Vejledning

Advokatens behandling af personoplysninger

ADVOKATSAMFUNDET
RETSSIKKERHED · UAFHÆNGIGHED · INTEGRITET

April 2018

Indhold

1. Indledning og afgrænsning 4
2. Hvilke oplysninger er omfattet? 6
   2.1. Definition 6
   2.2. Typer af oplysninger 6
3. Er advokaten databehandler eller dataansvarlig? 7
4. Hvad er ”behandling”? 11
5. Hvornår må advokaten behandle personoplysninger? 11
   5.1. Behandlingsprincipperne 11
   5.2. Behandlingsgrundlaget – alle oplysninger 13
   5.3. Behandlingsgrundlaget – almindelige oplysninger (artikel 6) 13
   5.4. Behandlingsgrundlaget – følsomme oplysninger (artikel 9) 14
   5.5. Behandlingsgrundlaget – strafbare forhold 15
   5.6. Behandlingsgrundlaget – personnumre 16
6. Den registreredes rettigheder 16
   6.1. Indledning 16
   6.2. Oplysningspligten 18
      6.2.1. Oplysninger kommer fra den registrerede (artikel 13) 18
      6.2.2. Oplysninger kommer ikke fra den registrerede (artikel 14) 22
   6.3. Retten til indsigt (artikel 15) 24
   6.4. Retten til berigtigelse (artikel 16) 25
   6.5. Retten til sletning (artikel 17) 25
   6.6. Andre rettigheder (artikel 18-22) 27
7. Databeskyttelsesrådgiveren (DPO’en) 28
8. Dokumentationskrav mv. 29
9. Behandlingssikkerhed 29
10. Tilsyn og sanktioner 33
11. Tjekliste 34

Bilag 1: Oversigt over personoplysninger 35

Bilag 2: Eksempel på advokaten som databehandler 36

Bilag 3: Eksempel på advokaten som dataansvarlig.....37

1. Indledning og afgrænsning

I denne vejledning finder du en række gode råd til, hvordan du som advokat forholder dig til de nye databeskyttelsesregler. Særligt vil der blive sat spot på problemstillingerne i krydsfeltet mellem advokatpligterne og persondataretten.

De nye databeskyttelsesregler findes i databeskyttelsesforordningen (forordningen)[1]. Forordningen har direkte virkning i Danmark fra den 25. maj 2018. Forordningen vil blive suppleret af databeskyttelsesloven (loven)[2], som forventes vedtaget af Folketinget i løbet af foråret 2018. Lovforslaget behandles lige nu i Folketinget, og det er således ikke givet, at lovforslaget vedtages i sin nuværende form, hvilket man skal have in mente, når der i denne vejledning henvises til lovforslaget.

Vejledningen skal ikke læses som en udtømmende beskrivelse af reglerne i forordningen og loven, og det er ikke ambitionen, at vejledningsmaterialet skal komme omkring alle dele af persondataretten. Datatilsynet har som tilsynsmyndighed offentliggjort en række vejledninger, der omfatter en lang række emner, herunder også emner, som ikke vil blive berørt i denne vejledning. Der vil i denne vejledning løbende blive henvist til og citeret fra de forskellige vejledninger fra Datatilsynet.

En stor del af forordningens regler og principper er videreført fra de tidligere persondataregler, men forordningen indfører også en række nye elementer og skærpede regler. Hvis du i forvejen lever op til den gældende persondatalov, vil der ikke være tale om omfattende ændringer. Har du derimod ikke tidligere haft fokus på reglerne, er der behov for, at du nu får overblik over, hvordan du behandler personoplysninger. Denne vejledning vil primært have fokus på de nyskabelser i forordningen og loven, som kan tænkes at få betydning for advokatens behandling af personoplysninger, men en lang række af de allerede kendte regler og principper vil også blive behandlet.

Forordningen og loven indeholder ikke særlige regler for advokater, som vi kender det fra eksempelvis hvidvaskområdet. Det er derfor ambitionen, at dette vejledningsmateriale skal give et generelt overblik over, hvilke regler, der er relevante for advokater, og sætte persondataretten ind i en advokatretlig sammenhæng. Vejledningen er således målrettet advokater, og der er fokus på det, der er relevant for advokater.

---

[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. (Databeskyttelsesforordningen).
[2] Lovforslag nr. L68 af 25. oktober 2017 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesloven).

Vejledningen vil ikke beskæftige sig med de mere driftsmæssige sider af advokatvirksomheden og interne håndteringer i advokatvirksomheden af eksempelvis personaleoplysninger. Det bemærkes, at Danske Advokater har lavet vejledninger om nogle af disse emner. Denne vejledning er rettet mod den enkelte advokat i dennes virke som advokat, og den klientrettede virksomhed vil være i centrum. Man skal som advokat udvise en adfærd, der stemmer med god advokatskik – også når man behandler personoplysninger. Hvor det er relevant, vil der derfor ske reference til de advokatetiske regler og deres betydning for advokatens håndtering af personoplysninger. Omdrejningspunktet vil være at komme med eksempler på udfordringer af advokatetisk og persondataretlig karakter, som advokaten i sin hverdag kan stå overfor.

En grundlæggende forudsætning for at komme i hus er, at man skaffer sig et overblik over, hvilke typer personoplysninger man behandler, hvordan man modtager oplysningerne, hvad oplysningerne bruges til, hvordan personoplysninger bliver videreformidlet internt i virksomheden og til eksterne parter, samt hvordan oplysningerne opbevares og hvor længe. Selve processen med kortlægning af personoplysningerne i din virksomhed er ikke beskrevet i denne vejledning, men du bør overveje, om du selv kan gennemføre en sådan, eller om du skal søge bistand hertil. Datatilsynet og Erhvervsstyrelsen har lanceret en ny udgave af PrivacyKompasset, hvor virksomheder kan tage en online test, der kan hjælpe dem i gang med at implementere databeskyttelsesreglerne i deres virksomhed samt få svar på helt basale spørgsmål i forhold til håndtering af persondata.[3]

Det er tanken, at vejledningen bliver et praktisk og dynamisk redskab, som løbende kan forbedres og opdateres. Kommentarer og forbedringsforslag modtages derfor gerne, ligesom vejledningen også løbende vil blive revideret med relevant praksis fra Advokatnævnet og Datatilsynet. Ved vejledningens offentliggørelse udestår endvidere en række vejledninger fra Datatilsynet. Af samme grund vil vejledningen på enkelte punkter være mere generel, fordi der som følge af manglende vejledninger fra Datatilsynet endnu ikke er vished om, hvordan tilsynet konkret forholder sig til reglerne.

