsgrundlag for dette. Hvis det oprindelige formål eksempelvis var at behandle personoplysninger til brug for at føre en retssag, vil en senere anvendelse til eksempelvis markedsføringsformål være uforenelig med det oprindelige formål.

Læs nærmere herom i afsnit 6.3.

1.3.1.3 Dataminimering
Behandlingen af personoplysninger skal begrænses til det, der er nødvendigt for at opfylde formålet, og der må ikke behandles personoplysninger, som der ikke er brug for.

Kravet om dataminimering betyder, at du som advokat skal overveje, hvilke personoplysninger der er nødvendige til et givent formål. Det er for eksempel tilfældet, når du indsamler oplysninger, deler dem internt eller opbevarer dem i advokatvirksomheden, eller videregiver oplysninger til tredjemand. Som nævnt er praktiske eller ressourcebesparende (både fsva. tid og økonomi) hensyn ikke saglige.

Dataminimering er relevant for dig som advokat i mange sammenhænge. Det kan for eksempel være i forbindelse med beskrivelse af faktum i en sag, mødereferater, videndeling i advokatfirmaet, specifikation af faktura mv.

Læs nærmere herom i afsnit 6.4.

1.3.1.4 Rigtighed
Oplysningerne skal være rigtige og ajourførte, og hvis de viser sig at være urigtige, skal de som udgangspunkt slettes eller berigtiges.

Kravet om rigtighed indebærer, at du som advokat løbende skal være opmærksom på, om de oplysninger, som du behandler, er korrekte og opdaterede. Hvis en oplysning viser sig at være forkert eller usand, skal den som udgangspunkt slettes. Hvis oplysningen ikke som sådan er forkert, men blot ikke korrekt eller ikke opdateret, skal den berigtiges. Sletning eller berigtigelse kan efter omstændighederne også ske på anmodning fra den registrerede.

Læs nærmere herom i afsnit 6.5.

1.3.1.5 Opbevaringsbegrænsning
Personoplysninger skal slettes eller anonymiseres, når det ikke længere er nødvendigt for den dataansvarlige at have dem. Det er i første omgang op til den enkelte dataansvarlige at vurdere, hvor længe det er nødvendigt at opbevare oplysningerne ud fra det formål, som oplysningerne oprindelig blev indsamlet til.

Kravet om opbevaringsbegrænsning betyder bl.a., at du som advokat løbende skal tage stilling til, om oplysninger fortsat skal opbevares, eller om de skal slettes.

Læs nærmere herom i afsnit 6.6.

1.3.1.6 Integritet og fortrolighed
Det skal sikres, at oplysninger ikke bliver beskadiget eller går tabt. Oplysningerne skal desuden beskyttes mod uautoriseret eller ulovlig behandling.

Kravet om integritet indebærer, at der skal være foranstaltninger til stede, som sikrer, at mistede, forkerte eller beskadigede oplysninger kan berigtiges eller genskabes ved for eksempel backup. Kravet om fortrolighed betyder, at der skal etableres en passende sikkerhed (it-mæssigt og fysisk), så uvedkommende ikke får adgang til oplysninger.

Læs nærmere om, hvordan du som advokat sikrer oplysningers integritet og fortrolighed i afsnit 6.7.

1.3.1.7 Ansvarlighed
GDPR artikel 5, stk. 2 indeholder yderligere et grundlæggende princip om ansvarlighed ("accountability"), hvorefter den dataansvarlige har ansvaret for at sikre og kunne dokumentere, at de i artikel 5, stk. 1 grundlæggende principper overholdes.

Læs nærmere i afsnit 3 om, hvordan du som advokat og dataansvarlig efterlever kravet om ansvarlighed.

1.3.2 Behandlingsgrundlag
Som nævnt under pkt. 1.3.1.1 forudsætter behandling af personoplysninger, at der er et behandlingsgrundlag, dvs. at der er hjemmel til behandlingen. Behandlingsgrundlaget varierer alt efter, hvilken type oplysning der er tale om, jf. for eksempel artikel 6 og artikel 9. Grundlaget kan for eksempel være samtykke, en kontrakt eller en aftale, som den registrerede er part i, en retlig forpligtelse eller retskrav.

Læs nærmere om relevante behandlingsgrundlag i afsnit 6.8.

1.4 Dataansvarlig eller databehandler?

I GDPR sondres der mellem, om man er dataansvarlig eller databehandler for en dataansvarlig. Det har afgørende betydning, at det afklares, hvad din rolle er, inden du begynder at behandle personoplysninger, fordi kravene til dataansvarlige og databehandlere er forskellige. I nogle situationer kan der også være fælles dataansvar.

Læs nærmere om, hvordan du afklarer, om du er dataansvarlig eller databehandler og om advokaters persondataretlige rolle i en række forskellige situationer i afsnit 4.2.

1.5 Regler med særlig betydning for advokaters behandling af personoplysninger

Udover databeskyttelsesreglerne er der en række andre regler, som har indvirkning på advokaters behandling af personoplysninger. Det gælder bl.a. retsplejelovens § 126 om god advokatskik og de advokatetiske regler ("AER"), hvor bl.a. AER artikel 7-10 om interessekonflikter, artikel 15-20 om fortrolighed og tavshedspligt, artikel 44 om forbud mod optagelse af samtaler mv., artikel 53 om advokatundersøgelser og artikel 70 om opbevaring af sagsakter. Desuden er retsplejelovens § 129 (herunder straffelovens § 152) om advokaters tavshedspligt samt lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorismes (hvidvaskloven) §§ 10-11, 16 og 30 relevante.

Det er som omtalt Datatilsynet, som er tilsynsmyndighed i forhold til databeskyttelsesreglerne. Overtrædelse af databeskyttelsesreglerne sanktioneres derfor som udgangspunkt ikke efter AER og af Advokatrådet samt Advokatnævnet. Advokatnævnet har således i flere tilfælde afvist at behandle klager over advokaters manglende overholdelse af databeskyttelsesreglerne efter deres beskaffenhed givetvis ud fra en betragtning om, at Datatilsynet vil være bedre til at behandle spørgsmålet.[10] Da en tilsidesættelse af lovgivningen imidlertid som udgangspunkt også vil være en tilsidesættelse af god advokatskik, findes der dog også afgørelser, hvor Advokatnævnet har sanktioneret en advokats behandling af personoplysninger.[11]

En overtrædelse af databeskyttelsesreglerne kan dog efter omstændighederne også være en overtrædelse af AER, for eksempel hvis en videregivelse sker uden behandlingsgrundlag og heller ikke lever op til kravene i AER artikel 18. Her kan du som advokat både have overtrådt databeskyttelsesreglerne og AER. I den forbindelse skal du være opmærksom på, at disciplinære sanktioner for manglende efterlevelse af AER både kan pålægges advokatselskaber og den enkelte advokat.

Læs nærmere herom i bl.a. afsnit 2.

10 Se for eksempel Advokatnævnets kendelse i sagsnummer 2021-551 og 2022-3944.
11 Se for eksempel Advokatnævnets kendelse i sagsnummer 2024-608.

2. Advokaters tavshedspligt og fortrolighed og betydningen heraf ved behandling af personoplysninger

2.1 Indledning

Som nævnt findes der i retsplejeloven, herunder straffeloven, og AER en række regler,[12] som er rettet mod advokater, og som har indvirkning på advokaters behandling af personoplysninger. Reglerne – og hvad du som advokat overordnet set skal være opmærksom på i en persondataretlig sammenhæng – beskrives her sammen med nogle praktiske eksempler på situationer, hvor både reglerne om tavshedspligt og reglerne om databeskyttelse finder anvendelse.

2.1.1 Retsplejelovens § 129, herunder straffelovens § 152 og § 152 e

Det følger af retsplejelovens § 129, at bl.a. straffelovens § 152 finder tilsvarende anvendelse på advokater samt deres autoriserede fuldmægtige, partnere, personale og andre, som i øvrigt beskæftiges i advokatvirksomheden. Retsplejelovens § 129 indeholder således en lovbestemt tavshedspligt for advokater, fuldmægtige mv., i forhold til oplysninger, som advokaten har modtaget i sit virke som advokat for klienten.[13]

Advokaters tavshedspligt er grundlæggende for opretholdelsen af den tillid og uafhængighed, som er nødvendig for advokaten og klienten og for, at retssystemet kan fungere. I tavshedspligten indgår således hensyn til advokat, klient og retssystemet, som også har betydning i forhold til databeskyttelsesreglerne, hvor overholdelse af for eksempel en retlig forpligtelse, beskyttelse af individers vitale interesser, legitime interesser, retskrav og samfundsinteresser er relevant i forhold til behandlingsgrundlag, men også i håndteringen af de registreredes rettigheder som for eksempel oplysningspligt og indsigtsret.

Efter straffelovens § 152 er det strafbart uberettiget at videregive eller udnytte fortrolige oplysninger, dvs. oplysninger som ved lov eller anden gyldig bestemmelse er betegnet som sådan, eller når det i øvrigt er nødvendigt at hemmeligholde dem for at varetage væsentlige hensyn til offentlige eller private interesser.

Det fremgår dog af straffelovens § 152 e, at § 152 ikke omfatter tilfælde, hvor den pågældende er forpligtet til at videregive oplysningen eller handler i berettiget varetagelse af åbenbar almeninteresse eller af eget eller andres tarv. Undtagelserne i straffelovens § 152 e indgår også i AER, hvor de i henhold til artikel 18, nr. 2 og 3, gælder med samme ordlyd.

Retsplejelovens § 129 og straffelovens § 152 gør det således strafbart for advokater mv. at videregive eller udnytte (dvs. behandle efter databeskyttelsesreglerne) oplysninger, hvis der er tale om fortrolige oplysninger, det sker uberettiget, og der ikke er tale om et tilfælde omfattet af straffelovens § 152 e.

En personoplysning kan være en fortrolig oplysning som nævnt i straffelovens § 152 – enten fordi den ved lov mv. betegnes som sådan, eller fordi det kan være nødvendigt at hemmeligholde den for at varetage væsentlige hensyn til offentlige eller private interesser. Det betyder, at hvis for eksempel en videregivelse af en personoplysning også er uberettiget og ikke omfattet af straffelovens § 152 e, kan

12 For en beskrivelse af reglernes generelle betydning for advokater se AER Kommenteret, 3. udgave, kapitel 5 side 126-150.
13 Dette har bl.a. også betydning i forhold til spørgsmålet om, hvorvidt advokaten er dataansvarlig eller databehandler, jf. afsnit 4.2.

du som advokat efter omstændighederne have handlet i strid med og overtrådt retsplejelovens § 129 og straffelovens § 152 ved at have videregivet personoplysningen.

2.1.2 De advokatetiske reglers kapitel 5 om fortrolighed (artikel 15-20)

Kapitel 5 i AER omhandler advokaters fortrolighed og tavshedspligt. Reglerne er ikke skrevet særligt med personoplysninger for øje (de gælder alle typer fortrolige oplysninger), men har desuagtet også stor betydning for advokaters behandling af personoplysninger og efterlevelse af både tavshedspligten og databeskyttelsesreglerne. De advokatetiske regler er vejledende retningslinjer for, hvad der er god advokatskik efter retsplejelovens § 126, som dette er fastlagt af Advokatnævnet og domstolene. En overtrædelse af AER vil derfor som udgangspunkt også være en overtrædelse af god advokatskik og retsplejelovens § 126. Dette er vigtigt at have for øje, når advokater har med oplysninger at gøre, som både er omfattet af tavshedspligten og databeskyttelsesreglerne.

2.1.2.1 AER artikel 15 fortrolighed

Artikel 15 cementerer advokaters fortrolighed og tavshedspligt. Det følger af bestemmelsen, at *"Fortrolighed er en betingelse for advokatens virke og en grundlæggende pligt og ret, som skal respekteres ikke kun i det enkelte individs, men også i retssamfundets interesse."*. I forhold til databeskyttelsesreglerne har det betydning, at advokaters fortrolighed skal respekteres både i forhold til det enkelte individs og retssamfundets interesse. Bestemmelsen hjemler således, at i for eksempel en interesseafvejning, jf. GDPR artikel 6, stk. 1 (f), kan hensyn til såvel advokatens (i virket som advokat), klientens og retssamfundets (og hermed også samfundets) interesse inddrages.

2.1.2.2 AER artikel 16 tavshedspligt uden tidsbegrænsning

Det følger af bestemmelsens stk. 1, at tavshedspligten gælder uden tidsbegrænsning og også efter sagens afslutning. Såfremt der er tale om en personoplysning, der er omfattet af tavshedspligten, skal den dermed efter AER artikel 16, stk. 1, holdes fortroligt uden nogen form for tidsbegrænsning og i princippet i al evighed. Er der for eksempel tale om en oplysning om en klient, som har været død i mere end 10 år, vil oplysningen ikke kunne videregives eller deles efter AER, selvom databeskyttelsesreglerne ikke beskytter sådanne personoplysninger.[14] Tilsvarende vil den tidsubegrænsede tavshedspligt kunne føre til, at oplysninger underlagt tavshedspligt ikke på noget tidspunkt vil være omfattet af oplysningspligten efter GDPR artikel 13 eller 14 eller af en anmodning om indsigt i personoplysninger efter GDPR artikel 15. Såfremt det modsatte var tilfældet, ville databeskyttelsesreglerne begrænse tavshedspligtens tidsmæssige udstrækning, medmindre en af undtagelserne i GDPR eller databeskyttelseslovens § 22 finder anvendelse og begrænser oplysningspligten eller indsigtsretten.

Bestemmelsens stk. 2 fastslår, at tavshedspligten gælder alle oplysninger, som advokaten modtager under sit virke for klienten. Personoplysninger er således også omfattet, men dog kun, hvis de er modtaget under advokatens virke. Er de modtaget på anden måde, er de ikke omfattet af tavshedspligten, men alene af databeskyttelsesreglerne. En forsvarsadvokat kan dog udtale sig til pressen i generelle vendinger om straffesagens fremdrift og lignende spørgsmål uden at bryde sin tavshedspligt, jf. stk. 2 in fine. Sådanne generelle ytringer vil efter omstændighederne også skulle overholde de persondataretlige regler, hvilket i denne sammenhæng betyder, at du som advokat bør have afstemt udtalelserne med din klient.

Tavshedspligten gælder i alle typer af sager, jf. stk. 3. Uanset hvilken type af sag, du varetager som advokat for en klient, vil personoplysninger således være omfattet af tavshedspligten.

14 Jf. databeskyttelseslovens § 2, stk. 5.

2.1.2.3 AER artikel 17 deling af fortrolige oplysninger

Efter artikel 17, stk. 1, kan en advokat dele fortrolige oplysninger med advokater og andre, der er beskæftiget i samme advokatfirma som advokaten, hvis det åbenbart er i klientens interesse. Bestemmelsen hjemler deling af ellers fortrolige oplysninger internt i advokatfirmaet, forudsat at dette åbenbart er i klientens interesse. Hvis den fortrolige oplysning også er en personoplysning, skal du sikre dig, at der også er et behandlingsgrundlag efter databeskyttelsesreglerne for deling af personoplysninger, for eksempel GDPR artikel 6 eller artikel 9. En deling af personoplysninger omfattet af tavshedspligten skal derfor både leve op til kravene i AER og databeskyttelsesreglerne.

Kravene til deling af personoplysninger omfattet af tavshedspligten indebærer også, at der ikke må være fri adgang til oplysningerne i advokatfirmaets kontorer eller it-systemer og applikationer, men at adgange og rettigheder begrænses. Andre advokater mv. i firmaet må således kun have fysisk og systemmæssig adgang til personoplysninger omfattet af tavshedspligten, hvis det åbenbart er i klientens interesse, og der er et behandlingsgrundlag efter databeskyttelsesreglerne. Det følger også af reglerne om dataminimering, at medarbejdere i advokatfirmaet alene må tilgå de personoplysninger, som de har et arbejdsbetinget behov for. Det skal således systemteknisk opsættes sådan, at man kun har adgang til bestemte sager i for eksempel sagsbehandlingssystemet. Herved indskrænkes adgang til sager til de personer, der har et arbejdsbetinget behov for at kunne tilgå sagerne. Der kan med fordel fastlægges en procedure for, hvordan der gives adgang til sager, hvis der opstår et arbejdsbetinget behov herfor, og hvem der kan give adgang til den pågældende sag. Herudover er det også vigtigt at præcisere løbende, at der ikke skal tilgås sager, der ikke er et arbejdsbetinget behov for at tilgå.

Efter stk. 2. skal en advokat indhente klientens samtykke til deling af fortrolige oplysninger med eksterne personer, herunder advokater. Efter bestemmelsen udgør klientens samtykke således det eneste grundlag, og deling af personoplysninger omfattet af tavshedspligten med eksterne personer må ikke ske, selvom andre behandlingsgrundlag end samtykke er til stede (for eksempel artikel 6, stk. 1 f). Hvis den fortrolige oplysning er en personoplysning, vil kravene til samtykke efter databeskyttelsesreglerne desuden skulle overholdes.

2.1.2.4 AER artikel 18 videregivelse af oplysninger

Det følger af artikel 18, at tavshedspligten ikke er til hinder for, at advokater kan videregive oplysninger i tre situationer.

Videregivelse kan således ske, hvis (1) klienten på oplyst grundlag har givet samtykke til, at konkrete oplysninger kan videregives, medmindre andet er bestemt i lovgivningen eller i pålæg i henhold til lovgivningen.[15] Hvis den tavshedsbelagte oplysning også er en personoplysning, vil samtykket – udover kravene om oplyst grundlag og konkrete oplysninger – også skulle overholde databeskyttelsesreglernes krav til et gyldigt samtykke. Videregivelse af oplysninger må dog uanset klientens samtykke ikke ske, hvis andet er bestemt i lovgivningen, og herunder også databeskyttelsesreglerne, eller i pålæg i henhold til lovgivningen.[16] Inden personoplysninger omfattet af tavshedspligten videregives med klientens samtykke, skal du derfor som advokat sikre dig, at videregivelsen ikke er i strid med de databeskyttelsesretlige regler. Det kan være tilfældet, hvis en klient anmoder om og samtykker til, at personoplysninger om en anden person videregives, men hvor dette vil være i strid med for eksempel indsigtsretten efter databeskyttelsesreglerne.

15 Hvis klienten instruerer advokaten og giver samtykke til at videregive konkrete oplysninger om klienten selv, er advokaten efter artikel 18 nr. 1 forpligtet til at videregive oplysningerne, jf. Advokatsamfundets nyhedsbrev af 9. februar 2023, som er tilgængeligt her https://www.advokatsamfundet.dk/nyheder-medier/nyheder/2023/dataradets-afgorelser-om-advokaters-videregivelse-og-brug-af-oplysninger/

16 For eksempel et pålæg til en forsvarer om hemmeligholdelse.

Videregivelse kan endvidere ske, hvis (2) du som advokat er retligt forpligtet til at videregive oplysningerne. Dette er efter omstændighederne for eksempel tilfældet i henhold til hvidvasklovens § 26 (forudsat, at der ikke er tale om en situation omfattet af § 27), whistleblowerlovens § 26 og arbejdsskadeforsikringslovens § 31. Hvis den tavshedsbelagte oplysning også er en personoplysning, skal videregivelsen også leve op til kravene i databeskyttelsesreglerne. Da overholdelse af en retlig forpligtelse også er et behandlingsgrundlag i henhold til GDPR artikel 6, stk. 1, c), fsva. almindelige personoplysninger og i visse tilfælde også fsva. følsomme oplysninger, jf. artikel 9, stk. 2, b), vil du som dataansvarlig advokat kunne videregive en personoplysning omfattet af tavshedspligten i overensstemmelse med både AER og databeskyttelsesreglerne.

Endelig kan videregivelse ske (3) i berettiget varetagelse af åbenbar almeninteresse eller af eget eller andres tarv. Som advokat kan du således efter AER videregive fortrolige oplysninger, hvis det enten sker i en berettiget varetagelse af (a) en åbenbar almeninteresse, (b) eget tarv eller (c) andres tarv. Hvis den tavshedsbelagte oplysning også er en personoplysning, skal videregivelsen som nævnt også leve op til kravene i databeskyttelsesreglerne.

GDPR indeholder lignende behandlingsgrundlag. For så vidt angår (a) berettiget varetagelse af åbenbar almeninteresse kan behandling af almindelige personoplysninger efter GDPR således ske, hvis den er nødvendig til udførelse af en opgave i samfundets interesse, jf. artikel 6, stk. 1, e), eller for følsomme oplysningers vedkommende af hensyn til væsentlige samfundsinteresser, jf. artikel 9, stk. 2, f). Hvis du som advokat berettiget varetager en klar og væsentlig almen- eller samfundsmæssig interesse ved at videregive personoplysninger omfattet af tavshedspligten, vil dette således kunne ske i overensstemmelse med både AER og databeskyttelsesreglerne.

I forhold til (b) berettiget varetagelse af eget tarv vil behandling af almindelige personoplysninger kunne ske, hvis den er nødvendig for, at du som dataansvarlig advokat kan forfølge en legitim interesse, jf. artikel 6, stk. 1, f), eller for følsomme oplysningers vedkommende af hensyn til fastlæggelse af et retskrav, jf. artikel 9, stk. 2, f). Hvis du som advokat berettiget varetager dit eget tarv, for eksempel i forbindelse med et forsvar af et krav rettet mod dig, eller med henblik på at fastlægge eller gøre et krav gældende ved at videregive personoplysninger omfattet af tavshedspligten, vil dette således kunne ske i overensstemmelse med både AER og databeskyttelsesreglerne.

For så vidt angår (c) berettiget varetagelse af andres tarv vil behandling af almindelige personoplysninger kunne ske, hvis den for eksempel er nødvendig for at beskytte den registreredes (for eksempel klientens) eller en persons vitale interesser, jf. artikel 6, stk. 1, d), eller for, at du som dataansvarlig advokat kan forfølge en legitim interesse af hensyn til andre, jf. artikel 6, stk. 1, f). For følsomme oplysningers vedkommende vil behandling kunne ske for at fastlægge, gøre gældende eller forsvare et retskrav, jf. artikel 9, stk. 2, f), eller af hensyn til væsentlige samfundsinteresser, jf. artikel 9, stk. 2, f). Hvis du som advokat varetager andres tarv ved at videregive personoplysninger omfattet af tavshedspligten, vil dette således kunne ske i overensstemmelse med både AER og databeskyttelsesreglerne.[17]

Som advokat skal du meget nøje vurdere grundlaget for at videregive personoplysninger omfattet af din tavshedspligt. Dette gælder især fsva. videregivelse i berettiget varetagelse af åbenbar almeninteresse eller af eget eller andres tarv (i henhold til 3 ovenfor), men også i forhold til en retlig forpligtelse eller efter samtykke fra klienten, som bør afstemmes nøje med klienten.

2.1.2.5 AER artikel 19 tavshedspligt for fuldmægtige og andre som beskæftiges i firmaet

17 De under (2) og (3) omtalte tilfælde er identiske med de i straffelovens § 152 e nævnte undtagelser til straffelovens § 152.