[3] https://startvaekst.virk.dk/privacykompasset

2. Hvilke oplysninger er omfattet?

2.1. Definition

Forordningen gælder for personoplysninger.

> ”Personoplysninger er enhver form for information, der kan henføres til bestemte personer, også selv om dette forudsætter kendskab til et personnummer, registreringsnummer eller lignende. Også oplysninger i form af eksempelvis et billede eller et fingeraftryk er personoplysninger. Selv om oplysninger som et navn eller en adresse er erstattet af en kode, er det stadig en personoplysning, hvis koden kan føres tilbage til den oprindelige personoplysning. For eksempel er oplysninger, der er krypteret, fortsat personoplysninger, så længe der er nogen, der kan gøre oplysningerne læsbare og identificere de personer, det drejer sig om.”[4]

Personoplysninger, der er krypteret eller pseudonymiseret, er fortsat personoplysninger, hvis de kan føres tilbage til en person, eksempelvis ved brug af en kode. Derimod kan kryptering eller pseudonymisering anvendes til at forbedre behandlingssikkerheden, da det ikke umiddelbart er muligt at identificere vedkommende, jf. også afsnit 9 om behandlingssikkerhed.

Det er kun oplysninger om ”fysiske personer”, der er omfattet af forordningen. Advokatens behandling af oplysninger om juridiske personer (A/S, ApS, K/S, fonde, foreninger mv.) falder uden for anvendelsesområdet. Virksomhedsoplysninger, der kan identificere enkeltpersoner (for eksempel enkeltmandsvirksomheder), er derimod omfattet.[5] Oplysninger om fysiske personer som eksempelvis aktionærer, anpartshavere, kommanditister mv., som advokaten måtte komme i besiddelse af i forbindelse med behandlingen af en sag om en juridisk person, er tillige omfattet af begrebet personoplysninger. I en sag om eksempelvis virksomhedsoverdragelse behandles også personoplysninger om ledelsen, de ansatte medarbejdere i virksomheden mv.

Bemærk, at databeskyttelsesloven forventes at komme til at indeholde særlige regler for behandling af oplysninger om juridiske personer (virksomheder mv.), hvis denne behandling udføres for kreditoplysningsbureauer.[6]

2.2. Typer af oplysninger

Der skelnes i forordningen grundlæggende mellem to typer af oplysninger: almindelige personoplysninger (artikel 6) og følsomme personoplysninger (artikel 9) (se bilag 1).

Følsomme oplysninger nyder en særlig høj beskyttelsesstatus. Grundlæggende kan man sige, at jo mere følsomme personoplysningerne er, jo strengere er betingelserne for at kunne behandle

[4] Datatilsynets vejledning om databeskyttelsesforordningen, oktober 2017, side 7.
[5] Datatilsynets vejledning om databeskyttelsesforordningen, oktober 2017, side 5.
[6] § 2, stk. 2.

oplysningerne. Det er kun de personoplysninger, der er nævnt i artikel 9, der anses for følsomme oplysninger, mens de personoplysninger, der ikke hører til kategorien følsomme oplysninger, kategoriseres som almindelige oplysninger. Man skal dog være opmærksom på, at behandlingen af oplysninger om strafbare forhold og lovovertrædelser (artikel 10) samt oplysninger om personnumre (artikel 87) er en særlig form for almindelige oplysninger, som forventes særskilt reguleret i databeskyttelseslovens §§ 8 og 11.[7]

3. Er advokaten databehandler eller dataansvarlig?

I forordningen sondres der mellem, om man er dataansvarlig for en behandling af personoplysninger, eller om man er databehandler for en dataansvarlig. Det har afgørende betydning, at du får afklaret, hvad din rolle er, inden du begynder at behandle personoplysninger, fordi kravene til en dataansvarlig er forskellige fra kravene til en databehandler. Det er den dataansvarlige, der står på mål for, at reglerne om persondata overholdes.

Den dataansvarlige skal blandt andet:

- Sikre sig, at principperne for behandling er overholdt og dokumentere dette, se afsnit 5.1.
- Sikre sig, at der er et grundlag for at behandle personoplysningerne, se afsnit 5.2-5.5.
- Sikre sig, at de registreredes rettigheder iagttages, se afsnit 6.
- Sikre sig, at Datatilsynet får besked ved sikkerhedsbrud, se afsnit 9.

I modsætning til de nugældende regler er databehandleren også et selvstændigt pligtsubjekt efter forordningen, og man skal derfor være opmærksom på sit ansvar, uanset om man agerer i rollen som dataansvarlig eller som databehandler.

I Datatilsynets vejledning om dataansvarlige og databehandlere, november 2017, side 22-23, er nævnt to eksempler om advokater. I det ene eksempel er advokatfirmaet databehandler (vedhæftet som bilag 2 til denne vejledning), mens advokatfirmaet i det andet eksempel er dataansvarlig (vedhæftet som bilag 3 til denne vejledning).

Som det fremgår af eksemplerne fra Datatilsynet, kan der i situationer vedrørende advokatbistand og anden rådgivning argumenteres for forskellige delinger af ansvaret, men oftest vil mest tale for at anse advokaten for dataansvarlig, fordi klienten typisk ikke henvender sig til advokaten for at få behandlet personoplysninger, men derimod retter henvendelse til advokaten for at få advokatbistand. Endvidere taler det for at anse advokaten for dataansvarlig, at advokaten træffer egne beslutninger om udførelsen af opgaven, og at advokaten, selvom der består et fuldmagtsforhold mellem advokat og klient, ikke er underlagt egentlig instruksionsbeføjelse fra

[7] Oplysninger om væsentlige sociale problemer og andre rent private forhold forventes i modsætning til tidligere ikke længere at være omfattet af særregulering i loven.

klienten. Advokater er underlagt retsplejelovens regler og de advokatetiske regler, som blandt andet forudsætter uafhængighed mellem advokat og klient. Det er derfor tvivlsomt, hvorvidt en advokat kan følge en detaljeret instruks fra en dataansvarlig om, hvordan advokaten skal behandle personoplysninger, ligesom advokaten heller ikke blot kan slette oplysninger efter instruks fra en dataansvarlig, da det vil kunne være i strid med de advokatetiske regler. Du vil som advokat træffe selvstændige beslutninger om, hvilke personoplysninger der skal indsamles, slettes og videregives, og behandlingen af personoplysningerne sker derfor typisk ikke efter instruks eller godkendelse fra klienten.