Artikel 19 indeholder et krav om, at en advokat skal sikre, at advokatens autoriserede fuldmægtige, partnere, jf. retsplejelovens § 124 c, stk. 1, nr. 2, personale og andre, som i øvrigt beskæftiges i advokatfirmaet, gøres bekendt med, at de pågældende har samme tavshedspligt som advokaten, uanset om de er advokater eller ej.

Henset til, at tavshedspligten også omfatter personoplysninger, og at behandling af disse oplysninger derfor både skal overholde kravene i AER og databeskyttelsesreglerne, bør du som advokat også sikre dig, at dine fuldmægtige mv. er blevet gjort bekendt hermed, og at det forud for deling eller videregivelse af personoplysninger omfattet af tavshedspligten vurderes, om behandlingen er i overensstemmelse med begge regelsæt.

2.1.2.6 AER artikel 20 tavshedspligt når advokatvirksomhed udøves i et fællesskab, advokatselskab, kontorfællesskab, samarbejder mv.

Det følger af artikel 20, at reglerne i artikel 15-19 også gælder, når advokater udøver advokatvirksomhed i et fællesskab, i et advokatselskab eller i et kontorfællesskab og i det indbyrdes forhold mellem dets deltagere, herunder ansatte advokater. Det samme gælder for andre samarbejder, samvirker og fællesskaber mellem advokater eller advokatfirmaer, såfremt de i forhold til tredjemand fremtræder som et fællesskab eller advokatfirma, dvs. kædesamarbejder. Det betyder, at du som advokat for eksempel ikke må dele personoplysninger omfattet af tavshedspligten med andre advokater mv. i et kontorfællesskab eller i et advokatfirma i samme kæde som dig, medmindre betingelserne herfor i AER og i databeskyttelsesreglerne er opfyldte.

2.1.3 Samspillet mellem AER's regler om tavshedspligt og databeskyttelsesreglerne

Som beskrevet ovenfor behandler du som advokat ofte personoplysninger, som både kan være omfattet af AER's regler om tavshedspligt og af databeskyttelsesreglerne. De to regelsæt varetager begge hensyn og interesser, som i et vist omfang er sammenfaldende, men du bør som advokat altid nøje vurdere, om for eksempel videregivelse af en personoplysning omfattet af din tavshedspligt, opfyldelse af din oplysningspligt, eller eventuel imødekommelse af andre af de registreredes rettigheder, er i overensstemmelse med begge regelsæt.

Datarådet har i to afgørelser vedrørende advokaters behandling af personoplysninger (hhv. videregivelse og brug) i forbindelse med en injuriesag, som Datatilsynet offentliggjorde den 5. januar 2023,[18] haft anledning til at vurdere samspillet mellem AER og databeskyttelsesreglerne. I de to afgørelser indgik begge regelsæt i vurderingen og førte konkret ikke til modsatrettede resultater. Du bør dog som nævnt altid vurdere de to regelsæts anvendelse på den givne situation. Datarådet fandt i øvrigt, at den advokat, som videregav oplysningerne, ikke havde et lovligt grundlag herfor, men at den advokat, som modtog dem, lovligt kunne bruge dem.[19]

18 Advokats videregivelse af oplysninger (journalnummer 2020-31-2882) og advokats brug af modtagne oplysninger (journalnummer 2020-31-3066). Afgørelserne er truffet af Datarådet, fordi de er af principiel karakter.

19 For en nærmere gennemgang af afgørelsernes betydning for dig som advokat se Advokatsamfundets nyhedsbrev af 9. februar 2023, som er tilgængeligt her https://www.advokatsamfundet.dk/nyheder-medier/nyheder/2023/dataradets-afgorelser-om-advokaters-videregivelse-og-brug-af-oplysninger/

2.1.4 Eksempler på situationer, hvor advokater behandler personoplysninger, som også kan være omfattet af tavshedspligten

2.1.4.1 Indledning

I dit arbejde som advokat skal du være opmærksom på, om de oplysninger, som du er i berøring med, er personoplysninger omfattet af databeskyttelsesreglerne, og om de er omfattet af din tavshedspligt.

Du bør derfor overveje følgende:

(i) er der er tale om personoplysninger? Hvis det er tilfældet, er databeskyttelsesreglerne relevante. Hvis der ikke er tale om personoplysninger, er det eventuelt kun AER, som er relevant.

(ii) er der tale om oplysninger omfattet af tavshedspligten? Hvis det er tilfældet, er AER relevant. Hvis oplysningerne ikke er omfattet af tavshedspligten, er det eventuelt kun databeskyttelsesreglerne, som er relevante.

Hvis der hverken er tale om personoplysninger eller oplysninger omfattet af tavshedspligten, er hverken databeskyttelsesreglerne eller AER relevante. Du kan derfor behandle oplysningerne uden at tage hensyn til reglerne. Er der omvendt tale om personoplysninger og oplysninger omfattet af tavshedspligten, finder både databeskyttelsesreglerne og AER anvendelse på oplysningerne. Du skal derfor sikre dig, at din behandling af oplysningerne efterlever begge regelsæt. I mange situationer vil det være muligt at efterleve begge regelsæt således, at der ikke opstår konflikt mellem databeskyttelsesreglerne (for eksempel oplysningspligt og indsigtsret) på den ene side og tavshedspligten på den anden, men der kan være tilfælde, hvor regelsættene fører til forskellige vurderinger, og hvor for eksempel din tavshedspligt som advokat må have forrang i forhold til databeskyttelsesreglerne. Nedenfor er givet nogle eksempler på situationer, hvor der behandles personoplysninger, som efter omstændighederne også kan være omfattet af din tavshedspligt, og hvad du skal være opmærksom på ved behandlingen.

2.1.4.2 Opfyldelse af oplysningspligt og overholdelse af tavshedspligt i forbindelse med undersøgelser og rådgivning i almindelige advokatopdrag

Hvis advokaten i forbindelse med et almindeligt opdrag for en klient, hvor klienten selv gennemfører en undersøgelse og indsamler oplysninger og dokumentation om for eksempel en medarbejders handlinger, og advokaten bistår med bevisvurdering og rådgivning om for eksempel disciplinære sanktioner, indhenter advokaten ikke oplysninger om medarbejderen direkte fra den registrerede, jf. GDPR artikel 13, men fra klienten, jf. GDPR artikel 14. I en sådan situation følger det af artikel 14, stk. 5, litra d, at de behandlede oplysninger undtages fra oplysningspligten, hvis de skal forblive fortrolige som følge af tavshedspligt. En sådan tavshedspligt følger af AER artikel 15 og retsplejelovens § 129.

Hvis det er advokaten, som indsamler oplysninger og dokumentation i forbindelse med undersøgelsen, jf. GDPR artikel 13, og dette sker fra andre end klienten, kan undtagelse ske ud fra en konkret vurdering med henvisning til databeskyttelsesloven § 22, stk. 1. Det afgørende er i givet fald, at tavshedspligten som et hensyn til private interesser skal afvejes mod hensynet til den registreredes interesser, hvilket kan begrunde, at advokaten er undtaget fra at opfylde oplysningspligten.

2.1.4.3 Opfyldelse af oplysningspligt og overholdelse af tavshedspligt i forbindelse med advokatundersøgelser på vegne af klienten (egentlige advokatundersøgelser)[20]

20 Om behandling af personoplysninger i forbindelse med advokatundersøgelser henvises i øvrigt også til *vejledning om advokatundersøgelser*, september 2022, afsnit 5 og bilag 1 https://www.advokatsamfundet.dk/media/a2adwgv2/vejledning-advokatunders%C3%B8gelser_final.pdf

Hvis der imidlertid er tale om, at advokaten gennemfører en egentlig advokatundersøgelse[21] i en personsag på vegne af en klient og indsamler dokumentation, herunder personoplysninger om både personen, som er genstand for undersøgelsen (den berørte), samt en række bipersoner for eksempel personens kollegaer og samarbejdspartnere (involverede), er advokaten som udgangspunkt dataansvarlig for den indsamling og behandling af personoplysninger, der sker. Advokaten er derfor enten omfattet af oplysningspligten i GDPR artikel 13 eller 14 alt efter, om oplysningerne er indsamlet direkte hos den registrerede eller hos andre. Advokaten er samtidig omfattet af de lovbestemte regler for tavshedspligt, der gælder for advokater, jf. AER artikel 15.

GDPR artikel 14, stk. 5, litra d, indeholder som nævnt en undtagelse til oplysningspligten for oplysninger, der ikke er indhentet direkte fra den registrerede. GDPR artikel 13 indeholder som ligeledes nævnt ikke en tilsvarende undtagelsesbestemmelse, men en undtagelse kan ud fra en konkret vurdering ske med henvisning til databeskyttelsesloven § 22, stk. 1. Det afgørende er i givet fald, at tavshedspligten som et hensyn til private interesser skal afvejes mod hensynet til den registreredes interesser, hvilket kan begrunde, at advokaten er undtaget fra at opfylde oplysningspligten. Tilsvarende hensyn kan gøres, hvis deltagere i undersøgelsen er lovet fortrolighed i forbindelse med deres udsagn i undersøgelsen.

Klienten bærer et selvstændigt dataansvar og dermed en selvstændig forpligtelse til at opfylde oplysningspligten. Klienten er oftest ikke underlagt tavshedspligt i samme omfang, hvorfor klienten er forpligtet til at sikre efterlevelse af oplysningspligten, så snart det kan ske uden kompromittering af advokatundersøgelsen. Det er muligt at udarbejde en fælles oplysningsskrivelse.

I samspillet mellem oplysningspligten efter databeskyttelsesreglerne og tavshedspligten efter AER, følger det af Advokatrådets vejledning om advokatundersøgelser, at advokatundersøgelsens karakter ofte tilsiger, at der skal udarbejdes en for undersøgelsen særskilt oplysningsskrivelse, hvor oplysningerne efter GDPR artikel 13 og 14 indgår.[22] Det vil derfor være muligt for advokaten at give de for advokatundersøgelsen nødvendige oplysninger i AER artikel 53 uden at bryde tavshedspligten, når advokaten gennemfører en egentlig advokatundersøgelse på vegne af en klient.

AER artikel 53 foreskriver for eksempel, at advokaten skal sikre, at de personer, der inddrages i undersøgelsen, har relevant mulighed for at varetage deres interesser, og hvorefter advokaten i forbindelse med den første reelle kontakt til de personer, der inddrages i en advokatundersøgelse, skal oplyse om undersøgelsens rammer og hovedelementer, herunder om advokatens og de pågældendes egne roller i undersøgelsen.

2.1.4.4 Opfyldelse af oplysningspligt og overholdelse af tavshedspligt i forbindelse med retssager

I forbindelse med retssager behandler advokaten personoplysninger om sagens parter, vidner, skønsmænd mv., og eventuelle bipersoner i sagen. Dette udgør en behandling af personoplysninger, hvor advokaten skal være opmærksom på at iagttage kravet om oplysning/underretning af de registrerede, som indeholder de oplysninger, som advokaten som dataansvarlig skal give for at opfylde oplysningspligten.

Personoplysningerne vil enten være indsamlet direkte hos den registrerede, jf. artikel 13, eller hos andre end den registrerede, jf. artikel 14.

For så vidt angår personoplysninger, som du selv indsamler hos modparter, vidner og skønsmænd mv., er det udgangspunktet, at oplysningspligten efter artikel 13 skal iagttages overfor disse personer, og at tavshedspligten ikke kan begrunde undtagelse. Oplysning/underretning kan her rent praktisk ske

21 Jf. definitionen heraf i Advokatrådets vejledning om Advokatundersøgelser (september 2022), afsnit 2.2, side 5.
22 Jf. Advokatrådets vejledning om Advokatundersøgelser (september 2022), bilag 1, side 25.

ved at linke til privatlivspolitikken i e-mail autosignaturen, der indeholder de oplysninger, som du som dataansvarlig skal give for at opfylde oplysningspligten.

I sager, hvor der skal indgives stævning på vegne af klienten, kan underretning ske ved, at der ved fremsendelsen af stævningen til modparten i e-mail autosignaturen linkes til privatlivspolitikken. Det er tilstrækkeligt, at modpartens advokat modtager underretningen. Det samme kan gøres, hvor en stævning modtages, og der kvitteres herfor.

Personoplysninger, som du modtager fra modparten, for eksempel i forbindelse med udveksling af processkrifter i en sag, herunder om vidner mv., indkaldt af modparten, er omfattet af artikel 14. Tilsvarende vil sagsakter fra klienten ofte indeholde oplysninger om andre end sagens parter i form af bipersoner (dvs. andre personer, som indgår eller omtales i en sag). Disse oplysninger er indsamlet hos andre end den registrerede, jf. artikel 14. Som udgangspunkt skal du ikke iagttage oplysningspligten over for disse personer, herunder bipersoner, idet du er underlagt tavshedspligt i forhold til de oplysninger, som du behandler som led i advokatopdraget, jf. artikel 14, stk. 5 litra d.

Du skal således ikke, efter at have modtaget sagsakter fra klienten, underrette alle de personer, som optræder i sagsakterne, om, at du behandler personoplysninger om dem. Der kan dog være undtagelser hertil, hvis en person, herunder biperson, i en retssag allerede er bekendt med sagen, og det vil derfor efter de konkrete omstændigheder ikke være et brud på tavshedspligten at iagttage oplysningspligten over for den pågældende person.

2.1.4.5 Opfyldelse af indsigtsanmodning og overholdelse af tavshedspligt i forbindelse med hvidvasksager
Hvis en advokat modtager en anmodning om indsigt i personoplysninger i henhold til GDPR artikel 15 fra en person, som indgår i en sag, som advokaten har varetaget for en klient, skal det vurderes, hvilke oplysninger anmoder kan få indsigt i, og om der er oplysninger, der er underlagt advokatens tavshedspligt. I forbindelse med sagen har advokaten foretaget underretning i henhold til hvidvasklovens § 26, bl.a. fordi personen/anmoder oplyste over for advokaten, at klienten havde været involveret i en mistænkelig transaktion.

Du skal vurdere, om der indgår personoplysninger i underretningen. Hvis din klient er en fysisk person, vil der være tale om behandling af personoplysninger (for eksempel af personens navn mv.), og databeskyttelsesreglerne finder anvendelse. Er der omvendt tale om et selskab og dermed en juridisk person, finder databeskyttelsesreglerne ikke anvendelse.

Efter GDPR artikel 15 er det udgangspunktet, at anmoder skal have adgang til og kopi af alle behandlede personoplysninger. I dette tilfælde vil det dog være muligt at undtage indsigt med hjemmel i databeskyttelseslovens § 22, stk. 2, nr. 4 (efterforskning af strafbare handlinger). Hvis din klient anmoder om indsigt, følger det af hvidvasklovens § 26, stk. 7, at der ikke er indsigtsret i registrerede personoplysninger vedrørende en underretning.

En underretning i henhold til hvidvasklovens § 26 er en fortrolig oplysning, som er omfattet af tavshedspligten, jf. retsplejelovens § 129 og AER artikel 15 samt artikel 16. Som følge heraf må du ikke videregive oplysningen til den, der anmoder om indsigt, medmindre du er retligt forpligtet til det, jf. AER artikel 18, nr. 2, eller videregivelse sker i berettiget varetagelse af åbenbar almeninteresse eller af eget eller andres tarv, jf. AER artikel 18, nr. 3. Da der er krav om hemmeligholdelse af underretninger efter hvidvaskloven, er det ikke muligt at videregive oplysningen med samtykke fra klienten, jf. AER artikel 18, nr. 1. Hvorvidt det er muligt at videregive oplysningen med henblik på varetagelse af en åbenbar almeninteresse eller af eget eller andres tarv beror på en konkret vurdering. Da konsekvensen

af en forkert vurdering efter omstændighederne kan være en overtrædelse af tavshedspligten, skal en videregivelse vurderes nøje.

Hvis der indgår personoplysninger i underretningen, vil der ikke være en retlig forpligtelse til at videregive dem i forbindelse med indsigtsanmodningen, idet det som sagt vil være muligt at undtage indsigt i henhold til databeskyttelsesloven § 22, stk. 2, nr. 4.

3. Dokumentationskrav for advokaten

3.1 Indledning

Der gælder et overordnet krav om, at efterlevelse af databeskyttelsesreglerne skal kunne dokumenteres, jf. artikel 5, stk. 2. Hvis et forhold, tiltag eller for eksempel en vurdering ikke kan dokumenteres, anses det derfor heller ikke som værende sket eller gjort. Dette betyder, at du som advokat skal sørge for at have dokumentation for din efterlevelse af databeskyttelsesreglerne. De vurderinger, som du løbende foretager i forbindelse med håndteringen og vurderingen af databeskyttelsesretlige sager og spørgsmål, bør du også dokumentere, så du kan redegøre for dit standpunkt.

3.2 Fortegnelse (artikel 30)

Fortegnelseskravet i GDPR artikel 30 er et af de mest centrale dokumentationskrav i GDPR. Kravet betyder, at du som dataansvarlig skal føre en skriftlig fortegnelse over de behandlingsaktiviteter, som du er ansvarlig for.[23] Er du (undtagelsesvis) selv databehandler, er du også omfattet af kravet. Kravene til det nærmere indhold følger af artikel 30, stk. 1 og 2., hvorefter det bl.a. skal fremgå, hvilke typer personoplysninger der behandles, hvordan oplysningerne modtages, hvad oplysningerne bruges til, hvordan personoplysningerne bliver behandlet internt i advokatvirksomheden, og til hvem og hvordan oplysningerne bliver videregivet til eksternt, samt hvordan oplysningerne opbevares og hvor længe. Formålet med fortegnelsen er at kunne dokumentere, hvordan databeskyttelsesreglerne efterleves. Fortegnelsen skal derfor også foreligge skriftligt og elektronisk og skal stilles til rådighed for Datatilsynet, hvis tilsynet anmoder herom. I øvrigt er fortegnelsen intern og ikke omfattet af for eksempel indsigtsretten.

Fortegnelsen skal indeholde oplysninger om behandlingsaktiviteterne vedrørende klientforholdet, herunder etablering, sagsoprettelse og løbende varetagelse, samt hvidvasktjek/KYC. Fortegnelsen vil for de fleste advokatvirksomheder også skulle omfatte behandlingsaktiviteter vedrørende:

- HR-administration, herunder rekruttering og ansættelse
- Markedsføring, herunder hjemmeside og cookies, arrangementer og kurser, CRM
- Økonomi, herunder for eksempel oprettelse af klientkonto i bank (hvis sådanne oprettes)
- Whistleblower-administration (hvis krav om ordning i forhold til whistleblowerloven eller hvis frivillig ordning)
- Offentlige registreringer (for eksempel tinglysning, CVR mv.)

I bilag 1 er givet overordnede forslag til, hvordan artikel 30 fortegnelsen kan udfyldes, hvor de overordnede formål med behandlingen af personoplysninger er hhv. juridisk rådgivning i forbindelse med retssager og voldgiftssager samt HR-administration. Afhængig af hvilken type juridisk rådgivning og hvilke sager advokatfirmaet leverer ydelser inden for, skal fortegnelsen også indeholde tilsvarende oplysninger om de personoplysninger, der behandles mv. i den forbindelse. Det kan for eksempel være i forbindelse med rådgivning og sager om bobehandling, fonde, fast ejendom og ejendomsadministration, ansættelsesret, undersøgelsessager, virksomhedsoverdragelser, selskabsret, forsikring, skat mv.

23 Selvom GDPR indeholder en undtagelse til kravet om at føre fortegnelser, hvis virksomheden beskæftiger under 250 personer, må fortegnelseskravet antages at omfatte langt de fleste advokater. Det skyldes, at undtagelsen bl.a. kun finder anvendelse, hvis behandlingen af personoplysninger kun er lejlighedsvis, eller hvis behandlingen ikke omfatter følsomme personoplysninger og/eller oplysninger om strafbare forhold. Situationen kan dog være den, at nogle af dine behandlingsaktiviteter er omfattet af fortegnelseskravet, mens andre er undtaget.

Hvis du som advokat er databehandler (for eksempel i forbindelse med udbud af datarum, værktøjer til udarbejdelse af dokumenter eller kontrakthåndtering, opbevaring af ledelses- og bestyrelsesmateriale mv.), hvor det blot er selve værktøjet, der stilles til rådighed, skal fortegnelsen også indeholde beskrivelse af behandlingsaktiviteterne vedrørende disse ydelser.

Datatilsynet har endvidere offentliggjort en vejledning om fortegnelsen.[24]

3.3 Øvrige dokumentationskrav

Udover kravet om at føre en fortegnelse over behandlingsaktiviteter indeholder GDPR mange yderligere krav om dokumentation i forhold til for eksempel følgende:

- Samtykke som behandlingsgrundlag, jf. artikel 7
- Opfyldelse af oplysningspligt, jf. artikel 13 og 14
- Databeskyttelsespolitik og retningslinjer (efter omstændighederne), jf. artikel 24
- Databehandleraftale, jf. artikel 28
- Risikovurderinger, jf. artikel 32
- Databrud, jf. artikel 33-34
- Konsekvensanalyser, jf. artikel 35
- Overførselsgrundlag til tredjelande, jf. artikel 46

En vigtig del af advokaters arbejde med GDPR er derfor at udarbejde og sikre den fornødne dokumentation.

24 Datatilsynets vejledning om fortegnelse: https://www.datatilsynet.dk/Media/E/5/Fortegnelse%20(3).pdf

4. Advokatens persondataretlige roller

4.1 Indledning

Som nævnt er det afgørende, at det afklares, om du er dataansvarlig eller databehandler, eller om der måske er tale om en situation, hvor du er dataansvarlig sammen med andre (fælles dataansvar) for eksempel et socialt medie som LinkedIn, X eller Facebook, i forhold til en behandling af personoplysninger.[25] I visse situationer kan der også være tale om, at advokaten og klienten hver især har et selvstændigt dataansvar.

Som dataansvarlig bestemmer du formålet med behandlingen (for eksempel rådgivning i forbindelse med retssager og voldgiftssager) og hjælpemidlerne (for eksempel Outlook). Det er dog også den dataansvarlige, der står på mål for, at databeskyttelsesreglerne overholdes, og som derfor bl.a. skal sikre sig, at:

- principperne for behandling er overholdt, og at det kan dokumenteres, jf. afsnit 6.2.
- der er grundlag for behandling af oplysninger, jf. afsnit 6.8.
- den registreredes rettigheder overholdes, jf. afsnit 7.
- persondatabrud, som skal anmeldes til Datatilsynet, bliver anmeldt korrekt, jf. afsnit 8.

Som databehandler bestemmer du ikke formålet med behandlingen og hjælpemidlerne, men handler efter instruks fra den dataansvarlige.

Inden du behandler personoplysninger, skal du også sikre dig, at der er et behandlingsgrundlag for behandlingen. Personoplysninger må nemlig kun behandles, hvis der er hjemmel til det.

I dette kapitel kan du læse, hvordan du afklarer, om du er dataansvarlig (eventuelt fælles dataansvarlig) eller databehandler og om advokaters dataretlige rolle i en række forskellige situationer.