Advokater modtager også personoplysninger fra andre end klienten, eksempelvis fra modparten eller modpartens advokat. Meget taler for at anse advokaten for dataansvarlig for sådanne personoplysninger, som advokaten modtager fra andre. Konsekvensen af, at du som advokat bliver ny selvstændig dataansvarlig for personoplysninger modtaget fra eksempelvis modparten eller dennes advokat, er, at du skal sikre dig, at du har et behandlingsgrundlag, og at oplysningspligten opfyldes. Du skal dog være særlig opmærksom på dine advokatpligter i den forbindelse, herunder særligt tavshedspligten. Der kan henvises til en mere detaljeret gennemgang af de registreredes rettigheder og oplysningspligten i afsnit 6 nedenfor.

Eksempel 1 - Advokaten som procesførende:

En advokat repræsenterer virksomhed B i en retssag om fratrædelsesgodtgørelse, som Jens Jensen har fremsat krav om mod virksomhed B. I forbindelse med forberedelsen og gennemførelsen af retssagen modtager advokaten en række personoplysninger om Jens Jensen fra virksomhed B, fra Jens Jensens advokat og fra retten. Advokaten er at anse som dataansvarlig for disse personoplysninger, eftersom advokaten står forholdsvis frit med hensyn til, hvordan han vil behandle dem, herunder videreformidle i forhold til retten og Jens Jensens advokat.

Det er imidlertid ikke altid lige let at finde ud af, om advokaten agerer som dataansvarlig eller databehandler. Hvis du er i tvivl om, hvorvidt du er dataansvarlig for en behandling af personoplysninger, kan du se på, hvilken ydelse der skal leveres. Hvis det primært drejer sig om levering af en anden ydelse end behandling af personoplysninger, taler det for at anse dig som dataansvarlig.[8] Hvis du træffer beslutninger om formålet med behandlingen af personoplysningerne samt bestemmer, hvordan personoplysningerne skal behandles, vil du oftest være dataansvarlig.[9] Resultatet kan dog også være, at dataansvaret er delt.[10] Datatilsynets vejledning om dataansvarlige

[8] Datatilsynets vejledning om dataansvarlige og databehandlere, november 2017, side 7-8.
[9] Datatilsynets vejledning om dataansvarlige og databehandlere, november 2017, side 9-11.
[10] Datatilsynets vejledning om dataansvarlige og databehandlere, november 2017, side 15.

og databehandlere indeholder en liste over udsagn, som du kan lægge vægt på ved din vurdering af, om du er dataansvarlig eller databehandler.[11]

Du skal være opmærksom på, at et dataansvar ikke er ensbetydende med, at du skal indgå en databehandleraftale med for eksempel din klient.[12] Du bør i den konkrete situation vurdere, om der er tale om en databehandlerkonstruktion, og i bekræftende fald skal du sikre dig, at der udarbejdes en databehandleraftale. I nogle tilfælde er det imidlertid oplagt, at der skal udarbejdes en databehandleraftale. Det vil typisk være tilfældet i forhold til eksempelvis en IT-leverandør eller en virksomhed, der hoster dine data eksternt. Datatilsynet har på sin hjemmeside offentliggjort en standard-databehandleraftale.[13]

Ud over det eksempel med advokatfirmaet som databehandler i forbindelse med administration af en whistleblowerordning, som er nævnt i Datatilsynets vejledning, jf. bilag 3 nedenfor, kan tænkes situationer, hvor advokatens behandling af personoplysninger er så bundne, at advokatens handlefrihed i forhold til håndteringen af persondata er så begrænset, at man vil komme frem til, at advokaten er databehandler. Her er nævnt nogle eksempler på situationer, hvor man kan argumentere for forskellige delinger af ansvaret.

Eksempel 2 - Inkassosag:

En advokat bliver bedt om at inddrive et tilgodehavende, som virksomhed A har hos en af sine kunder, Hans Hansen. I forbindelse med inddrivelsen vil advokaten modtage en række personoplysninger vedrørende Hans Hansen, herunder oplysninger om Hans Hansens bopæl og kontaktoplysninger samt oplysninger om Hans Hansens økonomi. Der kan på den ene side argumenteres for at anse advokaten for databehandler, fordi inddrivelsen sker efter nøje instruks fra klienten, og fordi fremgangsmåden for behandlingen af sagen i stort omfang er lovbunden. Advokatens arbejde i disse sager vil endvidere ofte være meget ekspeditionspræget. Omvendt taler mest dog for at anse advokaten som dataansvarlig for personoplysningerne om Hans Hansen, eftersom de snævre grænser for advokatens ageren i sagen i overvejende grad *ikke* relaterer sig til hans behandling af personoplysningerne i sagen. Hvordan han nærmere vil behandle personoplysningerne, herunder om han vil videregive dem til fogedretten med henblik på at realisere inddrivelsen af tilgodehavendet, er som udgangspunkt ikke undergivet strenge begrænsninger.

Eksempel 3 - Fondsadministration:

En advokat varetager hvervet som fondsadministrator i Fond A, og advokaten modtager løbende ansøgninger fra privatpersoner, der ønsker støtte fra fonden. Både fonden og

[11] Datatilsynets vejledning om dataansvarlige og databehandlere, november 2017, side 11-12.
[12] Datatilsynets vejledning om dataansvarlige og databehandlere, november 2017, side 12-14.
[13] https://www.datatilsynet.dk/vejledninger/vejledninger-databeskyttelsesforordningen/

advokaten er som udgangspunkt at anse som dataansvarlige for personoplysningerne fra ansøgerne, der kan bestå i ansøgernes kontaktoplysninger, økonomiske oplysninger, helbredsoplysninger mv. Såfremt fonden imidlertid har fastlagt snævre regler for behandlingen af indkomne ansøgninger, herunder eksempelvis regler om hvordan ansøgningerne registreres, hvordan de forelægges for fondsbestyrelsen, hvordan de efterfølgende gemmes, slettes mv., vil der også kunne argumenteres for at anse advokaten som databehandler for personoplysningerne vedrørende ansøgningerne. Fonden vil i den situation være dataansvarlig.

Eksempel 4 - Due diligence:

Advokat A aftaler med advokat B, at han vil bistå advokat B med visse udvalgte undersøgelser i en due diligence proces, hvor advokat B bistår selskab X i forberedelserne med købet af selskab Y. Advokat A får i forbindelse med sin bistand, ligesom advokat B, adgang til et online datarum, hvor der ligger en lang række oplysninger om selskab Y's medarbejdere. Advokat A har fået specifikke instrukser om, hvilke dokumenter han skal gennemgå, og hvordan han skal rapportere sine juridiske fund til advokat B, der vil rapportere samlet til selskab X. Advokat A vil på denne baggrund formentlig være at anse som databehandler i forhold til advokat B. Advokat B vil som udgangspunkt være at anse som dataansvarlig, medmindre der foreligger en meget specifik regulering/instruks fra selskab X vedrørende processen for håndtering, herunder formidling og opbevaring, af de omhandlede persondata.