4.2 Advokatens persondataretlige udgangspunkt

Som advokat er du som altovervejende hovedregel dataansvarlig, når du behandler personoplysninger i forbindelse med advokatbistand og anden juridisk rådgivning. Baggrunden herfor er bl.a., at du som advokat træffer egne beslutninger om udførelsen af opdraget, herunder formålet med og hjælpemidlerne til behandlingen af personoplysningerne, ikke er underlagt en instruktionsbeføjelse fra klienten og er underlagt særlige regler om bl.a. uafhængighed og tavshedspligt, jf. reglerne i retsplejeloven og AER. Hertil kommer, at formålet med din ydelse som advokat ikke er behandling af personoplysninger, men rådgivning om juridiske forhold. Hvis du er i tvivl om, hvilken rolle du har i en given situation, kan du anvende ovennævnte forhold til at vurdere, om du er dataansvarlig eller databehandler.

Med dataansvaret følger en række forpligtelser. En konsekvens af at være dataansvarlig er bl.a. oplysningspligten, hvorefter der skal gives en række oplysninger til den registrerede, jf. GDPR artikel 13 og 14. Bøderne for manglende overholdelse af databeskyttelsesreglerne, jf. GDPR artikel 83, følger også den dataansvarlige.[26]

25 Definitionen på en dataansvarlig og en databehandler fremgår af GDPR artikel 4, nr. 7 og artikel 4, nr. 8.
26 Bødeansvar for databehandlere er dog også muligt i situationer, hvor disse er pligtsubjekt i henhold til regler i GDPR.

Hovedreglen om at du som advokat er dataansvarlig modificeres dog, hvis der er tale om en bunden opgave, hvor din handlefrihed og mulighed for at bestemme formål og hjælpemidler er meget begrænset, for eksempel fordi du fungerer som underleverandør til en anden advokat i forbindelse med løsning af en opgave, eller fordi du måske stiller et it-system eller løsning til rådighed (for eksempel et datarum til brug for en M&A transaktion, hosting af dokumenter som for eksempel kontrakter, et whistleblowersystem eller lignende), jf. ovenfor afsnit 3.2, hvor det overvejende formål mere bliver behandling af personoplysninger end juridisk rådgivning. Databehandler har også en række forpligtelser efter GDPR og skal for eksempel også føre en fortegnelse over behandlingsaktiviteter, leve op til kravene i artikel 28, herunder stille fornødne garantier for passende organisatoriske og tekniske foranstaltninger, indgåelse af databehandleraftale mv. Et fælles dataansvar er også muligt, jf. artikel 26, hvis advokater i fællesskab bestemmer formålene og hjælpemidlerne med en behandling. Det kan for eksempel være tilfældet, hvor flere selvstændige advokater indgår i et kuratel, bistår en klient i en transaktion eller lign. Mange advokatfirmaer benytter sociale medier som for eksempel LinkedIn til markedsføring og publicering af forskellige former for indhold, og her vil der oftest være et fællesdataansvar for behandling af visse personoplysninger. Konsekvensen af et fælles dataansvar er bl.a., at de dataansvarlige på en gennemsigtig måde skal fastlægge deres respektive forpligtelser i forbindelse med for eksempel oplysningspligten og de øvrige af de registreredes rettigheder og for eksempel udpeger et fælles kontaktpunkt.

Bilag 2 til vejledningen indeholder en oversigt over advokatens persondataretlige rolle i en række situationer, herunder om advokaten er dataansvarlig eller databehandler, selvstændigt dataansvar for klienten mv.

4.3 Databehandleraftaler (artikel 28)

Advokatfirmaers aftaler med leverandører om køb af en ydelse eller for eksempel et it-system kan indebære, at leverandøren behandler personoplysninger på vegne af advokatfirmaet. I så fald skal der indgås en databehandleraftale mellem advokatfirmaet som dataansvarlig og leverandøren som databehandler. Aftalen skal indgås skriftligt, jf. artikel 28, stk. 3, og skal kunne dokumenteres.

Datatilsynet har udarbejdet en skabelon, som kan anvendes i forbindelse med indgåelse af databehandleraftaler. Ved anvendelse af skabelonen sikres det, at den indgåede aftale lever op til de krav, som Datatilsynet stiller til en gyldig databehandleraftale. Bilag 3 til vejledningen indeholder et forslag til, hvordan bilag A-C i Datatilsynets standarddatabehandleraftale kan udfyldes.

Det er vigtigt at påse, at der er interne processer, der sikrer, at der foretages en vurdering af risikoen for persondatassikkerhed og informationssikkerhed, jf. afsnit 8.1-8.4., herunder en forretningsmæssig vurdering, og at der indgås en databehandleraftaler, før behandlingen af personoplysninger påbegyndes.

Såfremt der ikke behandles personoplysninger, kan der i stedet være behov for at indgå en fortrolighedsaftale med den pågældende tredjepart, inden oplysninger må videregives.

5. Overførsel af personoplysninger til tredjelande

5.1 Indledning

Advokatfirmaer kan have behov for at overføre personoplysninger til tredjelande, dvs. lande udenfor EU/EØS. Dette kan for eksempel være tilfældet, hvis advokatfirmaet indgår aftale med en it-leverandør, som er hjemmehørende i et tredjeland eller for eksempel udfører support fra et eller flere tredjeland, og i den forbindelse behandler personoplysninger. I dette afsnit beskrives reglerne for sådanne overførsler. Overførsel til tredjelande sker ofte uagtsomt ved brug af softwareløsninger, herunder særligt cloud-løsninger, som downloades fra internettet, og hvor firmaet bag løsningen er etableret uden for EU/EØS. Det er således vigtigt at være opmærksom på reglerne om tredjelandsoverførsel, når du som advokat bruger ad-hoc softwareløsninger, eller hvis du skal indkøbe et it-system, der har data i cloud, da det kan indebære en utilsigtet overførsel til et tredjeland.

5.1.1 Anvendelse af overførselsgrundlag (artikel 45-46)

Overførsel af personoplysninger til tredjelande er underlagt GDPR's kapitel V, som forudsætter, at personoplysninger kun må overføres til tredjelande udenfor EU/EØS, hvis de nødvendige betingelser herfor er opfyldt.

Der skelnes mellem sikre tredjelande udenfor EU/EØS, som EU-Kommissionen har vurderet, har et tilstrækkeligt beskyttelsesniveau, jf. GDPR artikel 45, og usikre tredjelande udenfor EU/EØS, som ikke har denne vurdering.

5.1.1.1 Overførsel til sikre tredjelande:

Overførsel til et tredjeland kan finde sted uden specifik godkendelse, hvis EU-Kommissionen har fastslået, at landet har et tilstrækkeligt beskyttelsesniveau. Sikre tredjelande er pt.: [27]

- Andorra
- Argentina
- Guernsey
- Isle of Man
- Israel
- Jersey
- New Zealand
- Schweiz
- Storbritannien
- Sydkorea
- Uruguay

27 Data protection adequacy for non-EU countries (europa.eu)

Endvidere er følgende områder og sektorer i tredjelande godkendt som sikre:

- USA: Modtagere certificeret under EU-U.S. Data Privacy Framework
- Canada: Modtagere omfattet af den canadiske Personal Information Protection and Electronic Documents Act (PIPEDA)
- Færøerne: Modtagere omfattet af den færøske lov om behandling af personoplysninger. Overførsler til rigsmyndighederne på Færøerne er ikke omfattet
- Japan: Modtagere omfattet af den japanske Act on the Protection of Personal Information (APPI)

Eksempel:

Et advokatkontor etableret i Danmark ønsker at overføre personoplysninger til en databehandler i Singapore. Da EU-Kommissionen har fastslået, at Singapore har et tilstrækkeligt beskyttelsesniveau, kan overførslen som udgangspunkt ske uden videre. Hvis databehandleren var etableret i USA og certificeret under EU-U.S. Data Privacy Framework omfattende formålet med den konkrete overførsel, kan overførslen ligeledes som udgangspunkt også ske uden videre. Ingen af de nævnte overførsler kræver således at EU-Kommissionens standardkontraktbestemmelser (SCC) for overførsel af personoplysninger anvendes.

5.1.1.2 Overførsel til usikre tredjelande:
Hvis et tredjeland ikke er anerkendt som sikkert, kan overførsel stadig finde sted, hvis det kan tilsikres, at de fornødne garantier for, at beskyttelsesniveauet for de overførte oplysninger i det væsentlige svarer til beskyttelsesniveauet inden for EU/EØS, jf. GDPR artikel 46, stk. 1.

Ved overførsel af personoplysninger til usikre tredjelande skal følgende risikovurdering foretages: [28]

- Kortlægning af overførsler: Få et grundigt overblik ved at kortlægge overførslen af personoplysninger til tredjelande.
- Afklaring af overførselsgrundlag: Afklar, hvilket overførselsgrundlag der kan benyttes, for eksempel EU-Kommissionens standardkontraktbestemmelser (SCC) eller ad-hoc kontrakter godkendt af Datatilsynet.
- Vurdering af overførselsgrundlagets effektivitet: Sikre at det valgte overførselsgrundlag også er effektivt i praksis. Dette er ikke tilfældet, hvis dataimportøren pga. lovgivning og/eller praksis i tredjelandet er forhindret i at opfylde sine forpligtelser.
- Undersøgelse af tredjelandets praksis: Det er særligt relevant at undersøge offentlige myndigheders praksis i tredjelandet, hvis lovgivningen formelt lever op til EU's standarder, men ikke efterleves i praksis, eller hvis lovgivningen og praksis er uforenelig med de forpligtelser, der er fastsat i det valgte overførselsgrundlag.
- Inddragelse af dataimportøren i vurderingen: Det kan være naturligt at inddrage dataimportøren i tredjelandet i vurderingen, da denne typisk vil have et bedre lokalkendskab.
- Konsultation af informationskilder: Konsultere andre informationskilder, som for eksempel risikovurderinger fra Center for Cybersikkerhed, for at støtte vurderingen.

28 Vejledning om overførsel til tredjelande.pdf (datatilsynet.dk)

- Supplerende foranstaltninger: Hvis det vurderes, at det valgte overførselsgrundlag ikke er effektivt i praksis, skal der træffes passende supplerende foranstaltninger for at imødegå dette. Disse foranstaltninger kan være tekniske, organisatoriske og kontraktuelle.

Det er vigtigt at dokumentere, hvilke overvejelser og beslutninger der ligger til grund for vurderingen, og at der kan redegøres for disse efterfølgende.

Eksempel:

Et advokatkontor etableret i Danmark ønsker at overføre personoplysninger til en databehandler i Indien. Da EU-Kommissionen ikke har fastslået, at Indien har et tilstrækkeligt beskyttelsesniveau, kan overførslen som udgangspunkt ikke ske uden videre. Advokatkontoret må i denne situation foretage en risikovurdering med henblik på at sikre, at de fornødne garantier for at beskyttelsesniveauet for de overførte oplysninger i den konkrete overførsel til Indien i det væsentlige svarer til beskyttelsesniveauet inden for EU/EØS.

5.1.1.3 EU-Kommissionens standardkontraktbestemmelser (SCC)
Et af de primære overførselsgrundlag til brug for overførsel af personoplysninger til usikre tredjelande er EU-Kommissionens standardkontraktbestemmelser, jf. GDPR artikel 46, stk. 2, litra c. Disse bestemmelser fungerer som en skabelon, der udfyldes og underskrives af både dataeksportøren og dataimportøren, og omfatter forskellige moduler, der skal anvendes afhængigt af den specifikke overførselssituation. Disse situationer inkluderer:

- Modul 1 - overførsel fra dataansvarlig til dataansvarlig.
- Modul 2 - overførsel fra dataansvarlig til databehandler.
- Modul 3 - overførsel fra databehandler til databehandler.
- Modul 4 - overførsel fra databehandler til dataansvarlig.

Det er ikke nødvendigt at opnå forhåndsgodkendelse fra Datatilsynet for at anvende EU-Kommissionens standardkontraktbestemmelser. Det er dog essentielt, at dataeksportøren sikrer, at bestemmelserne anvendes korrekt, og at både dataeksportøren og dataimportøren er i stand til at opfylde de forpligtelser, der følger heraf.

Standardkontraktbestemmelserne indeholder en "docking clause", der tillader løbende tilføjelse eller udskiftning af parter i aftalen, hvilket kan være særligt relevant i komplekse behandlingssituationer.

Det er tilladt at integrere EU-Kommissionens standardkontraktbestemmelser som en del af en mere omfattende kontrakt mellem dataeksportøren og dataimportøren, samt at tilføje yderligere klausuler eller garantier, forudsat at disse ikke er i konflikt med standardkontraktbestemmelserne. Dette inkluderer muligheden for at inkludere bestemmelser om supplerende sikkerhedsforanstaltninger.

Ændringer i standardkontraktbestemmelserne, der ikke overholder deres oprindelige indhold, kan resultere i, at aftalen betragtes som en ad hoc-kontrakt, hvilket kræver godkendelse fra Datatilsynet.

5.1.1.4 Undtagelser i særlige situationer
GDPR artikel 49, stk. 1, indeholder bestemmelser for overførsel af personoplysninger til usikre tredjelande i særlige situationer, hvor der ikke foreligger en afgørelse om tilstrækkelighed fra EU-Kommissionen,

eller hvor det ikke kan tilsikres, at de fornødne garantier for, at beskyttelsesniveauet for de overførte oplysninger i den konkrete overførsel i det væsentlige svarer til beskyttelsesniveauet inden for EU/EØS.

Disse særlige undtagelser skal fortolkes restriktivt og kan kun benyttes i begrænset omfang. Eksempelvis kan ikke alle undtagelser anvendes ved gentagne overførsler, masseoverførsler og strukturelle overførsler, ligesom ikke alle undtagelser kan anvendes af offentlige myndigheder.

Undtagelserne omfatter således alene særlige situationer, hvor overførslen er nødvendig af følgende grunde:

- Den registrerede har udtrykkeligt samtykket til den foreslåede overførsel, efter at være blevet informeret om de mulige risici ved sådanne overførsler på grund af manglen på en afgørelse om tilstrækkelighed og passende sikkerhedsforanstaltninger.
- Overførslen er nødvendig for opfyldelsen af en kontrakt mellem den registrerede og den dataansvarlige eller for gennemførelsen af foranstaltninger, som den registrerede har anmodet om før indgåelsen af en kontrakt.
- Overførslen er nødvendig for indgåelsen eller opfyldelsen af en kontrakt, der er indgået i den registreredes interesse mellem den dataansvarlige og en anden fysisk eller juridisk person.
- Overførslen er nødvendig af væsentlige hensyn til offentlige interesser.
- Overførslen er nødvendig for fastlæggelse, udøvelse eller forsvar af retskrav.
- Overførslen er nødvendig for at beskytte den registreredes eller andres vitale interesser, når den registrerede fysisk eller juridisk er ude af stand til at give samtykke.
- Overførslen sker fra et register, som ifølge national lovgivning er beregnet til at give oplysninger til offentligheden, og som er åbent for konsultation enten af offentligheden generelt eller af enhver person, der kan påvise en legitim interesse, men kun i det omfang de betingelser, der er fastsat i national lovgivning for konsultation, er opfyldt i det konkrete tilfælde.

Eksempel:

Et advokatkontor etableret i Danmark repræsenterer en dansk klient, hvor myndighederne i Thailand har rejst tiltale for kartelvirksomhed. Til brug for at kunne forsvare sin klient i forbindelse med retssagen, der skal foregå i Thailand, har advokatkontoret behov for at overføre personoplysninger til klientens thailandske advokat. Da personoplysningerne er nødvendige for, at advokatkontoret kan forsvare klienten i retssagen, kan advokatkontoret overføre personoplysningerne til Thailand, som en særlig undtagelse på trods af, at EU-Kommissionen ikke har fastslået, at Thailand har et tilstrækkeligt beskyttelsesniveau.

6. Behandlingsprincipperne

6.1 Indledning

GDPR artikel 5 indeholder grundlæggende principper og regler for behandling af personoplysninger. Som advokat må du behandle personoplysninger, hvis 1) principperne iagttages, og 2) hvis du har et lovligt grundlag for behandlingen. Principperne indeholder krav, som du skal overholde, uanset hvilken type personoplysninger du behandler, og uanset hvilket grundlag oplysningerne behandles på. Behandlingsprincipperne bør således hele tiden være styrende for, hvordan du håndterer personoplysninger.

Principperne beskrives nærmere nedenfor med særligt fokus på kravet om opbevaring og sletning og dets betydning for advokater.

6.2 Lovlighed, rimelighed og gennemsigtighed

Princippet om lovlighed mv. indebærer, at behandling af personoplysninger skal være lovlig, rimelig og gennemsigtig.[29] Behandlingen skal således være i overensstemmelse med lovgivningen, dvs. primært GDPR og databeskyttelsesloven, men også anden lovgivning, for eksempel retsplejeloven og hvidvaskloven samt være rimelig.[30] Der stilles desuden krav om transparens, dvs. behandlingen skal ske på en måde, som er oplyst over for den registrerede.

6.3 Formålsbegrænsning

Personoplysninger må alene behandles til det oplyste formål og må ikke viderebehandles på en måde, som er uforenelig hermed.[31] Det betyder, at du som advokat ikke må bruge en oplysning, som du har indsamlet til et formål til et andet formål, medmindre det kan siges at være foreneligt med det. Dette skal du være opmærksom på, hvis du for eksempel i forbindelse med en sag har indsamlet oplysninger, som du efterfølgende også overvejer at bruge i en anden sammenhæng.[32]

6.4 Proportionalitet og dataminimering

Ifølge GDPR artikel 5, stk. 1 c) skal personoplysninger være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til formålene med deres behandling. Bestemmelsen indeholder både et krav om proportionalitet og et krav om dataminimering og betyder, at du for eksempel kun bør behandle personoplysninger i det omfang, det er nødvendigt for at løse den opgave, du sidder med. I praksis skal du derfor ikke indhente personoplysninger blot for at være på den sikre side, eller fordi du måske tænker, at du senere kan få brug for dem. Du bør løbende overveje, om du har behov for de personoplysninger, som du aktivt indhenter i sagen. Tilsvarende skal du slette personoplysninger, som du modtager i sagen, for eksempel fra din klient, hvis de ikke er relevante i forhold til håndteringen af sagen.

29 Jf. GDPR artikel 5, stk. 1, litra a).

30 I rimelighedsvurderingen indgår bl.a., hvordan (og af hvem) oplysninger er tilvejebragt, og hvilke modsatrettede interesser der er i behandling af oplysningerne, jf. Datatilsynets afgørelse i journalnummer 2024-32-0482, hvor behandling af ulovligt indhentede oplysninger fandtes at være i overensstemmelse med databeskyttelsesreglerne.

31 Jf. GDPR artikel 5, stk. 1, litra b).

32 Vær også opmærksom på, at oplysninger, som er indhentet efter krav i hvidvaskloven, udelukkende må benyttes til forebyggelse af hvidvask og terrorfinansiering. Oplysninger, som du som advokat indhenter om klientens identitet mv. til dette formål, kan altså ikke inddrages i andre sammenhænge, medmindre du som advokaten direkte eller indirekte har fået tilladelse hertil.

Det er vigtigt, at du som advokat hele tiden overvejer personoplysningernes nødvendighed i forhold til opgaven eller sagen. I situationer, hvor oplysningerne ikke er nødvendige, bør du derfor udelade eller anonymisere dem. Herudover har princippet også den betydning, at du alene må tilgå de personoplysninger, som du har et arbejdsbetinget behov for. Dette er også grunden til, at der systemteknisk skal opstilles begrænsninger i, hvilke sager der er adgang til, jf. afsnit 2.1.2.3.

Endelig er det også vigtigt løbende at overveje, om der er behov for at udlevere de personoplysninger, som du videregiver til andre. Det er vigtigt at forholde sig til, hvilke personoplysninger der er relevante for håndtering af sagen og sørge for at udelade de oplysninger, der ikke er relevante for at kunne håndtere sagen.

Dataminimering kan for eksempel være relevant i følgende situationer:

1) videndeling i advokatfirmaet,

2) deling af mødereferater,

3) sagsresuméer,

4) omtale af sager i medier, herunder på sociale medier og lign.,

5) fremsendelse af sag/oplysninger ifm. for eksempel anmodning om responsum, vurdering, omkostnings- godtgørelse, specifikation af faktura, indhentelse af tilbud, ansøgning eller lign., og

6) indlevering og videregivelse af oplysninger til retten.

For så vidt angår videregivelse af oplysninger til retten, oplyser Domstolsstyrelsen, at parter i en civil retssag ikke må videregive personoplysninger til retten, som ikke er relevante for retssagens behandling. Du skal som advokat forholde dig aktivt dig til, hvilke personoplysninger der ikke er relevante for sagen og udelade disse fra din sagsfremstilling og de bilag, som du sender til retten.

Domstolsstyrelsen nævner følgende som eksempler på overflødige oplysninger:[33]

- Identifikationsoplysninger om personer, som sagen ikke drejer sig om, for eksempel kontaktpersoner hos kommunen, som indgår i diverse bilag
- Oplysninger om sagsøgers eller sagsøgtes private forhold, som er sagen uvedkommende
- CPR-numre er normalt ikke relevante for sagens behandling og skal derfor som udgangspunkt udelades. Såfremt CPR-numre anvendes af en af parterne til identifikation af en person, kan de dog indgå i materialet

Retten kan i øvrigt bede dig om at fjerne personoplysninger, som ikke er relevante for sagen.

6.5 Rigtighed

Princippet om rigtighed indeholder en pligt til at sørge for, at de personoplysninger, du behandler, er korrekte og ajourførte samt en pligt til straks at slette eller ajourføre urigtige oplysninger.[34] Bliver du

33 Jf. Vejledning til professionelle om brug af minretssag.dk https://www.domstol.dk/media/ym3llzjv/vejledning-til-domstolenes-sagsportal-minretssagdk.pdf Domstolsstyrelsen har også tidligere nævnt følgende eksempler: (i) afgørelser i en materialesamling, som ikke er pseudomiserede, (ii) navne og personnumre på beboerne i sammenligningslejemålet i en boligretssag og (iii) afgørelser om tredjemænd som en part fremlægger under påberåbelse af lighedsgrundsætningen eller lign.
34 Jf. GDPR artikel 5, stk. 1, litra d).

opmærksom på, at en personoplysning er forkert, for eksempel fordi der er tale om en gammel og ikke opdateret oplysning, skal du enten slette eller ajourføre oplysningen.

6.6 Opbevaringsbegrænsning og sletning

GDPR indeholder som nævnt et krav om sletning. Således skal personoplysninger opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum, end det der er nødvendigt til de formål, hvortil de pågældende oplysninger behandles.[35] Hvis en oplysning ikke længere er nødvendig, skal den med andre ord enten anonymiseres eller slettes. Databeskyttelsesreglerne indeholder imidlertid ikke konkrete frister for, hvornår anonymisering eller sletning skal ske. Dette beror på en konkret vurdering af, om oplysningen (fortsat) er nødvendig. Forpligtelsen til sletning bør iagttages gennem interne slettefrister og så vidt muligt opsætning af automatisk sletning. Der kan herudover opstå situationer, hvor der opbevares personoplysninger, som der ikke længere er et sagligt behov for, hvorefter det er vigtigt at iværksætte en sletningsproces, hvis dette ikke sker automatisk.

GDPR indeholder heller ikke regler om, at personoplysninger skal opbevares i bestemte tidsperioder. Der er således ikke krav om opbevaring af personoplysninger i for eksempel 5 år eller lign. Hvis en personoplysning er nødvendig, korrekt og ajourført, skal den fortsat opbevares.

Konkrete frister for opbevaring af oplysninger, og herunder personoplysninger, fremgår dog i visse tilfælde af særlovgivningen. Således indeholder for eksempel bogføringsloven og hvidvaskloven i hhv. § 12 og § 30 konkrete tidsmæssige krav til opbevaring. Disse krav gælder naturligvis også for advokater.

Af særlig relevans for advokater indeholder AER krav om opbevaring af sagsakter efter sagens afslutning, jf. artikel 70, og reglerne om interessekonflikter, jf. bl.a. artikel 7, nødvendiggør også, at advokater opbevarer oplysninger med henblik på interessekonflikttjek og løbende vurdering. En manglende efterlevelse af disse regler vil være en tilsidesættelse af god advokatskik, jf. retsplejelovens § 126.

Forældelsesloven indeholder også frister, for eksempel den absolutte forældelsesfrist på 10 år, som er relevante i forhold til, hvor længe en personoplysning skal opbevares eller slettes. Som nævnt er det dog vigtigt at have for øje, at et krav om opbevaring i en bestemt tidsmæssig periode ikke er ensbetydende med, at personoplysninger uden videre skal slettes ved periodens udløb. Hvis oplysningerne stadig er relevante udover den nævnte periode, skal de fortsat opbevares.

I de følgende afsnit beskrives frister i særlovgivningen, som har særlig relevans for advokaters opbevaring og sletning af personoplysninger, AER's indvirkning herpå og forældelseslovens betydning.

6.6.1 Krav til opbevaring i særlovgivningen

Bogføringsloven indeholder i § 12 et krav om opbevaring af regnskabsmateriale i 5 år fra udgangen af det regnskabsår, materialet vedrører.[36] Dette krav gælder også for bogføringspligtige advokater og personoplysninger, som er nødvendige i denne sammenhæng.

Hvidvasklovens § 30 indeholder også konkrete tidsmæssige krav til opbevaring, som også gælder for advokater. Det følger af hvidvasklovens § 30, at bl.a. oplysninger indhentet i forbindelse med opfyldelse

35 Jf. GDPR artikel 5, stk. 1, litra e).

36 Se i øvrigt pkt. 6.5-6.7 i Erhvervsstyrelsens vejledning om bogføringsloven https://erhvervsstyrelsen.dk/vejledning-bogfoeringsloven#chapter6-5. Revisorloven indeholder i § 23 også et krav om opbevaring af arbejdspapirer i 5 år fra tidspunktet for underskrivelse af den erklæring, som materialet vedrører.

af kravene om kundekendskabsprocedurer, herunder identitets- og kontroloplysninger samt kopi af foreviste legitimationsdokumenter, skal opbevares i 5 år. Fristen regnes fra klientforholdets ophør, hvilket typisk vil være fra udstedelsen af slutafregningen i sagen, jf. Advokatrådets reviderede hvidvaskvejledning.[37] Som advokat skal du dermed som hovedregel opbevare eventuelle personoplysninger indhentet i medfør af hvidvasklovens § 30 i 5 år efter klientforholdes ophør ved udstedelse af slutafregningen. Det fremgår også af vejledningen, at i et løbende klientforhold med flere forskellige sager regnes fristen fra afslutningen af den enkelte sag.

Pligten efter bogføringsloven og hvidvaskloven til at opbevare de nævnte oplysninger i 5 år taler således for en generel opbevaringsperiode for advokater på mindst 5 år.

6.6.2 AER's regler om interessekonflikter og deres indvirkning på advokaters opbevaring og sletning af personoplysninger

AER kapitel 4 indeholder en række regler, som forpligter advokater til at sikre sig mod, at interessekonflikter ikke opstår og til ikke at bistå en klient, hvis en interessekonflikt opstår.

De mest centrale regler er artikel 7, som forpligter advokaten til at foretage interessekonflikttjek inden påtagelse af en sag og til løbende at vurdere, om der er risiko for konflikt, hvis forholdene ændrer sig, og artikel 8, hvorefter en advokat ikke må bistå en klient, hvis der er opstået en konflikt, eller der er nærliggende risiko herfor. Artikel 8 indeholder desuden en række eksempler på situationer, hvor der er eller kan foreligge en konflikt.

AER's regler og krav om iagttagelse af interessekonflikter forudsætter, at advokaten har oplysninger, som muliggør, at der kan gennemføres et effektivt konflikttjek, inden sagen påtages. Dette forudsætter bl.a. behandling af oplysninger om klienten, modparten og andre relevante personer, for eksempel reelle ejere, og interessenters navne, kontaktoplysninger, selskabsoplysninger, medarbejdere og partnere involveret i sagen, sagstype og en overordnet beskrivelse af sagens indhold. Den løbende vurdering af, om ændrede forhold indebærer en risiko for interessekonflikt og muligheden for indgivelse af klage for Advokatnævnet og eventuel sanktion, betyder imidlertid også, at advokaten under og efter afslutningen af sagen har oplysninger, og herunder personoplysninger, som gør det muligt for advokaten at forsvare og tilbagevise eventuelle klager[38] om manglende efterlevelse af god advokatskik. Dette kræver konkrete oplysninger om sagens faktum for eksempel om parter, forløb, instrukser, rådgivning mv., på detailniveau, som ofte vil fremgå af e-mailkorrespondance, møddereferater o. lign. Hvorvidt en oplysning, herunder en personoplysning, vil være nødvendig i en eventuel senere sag om interessekonflikt kan først vurderes efterfølgende. Det er i almindelighed ikke muligt at vurdere dette og slette løbende, da det vil kunne føre til en situation, hvor advokaten har slettet oplysninger, som senere viser sig at være nødvendige i en interessekonfliktsag. I den forbindelse bemærkes også, at klager over tilsidesættelse af god advokatskik efter retsplejelovens § 126 skal indgives for Advokatnævnet inden 1 år efter, at klageren er blevet bekendt med det forhold, som klagen vedrører, jf. retsplejelovens § 147 b, stk. 2, men at der ikke gælder nogen absolut forældelsesfrist for indgivelse af klage til Advokatnævnet.[39]

Vedrørende den tid, der er gået i forhold til, om der stadig foreligger en interessekonflikt, fremgår det af kommenterede AER, at tiden som sådan ikke har nogen indvirkning på en interessekonflikt, men

37 Jf. side 38-39 i Advokatrådets reviderede hvidvaskvejledning september 2022.
38 Eller indgive og fastslå manglende efterlevelse.
39 Jf. også Advokatnævnets afgørelse i sagsnummer 2014-1152.

at den, jo længere tid der går, kan udvande oplysningers fortrolighed og relevans, hvilket kan påvirke bedømmelsen.[40] Dette fremgår også af praksis vedrørende artikel 8, stk. 2, nr. 2.[41]

Advokatnævnet har desuden truffet flere afgørelser vedrørende interessekonfliktreglernes tidsmæssige udstrækning og bl.a. fundet, at de efter omstændighederne kan udstrækkes til at gælde i mange år og efter omstændighederne mere end 15 år.[42] Det bemærkes dog, at Advokatnævnet ikke har taget stilling til, hvor længe oplysninger, som er nødvendige for at gennemføre et interessekonflikttjek, skal opbevares.

AER's krav om iagttagelse af interessekonfliktreglerne nødvendiggør således, at advokater som udgangspunkt opbevarer oplysninger, herunder personoplysninger, i længere tid og efter omstændighederne i adskillige år. Det gælder på klientniveau, men også på sagsniveau for at kunne redegøre for sagen i forbindelse med en eventuel interessekonfliktsag, jf. afsnit 6.6.5.1 nedenfor.

6.6.3 AER artikel 70 om opbevaring af sagsakter efter sagens afslutning[43]

Det følger af AER artikel 70, at efter afslutning af en sag skal sagens akter, herunder elektroniske data, opbevares i en passende periode, som kan fastsættes generelt efter sagstype med fornødent hensyn til konkrete forhold. Reglen er primært rettet mod akter og altså fysiske dokumenter og herunder bl.a. originale dokumenter, men omfatter også elektroniske data, jf. ordlyden.

Perioden, hvori sagens akter og oplysninger skal opbevares, løber fra sagens afslutning, men det er ikke nærmere fastsat, hvornår den ophører. Der skal blot være tale om en passende periode. Kravet om opbevaring gælder både fysiske akter (dokumenter) og elektroniske data, men indeholder ikke noget nærmere om typer af oplysninger, for eksempel personoplysninger, tavshedsbelagte mv. Bestemmelsen giver mulighed for at fastsætte en generel og overordnet periode baseret på sagstype, for eksempel 5 år for ejendomshandler, idet der dog skal tages højde for konkrete forhold. Dette kan for eksempel være tilfældet, hvis der er tale om retsskabende dokumenter som for eksempel testamenter, eller krav, hvor der gælder en længere forældelsesfrist end 5 år.

Advokatrådet anbefaler, bl.a. under henvisning til revisorlovens § 23, bogføringslovens og hvidvasklovens krav om opbevaring i 5 år, at der tages udgangspunkt i en periode på 5 år fra sagens afslutning, men at perioden efter omstændighederne kan være længere.[44] Dette gælder bl.a. de omtalte retsskabende dokumenter.[45]

Advokatnævnet fandt i en kendelse fra 2001, at en advokats løbende sletning af almindelig korrespondance vedrørende ejendomsadministration for en udlejer efter 1 år, som advokaten repræsenterede løbende, var en tilsidesættelse af god advokatskik og udtalte, at der efter afslutning af en sag kan opstå behov for, at en advokat kan redegøre for sagens forløb. Hvor længe korrespondance og bilag, som ikke er tilbagesendt til klienten, skal opbevares, afhænger ifølge kendelsen af sagsforholdets karakter. Som nævnt er der desuden ikke nogen absolut frist for indgivelse af klager til Advokatnævnet.

40 Jf. Kommenterede AER, side 66.
41 Jf. Kommenterede AER, side 71.
42 17 år, jf. Advokatnævnets sagsnummer 2015-4241, 12 år, jf. Advokatnævnets kendelse af 12. december 2005 i sagsnummer 02-0401-05-0565, 10 år, jf. Advokatnævnets sagsnummer 2015-4224.
43 For en nærmere gennemgang af AER artikel 70, henvises til De Advokatetiske Regler – Kommenteret, 3. udgave 2022, side 303.
44 Jf. Advokatrådets vedtagelse af De Advokatetiske Regler – Kommenteret på rådets møde den 16. juni 2022.
45 Se også Advokatnævnets kendelse af 29. november 2022 (sagsnummer 2021-2665).

AER's krav om opbevaring af sagsakter nødvendiggør således, at advokater som udgangspunkt opbevarer sagsakter i mindst 5 år fra sagens afslutning, men at perioden efter omstændighederne kan være længere for retsskabende dokumenter eller i forhold til krav, hvor der gælder en længere forældelsesfrist end 5 år. Bemærk i øvrigt, at det forhold, at et retsskabende dokument skal opbevares i et offentligt system, for eksempel tinglysning, ikke fritager advokaten for at opbevare sin egen udgave af dokumentet.

6.6.4 Forældelseslovens betydning for advokaters opbevaring og sletning

Forældelseslovens regler og frister for forældelse af krav har som nævnt også betydning for advokaters opbevaring og sletning af personoplysninger. Som advokat er du underlagt et rådgiveransvar, og uden oplysninger om rådgivningen i korrespondance, dokumenter, osv., vil det ikke være muligt at dokumentere indholdet af og eventuelt forsvare rådgivningen.

Det kan derfor efter omstændighederne være nødvendigt at opbevare personoplysninger i mange år for at dokumentere rådgivningen og forsvare eventuelle krav.

Alt efter hvilken type sag og hvilket eventuelt krav der er tale om, kan personoplysninger som udgangspunkt opbevares i en periode svarende til den pågældende forældelsesfrist, for eksempel 3 år for fordringer, 5 år for ansættelsesforhold, 10 år for krav omfattet af den absolutte forældelsesfrist, herunder for eksempel krav i forbindelse med rådgivning, og 30 år for for eksempel personskade og forurening.

6.6.5 Konklusion – hvad er advokatens udgangspunkt for opbevaring og sletning?

De ovenfor omtalte regler i særlovgivningen, AER og forældelsesloven indeholder konkrete krav til tidsmæssig opbevaring – enten direkte eller ifølge praksis – af bestemte typer af oplysninger og herunder også personoplysninger. Fristerne kan illustreres som følger:

Bogføringsloven § 12	**5 år fra regnskabsårets afslutning**
Hvidvaskloven § 30	**5 år fra udstedelsen af slutafregningen men e.o. længere hvis løbende klientforhold, hvor oplysninger bruges i forbindelse med nye sager**
AER artikel 70	**5 år fra sagens afslutning men e.o. længere for retsskabende dokumenter**
AER. artikel 7-8 (og øvrige regler i kap. 4 om interessekonflikter)	**15 år fra sagens afslutning som udgangspunkt**
Forældelsesloven	**10 år fra tidspunktet for rådgivningen som udgangspunkt men e.o. fra 3 til 30 år alt efter type af krav**

Det er ikke muligt at fastsætte en generel og gennemgående frist for advokaters opbevaring af personoplysninger, men med udgangspunkt i bogføringsloven, hvidvaskloven og AER artikel 70 må det antages, at advokater i hvert fald må opbevare personoplysninger i **minimum 5 år**.

Af hensyn til rådgiveransvaret og med støtte i den absolutte forældelsesfrist på 10 år må det endvidere antages, at advokater generelt kan opbevare sagsrelaterede personoplysninger i **op til 10 år** fra afslutningen af sagen.

Som nævnt ovenfor forudsætter interessekonfliktreglerne, at omfattende oplysninger på detailniveau i nødvendigt omfang kan tilgås, idet advokater ellers ikke vil kunne overholde AER, hvis der opstår en interessekonflikt. I sager hvor interessekonflikter kan forekomme, anbefales det derfor, at nødvendige personoplysninger indhentet og behandlet i forbindelse med interessekonflikttjek og i forbindelse med håndteringen af sagen (sagsrelaterede oplysninger) opbevares i **15 år** efter sagens afslutning.[46] Som anført ovenfor har Advokatnævnet taget stilling den tidsmæssige udstrækning af interessekonfliktreglerne, men ikke til, hvor længe oplysninger til brug for gennemførelse af konflikttjek skal opbevares. Derfor må denne anbefaling tages med et forbehold for praksis fra Advokatnævnet.

De nævnte frister er som nævnt alene udgangspunkter. Hvor længe oplysninger skal og må opbevares beror altid på en konkret vurdering, hvori kravene efter databeskyttelsesreglerne, særlovgivning og god advokatskik samt forældelseslovens frister indgår. Er der for eksempel tale om en sag, hvor advokaten har rådgivet om et uskiftet bo og for eksempel udarbejdet et testamente og/eller en fremtidsfuldmagt, kan det være berettiget at opbevare oplysninger og retsskabende dokumenter i mere end 15 år. Det samme kan for eksempel også være tilfældet, hvor advokaten har repræsenteret en klient i en personskadeerstatningssag.

6.6.5.1 Sletning på sags- eller oplysningsniveau?

Som nævnt indeholder GDPR et krav om sletning (eller anonymisering) af personoplysninger, som ikke længere er nødvendige til formålet, jf. artikel 5, stk. 1, litra e. Bestemmelsen omtaler oplysninger og ikke sager. Hvis alle oplysninger på en sag skal kunne opbevares i det samme tidsrum, skal den enkelte oplysning dermed være nødvendig til det formål, som den behandles til. Det er efter GDPR således ikke muligt uden videre at opbevare alle oplysninger på en sag uden at vurdere, om deres opbevaring er nødvendig.

De krav, der gælder til advokaters opbevaring af hvidvaskdokumentation, interessekonflikttjek og dokumenter, vedrører imidlertid sagen,[47] og dokumentation af rådgivning forudsætter ligeledes, at der opbevares oplysninger om sagen. Hvis kravene skal efterleves, er det nødvendigt, at der opbevares detaljerede og konkrete oplysninger om sagen og ikke blot generelle og overordnede oplysninger som for eksempel sagstype og identifikationsoplysninger.[48] Dette gælder i særdeleshed i forhold til vurdering af konflikttjek og ansvar for rådgivning og god advokatskik, hvor også oplysninger i sagsmateriale, som kan dokumentere for eksempel kontekst, er nødvendige.

Forudsat, at de øvrige behandlingsprincipper i artikel 5, stk. 1, litra a-d er iagttaget løbende, herunder for eksempel dataminimering og rigtighed samt bruger- og rettighedsstyring, anbefales det, at du som advokat sletter personoplysninger på sagsniveau efter samme slettefrist.

46 § 36 i den norske advokatlov indeholder krav om arkivhold i 10 år (alle typer af oplysninger) eller længere, hvis opdragets karakter eller indholdet af dokumenter tilsiger det. Ifølge den norske advokatforening kan de bagvedliggende interesser for klient og advokat begrunde en generel opbevaringsperiode på **30 år**, som dog kan være kortere eller længere alt efter omstændighederne, jf. side 15 i Advokatforeningens veileder om advokatvirksomheters etterlevelse av GDPR, versjon 2, 24. oktober 2024.

47 Ved sag forstås i denne sammenhæng den egentlige sagsbehandling, som advokaten foretager (typisk under et sagsnummer i advokatvirksomhedens sagsbehandlingssystem) i forbindelse med for eksempel juridisk vurdering af et spørgsmål, en transaktion, en retssag, mv.

48 Advokatnævnets afgørelse i sagsnummer 2011-2966 er et eksempel på, at der kræves flere oplysninger end identifikationsoplysninger.

6.6.6 Opbevaring/sletning inden for bestemte områder/sagstyper

I bilag 4 findes en ikke udtømmende oversigt med vejledende eksempler på opbevaringsperioder og slettefrister. Områder og sagstyper afhænger af, hvilken form for advokatvirksomhed der drives (for eksempel full service eller specialiseret advokatfirma), idet dog alle advokatvirksomheder bør have fastsat opbevarings- og slettefrister for henholdsvis sagsakter og grundlæggende forhold som for eksempel etablering og varetagelse af klientforholdet, herunder interessekonflikttjek, hvidvaskdokumentation og bogføringsmateriale. De nævnte frister regnes fra afslutningen af regnskabsåret, udstedelsen af slutafregningen, sagen mv. Slettepolitikken bør udover slettefrister for sagsrelaterede oplysninger, også indeholder opbevarings- og slettefrister for sager og systemer, hvor der i øvrigt behandles personoplysninger i advokatvirksomheden.

6.6.7 Hvordan slettes der?

En sletning skal være effektiv, og det er vigtigt, at sletning rent faktisk sker. Det er ikke tilstrækkeligt bare at flytte og opbevare oplysningerne et andet sted. Det er heller ikke tilstrækkeligt at begrænse, hvem der har adgang til oplysningerne. For eksempel er det vigtigt, at "slettet post" i mailsystemet bliver slettet, og det ikke fungerer som et arkiv.[49]

Hvis oplysningerne opbevares flere steder, er det vigtigt, at oplysningerne slettes alle steder (for eksempel også under downloadede filer under "overførsler" eller "downloads").

Hvis man logger de handlinger, der foretages i et system, skal det også overvejes, hvordan loggen slettes.

Oplysninger skal også slettes fra backups, hvis det er muligt. Hvis det ikke er teknisk muligt at slette enkelte data fra backups, skal der være foranstaltninger, der gør, at disse oplysninger slettes, hvis backuppen skal bruges.

Et alternativ til sletning er anonymisering, hvorefter det uigenkaldeligt ikke længere er muligt at identificere en fysisk person ud fra oplysningerne eller i kombination med andre oplysninger. I praksis er anonymisering af personoplysninger dog alene et begrænset alternativ, når bortses fra anonymisering af personoplysninger i dokumenter i en paradigme- og vidensamling.

6.6.8 Overvejelser om tilgangen til kravet om opbevaringsbegrænsning og sletning

Som advokat kan du indføre en række foranstaltninger til sikring af overholdelse af kravet om opbevaringsbegrænsning og sletning.[50]

En måde, hvorpå kravet lettere kan overholdes, er at have fokus på princippet om dataminimering, så der kun indsamles og modtages nødvendige oplysninger. Ved opstart af en sag vil klienten ofte sende alle de oplysninger, som klienter har, men inden det sker, bør advokaten have oplyst klienten, hvilke oplysninger der er relevante og nødvendige, så det i videst muligt omfang undgås, at klienten sender oplysninger, som ikke er nødvendige for sagen. Umiddelbart efter modtagelsen vurderes det,

49 Advokatnævnet har i øvrigt i kendelse af 29. november 2022 (sagsnummer 2021-3110) fundet, at en advokat som udgangspunkt ikke kan anvende retssagsportalen som arkiv til opbevaring af sagsakter efter afslutningen af en sag.

50 Der sondres mellem tekniske foranstaltninger, som for eksempel automatisk sletning i et system, og organisatoriske foranstaltninger, som for eksempel en procedure for medarbejderes sletning.

om de fremsendte oplysninger er nødvendige, og eventuelle unødvendige oplysninger slettes med det samme. På den måde bliver der færre oplysninger at opbevare og slette (og det sikres i øvrigt også, at oplysningerne er nødvendige til formålet, behandlingsgrundlaget er dækkende, mv.). Instruer derfor medarbejderne i advokatfirmaet herom. Sørg også for, at de it-systemer, applikationer mv., som anvendes, er designet på en måde, hvor kun de nødvendige personoplysninger behandles. Det kan for eksempel være tilfældet, hvor oplysninger indsamles via en hjemmeside, app, formular, eller lign.

Indret også sagssystemet, og herunder oprettelse af sager, på en måde, hvor der tages højde for opbevaringsperioder og sletning, og hvor det for eksempel er muligt at markere sager og retsskabende dokumenter, som skal opbevares i længere tid end den fastsatte periode, jf. afsnit 6.6.3. Hvis advokatvirksomheden anvender et sagsbehandlingssystem fra en leverandør, skal det sikres, at løsningen muliggør fastsættelse af opbevaringsperioder og sletning (automatisk eller manuelt). Du skal som advokatfirma og advokat forholde dig kritisk til om løsninger, der udbydes, lever op til kravene.

Udarbejd også en politik for oprettelse, opbevaring og arkivering af sager med regler for navngivelse, type, emne, parter mv., opbevaringssted og -perioder, og suppler med konkrete retningslinjer og forretningsgange for, hvordan det nærmere gøres.