Det er således ikke altid givet, at en advokat er dataansvarlig. Det er imidlertid Advokatrådets opfattelse, at en advokat i langt de fleste tilfælde må anses for dataansvarlig for de personoplysninger, som advokaten behandler som led i sit advokathverv og hermed forbundne funktioner som eksempelvis fondsadministrator, bobestyrer, kurator, medhjælper i gældssaneringssager mv. Dette blandt andet som følge af de regler og advokatetiske pligter, der sædvanligvis knytter sig til advokatens udførelse af sit hverv. Er advokaten dataansvarlig, skal advokaten overholde behandlingsprincipperne, sikre tilstedeværelsen af gyldigt behandlingsgrundlag, iagttage de registreredes rettigheder osv. Det kan dog forekomme, at der i et konkret hverv er lagt så snævre rammer for advokatens udførelse af det konkrete hverv, herunder med hensyn til videregivelse og anden praktisk håndtering af personoplysninger, at advokaten er databehandler i forhold til hvervgiver. Dette kan være tilfældet, hvor advokaten leverer specifikke afgrænsede serviceydelser i underentreprise for eksempelvis andre advokater, eller hvor advokaten stiller it-understøttende systemer til rådighed for sine klienter. I sådanne situationer skal advokaten være opmærksom på de regler, der knytter sig til rollen som databehandler, herunder hvis advokaten benytter sig af andre underleverandører (underdatabehandlere).[14]

[14] Datatilsynets vejledning om dataansvarlige og databehandlere, november 2017, side 13-14.

4. Hvad er ”behandling”?

Forordningen finder anvendelse på behandling af personoplysninger, og begrebet behandling skal forstås i meget bred forstand. Behandling er ikke lig med ”sagsbehandling”, men er derimod et særskilt persondataretligt begreb.

> ”Begrebet ”behandling” omfatter enhver form for håndtering af personoplysninger. Det er først og fremmest elektronisk behandling af oplysninger, der er omfattet af reglerne. Det kan for eksempel være indsamling, registrering, systematisering, opbevaring, søgning, brug, videregivelse eller sletning af oplysninger.”[15]

Bemærk, at den blotte adgang til at se personoplysninger er en behandling i forordningens forstand, ligesom sletning af personoplysninger er at betragte som en behandling – også selvom sletning er det eneste, du gør med oplysningen.

> ”Forordningen finder anvendelse på behandling af personoplysninger, der helt eller delvis fortages ved hjælp af automatisk behandling, og på anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register. Det er nemlig, når personoplysninger bruges på en måde, som gør dem let og hurtigt søgbare, at interessen for at beskytte dem aktualiseres.”[16]

Begrebet ”automatisk” behandling er sammenfaldende med elektronisk behandling. Benytter du dig af manuelle registre som eksempelvis kartotekskasser eller lignende, er disse som udgangspunkt også omfattet.

5. 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.

5.1. Behandlingsprincipperne

De grundlæggende principper for behandlingen er:

> ”Lovlighed, rimelighed og gennemsigtighed: Den dataansvarlige skal overholde reglerne for behandling af oplysninger og skal give let tilgængelig information om behandlingen af oplysninger. Det indebærer blandt andet, 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.

[15] Datatilsynets vejledning om databeskyttelsesforordningen, oktober 2017, side 9.
[16] Datatilsynets vejledning om databeskyttelsesforordningen, oktober 2017, side 5.

Formålsbegrænsning: Når der indsamles oplysninger, skal den dataansvarlige gøre sig klart, hvilke formål oplysningerne indsamles til, og det skal være saglige formål. Man må ikke indsamle oplysninger med den begrundelse, at det måske senere kan vise sig nyttigt at være i besiddelse af oplysningerne. Det er i første omgang den virksomhed eller myndighed mv., der indsamler oplysninger, som skal vurdere, om en bestemt indsamling af oplysninger er saglig. Det kan blandt andet bedømmes ud fra, om indsamlingen sker i forbindelse med løsningen af en opgave, som det er naturligt for virksomheden eller myndigheden at løse.

Dataminimering: Behandlingen af personoplysninger skal begrænses til det, der er nødvendigt for at opfylde formålet.

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

Opbevaringsbegrænsning: Personoplysninger skal slettes eller gøres anonyme, når det ikke længere er nødvendigt for den dataansvarlige at have oplysningerne. 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.

Integritet og fortrolighed: Oplysninger skal beskyttes mod uautoriseret eller ulovlig behandling, ligesom det skal sikres, at oplysninger ikke går tabt eller bliver beskadiget."[17]

Principperne for behandling af personoplysninger skal du 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 de personoplysninger, som du modtager. Det betyder, at du for eksempel skal slette personoplysninger efter princippet om opbevaringsbegrænsning, hvis det ikke længere er nødvendigt for dig at have oplysningerne. Princippet om dataminimering 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 tror, at du senere kan få brug for oplysningerne. Tilsvarende skal du slette personoplysninger, som du modtager i sagen, for eksempel fra din klient, hvis ikke personoplysningerne er relevante i forhold til håndteringen af sagen. Med princippet om rigtighed følger en pligt til at sørge for, at de personoplysninger, du behandler, er korrekte og ajourførte, samt en pligt til at slette eller ajourføre urigtige oplysninger.

Principperne følger af artikel 5, stk. 1. Derudover følger det af 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 8 om dokumentationskrav mv.

[17] Datatilsynets vejledning om databeskyttelsesforordningen, oktober 2017, side 10-11.

5.2. Behandlingsgrundlaget – alle oplysninger

Grundlaget for behandling af personoplysninger veksler mellem, hvilken type af oplysninger der er tale om (følsomme eller almindelige personoplysninger). Behandlingen kan dog altid finde sted på grundlag af et samtykke fra den registrerede. Vælger du *samtykke* som dit behandlingsgrundlag, skal du være opmærksom på, at der stilles en række krav til samtykket, før det er gyldigt, og du skal som dataansvarlig kunne bevise, at der foreligger et samtykke.[18]

Behandler du i dag personoplysninger på baggrund af et allerede indhentet samtykke, kan behandlingen fortsætte, såfremt det tidligere indhentede samtykke opfylder gyldighedskravene i forordningen.[19] Som noget nyt i forordningen sammenlignet med nugældende regler er det en betingelse for samtykkets gyldighed, at den, der giver samtykke, på forhånd er blevet oplyst om, at samtykket kan tilbagekaldes. Oplysningen om muligheden for at tilbagekalde et samtykke antages imidlertid ikke at være en gyldighedsbetingelse for et allerede indhentet samtykke fra før 25. maj 2018.[20] Du skal være opmærksom på, at udfordringen ved at behandle personoplysninger på baggrund af et samtykke er, at et samtykke til enhver tid kan trækkes tilbage. Du bør derfor overveje, om din behandling af personoplysninger kan ske på et andet behandlingsgrundlag end samtykke, da samtykke som grundlag som følge af tilbagekaldelsesadgangen medfører en vis usikkerhed.