Vær i forbindelse med oprettelse af sager opmærksom på at anvendelse af generelle, diverse eller løbende sager ud fra for eksempel årstal kan vanskeliggøre korrekt opbevaring og sletning, hvis ikke der ved siden af oprettes isolerede og konkrete sager for de opgaver, som opstår og udspringer af den generelle og løbende rådgivning, og den generelle sag blot fortsætter uden nogen form for tidsbegrænsning og måske bare omdøbes til det nye årstal. I den forbindelse anbefales det, at sådanne sager gennemgås periodisk for eksempel en gang årligt eventuelt ved udsendelse af lister med henblik på at vurdere, om der bør oprettes konkrete sager, og om den løbende sag bør afsluttes (og en ny eventuelt oprettes).

Overvej at indføre automatisk sletning af for eksempel e-mailkorrespondance efter en bestemt periode (for eksempel 1 år) og instruer medarbejderne i at flytte e-mails mv. fra mailsystemet, som det er nødvendigt at opbevare i længere tid, til opbevaring på sagen i sagssystemet eller arkivet. Hvis automatisk sletning ikke er muligt eller begrænset, bør sletning ske manuelt. Instruer medarbejderne til at gøre dette (eventuelt i forbindelse med slettedage) og send påmindelser herom.

Opbevaring af oplysninger bør desuden begrænses til et eller så få steder som muligt, så det undgås, at de samme oplysninger opbevares flere forskellige steder, da dette besværliggør sletning. Instruer medarbejderne i, hvor opbevaring skal ske.

Etabler i den forbindelse også et overblik over de systemer der opbevares personoplysninger i. Dette kan ske med udgangspunkt i artikel 30 fortegnelsen og en liste over de it-systemer mv., som advokatvirksomheden bruger. Det kan som supplement også overvejes at anvende værktøjer, som scanner systemer for personoplysninger.

Overvej også – på baggrund af fortegnelsen og listen over systemer – at målrette indsatsen sådan, at fokus på sletning er størst i forhold til sager og systemer, hvor der behandles og opbevares mange personoplysninger, herunder især hvis der er tale om følsomme personoplysninger, og et mere begrænset fokus på sager, hvor der alene indgår få og almindelige personoplysninger som for eksempel kontaktoplysninger.

Husk også at kontrollere, at sletning rent faktisk sker.

6.6.9 Fordele ved sletning

Der er mange fordele ved alene at opbevare de personoplysninger, som er nødvendige (udover overholdelse af databeskyttelsesreglerne). Generelt undgås det, at der ophobes flere og flere oplysninger i advokatvirksomhedens systemer, og konkret betyder det for eksempel også, at der ved behandlingen eller vurderingen af en sag alene vil indgå de oplysninger, som er nødvendige, relevante og ajourførte. I tilfælde af et sikkerhedsbrud vil omfanget af personoplysninger og dermed også bruddet være mindre. Indsigtsanmodninger bliver desuden lettere at behandle, idet omfanget af personoplysninger også vil være begrænset til de relevante og nødvendige. Manglende sletning af personoplysninger, som burde være slettede, indebærer også en unødig høj risiko for de registrerede.

6.7 Integritet og fortrolighed

Oplysninger skal beskyttes mod uautoriseret eller ulovlig behandling, og det skal sikres, at oplysninger ikke går tabt eller bliver beskadiget.[51]

6.8 Behandlingsgrundlag

Udover at overholde behandlingsprincipperne skal du som advokat også have et behandlingsgrundlag. Grundlaget for behandling af personoplysninger veksler mellem, hvilken type af oplysninger der er tale om og kan for eksempel findes i artikel 6 (almindelige personoplysninger), artikel 9 (følsomme personoplysninger), artikel 10 og databeskyttelseslovens § 8 (strafbare forhold) samt databeskyttelseslovens § 11 (personnummer).

I vurderingen af om det enkelte behandlingsgrundlag er opfyldt anlægges der en snæver fortolkning. Det er ikke muligt at anvende en udvidet fortolkning.

En behandling kan være omfattet af flere grundlag, hvilket kan være en fordel, hvis forholdene ændrer sig, og et af grundlagene ikke længere er til stede.

Samtykke er et behandlingsgrundlag for både almindelige og følsomme oplysninger, strafbare forhold og personnummer, men der stilles en række krav til samtykkets gyldighed (bl.a. at der på forhånd er oplyst om muligheden for tilbagekaldelse), og det skal kunne bevises, at der er givet samtykke. På grund af tilbagekaldelsesadgangen medfører samtykke som grundlag en vis usikkerhed, idet du – hvis der ikke samtidig er et andet grundlag – ikke længere kan behandle oplysningen, hvis samtykket tilbagekaldes. Du bør derfor overveje, om din behandling kan ske på et andet grundlag end samtykke.

Du skal også være opmærksom på, at samtykke til én form for behandling kun omfatter det pågældende formål. Du kan ikke anvende samtykket til andre formål, end det der er oplyst.

Vær som nævnt også opmærksom på om formålet med behandlingen har ændret sig, og om dette har betydning for behandlingsgrundlaget.

Alle advokater behandler som minimum personoplysninger i forbindelse med etablering af klientforholdet, hvidvaskdokumentation[52] og den løbende kontakt med klienten. Grundlaget for disse behandlinger

51 Jf. GDPR artikel 5, stk. 1, litra f).
52 Forudsat, at der er tale om en transaktion omfattet af hvidvasklovens § 1, stk. 1, nr. 13.

vil være det samme. Herudover afhænger behandlingsgrundlaget af, hvilken type advokatvirksomhed der er tale om.

6.8.1 Almindelige oplysninger (artikel 6)

Grundlaget for behandling af almindelige personoplysninger kan være en **kontrakt eller en aftale**, som den registrerede er part i. Advokatopdraget vil være et eksempel herpå, og opdraget kan derfor danne grundlag for behandling af oplysninger om din klient.

Behandlingsgrundlaget kan også være en **retlig forpligtelse**. Der kan for eksempel i anden lovgivning end GDPR og databeskyttelsesloven være regler om, at en behandling af personoplysninger kan eller skal finde sted. I visse situationer kan du som advokat have pligt til at behandle personoplysninger. Hvis du har en pligt til at indhente nogle personoplysninger, må du antages også at have ret til at behandle personoplysningerne. Det gælder for eksempel efter hvidvasklovens §§ 10-11, hvor du som advokat i visse situationer har pligt til at indhente og opbevare oplysninger om din klients identitet. Oplysninger om fysiske personer indhentet efter hvidvasklovens kundekendskabsprocedure er personoplysninger omfattet af GDPR, og behandlingsgrundlaget vil være hvidvaskloven

Undlad at indhente oplysninger i videre omfang, end hvad hvidvaskloven pålægger dig – også selvom du ønsker at være på den sikre side. Du kan risikere, at din behandling er i strid med behandlingsprincipperne i GDPR, og/eller at dit grundlag i hvidvaskloven til at behandle oplysningerne ikke længere er tilstrækkeligt.

Et andet behandlingsgrundlag for almindelige personoplysninger kan være **interesseafvejningsreglen**, som betyder, at behandlingen kan finde sted, hvis det er nødvendigt for, at den dataansvarlige kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse. Med andre ord kan du behandle personoplysninger, hvis du vurderer, at din (eller din klients) legitime interesse kan tillægges større vægt end de modstående interesser hos den, du behandler personoplysninger om. Personoplysninger om børn vejer særlig tungt.

Husk at oplyse den registrerede om de interesser, hvorpå behandlingen baseres, jf. afsnit 7.2 om oplysningspligten. Interesseafvejningsreglen er ofte relevant ved behandling af personoplysninger vedrørende andre end din klient.

6.8.2 Følsomme oplysninger (artikel 9)

Hvis du håndterer følsomme personoplysninger, er betingelserne for at behandle disse strengere end for almindelige personoplysninger.

Der gælder som udgangspunkt et forbud mod at behandle følsomme personoplysninger, medmindre en af undtagelserne i artikel 9, stk. 2, eller en af de supplerende regler i databeskyttelsesloven finder anvendelse. Grundlaget for behandling af følsomme personoplysninger kan være, at behandlingen er nødvendig for, at **retskrav** kan fastlægges, gøres gældende eller forsvares. Dette grundlag for behandling af følsomme personoplysninger vurderes at være relevant for advokater. Du bør nøje overveje, om oplysningerne er nødvendige for, at retskravet kan fastlægges, jf. endvidere dataminimeringsprincippet ovenfor i afsnit 6.4.

Kan du ikke støtte din behandling af følsomme personoplysninger på et samtykke eller et retskrav, kan du overveje, om et af de andre behandlingsgrundlag i artikel 9, stk. 2, kan udgøre hjemmel for din behandling af følsomme personoplysninger. For eksempel kan du behandle følsomme personoplysninger, som er offentliggjort af den registrerede.

6.8.3 Strafbare forhold (databeskyttelseslovens § 8)

Databeskyttelseslovens § 8 indeholder regler om behandling af oplysninger om strafbare forhold.[53]

Betingelserne for privates, herunder advokaters, behandling af disse oplysninger er snævre. Grundlaget kan være, hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede (**interesseafvejning**), jf. databeskyttelseslovens § 8, stk. 3. Behandling kan også finde sted, hvis **betingelserne for at behandle følsomme oplysninger er opfyldt**, jf. henvisningen til § 7 i § 8, stk. 5. Det oplagte eksempel er forsvarsadvokaten, der som led i sit virke ofte vil modtage oplysninger fra sin klient om strafbare forhold, som relaterer sig til klienten selv eller andre. Forsvarsadvokaten vil typisk kunne behandle sådanne oplysninger ud fra en interesseafvejning eller under henvisning til, at behandlingen er nødvendig, for at retskrav kan fastlægges. Men der kan også tænkes andre situationer, hvor en advokat – enten via en klient eller andre – modtager oplysninger om strafbare forhold, og hvor der er behov for at tænke en ekstra gang over, om der er det fornødne grundlag for at behandle oplysningerne.

Oplysninger om strafbare forhold kan kun videregives efter samtykke, medmindre videregivelse sker til varetagelse af offentlige eller private interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, jf. databeskyttelseslovens § 8, stk. 4. Strafbare forhold omfatter ikke blot oplysninger om, at en person har begået et strafbart forhold, men omfatter også oplysninger om overtrædelse af lovgivningen, uden at det har udløst et strafansvar. I praksis vil for eksempel registrering af oplysninger om strafbare forhold med henblik på indgivelse af politianmeldelse og senere afgivelse af vidneforklaring i retten kunne være omfattet af strafbare forhold. Det må dog kræves, at anmeldelsen til politiet er underbygget og kvalificeret, før der er tale om strafbare forhold.[54]

Det vil i øvrigt være i strid med god advokatskik at indgive politianmeldelse, medmindre der foreligger fornødent grundlag herfor, jf. AER artikel 17, stk. 1. Vær i den forbindelse opmærksom på tavshedspligten, og at oplysninger om strafbare forhold, som modtages som led i virket for klienten, er omfattet af tavshedspligten. Der kan efter anden lovgivning være pligt til at indberette eller videregive oplysninger om strafbare forhold. I den situation har du også ret til at behandle oplysningerne efter GDPR. Det gælder for eksempel efter hvidvasklovens § 26, hvorefter advokater i visse tilfælde har pligt til at videregive oplysninger om deres mistanke om hvidvask og terrorfinansiering.[55]

6.8.4 Personnumre (databeskyttelseslovens § 11, stk. 2)

Behandling af oplysninger om personnumre er reguleret i databeskyttelseslovens § 11. Grundlaget for privates behandling af oplysninger om personnumre kan være, at det **følger af lov eller bestemmelser fastsat i henhold til lov**. Der kan for eksempel være en indberetningspligt eller lignende, som bestemmer, at indberetning skal ske med angivelse af personnummer. Det gælder for eksempel efter skattelovgiv-

53 Reglerne er fastsat med hjemmel i GDRP artikel 10, hvorefter der kan fastsættes nationale særregler om behandling af oplysninger om straffedomme og lovovertrædelser.
54 Betænkning nr. 1565/2017 om databeskyttelsesforordningen, side 236.
55 Vær dog opmærksom på hvidvasklovens § 27 om undtagelse til underretningspligten.

ningen og efter hvidvasklovens § 11, hvor der skal indhentes identitetsoplysninger i form af navn og personnummer eller lignende. Der gælder særlige regler for videregivelse, som bl.a. kan ske, hvis der er tale om videregivelse af oplysninger om personnummer, når videregivelsen er et naturligt led i den normale drift af virksomheder mv. af den pågældende art, og når videregivelsen er af afgørende betydning for at sikre en entydig identifikation af den registrerede, eller videregivelsen kræves af en offentlig myndighed, jf. § 11, stk. 2, nr. 3. Videregivelse i øvrigt kræver, at du har samtykke hertil (eller at det følger af lov). Behandling af personnumre kan herudover finde sted, hvis **betingelserne for at behandle følsomme oplysninger er opfyldt**. Det kan være tilfældet, hvor behandlingen af personnummeret for eksempel er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares.

6.9 Ansvar (accountability)

Det følger af GDPR artikel 5, stk. 2, at det er den dataansvarlige – hvilket du ofte vil være som advokat – der er ansvarlig for, at principperne overholdes, og som skal kunne dokumentere dette, jf. afsnit 3 om dokumentationskrav mv.

7. Den registreredes rettigheder

7.1 Indledning om rettighederne

Den person (for eksempel din klient, modpart, kontaktpersoner, vidner mv.), som du behandler personoplysninger om (den registrerede), har en række rettigheder efter GDPR. Rettighederne indebærer forpligtelser for dig som dataansvarlig advokat, og du har pligt til at sikre, at personen kan gøre brug af sine rettigheder. Den registreredes rettigheder er som følger:

Artikel 12: **Gennemsigtighed** og regler for udøvelsen af rettighederne

Artikel 13: Oplysningspligt (når oplysningerne indsamles **direkte** hos den registrerede)

Artikel 14: Oplysningspligt (når oplysningerne indsamles hos **andre** end den registrerede)

Artikel 15: Ret til **indsigt** i personoplysninger, der behandles

Artikel 16: Ret til **berigtigelse** af personoplysninger

Artikel 17: Ret til **sletning** af personoplysninger (retten til at blive glemt)

Artikel 18: Ret til **begrænsning** af personoplysninger, der behandles

Artikel 19: Ret til **underretning,** hvor modtagere er blevet bedt om at berigtige, slette, begrænse

Artikel 20: Ret til **dataportabilitet**

Artikel 21: Ret til **indsigelse**

Artikel 22: Ret til ikke at være genstand for afgørelse alene baseret på **automatisk behandling**

Artiklerne indeholder undtagelser til rettighederne, jf. for eksempel artikel 14, stk. 5, litra d, om tavshedspligt, men databeskyttelsesloven § 22[56] indeholder også begrænsninger, som har væsentlig betydning. For advokater gælder det især undtagelsen om afgørende hensyn til private interesser, der vil kunne begrunde undtagelse til oplysningspligten, som følge af den tavshedspligt advokater er underlagt. Herudover indeholder AER også bestemmelser, som kan indebære en begrænsning af rettighederne. Det gælder især reglerne i kapitel 5 om fortrolighed, jf. den nærmere omtale heraf i afsnit 2.1.2.

Af de nævnte rettigheder er det primært kravet om gennemsigtighed i artikel 12, oplysningspligten i artikel 13-14 og indsigtsretten i artikel 15, som er relevante for advokater. Fokus er derfor på disse rettigheder, og de øvrige rettigheder omtales alene mere overordnet.[57]

7.1.1 Gennemsigtighed – artikel 12 (processuelle regler vedrørende udøvelsen)

Der gælder en række processuelle krav, som du skal være opmærksom på i forbindelse med håndteringen af rettighederne. Man skal bl.a. henvende sig skriftligt til den registrerede i en letforståelig og tilgængelig form og benytte et klart og enkelt sprog.[58] GDPR indeholder også tidsfrister for, hvor hurtigt en anmodning fra den registrerede skal besvares. Udgangspunktet er, at en anmodning fra en registreret skal besvares uden unødig forsinkelse og senest en måned efter modtagelsen. Husk også at sikre dig, at

56 § 22 er udstedt med hjemmel i artikel 23.
57 For en mere detaljeret beskrivelse af rettighederne henvises til Datatilsynets vejledning fra juli 2018.
58 Kravene til sprog og form er strengere i forbrugerforhold end i erhvervsforhold. Det samme gælder, hvis den registrerede er et barn.

den registrerede er den, som vedkommende giver sig ud for at være, så du ikke giver uvedkommende personer oplysninger om en registreret (og hermed bryder persondatasikkerheden) eller kommer til at slette personoplysninger, som ikke skulle have været slettet. Dette betyder, at du efter omstændighederne skal have dokumentation for, at der er tale om den registrerede person.

7.2 Oplysningspligten – generelt

Efter GDPR er der pligt til at give den registrerede oplysninger om en række forhold, når der behandles personoplysninger om vedkommende. Udgangspunktet er altså, at du altid har en oplysningspligt over for den registrerede. Det er imidlertid ikke altid lige hensigtsmæssigt, at man skal underrette personer, som man har registreret oplysninger om, og det kan desuden være problematisk i forhold til advokaters tavshedspligt. Nedenfor er derfor også beskrevet en række undtagelser til oplysningspligten, som har relevans for advokater. Oplysningspligten påhviler den dataansvarlige og udløses automatisk, når der indsamles personoplysninger (eller når du modtager personoplysninger). Du skal derfor opfylde pligten på eget initiativ. Pligten gælder som udgangspunkt i forhold til alle registrerede, du indsamler eller modtager oplysninger om. Det gælder ikke blot din klient, men også andre, som optræder accessorisk i tilknytning til oplysningerne om din klient, jf. afsnit 7.2.1 om bipersoner. Oplysningspligten, og hvad der skal gives oplysninger om til den registrerede, varierer alt efter, om personoplysningerne kommer direkte fra den registrerede, jf. afsnit 7.2.2 eller fra andre, dvs. tredjemand, jf. afsnit 7.2.3. Den situation, hvor du typisk vil modtage personoplysningerne direkte fra den registrerede, er i forhold til din klient. En klient retter måske henvendelse til dig med henblik på at få din bistand i en konkret sag og giver dig i den forbindelse en række personoplysninger om sig selv. Oplysningerne kommer her direkte fra den registrerede, nemlig din klient. Ofte er det dog også sådan, at klienten samtidig giver dig personoplysninger vedrørende andre personer. Oplysningerne kommer her fra en anden end den registrerede selv.

Da reglerne vedrørende oplysningspligten er omfangsrige og detaljerede (hovedregler, undtagelser, form, indhold, tidsfrister mv.), bør advokatfirmaet have en procedure eller fremgangsmåde, som følges. Bilag 5 indeholder en oversigt over hovedregler og undtagelser mv.

7.2.1 Bipersoner

Oplysningspligten gælder som nævnt som udgangspunkt i forhold til alle personer, som der behandles personoplysninger om, og ikke kun klienten eller andre (hoved)personer, som kan siges at være den egentlige genstand for behandlingen. Pligten gælder således også i forhold til bipersoner. Databeskyttelsesreglerne indeholder ikke en definition af bipersoner, men kan defineres som personer, der alene har en accessorisk tilknytning til oplysningerne om den registrerede og ikke er den egentlige genstand for behandlingen. Det kan for eksempel være pårørende til en registreret eller fagpersoner som for eksempel læger el.lign.[59] Det er dog ud fra denne definition forsat ikke klart, hvor grænsen går. Et yderligere kriterie kunne være, at personen skal kunne sidestilles med en part i sagen. Når du selv indsamler eller modtager personoplysninger fra andre, vil der ofte være oplysninger om personer, som ikke er den egentlige genstand for behandlingen. Hvis du skulle opfylde oplysningspligten over for alle sådanne personer, ville det have vidtrækkende konsekvenser, medmindre en af undtagelserne til pligten finder anvendelse. Datatilsynet har i den forbindelse oplyst,[60] at det er muligt at anvende undtagelserne i videre omfang i forhold til bipersoner, da opfyldelse af oplysningspligten her ofte vil

59 Jf. Datatilsynets vejledning om de registreredes rettigheder, juli 2018, side 13.
60 Jf. Datatilsynets vejledning om de registreredes rettigheder, juli 2018, side 21.

være umulig eller kræve en – relativt set i forhold til den beskedne rolle, bipersonen spiller i sagen – uforholdsmæssigt stor indsats.[61]

7.2.2 Oplysningspligt– artikel 13 (oplysningerne kommer direkte fra den registrerede)

Efter GDPR er der som nævnt pligt til at give den registrerede oplysninger om en række forhold, når der behandles personoplysninger om vedkommende, jf. artikel 13, stk. 1-3. Undtagelse fra oplysningspligten efter artikel 13 kan kun gøres, hvis personen må antages allerede at være bekendt med de oplysninger, som man ellers er forpligtet til at give. I den forbindelse skal du være opmærksom på, at oplysningsforpligtelsen indeholder en pligt til at oplyse om forhold, som den registrerede sjældent vil være bekendt med. Muligheden for at anvende undtagelsen er således begrænset. Undtagelserne til oplysningspligten, når oplysningerne kommer fra den registrerede selv, indeholder ikke en undtagelse om tavshedspligt, som det er tilfældet, når oplysningerne kommer fra andre end den registrerede, jf. artikel 14, stk. 5, litra d.

Der er imidlertid også en undtagelsesmulighed i databeskyttelseslovens § 22, stk. 1, hvorefter man kan undlade at opfylde oplysningspligten, hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv. Tilsvarende kan hensynet til offentlige interesser også begrunde undtagelse til oplysningspligten, jf. § 22, stk. 2.

Det er yderligere et krav for at kunne benytte undtagelsen, at der er nærliggende fare for, at de private eller offentlige interesser vil lide skade af væsentlig betydning.[62]

Private og offentlige interesser, som kan beskyttes, er såvel den dataansvarliges som tredjemands interesser. Private interesser, der vil kunne begrunde undtagelse til oplysningspligten, er bl.a. forretningshemmeligheder og professionel tavshedspligt hos advokater. Retten til at forberede sit eget forsvar i retssager antages også at kunne begrunde undtagelse til oplysningspligten.[63]

Vær derfor opmærksom på din tavshedspligt, som begrænser oplysningspligten, ligesom hensynet til at kunne forberede en eventuel retssag kan begrunde hemmeligholdelse, så du i sådanne situationer ikke har pligt til at give oplysninger til den registrerede, jf. databeskyttelseslovens § 22, stk. 1. Dette kan betyde, at du for eksempel som forsvarer ikke vil kunne give oplysningspligt til vidner, hvis det er afgørende for, at du kan overholde din tavshedspligt. Dette vil dog kun være tilfældet, så længe oplysningerne er omfattet af tavshedspligten.