Du skal være opmærksom på, at samtykke til én form for behandling ikke nødvendigvis omfatter samtykke til en anden form for behandling – for eksempel hvis behandlingen består i en videregivelse til tredjemand. Der skal i øvrigt gives besked til den registrerede om en sådan ændring af behandlingen, hvis dette ikke oprindeligt er meddelt den registrerede, jf. artikel 13, stk. 3, og 14, stk. 4, samt afsnit 6.2 om oplysningspligten.

5.3. Behandlingsgrundlaget – almindelige oplysninger (artikel 6)

Grundlaget for behandling af almindelige personoplysninger kan – udover samtykke – 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 forordningen 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 efter forordningen.[21] Det gælder for

---

[18] Forordningen artikel 7 og præambelbetragtning nr. 171, Datatilsynets vejledning om samtykke, november 2017, samt Artikel 29-gruppens udtalelse nr. 15 af 13. juli 2011 om samtykke.
[19] Datatilsynets vejledning om samtykke, november 2017, side 17.
[20] Datatilsynets vejledning om samtykke, november 2017, side 17.
[21] Artikel 6, stk. 1, litra c.

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 persondataforordningen, 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 forordningen, og/eller at dit grundlag i hvidvaskloven til at behandle oplysningerne ikke længere er tilstrækkeligt.

Kan du ikke støtte din behandling af almindelige personoplysninger på et samtykke, en kontrakt eller en retlig forpligtelse, kan du overveje, om et af de andre behandlingsgrundlag i forordningens artikel 6 kan udgøre hjemmel for din behandling af almindelige personoplysninger. Et andet behandlingsgrundlag kan være den såkaldte *interesseafvejningsregel*, 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. Som noget nyt vejer personoplysninger om børn særlig tungt. Husk, at oplyse den registrerede om de interesser, hvorpå behandlingen baseres, jf. afsnit 6 om oplysningspligten. Interesseafvejningsreglen er ofte relevant ved behandling af personoplysninger vedrørende andre end din klient. I eksemplet med advokaten som dataansvarlig (se bilag 3) vil advokaten kunne behandle almindelige personoplysninger om de unge mennesker i erstatningssagen efter interesseafvejningsreglen.

5.4. Behandlingsgrundlaget – 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, finder anvendelse.

Grundlaget for behandling af følsomme personoplysninger kan – ud over samtykke – være, at behandlingen er nødvendig for, at *retskrav* kan fastlægges, gøres gældende eller forsvares.[22] Behandlingen kan være i den registreredes interesse, den dataansvarliges interesse eller tredjemands interesse. 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 5.1. Igen kan henvises til eksemplet med advokaten som dataansvarlig (se bilag 3), hvor advokaten formentlig vil kunne behandle følsomme personoplysninger om de unge mennesker i erstatningssagen under henvisning til, at behandlingen er nødvendig for, at erstatningskravet (retskravet) kan gøres gældende.

[22] Artikel 9, stk. 2, litra f, og præambelbetragtning nr. 52.

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 forordningens artikel 9, stk. 2, kan udgøre hjemmel for din behandling af følsomme personoplysninger. For eksempel kan du behandle følsomme personoplysninger, som tydeligvis er offentliggjort af den registrerede.

5.5. Behandlingsgrundlaget – strafbare forhold

Der er i forordningen mulighed for at fastsætte særskilte nationale regler om behandling af oplysninger om strafbare forhold.[23] Regler om behandlingen af oplysninger om strafbare forhold forventes fastsat i databeskyttelseslovens § 8. Betingelserne for privates, herunder advokaters, behandling af oplysninger om strafbare forhold er snævre.

Grundlaget for behandlingen af oplysninger om strafbare forhold kan – udover samtykke – være, hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede (interesseafvejning).[24] Behandling kan derudover finde sted, hvis betingelserne for at behandle følsomme oplysninger er opfyldt, jf. afsnit 5.4.

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, jf. afsnit 5.4. 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.[25]

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 eksempelvis 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.[26] Det vil i øvrigt være i strid med god advokatskik at indgive politianmeldelse, medmindre der foreligger fornødent grundlag herfor.[27] Vær i den forbindelse

---

[23] Artikel 10.
[24] § 8, stk. 3.
[25] § 8, stk. 4.
[26] Betænkning nr. 1565/2017 om databeskyttelsesforordningen, side 236.
[27] AER pkt. 17.1.

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 forordningen. 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.[28]

5.6. Behandlingsgrundlaget – personnumre

Behandling af oplysninger om personnumre forventes reguleret i databeskyttelseslovens § 11.[29] Grundlaget for privates behandling af oplysninger om personnumre kan – udover samtykke – være, at det følger af *lov eller bestemmelser fastsat i henhold til lov*. Der kan eksempelvis være fastsat en indberetningspligt eller lignende i lovgivningen, som bestemmer, at indberetning skal ske med angivelse af personnummer. Det gælder for eksempel efter skattelovgivningen og efter hvidvasklovens § 11, hvor der skal indhentes identitetsoplysninger i form af navn og cpr-nummer eller lignende.

Der gælder særlige regler for videregivelse, som kan ske – uden samtykke – hvis det alene finder sted til videnskabelige eller statistiske formål, eller hvis der er tale om videregivelse af oplysninger om personnummer, når videregivelsen er et naturligt led i den normale drift af virksomheder m.v. 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. Videregivelse i øvrigt kræver, at du har samtykke hertil (eller at det følger af lov). Vær opmærksom på, at Datatilsynet anbefaler, at der anvendes kryptering, når en e-mail eller et vedhæftet dokument hertil indeholder cpr-numre eller følsomme personoplysninger, jf. afsnit 9.

Behandling af personnumre kan herudover finde sted, hvis betingelserne for at behandle følsomme oplysninger er opfyldt, jf. afsnit 5.4. Det kan være tilfældet, hvor behandlingen af cpr-nummeret for eksempel er nødvendig for, at retskrav kan fastlægges.