Hvis du på et senere tidspunkt behandler oplysningerne om den registrerede til andre formål end dem, du oprindeligt indsamlede dem til, skal du give den registrerede ny underretning om de nye formål, jf. artikel 13, stk. 3. Her skal du også huske at sikre dig, at du har det fornødne behandlingsgrundlag i forhold til de nye formål.[64]

Indholdet af oplysningspligten – dvs., hvilke oplysninger du skal give til den registrerede, når oplysninger kommer fra den registrerede – følger af artikel 13, stk. 1-2. Visse oplysninger skal du altid give,

61 Undtagelserne vedrører den situation hvor oplysninger kommer fra andre end den registrerede, jf. artikel 14, stk. 5, litra b.
62 Jf. Datatilsynets vejledning om de registreredes rettigheder, juli 2018, side 18.
63 Betænkning nr. 1565/2017 om databeskyttelsesforordningen, side 395.
64 Det samme gælder i forhold til oplysningspligten efter artikel 14, stk. 4, hvor oplysningerne kommer fra andre end den registrerede.

mens andre skal gives efter en konkret vurdering.[65] I praksis er oplysningerne typisk indeholdt i en persondatapolitik (eller privatlivspolitik), som uploades på hjemmesiden.

7.2.3 Oplysningspligt – artikel 14 (oplysningerne kommer fra andre end den registrerede)

I mange tilfælde vil du som advokat modtage personoplysninger, der kommer fra andre end den registrerede. Det kan være, at din klient – udover at give dig oplysninger om sig selv – samtidig giver dig personoplysninger vedrørende andre personer. Oplysningerne kommer her fra en anden end den registrerede selv. Situationen, hvor du udveksler personoplysninger med modpartens advokat, er også et typisk eksempel herpå. Der sker her en løbende udveksling af oplysninger om parterne og om andre.

Kommer oplysningerne fra andre end den registrerede, er det ofte forbundet med større vanskeligheder at opfylde oplysningspligten, fordi der ikke er direkte kontakt mellem den dataansvarlige og den registrerede. Derfor er der også flere undtagelser til oplysningspligten, når personoplysningerne kommer fra andre end den registrerede.

Indholdet af oplysningspligten – dvs. hvilke oplysninger, du skal give til den registrerede, når oplysningerne kommer fra andre end den registrerede – følger af artikel 14, stk. 1-2. Her er der også visse oplysninger, som altid skal gives, mens andre alene skal gives efter en konkret vurdering.[66]

Ligesom det er tilfældet i forhold til artikel 13, kan der også gøres undtagelse, hvis den registrerede allerede er bekendt med oplysningerne, jf. artikel 14, stk. 5, litra a.

Derudover kan underretning til den registrerede undlades, hvis det er umuligt at give den registrerede oplysningerne, jf. artikel 14, stk. 5, litra b. Det kan tænkes at være tilfældet, hvis det for eksempel er umuligt for dig entydigt at identificere vedkommende. Den dataansvarlige bærer bevisbyrden for umuligheden, og det antages, at der skal ganske meget til, før der foreligger umulighed. Underretning til den registrerede kan endvidere undlades, hvis det vil kræve en uforholdsmæssig stor indsats af den dataansvarlige at give oplysningerne, jf. artikel 14, stk. 5, litra b. Ved vurderingen heraf kan man lægge vægt på antallet af registrerede og oplysningernes alder, samt på om der på anden vis er stillet fornødne garantier for den registrerede. Endvidere kan en underretning af den registrerede undlades, såfremt underretning sandsynligvis vil gøre det umuligt eller i alvorlig grad vil hindre opfyldelse af formålene med behandlingen, jf. artikel 14, stk. 5, litra b.

Selvom oplysningspligten som udgangspunkt gælder for alle registrerede, herunder også bipersoner, vil der kunne være situationer, hvor det under henvisning til undtagelserne vil være umuligt, kræve uforholdsmæssig stor indsats eller hindre opfyldelse af formålene med behandlingen at underrette alle de registrerede.[67]

Hvis indsamling og videregivelse af personoplysninger udtrykkeligt er fastsat ved lov, kan underretning undlades, jf. artikel 14, stk. 5, litra c. Det gælder for eksempel efter skattelovgivningen og hvidvaskloven.[68]

65 Dette er nærmere beskrevet i Datatilsynets vejledning om de registreredes rettigheder, juli 2018 side 16-18.
66 Datatilsynets vejledning om de registreredes rettigheder, juli 2018, side 19.
67 I denne situation vil generel information i for eksempel persondatapolitikken på advokatvirksomhedens hjemmeside være tilstrækkelig til opfyldelse af oplysningspligten, jf. Datatilsynets vejledning om de registreredes rettigheder, juli 2018, side 21.
68 Her skal dog gives de oplysninger, der kræves efter hvidvasklovens § 16.

Centralt er det endvidere, at der som nævnt kan gøres undtagelse, hvis personoplysningerne skal forblive fortrolige som følge af tavshedspligt i henhold til EU-retten eller medlemsstaternes nationale ret, herunder lovbestemt tavshedspligt, jf. artikel 14, stk. 5, litra d, eller hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private eller offentlige interesser, herunder hensynet til den pågældende selv, jf. databeskyttelseslovens § 22, stk. 1 og 2.

Datatilsynet har i en sag vedrørende et advokatfirmas gennemførelse af en advokatundersøgelse truffet afgørelse om, at oplysningspligten i henhold til artikel 12 og 14 ikke var opfyldt.[69] I forhold til artikel 12, stk. 1, lagde Datatilsynet vægt på, at oplysningerne ikke var givet i et klart og enkelt sprog, idet det bl.a. var uklart, hvad det præcise formål med undersøgelsen var. Datatilsynet fandt desuden, at advokatfirmaets procesbeskrivelse af undersøgelsen, dets databeskyttelsespolitik og efterfølgende e-mails med en (mindre) uddybning af retsgrundlaget, hverken samlet eller enkeltvis opfyldte kravene til oplysningspligten efter artikel 14, fordi oplysninger var for generelle og ikke konkrete nok. I en tilsvarende sag[70] fandt Datatilsynet, at advokatfirmaets oplysninger i en e-mail til den registrerede klagers advokat om undersøgelsen med link til advokatfirmaets privatlivspolitik (som var tilsvarende generelt og overordnet udfærdiget) i autosignaturen, ikke udgjorde tilstrækkelige oplysninger til, at oplysningspligten i artikel 14 var opfyldt.

Datatilsynet har også taget stilling til, om en advokatvirksomhed i forbindelse med en advokatundersøgelse kunne undlade at iagttage oplysningspligten efter artikel 14 med hjemmel i databeskyttelseslovens § 22, stk. 1 og 2.[71] Datatilsynet udtalte, at hensynet til at hindre klager eller andre involverede i at påvirke vidneudsagn udgjorde en interesse, der efter omstændighederne kunne tages afgørende hensyn til, og som konkret kunne begrunde en hel eller delvis undladelse af oplysningspligten. Når disse hensyn var bortfaldet, var der dog efter Datatilsynets opfattelse pligt til at opfylde oplysningspligten. Advokatvirksomheden burde have foretaget en løbende vurdering heraf. Som rettesnor anførte Datatilsynet, at afslutningen af interviews kunne anvendes, men at dette måtte bero på en konkret vurdering af sagens omstændigheder. Afgørelsen viser, at advokatfirmaer løbende skal vurdere, om grundlaget for at undlade at opfylde oplysningsforpligtelsen er til stede. Er det ikke længere det, skal oplysningsforpligtelsen efter Datatilsynets opfattelse iagttages.

I en lignende sag, hvor et advokatfirma havde indsamlet personoplysninger som led i behandlingen af en konkursbegæring uden at opfylde oplysningsforpligtelsen efter artikel 14, henviste Advokatfirmaet til undtagelserne i artikel 14, stk. 5, litra d (tavshedspligt), databeskyttelseslovens § 22, stk. 1 (afgørende hensyn til private interesser), og retsplejelovens § 129.[72] Her fandt Datatilsynet, at oplysningspligten ikke omfattede tilfælde, hvor der var lovbestemt tavshedspligt, herunder ved udøvelse af advokatvirksomhed. Tilsynet fandt desuden, at advokatfirmaets brug af oplysningerne til procesførelse kunne rummes inden for § 22, stk. 1, som undtagelsesmulighed til oplysningspligten.

7.2.3.1 Den praktiske gennemførelse af oplysningspligten

Den praktiske gennemførelse af oplysningspligten sker ved, at du skriftligt giver den registrerede de oplysninger, som du skal give efter artikel 13 eller 14. Da det er et krav, at oplysninger gives til den registrerede, er det ikke tilstrækkeligt blot at have oplysningerne på en hjemmeside el. lign., som den registrerede selv må finde.[73] I praksis indsætter mange advokatfirmaer en kort tekst i e-mailsignatur og brevskabeloner med henvisning og link til advokatvirksomhedens persondatapolitik (eller privatlivspolitik) på hjemmesiden. Overvej også at udarbejde og linke til mere detaljerede oplysningspligter

69 Datatilsynets afgørelse i journalnummer 2021-31-4751.
70 Datatilsynets afgørelse i journalnummer 2021-31-5542.
71 Datatilsynets afgørelse i journalnummer 2021-31-5307.
72 Datatilsynets afgørelse i journalnummer 2018-31-0842.
73 Dette vil kun være tilstrækkeligt i den situation, hvor undtagelsen i artikel 14, stk. 5, litra b finder anvendelse.

for konkrete sagstyper, som supplerer den mere generelle oplysningspligt. Oplysningspligten kan også vedhæftes (eller indarbejdes i) den første e-mail, hvor sagen påtages og i forbindelse med fremsendelse af aftalebrev, andre almene oplysningspligter mv. Husk, at de oplysninger, som du er forpligtet til at give den registrerede i medfør af oplysningspligten, skal være tydeligt adskilt fra andre oplysninger, jf. kravet om, at oplysningerne skal gives i en letforståelig og lettilgængelig form. I bilag 6 er givet et forslag til, hvordan oplysningspligten til en klient efter GDPR artikel 13 kan udarbejdes. Datatilsynet har udarbejdet et eksempel på, hvordan oplysningspligten kan iagttages efter artikel 14.[74]

Udover at have en procedure eller fremgangsmåde, som følges i forbindelse med håndtering af oplysningspligten, kan det være en god idé at anvende en skabelon eller liste, der indeholder alle de oplysninger, som du skal give din klient, når du påtager dig en ny sag. Derved sikres det, at du allerede ved klientforholdets etablering opfylder din oplysningspligt, og samtidig tvinger det dig til fra starten at overveje formålet med behandlingen, eventuelle modtagere af oplysningerne, opbevaringsperiode mv.

Hvis en registreret er repræsenteret af en advokat, vil oplysningspligten normalt kunne iagttages over for repræsentanten.[75] Oplysningspligten kan således opfyldes ved at give oplysningerne til advokaten. Det er også muligt at iagttage oplysningspligten over for modparten til din klient. Hvis modparten er repræsenteret ved advokat, bør kopi af oplysningspligten til modparten samtidig sendes til modpartens advokat.[76] Husk, at oplysningspligten skal ske med respekt for tavshedspligten i forhold til din egen klient.

7.2.4 Hvidvasklovens § 16 – information om behandling af personoplysninger

Hvis advokatvirksomheden er omfattet af hvidvasklovens regler, jf. § 1, stk. 1, nr. 13, skal den informere om de regler, der gælder for behandling af personoplysninger (særligt id-oplysninger), som sker med henblik på forebyggelse af hvidvask mv.[77] Denne hvidvaskoplysningsforpligtelse skal opfyldes inden etableringen af forretningsforbindelsen med klienten eller gennemførelsen af transaktionen (hvis der er tale om en enkeltstående transaktion).[78]

7.3 Retten til indsigt (artikel 15)

Den registrerede har ret til at få indsigt i, om der behandles personoplysninger om vedkommende og i givet fald adgang til kopi af oplysningerne. Herudover har den registrerede krav på en række oplysninger om behandlingen, herunder formålet hermed, kategorier af personoplysninger, eventuelle modtagere som oplysninger er videregivet til mv., samt fornødne artikel 46 garantier (for eksempel standardbestemmelser), hvis der sker overførsel til et tredjeland, jf. artikel 15, stk. 1-2. Oplysningspligten, jf. afsnit 7.2, har til formål at gøre den registrerede bekendt med, at advokatfirmaet behandler personoplysninger om vedkommende, så vedkommende kan udnytte sine rettigheder. Oplysningspligten skal som nævnt varetages på eget initiativ, dvs. uden forudgående henvendelse fra de registrerede. Retten til indsigt kræver derimod en henvendelse fra den registrerede.

74 Datatilsynets vejledning om de registreredes rettigheder, juli 2018, Bilag A, side 52.
75 Jf. Datatilsynets vejledning om de registreredes rettigheder juli 2018, side 11.
76 Jf. De Advokatetiske Regler – Kommenteret, 3. udgave 2022, side 371.
77 For nærmere beskrivelse af hvidvaskoplysningsforpligtelsen henvises til Advokatrådets reviderede hvidvaskvejledning, september 2022, side 41.
78 For ideoplæg til oplysningsforpligtelsen efter hvidvaskloven § 16 henvises til Advokatsamfundets hjemmeside Vejledning og idéoplæg | Advokatsamfundet

Modtager du en indsigtsanmodning i henhold til artikel 15, er udgangspunktet således, at du skal give de nævnte oplysninger og kopi af de behandlede personoplysninger.[79]

Retten til at modtage kopi af behandlede personoplysninger gælder imidlertid ikke, hvis dette vil krænke andres rettigheder og friheder, jf. artikel 15, stk. 4. Dette kan for eksempel være databeskyttelsesrettigheder for andre end den registrerede, men omfatter for eksempel også forretningshemmeligheder eller intellektuel ejendomsret som for eksempel ophavsret til software eller lign.

Udover den nævnte undtagelse i artikel 15, stk. 4, indeholder databeskyttelsesloven vigtige undtagelser for advokater, idet en anmodning om indsigt også kan afvises, hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv, jf. § 22, stk. 1, eller til offentlige interesser, jf. § 22, stk. 2. Advokaters tavshedspligt og retten til at forberede eget forsvar i retssager er eksempler på sådanne interesser og kan begrunde afvisning af en anmodning om indsigt.[80] Af den grund vil retten til indsigt i praksis ofte have begrænset betydning for advokater, medmindre der er tale om en anmodning fra advokatens egen klient eller eventuelt fra medarbejdere i advokatfirmaet.

Indsigtsretten kan dog i praksis have betydning for advokatvirksomheder, som gennemfører egentlige advokatundersøgelser. I den ovenfor omtalte sag, hvor Datatilsynet fandt, at en advokatvirksomhed ikke kunne undlade at iagttage oplysningspligten med henvisning til databeskyttelseslovens § 22, stk. 1 og 2,[81] fandt Datatilsynet også, at advokatvirksomheden burde have imødekommet klagers (den berørte persons) anmodning om kopi af personoplysninger, jf. GDPR artikel 15, stk. 3. Undladelsen af at udlevere kopi af oplysninger kunne efter Datatilsynets opfattelse ikke ske inden for rammerne af databeskyttelseslovens § 22, stk. 1 og 2, idet de interesser og hensyn, som ifølge advokatvirksomheden var årsagen til at oplysningerne ikke kunne gives, efter Datatilsynets opfattelse ikke var tilstede, når interviews i undersøgelsen var gennemført. Det var desuden ikke tilstrækkeligt at forelægge klager oplysningerne.

Det vil også være muligt at afslå en indsigtsanmodning helt eller delvist, hvis anmodningen er åbenbart grundløs eller overdreven, især fordi der er tale om gentagelse, jf. artikel 12, stk. 5, litra b. Der vil dog skulle meget til, før dette er tilfældet, og det er den dataansvarlige, der har bevisbyrden for, at dette er tilfældet. I en sag, hvor et advokatfirma havde anmodet om indsigt i personoplysninger hos et andet advokatfirma, vurderede Datatilsynet, at en afvisning af at imødekomme anmodningen ikke gav anledning til kritik, idet det ville have været nødvendigt at identificere, indsamle, gennemgå og vurdere mere end en mio. dokumenter for at afgøre, om de indeholdt personoplysninger om den registrerede. Ved vurderingen blev der desuden lagt vægt på, at anmodningen ikke var specificeret på en måde, der begrænsede omfanget af materiale, som skulle gennemgås for at identificere personlysningerne, og at det også måtte antages, at eventuelle oplysninger alene ville være accessoriske i forhold til formålet med dokumenterne.[82]

Retten til indsigt kan ydermere også være afskåret i lovgivningen. Det gælder for eksempel efter hvidvaskloven, hvorefter advokater skal hemmeligholde, at de har givet underretning, at underretning overvejes, og at der er eller vil blive iværksat en undersøgelse. I tråd hermed har personer, der er under mistanke, ikke adgang til at få oplysninger om, at de er under undersøgelse, eller at der er foretaget underretning som følge af mistanke, som vedrører dem, jf. § 26, stk. 5.

79 Eventuelt kopieret over i et nyt dokument eller mulighed for at tilgå oplysningerne elektronisk, jf. Datatilsynets vejledning om de registreredes rettigheder, juli 2018, side 27.
80 Betænkning nr. 1565/2017 om databeskyttelsesforordningen, side 395.
81 Datatilsynets afgørelse i journalnummer 2021-31-5307.
82 Datatilsynets afgørelse i journalnummer 2021-31-5085.

Hvis en anmodning ikke er omfattet af undtagelserne, og derfor skal opfyldes, skal det sikres, at der gives indsigt til den rette person, og at oplysninger vedrørende andre, som der ikke skal gives indsigt i, sløres. Sker dette ikke, kan det resultere i et brud på persondatasikkerheden.

En anmodning om indsigt skal besvares hurtigst muligt og senest en måned efter modtagelsen, jf. artikel 12, stk. 3. Hvis der er tale om en kompleks eller omfattende anmodning, kan fristen forlænges til to måneder efter modtagelsen.

Datatilsynet har udarbejdet en skabelon for, hvordan en anmodning om indsigt fra en registreret kan besvares, som der kan tages udgangspunkt i, hvis en anmodning skal imødekommes.[83]

7.4 Retten til berigtigelse (artikel 16)

Den registrerede har efter artikel 16 ret til uden unødig forsinkelse at få rettet urigtige eller forkerte oplysninger om sig selv.[84] Retten gælder kun i forhold til oplysninger, som objektivt set er forkerte. Den registrerede har således ikke krav på at få en oplysning berigtiget, hvis den blot er udtryk for en anden subjektiv eller faglig vurdering.[85]

I sager, hvor der er flere parter, herunder en eller flere modparter, behandler advokater ofte personoplysninger, som der ikke er enighed om. Det er især tilfældet, når der rådgives om tvister og faktum i et hændelsesforløb skal fastslås. I retssager kommer man for eksempel ofte ud for, at parterne er uenige om for eksempel indholdet af en sagkyndig erklæring eller rigtigheden af en skønsmands forklaring. I en ansættelsesretssag kan der også meget vel være uenighed om oplysninger. I sådanne situationer skal oplysningerne selvsagt ikke ukritisk berigtiges, selvom man modtager en anmodning fra den registrerede. Omvendt bør en anmodning ikke automatisk afvises med henvisning til, at der ikke er enighed om oplysningens rigtighed. Der bør foretages en egentlig vurdering, og den registreredes synspunkter bør noteres på sagen. Hvis der fortsat ikke er enighed, om hvorvidt oplysningen er korrekt, bør den registreredes oplysninger (for eksempel en lægeerklæring) tilføjes til sagen.

Hvis du modtager en anmodning om berigtigelse fra en registreret – det kan for eksempel være et vidne, der berigtiger sine kontaktoplysninger – har du som dataansvarlig pligt til at sikre, at oplysningerne berigtiges hos dig selv, men samtidig skal du som hovedregel tillige sikre dig, at andre, som du har videregivet oplysningerne til, får besked.[86] Det kan for eksempel være modparten eller retten.

7.5 Retten til sletning (artikel 17)

Efter GDPR artikel 17 har den registrerede som udgangspunkt ret til at få slettet personoplysninger om sig selv og kan anmode den dataansvarlige om at foretage sletning. Rettigheden går hånd i hånd med den dataansvarliges pligt til efter princippet om opbevaringsbegrænsning at slette personoplysninger, når det ikke længere er nødvendigt at opbevare dem.

Retten til sletning har i praksis relevans i den situation, hvor for eksempel en klient anmoder om sletning, men hvor personoplysningerne endnu ikke er slettet, fordi advokatvirksomheden har fastsat en længere opbevaringsperiode og frist for sletning.

83 Datatilsynets vejledning om de registreredes rettigheder, juli 2018, Bilag A, side 56-60.
84 Retten går hånd i hånd med princippet om rigtighed i artikel 5, stk. 1, litra d).
85 Datatilsynets vejledning om de registreredes rettigheder, juli 2018, side 32.
86 Jf. artikel 19.

Modtager du en anmodning om sletning, må du tage stilling til, om anmodningen er berettiget,[87] eller om du har det fornødne grundlag for at fortsætte med at behandle personoplysningerne (indtil oplysningerne på et senere tidspunkt skal slettes i overensstemmelse med dine egne sletteprocedurer/-frister).

Der er som nævnt undtagelser til retten om sletning, og i en række situationer er der ikke pligt til at imødekomme en anmodning om sletning. Undtagelserne fremgår af artikel 17, stk. 3, hvor især litra b og e, er relevante for advokater, idet (fortsat) behandling er nødvendig for at overholde en retlig forpligtelse (for eksempel tavshedspligt), eller for at et retskrav kan fastlægges, gøres gældende eller forsvares. Konkret kan det betyde, at advokaten ikke kan imødekomme en anmodning om sletning, fordi de pågældende oplysninger for eksempel skal opbevares til konflikttjek eller for at dokumentere og forsvare advokatens rådgivning, jf. beskrivelsen heraf i afsnit 6.6.2 og 6.6.4.

7.6 Retten til begrænset behandling (artikel 18)

Det følger af artikel 18, at den registrerede i visse situationer har ret til begrænset behandling af personoplysninger. I de nævnte situationer må du som advokat ikke behandle, herunder videregive, oplysninger på anden måde end at opbevare dem (anden behandling vil kræve samtykke), medmindre det sker for, at et retskrav kan fastlægges, gøres gældende eller forsvares, for at beskytte en anden fysisk eller juridisk person eller af hensyn til vigtige samfundsinteresser.

Retten må antages at have begrænset relevans for advokater, idet de nævnte undtagelser ofte vil kunne finde anvendelse. Dette vil dog skulle vurderes, hvis der anmodes om begrænset behandling.

7.7 Underretningspligt ifm. berigtigelse, sletning og begrænsning (artikel 19)

Hvis du som advokat berigtiger en forkert oplysning, sletter en oplysning eller begrænser behandling i henhold til hhv. artikel 16, artikel 17 og artikel 18, skal du underrette alle, som oplysningerne er videregivet til, herom. Formålet med reglen er, at for eksempel en forkert oplysning, som er blevet videregivet, også efterfølgende berigtiges hos modtagere af oplysningen. Underretningspligten gælder dog ikke, hvis det vil være umuligt eller er uforholdsmæssigt vanskeligt at foretage underretning. Du skal også oplyse den registrerede om modtagerne, hvis vedkommende anmoder om det.

7.8 Retten til dataportabilitet (artikel 20)

Efter artikel 20 har den registrerede ret til at modtage personoplysninger om sig selv i et struktureret, almindeligt anvendt og maskinlæsbart format og til at transmittere oplysningerne fra en dataansvarlig til en anden (for eksempel fra en advokatvirksomhed til en anden advokatvirksomhed).[88]

Retten er betinget af, at behandlingen af oplysningerne om den registrerede foretages automatisk, og at behandlingen er baseret på et samtykke eller er nødvendig for at opfylde en kontrakt. Det er desuden en betingelse, at den registrerede selv har givet dig personoplysningerne, og at en imødekommelse af retten ikke krænker andre rettigheder eller frihedsrettigheder.

87 Du skal i denne situation også sikre dig, at det rent faktisk er den registrerede, som anmoder om sletning.
88 Datatilsynets vejledning om de registreredes rettigheder, juli 2018, side 40.

Forudsat at betingelserne mv. er opfyldt, kan retten til dataportabilitet i praksis efter omstændighederne betyde, at for eksempel en (tidligere) klient kan kræve, at personoplysninger om vedkommende gives i et format, så de er egnede til elektronisk at blive sendt til og modtaget af klientens nye advokat, jf. advokatens pligt til ved udtræden at aflevere sagens akter til en ny advokat.[89]

Hvis du modtager en anmodning om dataportabilitet, må du således vurdere, om betingelserne i artikel 20 er opfyldt.[90]

7.9 Retten til indsigelse mod behandling (artikel 21)

Den registrerede kan efter artikel 21 under visse betingelser (bl.a. at det vedrører den pågældendes særlige situation) gøre indsigelse mod behandling af sine personoplysninger, hvis den er baseret på interesseafvejningsreglen i artikel 6, stk. 1, litra f), herunder profilering baseret på bestemmelsen. Hvis det kan påvises, at der er vægtige legitime grunde til behandlingen, der går forud for den registreredes interesser, rettigheder og frihedsrettigheder, eller behandlingen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares, kan indsigelsen afvises.

Retten må antages at have begrænset relevans for advokater, idet de nævnte undtagelser ofte vil kunne finde anvendelse. Dette vil dog skulle vurderes og kunne påvises, hvis der gøres indsigelse mod en behandling.

7.10 Retten til ikke at være genstand for automatisk behandling, profilering (artikel 22)

Artikel 22 indeholder som udgangspunkt et forbud mod, at den registrerede er genstand for en afgørelse, der udelukkende er baseret på automatisk behandling, herunder profilering, af den registreredes personoplysninger, og hvor der ikke er nogen form for menneskelig involvering hos den dataansvarlige eller mulighed for den registrerede for at blive hørt forbindelse med afgørelsen.

Bestemmelsen må antages at have begrænset praktisk relevans for advokater. I forbindelse med eventuel anvendelse af AI bør advokater dog være opmærksomme på forbuddet og sikre, at der ikke sker en automatisk behandling af personoplysninger, uden at nogle af undtagelserne i artikel 22, for eksempel samtykke, finder anvendelse. Det samme gælder fsva. LegalTech-ydelser.

89 Jf. omtalen af "uden skadevirkning" i AER artikel 68, stk. 2 i De Advokatetiske Regler – Kommenteret, 3. udgave 2022, side 300.
90 For en nærmere gennemgang heraf henvises til Datatilsynets vejledning om de registreredes rettigheder, juli 2018, side 40-43.

8. Behandlingssikkerhed

8.1 Indledning

GDPR indeholder krav om, at personoplysninger skal behandles sikkert under anvendelse/gennemførelse af passende tekniske og organisatoriske foranstaltninger bl.a. under hensyntagen til risiciene for fysiske personers rettigheder og frihedsrettigheder. Dette følger bl.a. af artikel 5, stk. 1 f), artikel 24, stk. 1 og artikel 32. De nævnte foranstaltninger og risikovurderinger er således centrale elementer i forhold til behandlingssikkerhed og beskrives derfor i det følgende.

8.2 Risikovurdering (artikel 32)

Vurdering af risici er et gennemgående tema i GDPR og arbejdet med overholdelse af GDPR forudsættes at ske ud fra en risikobaseret tilgang. Derfor er risikovurderinger af behandlingssikkerheden en vigtig del af grundlaget for en advokatvirksomheds tilrettelæggelse af sine aktiviteter, processer og politikker, og for hvordan virksomhedens systemer konfigureres.

Risikovurderingerne angår de registreredes rettigheder, og nærmere i hvilket omfang behandlingen af de registreredes personoplysninger i en given sammenhæng medfører konkrete risici for de registrerede. Arbejdet med risikovurderinger består overordnet i at kortlægge konkrete risici i en given sammenhæng og derefter enkeltvis at vurdere for hver af disse risici (og tiltag de kan give anledning til). Risikovurderingerne skal kunne dokumenteres. I praksis er det derfor sædvanligt at udarbejde risikovurderingerne skriftligt (som særskilte dokumenter eller elektronisk i et it-system).

Risikovurderinger er eksplicit påkrævet i flere forskellige sammenhænge. Generelt skal risici vurderes i forhold til behandlingssikkerheden efter GDPR artikel 32, og ved behandlinger, der medfører høj risiko, kan det være påkrævet at foretage en risikovurdering efter GDPR artikel 35 (konsekvensanalyse). Advokatvirksomheders udarbejdelse af konsekvensanalyser er nærmere behandlet i afsnit 8.3. Herudover skal risici vurderes som led i sikringen af, at behandlingen sker lovligt efter GDPR artikel 24, og at de tekniske og organisatoriske foranstaltninger er designet med henblik på en effektiv implementering af databeskyttelsesprincipperne efter GDPR artikel 25. Det kan tillige være påkrævet at foretage risikovurderinger i relation til overførsel af data til tredjelande, som nærmere beskrevet i afsnit 5.

Inden risikovurderingen skal foretages, skal advokatvirksomheden foretage en afgræsning af, hvad risikovurderingen skal omfatte. Risikovurderinger kan afgrænses på flere måder, men i praksis viser det sig ofte hensigtsmæssigt at afgrænse i forhold til den behandlingsaktivitet, der udføres, og med dette udgangspunkt beskrive konteksten for behandlingsaktiviteten. Alternativt kan der tages udgangspunkt i det it-system, som behandlingen vedrører. Dette kan for eksempel være en pragmatisk løsning at anvende, hvor risikovurderingen udarbejdes med henblik på at fastsætte passende sikkerhedsforanstaltninger i forbindelse med udarbejdelsen af en databehandleraftale vedrørende en databehandlers behandling af personoplysninger i tilknytning til levering af det pågældende it-system til advokatvirksomheden. I disse tilfælde er det dog vigtigt at være opmærksom på, at også forhold uden for it-systemet kan have relevans for risikovurderingen.

Datatilsynet har udarbejdet en skabelon til konsekvensanalyse vedrørende databeskyttelse, der kan findes via www.datatilsynet.dk. Skabelonen indeholder to afsnit (faner) med evalueringskriterier og en risici-oversigt, som i praksis både kan anvendes til egentlige konsekvensanalyser og til øvrige risiko-

vurderinger. Eksempelvis kan skabelonen anvendes til risikovurderinger af behandlingssikkerheden efter GDPR artikel 32.

Evalueringen i Datatilsynets skabelon er baseret på en simpel og udbredt model for risikoanalyse, hvor de enkelte risici analyseres i forhold til henholdsvis konsekvens (hvis risikoen materialiserer sig) og sandsynlighed (for at konsekvensen indtræder). Ud fra modellen kan de enkelte risici placeres i en risikomatrix, der giver et samlet overblik over de kortlagte og analyserede risici. I Datatilsynets model er der fire niveauer for hhv. konsekvens og sandsynlighed. For en given risiko kan konsekvensen være "ubetydelig", "mindre alvorlig", "meget alvorlig" eller "ødelæggende" og sandsynligheden for, at konsekvensen indtræder, kan være "usandsynligt", "mindre sandsynligt", "sandsynligt" eller "forventet". I skabelonen er nærmere beskrevet, hvad der forstås ved de forskellige grader af konsekvens.

Med skabelonen kan en simpel risikovurdering af behandlingssikkerheden for en konkret behandlingsaktivitet (for eksempel behandlingen i et advokatfirmas sagsstyringssystem) i praksis foretages efter følgende fremgangsmåde:

1. Der foretages en indledende afklaring af (i) hvilke personoplysninger der behandles som led i aktiviteten (hvilke typer af oplysninger rummer systemet), og (ii) hvordan oplysningerne behandles og i hvilket omfang oplysningerne kan tilgås, ændres og slettes (hvilke systemer er involveret, hvor opbevares og behandles data, hvem har adgang osv.).

2. Med udgangspunkt i afklaringen af behandlingen kortlægges de konkrete risikoscenarier, der skal vurderes. Det kan for eksempel gøres med udgangspunkt i den gængse metode, der også kendes inden for informationssikkerhedsområdet, hvor man identificerer de trusler, der i praksis kan forventes at medføre risiko i forhold til oplysningernes fortrolighed, tilgængelighed og integritet. Dvs. risikoscenarier hvor der for eksempel er risiko for (i) at oplysningerne tilgås og/eller videredistribueres uberettiget (**fortrolighed**), (ii) at oplysningerne i et eller andet omfang utilsigtet bliver utilgængelige (**tilgængelighed**), og (iii) at oplysningerne utilsigtet ændres eller slettes (**integritet**).

3. For hver af de kortlagte risikoscenarier vurderes derefter – med udgangspunkt i den aktuelle opsætning og behandlingsproces – hvor sandsynligt det er, at den identificerede trussel/hændelse vil indtræde ("Sandsynlighed for indtræden"), og hvilken konsekvens indtræden vil have ("Konsekvens ved indtræden"). Derved fremkommer den iboende risiko.

4. Når den iboende risiko for et risikoscenarie er fastslået, vurderes om den iboende risiko er acceptabel – og hvis ikke – om den kan formindskes ved mitigerende foranstaltninger (dvs. ændringer i opsætningen/systemerne og/eller behandlingsprocessen, som medfører, at den konkrete iboende risiko begrænses). Når eventuelle mitigerende foranstaltninger er beskrevet vurderes, hvilken betydning foranstaltningerne vil have for hhv. sandsynlighed for indtræden og konsekvens ved indtræden, hvorved residualrisikoen fremkommer.

5. Afslutningsvist anføres navnet på den person i advokatvirksomheden, der har ansvaret for det konkrete risikoscenarie, status for implementering af eventuelle mitigerende foranstaltninger beskrives, og dato (deadline) for gennemførelse af de mitigerende foranstaltninger.

Efter den første kortlægning og beskrivelse af de enkelte risikoscenarier fungerer risikooversigten som et redskab til det løbende arbejde med at implementere passende tekniske og organisatoriske foranstaltninger til sikring af fortrolighed, tilgængelighed og integritet af personoplysningerne. Ud over opfølgning på implementeringen af mitigerende foranstaltninger bør risikovurderingerne genbesøges med passende mellemrum.

8.3 Konsekvensanalyse (artikel 35)

8.3.1 Hvad er en konsekvensanalyse og dens formål?

Som det fremgår af afsnit 8.2, er det et krav efter GDPR artikel 32, at advokatvirksomheder som dataansvarlige foretager en risikovurdering af behandlingssikkerheden, inden en behandling af personoplysninger foretages, og at risikovurderingen løbende opdateres.

Efter GDPR artikel 35 skal der herudover udarbejdes en konsekvensanalyse vedrørende databeskyttelse (Data Protection Impact Assessment (DPIA)), hvis behandlingen sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Konsekvensanalysen har således et snævrere anvendelsesområde end risikovurderingen af behandlingssikkerheden, da den kun skal udarbejdes i de tilfælde, hvor en konkret risikovurdering af behandlingssikkerheden viser en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

Formålet med at udarbejde en konsekvensanalyse er at foretage en bredere vurdering end risikovurderingen af behandlingssikkerheden. Konsekvensanalysen skal således omfatte vurdering af risici for manglende overholdelse af alle GDPR's regler og ikke kun behandlingssikkerheden.

Herudover skal der foretages høring hos Datatilsynet, og de registreredes synspunkter skal indhentes vedrørende den planlagte behandling, hvis konsekvensanalysen viser en høj risiko.

Datatilsynet har offentliggjort to skabeloner i form af en generel skabelon til konsekvensanalyse og en skabelon til konsekvensanalyse vedrørende kunstig intelligens (AI), som advokatvirksomheder kan benytte til at udarbejde konsekvensanalyser.[91] Disse skabeloner henviser til den metode, der fremgår af den internationale standard for udarbejdelse af konsekvensanalyser vedrørende databeskyttelse, ISO/IEC DIS 29134, med nødvendige tilpasninger af hensyn til behandlingens karakter.

8.3.2 Hvornår skal der laves en konsekvensanalyse?

GDPR opregner i artikel 35, stk. 3, en række tilfælde, hvor det navnlig er påkrævet med en konsekvensanalyse. Der er tale om en ikke-udtømmende liste. Det Europæiske Databeskyttelsesråd (EDPB) (tidligere artikel 29-gruppen) har fastsat kriterier, der kan hjælpe advokatvirksomheder som dataansvarlige med at identificere de behandlinger, der kræver udarbejdelse af en konsekvensanalyse. Datatilsynet har offentliggjort en liste over de behandlingssituationer, hvor en konsekvensanalyse er påkrævet (positivliste).[92]

Datatilsynet kan offentliggøre en liste for, hvornår en konsekvensanalyse ikke er påkrævet, jf. artikel 35, stk. 5, men det har Datatilsynet endnu ikke gjort.

91 Skabelonerne kan findes via Datatilsynets hjemmeside Konsekvensanalyse (datatilsynet.dk), hvor der også er en vejledning til konsekvensanalyser.
92 Listen kan findes via Datatilsynets hjemmeside Datatilsynets liste over de typer af behandlingsaktiviteter, der er underlagt kravet om en konsekvensanalyse.

Det er i første omgang advokatvirksomheden som dataansvarlig, der skal foretage vurderingen af, om en konsekvensanalyse skal udarbejdes. Hvis behandlingen i risikovurderingen af behandlingssikkerheden ikke udgør en høj risiko, eller ikke er omfattet af kriterierne i Datatilsynets liste eller opfylder to eller flere af kriterierne på EDPB's liste, skal der normalt ikke foretages en konsekvensanalyse. Da listerne imidlertid ikke er udtømmende, skal advokatvirksomheden altid foretage en konkret vurdering af, om der alligevel skal laves en konsekvensvurdering.

Hvis en konsekvensanalyse viser, at behandlingen af personoplysninger vil føre til en høj risiko for de registrerede i mangel af foranstaltninger truffet af advokatvirksomheden for at begrænse risikoen (residualrisikoen), skal Datatilsynet høres om behandlingen, inden behandlingen påbegyndes, jf. artikel 36, stk. 1.

8.3.3 GDPR artikel 35, stk. 3

Det følger af artikel 35, stk. 3, at en konsekvensanalyse navnlig er påkrævet i følgende tilfælde:

- en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, og som er grundlag for afgørelser
- behandling i stort omfang af følsomme personoplysninger (artikel 9) eller oplysninger om strafbare forhold (artikel 10), eller
- systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

Det bemærkes i den forbindelse, at det fremgår af betragtning 91 i præamblen til GDPR, at behandling af personoplysninger ikke bør anses for at være omfattende, hvis der er tale om bl.a. en advokats behandling af personoplysninger om klienter, og at en konsekvensanalyse i dette tilfælde ikke bør være obligatorisk.

Dette må indebære et udgangspunkt, hvorefter der ikke automatisk skal udarbejdes konsekvensanalyse, blot fordi en advokat for eksempel er i besiddelse af en større mængde følsomme personoplysninger. Omvendt kan en konsekvensanalyse ud fra en konkret vurdering alligevel være påkrævet, men formentlig først når der er tale om advokatvirksomheder, som behandler meget store mængder af de omtalte typer af oplysninger.

8.3.4 Datatilsynets liste

Datatilsynets positivliste over de behandlingssituationer, hvor konsekvensanalysen er påkrævet, indeholder følgende:

- Behandling af biometriske data med det formål entydigt at identificere en fysisk person i sammenhæng med mindst et yderligere kriterie fra artikel 29-gruppens retningslinjer (WP248 rev. 01).
- Behandling af genetiske data i sammenhæng med mindst et yderligere kriterie fra artikel 29-gruppens retningslinjer (WP248 rev. 01)
- Behandling af lokationsdata i sammenhæng med mindst et yderligere kriterie fra artikel 29-gruppens retningslinjer (WP248 rev. 01)
- Behandling ved brug af nye teknologier i sammenhæng med mindst et yderligere kriterie fra artikel 29-gruppens retningslinjer (WP248 rev. 01)

- Behandling der fører til afgørelser om en fysisk persons rettigheder til et produkt, en service, en potentiel mulighed eller begunstigelse, der er baseret på en hvilken som helst form for automatiseret afgørelse (herunder profilering)
- Behandling der omfatter profilering af fysiske personer i stor skala, sådan som dette er defineret i artikel 29-gruppens retningslinjer (WP248 rev. 01)
- Behandling af personoplysninger om sårbare personer eller hvor der er tale om behandling af følsomme oplysninger (særlige kategorier), og hvor der benyttes profilering eller andre former for automatiserede afgørelser
- Behandlinger hvor et brud på persondatasikkerheden kan have en direkte effekt på en persons fysiske helbred eller på sikkerheden for en fysisk person.

8.3.5 EDPB's retningslinjer

EDPB (artikel 29-gruppen) har fastsat følgende ni kriterier (WP248 rev. 01),[93] der kan anvendes til at vurdere, hvorvidt en given behandling kræver en konsekvensanalyse:

- Evaluering eller analyse, herunder profilering og forudsigelse
- Automatiseret beslutningstagning med juridisk eller tilsvarende betydelig virkning
- Systematisk overvågning
- Følsomme oplysninger eller oplysninger af meget personlig karakter
- Omfattende behandling af personoplysninger
- Matching eller kombination af datasæt
- Behandling af oplysninger om sårbare registrerede
- Innovativ brug eller anvendelse af ny teknologi eller nye organisatoriske løsninger
- Hvis behandlingen i sig selv "hindrer registrerede i at udøve en rettighed eller gøre brug af en tjeneste eller en kontrakt".

8.3.6 Hvordan vurderes det, om der skal laves en konsekvensanalyse?

Hvis risikovurderingen af behandlingssikkerheden viser en høj risiko for de registrerede, eller behandlingsaktiviteten er på Datatilsynets "plus-liste", eller hvis behandlingsaktiviteten opfylder to eller flere af kriterierne på EDPB's liste, skal der laves en konsekvensanalyse.

Er den dataansvarlige advokatvirksomhed i tvivl om, hvorvidt der er behov at udarbejde en konsekvensanalyse, kan der eventuelt laves en indledende tærskelanalyse, som kan bidrage til at vurdere risikoniveauet, herunder om behandlingsaktiviteten overskrider tærsklen i forhold til, om der er behov for at udarbejde en konsekvensanalyse.

Selve vurderingen af, om der skal udarbejdes en konsekvensanalyse, skal advokatvirksomheden sørge for løbende at ajourføre, hvis der sker ændringer i behandlingsaktiviteten, der medfører en større risiko for de registreredes rettigheder og frihedsrettigheder.

93 EDPB's kriterier kan findes via Datatilsynets hjemmeside wp248 rev.01_da (datatilsynet.dk).

8.3.7 Hvad skal konsekvensanalysen vedrørende databeskyttelse indeholde?

En konsekvensanalyse består af at beskrive behandlingen af personoplysninger, vurdere behandlingens nødvendighed og proportionalitet samt bidrage til at håndtere de risici for fysiske personers rettigheder og frihedsrettigheder, som behandlingen af personoplysninger ved den konkrete behandling medfører, ved at vurdere dem og fastlægge foranstaltninger til at afhjælpe dem.

GDPR fastsætter følgende minimumskrav til konsekvensanalysens indhold, jf. artikel 35, stk. 7:

- En systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen, herunder i givet fald de legitime interesser, der forfølges af den dataansvarlige
- En vurdering af om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene
- En vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder
- De foranstaltninger, der påtænkes for at imødegå disse risici, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af GDPR, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

EDPB (artikel 29-gruppen) oplister i WP 248 rev. 01 en række kriterier for indholdet i en konsekvensanalyse.

Til brug for udarbejdelse af konsekvensanalyser kan advokatvirksomheder som nævnt tage udgangspunkt i Datatilsynets skabeloner til udarbejdelse af konsekvensanalyser, som kan findes via www.datatilsynet.dk.

8.4 Sikkerhed

Det er som nævnt et krav efter GDPR, at der implementeres passende tekniske og organisatoriske tiltag med henblik på at sikre beskyttelse af personoplysninger. Nedenfor er givet en beskrivelse af tiltag, som kan anvendes, herunder også en række tiltag vedrørende fysisk sikkerhed.

Tekniske foranstaltninger

Advokater skal implementere solide tekniske løsninger for at beskytte personoplysninger mod uautoriseret adgang, tab eller ødelæggelse. Følgende ikke udtømmende løsninger kan anvendes:

- Adgangskontrol: Begræns adgang til personoplysninger gennem brug af adgangsrettigheder og tofaktorgodkendelse.
- Kryptering: Krypter data både under opbevaring og ved overførsel for at minimere risikoen for datalæk. Brug relevante opdaterede krypteringsstandarder som for eksempel TLS og AES-256 eller afsendelse af e-mails end-to-end krypterede (for eksempel via tunnel eller certifikat).

- Sikker backup: Etabler backup-løsninger, der sikrer, at data kan gendannes i tilfælde af tekniske fejl eller sikkerhedsbrud. Automatisér backups og opbevar dem i adskilte, sikre miljøer.
- Netværkssikkerhed: Implementér firewalls, intrusion detection systems (IDS) og regelmæssige opdateringer af systemer for at beskytte mod cyberangreb. Anvend VPN til fjernadgang og sikre forbindelser.
- Overvågning og logning**:** Overvåg adgang og brug af it-systemer, og gem logfiler som dokumentation for sikkerhedsrelaterede aktiviteter. Analyser logfiler regelmæssigt for at opdage uregelmæssigheder.
- **Antivirus og opdateringer:** Installer og vedligehold antivirusprogrammer, og sørg for, at software og operativsystemer altid er opdaterede.

For vejledninger og standarder anbefales det at konsultere ENISA (European Union Agency for Cybersecurity) for detaljerede risikovurderingsmetoder og tekniske anbefalinger.

Eksempler:

1. Et advokatkontor kan opsætte tofaktorgodkendelse på alle mobiltelefoner og arbejdsstationer for at forhindre uautoriseret adgang.
2. Et advokatkontor kan udføre regelmæssige penetrationstests for at identificere og rette sikkerhedssvagheder.