6. Den registreredes rettigheder

6.1. Indledning

Den person, som du behandler oplysninger om, har en række rettigheder. Som dataansvarlig har du pligt til at sikre, at den person, du har registreret oplysninger om, kan gøre brug af sine rettigheder. I denne vejledning vil de problemstillinger i relation til opfyldelsen af de registreredes rettigheder, som er særligt relevante for advokater, blive berørt. Der vil imidlertid ikke ske en detaljeret

[28] Se dog hvidvasklovens § 27 om undtagelse til underretningspligten.
[29] Artikel 87.

gennemgang af alle elementerne i den registreredes rettigheder. Datatilsynet har i marts 2018 offentliggjort en vejledning om de registreredes rettigheder, hvortil der generelt henvises.[30]

Reglerne i forordningen om de registreredes rettigheder er på en række punkter justeret og indeholder også nogle nye krav sammenlignet med de nugældende persondataregler.

Indledningsvis skal du være opmærksom på, at hvis du ikke tidligere har haft fokus på persondatareglerne, er der behov for, at du nu får overblik over, hvordan du vil efterleve reglerne om de registreredes rettigheder. Det skyldes, at reglerne om de registreredes rettigheder er meget centrale og en grundlæggende forudsætning for, at de registrerede kan få indsigt i, hvilke oplysninger der behandles om dem, og hvem der behandler oplysningerne. Det må tilmed også forventes, at en tilsidesættelse af de registreredes rettigheder vil blive sanktioneret strengere end en række af de øvrige regler i forordningen, jf. afsnit 10 om tilsyn og sanktioner. Hvis din håndtering af de registreredes rettigheder ikke lever op til forordningens krav, skal du nu sikre dig, at du får tilrettet din praksis og indarbejdet nogle retningslinjer eller rutiner, som gør, at du fuldt ud kan leve op til forordningens krav vedrørende de registreredes rettigheder. Det gælder både i forhold til nye sager, som du modtager, men også eksisterende sager. Du bør også overveje at supplere de oplysninger, som du allerede har givet i medfør af din oplysningsforpligtelse, hvis du alligevel er i kontakt med de registrerede, eller hvor en opdatering af oplysningerne af andre grunde synes at være oplagt.

Der gælder en række processuelle krav, som du skal være opmærksom på i forbindelse med håndteringen af den registreredes rettigheder.[31] Man skal blandt andet henvende sig til den registrerede i en letforståelig og lettilgængelig form og benytte et klart og enkelt sprog. Det må forventes, at kravene til sprog og form er strengere i forbrugerforhold end i erhvervsforhold. Endvidere gælder et krav om skriftlighed. Forordningen 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.[32] Husk også at sikre dig, at den registrerede er den, som vedkommende præsenterer sig som, så du ikke giver uvedkommende personer indsigt i oplysninger om en registreret eller kommer til at slette personoplysninger, som ikke skulle have været slettet.[33] Se Datatilsynets vejledning for yderligere omkring de processuelle krav.

[30] Datatilsynets vejledning om de registreredes rettigheder, marts 2018.
[31] Artikel 12 og Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 7-12.
[32] Artikel 12, stk. 3-4 og Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 8-9.
[33] Artikel 12, stk. 6.

6.2. Oplysningspligten

Efter forordningen er der pligt til at give den registrerede oplysninger om en række forhold, når der behandles personoplysninger om vedkommende.

> "Den enkelte registrerede skal som udgangspunkt have besked om, at der behandles oplysninger om den pågældende. Man skal blandt andet have besked om, hvem der er dataansvarlig, om formålet med behandlingen, om eventuelle modtagere af oplysningerne, mv."[34]

Udgangspunktet er altså, at du altid har en oplysningspligt over for den registrerede. Det er imidlertid ikke altid lige hensigtsmæssigt, at man skal give personer, som man har registreret oplysninger om, underretning herom, og det kan endvidere være problematisk i relation til advokaters tavshedspligt. Nedenfor i afsnit 6.2.1 og 6.2.2 er derfor også beskrevet en række undtagelser til oplysningspligten, som kan tænkes at have 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 i forhold til din klient, men også andre, som optræder accessorisk i tilknytning til oplysningerne om din klient, jf. dog afsnit 6.2.2 om bipersoner.[35]

Oplysningspligten, samt hvad der skal gives oplysninger om til den registrerede, veksler alt efter, om personoplysningerne kommer fra den registrerede selv (afsnit 6.2.1) eller en tredjemand (afsnit 6.2.2). Den situation, hvor du typisk vil modtage personoplysningerne fra den registrerede selv, er i forhold til din klient. En klient retter måske henvendelse til dig med henblik på 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. Denne situation behandles under afsnit 6.2.2.

6.2.1. Oplysninger kommer fra den registrerede (artikel 13)

> **Hovedregel**: Oplysningspligt, jf. artikel 13, stk. 1-3.
>
> **Undtagelse i forordningen:** Den registrerede antages allerede at være bekendt med de oplysninger, som man ellers er forpligtet til at give i medfør af oplysningspligten, jf. artikel 13, stk. 4.

[34] Datatilsynets vejledning om databeskyttelsesforordningen, oktober 2017, side 13.
[35] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 13.

Undtagelse i loven: Den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til enten private eller offentlige interesser, jf. § 22, stk. 1 og 2. Eksempelvis tavshedspligt eller retten til at forberede eget forsvar i retssager.

Undtagelse fra oplysningspligten, når oplysningerne indsamles direkte hos den registrerede, kan efter forordningens artikel 13 kun gøres, hvis personen må antages allerede at være bekendt med de oplysninger, som man ellers er forpligtet til at give i medfør af oplysningspligten.[36] 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. Imidlertid er der mulighed for at begrænse rækkevidden af oplysningspligten i national ret. Den adgang forventes at blive benyttet 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. Hensynet til offentlige interesser kan også begrunde undtagelse til oplysningspligten, jf. lovens § 22, stk. 2.