Organisatoriske foranstaltninger

Effektive organisatoriske tiltag sikrer, at tekniske foranstaltninger understøttes af klare retningslinjer og procedurer. Følgende ikke udtømmende løsninger kan anvendes:

- Sikkerhedspolitikker: Udarbejd og vedligehold interne sikkerhedspolitikker for behandling og beskyttelse af personoplysninger. Politikkerne skal være tilgængelige og forståelige for alle medarbejdere.
- Medarbejdertræning: Afhold løbende uddannelse og workshops for at sikre, at alle medarbejdere kender deres ansvar under GDPR. Fokusér på områder som phishing-angreb og korrekt håndtering af personoplysninger.
- Intern kontrol: Gennemfør regelmæssige audits og kontroller for at sikre, at procedurer og sikkerhedsforanstaltninger overholdes. Dokumentér resultaterne og opfølgningen på disse.
- Adgangshåndtering: Gennemgå og revider regelmæssigt adgangsrettigheder for at sikre, at ingen medarbejdere har adgang til oplysninger, de ikke længere har behov for.
- God it-hygiejne: Opmuntre til praksisser som at bruge stærke, unikke adgangskoder, undgå genbrug af koder og logge ud af systemer, når de ikke bruges.

Eksempler:

1. En advokatvirksomhed kan etablere en årlig træningsdag med fokus på cybersikkerhed og GDPR-compliance.
2. Ledelsen kan udpege en databeskyttelsesansvarlig, der løbende evaluerer kontorets procedurer og sikkerhedsforanstaltninger.

Fysiske foranstaltninger

For at beskytte personoplysninger skal advokater også tage hensyn til fysiske sikkerhedsforanstaltninger. Følgende ikke udtømmende løsninger kan anvendes:

- Adgangsbegrænsning til lokaler: Sikring af, at kun autoriserede personer har adgang til kontorer, serverrum og arkiver. Brug adgangskontrolsystemer som nøglekort eller biometrisk identifikation.
- Opbevaring af fysiske dokumenter: Opbevar papirdokumenter i aflåste skabe eller rum med adgangsbegrænsning. Marker arkiver tydeligt for at forhindre fejladgang.
- Overvågningssystemer: Brug overvågningskameraer og alarmsystemer til at beskytte lokaler mod uautoriseret adgang. Sørg for, at kameraerne er placeret, så de ikke krænker privatlivets fred.
- Bortskaffelse af dokumenter: Brug makulatorer eller sikre bortskaffelsesservices til destruktion af fysiske dokumenter, der ikke længere er relevante. Overvej certificerede destruktionsfirmaer til større mængder.
- Beskyttelse af arbejdsstationer: Sørg for, at computere og skærme ikke er synlige for uvedkommende, og anvend skærmlåse.

Eksempler:

1. Et advokatkontor kan installere overvågningskameraer i receptionen og sikre, at alle besøgende registreres.
2. Papirdokumenter med klientdata, der skal bortskaffes, kan makuleres straks for at eliminere risikoen for, at oplysningerne havner i forkerte hænder.

Løbende kontrol og opdatering

Sikkerhed er en løbende proces, der kræver regelmæssig kontrol og opdatering af procedurer og teknologier:

- Audits: Gennemfør årlige gennemgange af sikkerhedsforanstaltninger for at sikre effektivitet og overholdelse. Brug eventuelt eksterne eksperter til at validere compliance-niveauet.
- Opdatering: Juster procedurer og teknologier baseret på nye trusler, teknologiske fremskridt og lovændringer.
- Test af beredskab: Simuler sikkerhedshændelser for at træne medarbejdere og teste robustheden af de implementerede foranstaltninger.

For en sammenhængende tilgang til GDPR-compliance anbefales det at konsultere ENISA (European Union Agency for Cybersecurity) for detaljerede risikovurderingsmetoder og tekniske anbefalinger. Derudover tilbyder Datatilsynets vejledninger værdifulde råd om organisatoriske procedurer og kontrolmekanismer, der kan understøtte overholdelsen af GDPR.

8.4.1 Afgørelser vedrørende advokaters behandlingssikkerhed

Datatilsynet har i forbindelse med tilsyn hos et advokatfirma og et kontorfællesskaber af advokatfirmaer i 2019 vurderet behandlingssikkerheden ved fremsendelse af e-mails. I den ene sag fandt Datatilsynet, at advokatfirmaets fremsendelse af e-mails over internettet var i overensstemmelse med GDPR og Datatilsynets retningslinjer, og at advokatfirmaet havde foretaget en risikovurdering heraf.[94] I den anden sag udtalte Datatilsynet imidlertid kritik af, at kontorfællesskabet ikke havde efterlevet GDPR, idet der ikke var indført procedurer, der sikrede, at der anvendtes kryptering på transportlaget via TLS til fremsendelse af e-mails over internettet, og at kontorfællesskabet ikke havde påvist at have udarbejdet en risikovurdering.[95]

I 2022 anmeldte Datatilsynet desuden et advokatfirma til Politiet med indstilling om en bøde på DKK 500.000 for utilstrækkelig behandlingssikkerhed, fordi advokatfirmaet ikke havde foranstaltninger til verifikation, for eksempel multifaktorlogin, i forbindelse med fjernadgang til advokatfirmaets it-systemer. Som følge af den utilstrækkelige sikkerhed var der sket et brud på persondatasikkerheden, hvor hackere havde fået adgang til et stort antal personoplysninger af særlig beskyttelsesværdig karakter.

8.5 Brud på persondatasikkerheden – når uheldet er ude

8.5.1 Hvad er et brud?

Hvis personoplysninger indgår i et sikkerhedsbrud, er der tre steps, som dataansvarlige skal forholde sig til (ud over at få stoppet bruddet hurtigst muligt):

1. Alle sikkerhedsbrud skal logges
2. Sikkerhedsbrud skal indberettes til Datatilsynet, dog afhængig af risikoen
3. Sikkerhedsbrud skal underrettes til de registrerede personer, hvis personoplysninger er omfattet af bruddet, dog afhængig af risikoen

Først skal det dog afklares, om der er tale om et "brud på persondatasikkerheden", som er den legale definition på et sikkerhedsbrud, jf. artikel 4, nr. 12 i GDPR:

"Et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet".

I praksis kan et sikkerhedsbrud for eksempel ske, når den dataansvarliges it-systemer ikke er tilstrækkeligt sikret, og udefrakommende får adgang til oplysninger for eksempel via ransomware, men også den interne håndtering kan forårsage et sikkerhedsbrud for eksempel ved afsendelse af en e-mail til en forkert modtager eller nedbrud af systemer, hvor der ikke er backup. Advokatvirksomheden skal derfor være både opmærksom på at få opdaget brud, der opstår hos selve advokatvirksomheden, men skal også særligt sikre, at eventuelle brud hos databehandlere håndteres i tilstrækkeligt omfang.

94 Datatilsynets afgørelse i journalnummer 2019-41-0026.
95 Datatilsynets afgørelse i journalnummer 2019-41-0029.

8.5.2 Fremgangsmåde ved brud

Som det fremgår ovenfor, skal tre punkter følges ved sådanne brud:

1. Intern logning (artikel 33 i GDPR)

Alle brud på persondatasikkerheden skal logges i en intern liste af den dataansvarlige. I listen skal indgå de faktiske omstændigheder ved bruddet, dets virkninger og de trufne afhjælpende foranstaltninger. Forpligtelsen til logning er uafhængig af forpligtelserne til at anmelde og underrette.

2. Anmeldelse til Datatilsynet (artikel 33 i GDPR)

Kravet om anmeldelse afhænger af, om "det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder".

Den dataansvarlige skal straks efter at være blevet bekendt med bruddet foretage en risikovurdering, hvor der er tale om en konkret og reaktiv risikovurdering specifikt i forhold til konsekvenserne af bruddet på persondatasikkerheden for de berørte personer som følge af sikkerhedsbruddet. Systematikken for risikovurderingen fremgår nedenfor.

Fristen er 72 timer for anmeldelse, og en foreløbig anmeldelse kan sendes ind, hvis ikke alle oplysninger er til stede.

Foretages anmeldelsen til Datatilsynet ikke inden for 72 timer, skal den ledsages af en begrundelse for forsinkelsen. Anmeldelsen af et sikkerhedsbrud til Datatilsynet sker igennem virk.dk, hvor man step-by-step skal udfylde anmeldelsesblanketten.[96]

Risikovurderingen skal dokumenteres.

3. Underretning af de registrerede (artikel 34 i GDPR)

Kravet om underretning afhænger af, om "et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder".

Hvis der for eksempel er risiko for skade på omdømme eller tab af fortrolighed af personoplysninger underlagt tavshedspligt, er det som udgangspunkt høj risiko. Risikovurderingen følger den samme systematik, der er beskrevet nedenfor.

Fristen er "uden unødig forsinkelse", og informationen skal gives hurtigst muligt af hensyn til de registrerede, så de kan nå at tage de anbefalede foranstaltninger, inden uvedkommende misbruger personoplysninger om dem.

Risikovurderingen efter artikel 34 skal også dokumenteres.

8.5.3 Risikovurdering

En risiko for fysiske personers rettigheder og frihedsrettigheder omfatter bl.a. diskrimination, identitetstyveri eller -svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af personoplysninger underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den registrerede.

96 For nærmere vejledning om håndtering af brud på persondatasikkerheden henvises til Datatilsynets vejledning fra februar 2025 https://www.datatilsynet.dk/Media/637886298435856391/H%C3%A5ndtering%20af%20brud%20p%C3%A5%20persondatasikkerheden.pdf

Selvom der er tale om en høj risiko, er der undtagelser til anmeldelses- og underretningspligten, når der er gennemført passende tekniske og organisatoriske foranstaltninger, der har medført, at den høje risiko for de registrerede sandsynligvis ikke længere er reel, hvis underretning kræver en uforholdsmæssig indsats, eller hvis underretning kan udsættes i henhold til national lovgivning.

I den konkrete vurdering af risikoen for de registreredes rettigheder og frihedsrettigheder som følge af et brud på persondatasikkerheden, bør følgende forhold altid indgå:

- Typen af sikkerhedsbrud, herunder om der er sket tab af oplysninger, brud på fortroligheden eller en integritetskrænkelse
- Oplysningernes art og omfang
- Risikoen for at registrerede kan identificeres
- Konsekvenser bruddet kan have for de registrerede
- Hvorvidt bruddet omfatter særlige registrerede (for eksempel hvis der er tale om børn eller særligt udsatte)
- Antallet af berørte fysiske personer

Som eksempel på et sikkerhedsbrud med lav risiko for de registrerede kan nævnes, at personoplysningerne er pseudonymiserede, dvs. at der er to lister: En liste med et nummer og de oplysninger, der egentlig identificerer de registrerede som CPR-nummer eller navn, og en anden liste med et nummer for hver person sammen med de øvrige oplysninger. De to lister opbevares separat. Hvis kun listen med numre og de øvrige oplysninger er omfattet af bruddet, vil der ofte være lav risiko, da individet ikke umiddelbart er identificerbart for den, der har listen, selvom det i teorien er omfattet af definitionen af personoplysninger. I sådanne tilfælde skal der som udgangspunkt hverken ske anmeldelse til Datatilsynet eller underretning af de registrerede.

Et eksempel på et sikkerhedsbrud med mellem risiko kan være en medarbejders uautoriserede adgang til en intern sag med fortrolige oplysninger, hvor der er tillid til medarbejderen, og hvor en log dokumenterer, at kun den pågældende medarbejder har tilgået sagen. Her kan den dataansvarlige for eksempel vurdere, at sikkerhedsbruddet ikke udgør en risiko for den registrerede. Hvis det vurderes, at der ikke er pligt til at underrette Datatilsynet, vil der heller ikke være pligt til underretning af de registrerede.

Afslutningsvist kan som eksempel på et sikkerhedsbrud med høj risiko nævnes, at en e-mail med fortrolige oplysninger om et individs helbredsoplysninger sendes til en forkert modtager. I dette tilfælde skal der som udgangspunkt både ske anmeldelse til Datatilsynet og underretning af den registrerede.

Ovenstående eksempler er alene pejlemærker, og risikovurderinger skal altid foretages ud fra en vurdering af de konkrete forhold.

9. Tilsyn og sanktioner

9.1 Indledning

Som nævnt i indledningen er det Datatilsynet, der fører tilsyn med, at advokater overholder GDPR og den supplerende lovgivning. Datatilsynet påser af egen drift eller efter klage fra en registreret, at behandlingen af personoplysninger finder sted i overensstemmelse med reglerne. Datatilsynet kan i dag i forbindelse med sit tilsyn kræve enhver oplysning, der er af betydning for dets virksomhed, og tilsynet har til enhver tid uden retskendelse adgang til lokaler, hvorfra behandling af personoplysninger foretages. Det gælder som udgangspunkt også adgang til oplysninger, der er underlagt tavshedspligt.

9.2 Ret til erstatning og erstatningsansvar (artikel 82)

Enhver person, som har lidt materiel eller immateriel skade som følge af en ulovlig behandling af personoplysninger eller anden behandling i strid med GDPR eller databeskyttelsesloven, har ret til erstatning efter artikel 82.

9.3 Pålæggelse af administrative bøder (artikel 83)

GDPR indeholder i artikel 83, stk. 4, mulighed for bødestraf på op til 10 millioner EUR eller 2 procent af virksomhedens samlede globale årlige omsætning for manglende efterlevelse af pligterne efter GDPR.

For manglende efterlevelse af de registreredes rettigheder, de grundlæggende principper for behandling, reglerne for overførsel af persondata til lande uden for EU eller afgørelser fra Datatilsynet kan der straffes med bøder på op til 20 millioner EUR eller 4 procent af dens samlede globale årlige omsætning, jf. artikel 83, stk. 5.

I Danmark er det domstolene, som idømmer straf for overtrædelse af GDPR. Datatilsynet kan alene indstille hertil, men kan for eksempel udtale kritik, udstede påbud, osv.

Datatilsynet har udarbejdet vejledninger om udmåling af bøder til hhv. virksomheder[97] og fysiske personer.[98] Vejledningerne indeholder nærmere oplysninger om bl.a. kategorisering og fastsættelse af beløb for overtrædelserne (ud fra de beløb og procentsatser, der gælder for virksomheder), et katalog over standardiserede bødeindstillinger (for fysiske personer), skærpende og formidlende omstændigheder samt betalingsevne og indkomstforhold. Af vejledningen vedrørende fysiske personer fremgår det desuden, at en virksomhed (for eksempel et advokatfirma) efter omstændighederne kan idømmes en bøde, selv hvor medarbejderen (for eksempel en advokat) handler uden for instruks, men dog klart i arbejdsgiverens (advokatfirmaets) interesse. Som eksempel herpå nævnes en situation, hvor en medarbejder er nødsaget til at fremsende et vigtigt dokument indeholdende personoplysninger ukrypteret på vegne af sin arbejdsgiver – og medarbejderen i den konkrete situation vurderer, at arbejdsgiveren ville have godkendt fremsendelsen – på trods af, at modtageren ikke understøtter et krypteringsniveau, der imødegår de risici, som fremsendelsen af dokumentet kræver.[99] Er der omvendt tale om en situation, hvor medarbejderen (advokaten) behandler personoplysninger til egne formål, der ligger klart uden for arbejdsgiverens (advokatfirmaets) aktiviteter, taler dette for at se medarbejderen som selvstændig

97 https://www.datatilsynet.dk/Media/1/9/B%C3%B8devejledning.pdf
98 https://www.datatilsynet.dk/Media/638145553634879070/B%C3%B8devejledning%20fysiske%20personer.pdf
99 Jf. Datatilsynets vejledning om udmåling af bøder til fysiske personer, marts 2023, side 6.

dataansvarlig for behandlingen (og dermed bøden). Som eksempel herpå nævnes den situation, hvor medarbejderen har handlet i det, som den pågældende medarbejder fejlagtigt har vurderet, var arbejdsgiverens interesse, men hvor arbejdsgiveren har givet klare instrukser om det modsatte.

9.3.1 Afgørelser vedrørende advokaters manglende overholdelse

Efter GDPR's ikrafttrædelse i maj 2018 forventedes der umiddelbart væsentligt højere bøder end efter den tidligere retstilstand, hvor der alene blev givet mindre bøder eller udtalt kritik fra Datatilsynet. Dette er også tilfældet i dag, hvor Datatilsynet i dets afgørelser har indstillet til betydelige og væsentligt højere bøder for overtrædelse.

Siden GDPR's ikrafttrædelse har Datatilsynet også truffet en række afgørelser, som vedrører advokaters manglende overholdelse af databeskyttelsesreglerne. Niveauet i disse sager har varieret fra kritik som laveste grad af sanktion til indstilling om pålæggelse af bøde på DKK 500.000 som højeste sanktionsgrad. I bilag 7 er givet en oversigt over Datatilsynets offentliggjorte afgørelser vedrørende advokaters manglende efterlevelse af reglerne.

10. DPO (databeskyttelsesrådgiver)

10.1 DPO (artikel 37)

GDPR indeholder regler om, at visse virksomheder skal have en databeskyttelsesrådgiver. En databeskyttelsesrådgiver er en rådgiverfunktion i en organisation eller virksomhed, der skal inddrages i alle spørgsmål om databeskyttelse og rådgive om de databeskyttelsesretlige regler.

I de fleste tilfælde skal private virksomheder ikke udpege en databeskyttelsesrådgiver. Der kan dog være pligt til at udpege en databeskyttelsesrådgiver, hvis behandlingen af personoplysninger er din kerneaktivitet, og behandlingen sker i stort omfang. Behandlingen skal endvidere enten bestå i en regelmæssig og systematisk overvågning af personer eller vedrøre følsomme oplysninger eller oplysninger om strafbare forhold.

10.2 Skal advokatfirmaer udpege en DPO?

Udgangspunktet vil være, at advokater ikke har pligt til at udpege en databeskyttelsesrådgiver, fordi behandling af personoplysninger ikke kan siges at udgøre advokaters kerneaktivitet. Dette gælder, selvom advokater i dag behandler personoplysninger i stort omfang.

Du kan vælge frivilligt at udpege en databeskyttelsesrådgiver. I så fald skal du være opmærksom på, at du underlægges samme krav til databeskyttelsesrådgiveren, som hvis du var forpligtet til at udpege en sådan.

10.3 Persondatapolitik (artikel 24)

Selvom du vælger ikke at udpege en DPO, anbefales det dog, at der udpeges en eller flere personer i advokatvirksomheden, som kan varetage arbejdet med GDPR og internt kan rådgive om, hvordan databeskyttelsesreglerne efterleves.

Det følger også af GDPR artikel 24, at du som dataansvarlig skal implementere passende tekniske og organisatoriske foranstaltninger for at sikre, at behandling af personoplysninger sker i overensstemmelse med databeskyttelsesreglerne. I denne sammenhæng er en overordnet persondatapolitik et vigtigt redskab, da den fastlægger rammerne for, hvordan personoplysninger skal beskyttes og må behandles af den konkrete advokatvirksomhed. En persondatapolitik bør således skitsere, hvem der i advokatvirksomheden har ansvaret for at sikre, at reglerne overholdes, og hvordan dette mere konkret sikres ved for eksempel udarbejdelse og implementering af retningslinjer og procedurer for behandlingen og beskyttelsen af personoplysninger.

Det er ikke direkte påkrævet at udarbejde en persondatapolitik, og der er derfor heller ingen faste krav til indholdet af en sådan. Det er dog nødvendigt, at du som dataansvarlig fastlægger, hvordan du vil overholde reglerne og de forpligtelser, der følger deraf. Hvis I som mange andre vælger at fastlægge dette gennem en overordnet persondatapolitik, bør den bl.a. have følgende indhold:

1. Formål og anvendelsesområde: Beskrivelse af formålet med politikken, og hvem den gælder for.
2. Ansvar og roller (governance) – Hvem har ansvar for overholdelse af databeskyttelsesreglerne, og hvordan sikres det, at dette ansvar kan løftes? Sker der løbende træning af medarbejderne i databeskyttelsesreglerne?

3. Indsamling og behandling af personlysninger – Overordnede retningslinjer for, hvilke oplysninger der indsamles, hvordan de anvendes, og til hvilke formål. Beskrivelse af hvordan de grundlæggende principper for behandling af personoplysninger iagttages.
4. Behandlingssikkerhed – Hvordan vurderes det, hvilket sikkerhedsniveau der er passende for forskellige behandlingsaktiviteter og systemer?
5. Registreredes rettigheder – Hvordan sikrer advokatvirksomheden registreredes rettigheder?
6. Brud på persondatasikkerheden – Hvordan håndterer advokatvirksomheden brud på persondatasikkerheden?
7. Databehandlere og tredjelandsoverførsler – Krav til samarbejde med databehandlere og overførsel af personoplysninger til tredjelande.

Politikken bør løbende opdateres, og der bør i nødvendigt omfang henvises til andre relevante politikker, retningslinjer og procedurer, for eksempel procedurer for håndtering af brud på persondatasikkerheden, håndtering af registreredes rettigheder osv.

10.4 DPO-funktion som advokatydelse

Med GDPR er der opstået et nyt forretningsområde, hvor bl.a. advokatfirmaer sælger DPO-funktionen som advokatydelse, og klienten udpeger advokatfirmaet som dets DPO. Datatilsynet har i en række sager vurderet, at udpegelsen af et advokatfirma som ekstern DPO levede op til kravene i artikel 37.[100]

Hvis du som advokat varetager DPO-funktionen for en klient, skal du være opmærksom på risikoen for, at der kan opstå interessekonflikter i forbindelse med varetagelsen heraf og din rådgivning af klienten i andre sager, hvor der kan indgå databeskyttelsesretlige spørgsmål.

100 Tilsyn med databeskyttelsesrådgiverens opgavevaretagelse i Mariagerfjord Kommune (journalnummer 2019-423-0224) og Tilsyn med databeskyttelsesrådgiverens opgavevaretagelse i Vejle Kommune journalnummer 2019-423-0220).

11. Bilagsliste

Bilag 1 - Forslag til art. 30 fortegnelser - personaleadministration og juridisk rådgivning (afsnit 3.2)

Bilag 2 - Advokaters persondataretlige roller (afsnit 4.2)

Bilag 3 - Forslag til bilag A-C i databehandleraftale (afsnit 4.3)

Bilag 4 - Oversigt advokaters opbevaring af personoplysninger (afsnit 6.6.6)

Bilag 5 - Oversigt advokaters oplysningspligt - hovedregler og undtagelser (afsnit 7.2)

Bilag 6 - Forslag til art. 13 stk. 1 oplysningspligt (afsnit 7.2.3.1)

Bilag 7 - Oversigt over Datatilsynets afgørelser vedr. advokaters overholdelse af GDPR (afsnit 9.3.1)

ADVOKAT SAMFUNDET

Vejledning
– Advokatens behandling af personoplysninger

Udgiver: Advokatsamfundet
Kronprinsessegade 28
1306 København K
Telefon 33 96 97 98
postkasse@advokatsamfundet.dk
Advokatsamfundet.dk

Layout: Bilgrav Design