Det er yderligere et krav for at kunne benytte undtagelsen, at der er en nærliggende fare for, at de private eller offentlige interesser vil lide skade af væsentlig betydning.[37]

Private og offentlige interesser, som kan beskyttes, er såvel den dataansvarliges som tredjemands interesser. Private interesser, der vil kunne begrunde undtagelse til oplysningspligten, er blandt andet forretningshemmeligheder og professionel tavshedspligt hos eksempelvis læger og advokater. Endvidere antages retten til at forberede sit eget forsvar i retssager at kunne begrunde undtagelse til oplysningspligten.[38]

Den praktiske gennemførelse af oplysningspligten sker ved, at du skriftligt giver den registrerede de oplysninger, som du skal give efter forordningen. Det vil ifølge Datatilsynet ikke være tilstrækkeligt at have oplysningerne liggende på en hjemmeside eller lignende.[39] Du bør prioritere at iværksætte en procedure eller fremgangsmåde, som du følger i relation til oplysningspligten.[40]

De advokatetiske regler samt en række love og bekendtgørelser indeholder allerede regler, der pålægger advokater en oplysningspligt over for klienten, og det er en naturlig del af en god sagsbehandling løbende at forsyne klienten med relevante oplysninger.[41] Det er som oftest anbefalelsesværdigt – og i visse tilfælde er der pligt til – at give din klient opdrags- og prisoplysning i forbindelse med, at du påtager dig sagen, og klienten bør have oplyst, hvis forholdene ændrer sig.[42] Når du alligevel afstemmer forventninger med din klient og herunder giver

[36] Artikel 13, stk. 4.
[37] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 18.
[38] Betænkning nr. 1565/2017 om databeskyttelsesforordningen, side 395.
[39] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 14.
[40] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 11-12.
[41] AER pkt. 9.2 og 13.
[42] AER pkt. 14-15.

opdrags- og prisoplysning, kan du overveje samtidig at give klienten oplysninger vedrørende din behandling af personoplysninger. Det samme kan du overveje, når du løbende orienterer klienten om sagen.

Det kan være en god idé at anvende en skabelon eller en liste, der indeholder alle de oplysninger, som du har pligt til at give din klient. Har du allerede en skabelon for dine oplysningspligter, som du benytter, når du påtager dig en ny sag, kan du overveje at supplere skabelonen med oplysningerne vedrørende din behandling af personoplysninger. Derved sikres det, at du allerede ved klientforholdets etablering opfylder din oplysningspligt efter forordningen, og samtidig tvinger det dig til fra starten at overveje formålet med behandlingen, eventuelle modtagere af oplysningerne, opbevaringsperiode 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. Det hænger sammen med kravet om, at oplysningerne skal gives til den registrerede i en letforståelig og lettilgængelig form.[43] Datatilsynet har udarbejdet et eksempel på, hvordan oplysningspligten kan iagttages over for en registreret.[44] Eksemplet fremgår af bilag A til Datatilsynets vejledning og vedrører oplysningspligten efter artikel 14, se nedenfor i afsnit 6.2.2, men kan med nogle justeringer også bruges i relation til oplysningspligten efter artikel 13.

Vær endvidere opmærksom på, at der gælder særlige tidsfrister for, hvornår du skal opfylde din oplysningspligt.[45]

Hvis du modtager personoplysninger fra den registrerede, men den registrerede ikke er din klient, skal du på samme måde opfylde oplysningspligten. Vær dog opmærksom på din tavshedspligt, som begrænser oplysningspligten, ligesom hensynet til at kunne forberede en eventuel retssag kan begrunde hemmeligholdelse, således at du i sådanne situationer ikke har pligt til at give oplysninger til den registrerede, jf. lovens § 22, stk. 1.

Modtager du personoplysninger om modparten direkte fra denne, skal du naturligvis være opmærksom på forbuddet mod henvendelse direkte til modparten, hvor denne er repræsenteret ved advokat.[46] Efter Advokatrådets opfattelse vil oplysningspligten efter databeskyttelsesforordningen imidlertid kunne sidestilles med et påkravstilfælde, således at en henvendelse direkte til modparten med det formål at iagttage oplysningspligten efter forordningen ikke er i strid med god advokatskik, selvom modparten er repræsenteret ved advokat. Men husk, at det skal ske med respekt for tavshedspligten i forhold til din egen klient. Kopi af henvendelsen til modparten bør samtidig sendes til modpartens advokat.[47] Af afgørende betydning for at fravige forbuddet mod direkte henvendelse til modparten er efter rådets opfattelse, at oplysningspligten alene kan opfyldes ved, at

[43] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 14.
[44] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, bilag A, side 51-55.
[45] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 14-16.
[46] AER pkt. 17.3
[47] Lars Økjær Jørgensen og Martin Lavesen, De advokatetiske regler, 2. udgave, side 253-254.

du *giver* oplysningerne til *den registrerede*, ligesom også formålet med reglerne om de registreredes rettigheder tilsiger, at oplysningerne skal gives direkte til den registrerede. Umiddelbart er det ikke utvetydigt, at advokaten har fuldmagt til på vegne af klienten at modtage underretning om behandling af personoplysninger om klienten. Ovenstående vurdering er derfor baseret på den forudsætning, at oplysningspligten ikke kan opfyldes ved at give oplysningerne til andre, herunder den registreredes advokat, ligesom det heller ikke er tilstrækkeligt at have oplysningerne liggende på din hjemmeside.[48]

Når du overvejer, hvilken vidneførsel der er relevant, vil du ofte indsamle og registrere personoplysninger om relevante vidner. I første omgang vil oplysningerne typisk bestå af kontaktoplysninger på vidnet, vidnets relation til sagen og måske en kort beskrivelse af de oplysninger, som vidnet kan tænkes at kunne bidrage med til sagen. Det kan senere vise sig, at det kun er relevant at indkalde nogle af de vidner, som du har indsamlet oplysninger om. Du bør også i forhold til vidner overveje vidnets rettigheder efter forordningen, herunder skal du slette personoplysninger om vidner, som du ikke senere benytter. Måske har du allerede tidligere i forbindelse med retssagens forberedelse iagttaget vidnets rettigheder og givet vidnet underretning om, at du har registeret personoplysninger om vedkommende – men du bør senest, når du giver retten og modparten besked om, hvilke vidner du ønsker at føre, sikre dig, at oplysningspligten er iagttaget over for vidnerne. Lignende betragtninger gør sig gældende i forbindelse med valg af skønsmænd, sagkyndige vidner mv. Personoplysninger om vidner indkaldt af modparten, som du modtager fra modparten, for eksempel i forbindelse med udveksling af processkrifter i en sag, er omfattet af artikel 14, jf. afsnit 6.2.2 nedenfor.

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. Såfremt du ønsker at benytte oplysningerne til et andet formål, skal du sikre dig, at du har det fornødne behandlingsgrundlag i forhold til denne behandling, jf. afsnit 5.2-5.6.

Indholdet af oplysningspligten – det vil sige, hvilke oplysninger du skal give til den registrerede – følger af artikel 13, stk. 1-2. Visse oplysninger skal du altid give til den registrerede, mens andre oplysninger skal gives efter en konkret vurdering. Dette er nærmere beskrevet i Datatilsynets vejledning om de registreredes rettigheder, side 16-18.

[48] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 14.

6.2.2. Oplysninger kommer ikke fra den registrerede (artikel 14)

Hovedregel: Oplysningspligt, jf. artikel 14, stk. 1-4.

Undtagelser i forordningen:

- Den registrerede antages allerede at være bekendt med de oplysninger, som man ellers er forpligtet til at give i medfør af oplysningspligten, jf. artikel 14, stk. 5, litra a.

- Umuligt eller vil kræve uforholdsmæssig stor indsats eller hindre opfyldelse af formålene med behandlingen at opfylde oplysningspligten, jf. artikel 14, stk. 5, litra b.

- Behandling udtrykkeligt fastsat ved lov, jf. artikel 14, stk. 5, litra c.

- Tavshedspligt, jf. artikel 14, stk. 4, litra d.

Undtagelse i loven: Den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til enten private eller offentlige interesser, jf. § 22, stk. 1 og 2. Eksempelvis tavshedspligt eller retten til at forberede eget forsvar i retssager.

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. Der kan endvidere henvises til eksemplet med advokaten som dataansvarlig (se bilag 3), hvor advokaten som led i behandlingen af erstatningssagen modtager personoplysninger fra virksomheden om de unge mennesker i erstatningssagen.

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.

Undtagelse til oplysningspligten, hvor oplysningerne modtages fra tredjemand, kan gøres i samme omfang som beskrevet ovenfor under afsnit 6.2.1 – det vil sige, 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. lovens § 22, stk. 1 og 2, eller hvis personen må antages allerede at være bekendt med de oplysninger, som man ellers er forpligtet til at give i medfør af oplysningspligten.[49]

[49] Artikel 14, stk. 5, litra a.

Derudover kan underretning til den registrerede eksempelvis undlades, hvis det er *umuligt* at give den registrerede oplysningerne. 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.[50]

Underretning til den registrerede kan endvidere undlades, hvis det vil kræve en *uforholdsmæssig stor indsats* af den dataansvarlige at give oplysningerne. 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.[51] 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.*

Selvom oplysningspligten som udgangspunkt gælder for alle registrerede, herunder også bipersoner, som optræder accessorisk i tilknytning til oplysningerne om den person, som du primært behandler oplysninger om, 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.

> ”Hvis du når frem til, at det er umuligt eller vil kræve en uforholdsmæssig stor indsats for dig at give oplysningerne til den registrerede, skal du så vidt muligt tage hensyn til den registrerede på anden vis, for eksempel ved at give generel information om indsamlingen. Som eksempler herpå kan nævnes oplysninger på din hjemmeside, oplysningskampagner mv.”[52]

Langt de fleste advokater har i forvejen indrettet deres hjemmeside med oplysninger omfattet af oplysningspligten efter advokatreglerne. Du bør derfor overveje at supplere dine generelle oplysninger på hjemmesiden med generelle oplysninger om din persondatabehandling. Du skal dog være opmærksom på, at sådan generel oplysning kun er tilstrækkelig i forhold til iagttagelsen af dine oplysningsforpligtelser, hvis undtagelserne finder anvendelse.[53]

Hvis indsamling og videregivelse af personoplysninger udtrykkeligt er fastsat ved lov, kan underretning undlades.[54] Det gælder for eksempel efter skattelovgivningen og hvidvaskloven[55]. Centralt er det endvidere, at der kan gøres undtagelse, hvor oplysningerne skal forblive fortrolige som følge af tavshedspligt.

---

[50] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 20.
[51] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 21.
[52] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 21.
[53] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 14.
[54] Artikel 14, stk. 5, litra c.
[55] Der skal dog gives oplysninger efter hvidvasklovens § 16.

Eksempel 5 - Testamente:

En advokat modtager en henvendelse fra en ældre dame, som ønsker at oprette et testamente, der begunstiger en række privatpersoner. Mest taler for at anse advokaten som dataansvarlig for de personoplysninger, herunder oplysninger om adresser og arvelod/legater for arvingerne, som han modtager som led i sit hverv, eftersom han står forholdsvis frit med hensyn til, hvordan han vil behandle, herunder opbevare oplysningerne, i forbindelse med sin bistand med oprettelse af testamentet. Advokaten har en oplysningspligt over for den ældre dame, som ønsker at oprette et testamente, hvilket medfører, at advokaten skal give hende underretning efter artikel 13, stk. 1 og 2. Advokaten kan med henvisning til tavshedspligten undlade at give underretning til de arvinger, som han har modtaget oplysninger om, jf. artikel 14, stk. 4, litra d.

Vær endvidere opmærksom på, at der gælder særlige tidsfrister for, hvornår du skal opfylde din oplysningspligt.[56]

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 14, stk. 4.

Indholdet af oplysningspligten – det vil sige hvilke oplysninger, du skal give til den registrerede – følger af artikel 14, stk. 1-2. Visse oplysninger skal du altid give til den registrerede, mens andre oplysninger skal gives efter en konkret vurdering. Dette er nærmere beskrevet i Datatilsynets vejledning om registreredes rettigheder, side 19.

Datatilsynet har udarbejdet et eksempel på, hvordan oplysningspligten kan iagttages over for en registreret.[57]

6.3. Retten til indsigt (artikel 15)

Hovedregel: Ret til indsigt, jf. artikel 15, stk. 1-3.

Undtagelse i forordningen: Imødekommelsen vil krænke andre rettigheder og friheder, jf. artikel 15, stk. 4.

Undtagelse i loven: Den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til enten private eller offentlige interesser, jf. § 22, stk. 1 og 2. Eksempelvis tavshedspligt eller retten til at forberede eget forsvar i retssager.

Indsigtsretten betyder, at en registreret kan rette henvendelse til dig og bede om at få indsigt i indholdet af de personoplysninger, som du behandler om vedkommende. Hvis den registrerede

[56] Artikel 14, stk. 3 og Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 15-16.
[57] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, bilag A, side 51-55.

beder om det, skal der også gives en udskrift eller kopi af oplysningerne. Den nærmere fremgangsmåde i forbindelse med en anmodning om indsigt er beskrevet i Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 25-28.

Du kan afvise at imødekomme en anmodning om indsigt, 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. lovens § 22, stk. 1 og 2, jf. afsnit 6.2.1.

Vær opmærksom på, at retten til indsigt også kan 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. Dette fremgår af lovens § 26, stk. 5, som dermed er en undtagelse til indsigtsretten.

Datatilsynet har udarbejdet en skabelon for, hvordan en anmodning om indsigt fra en registreret kan besvares.[58]

6.4. Retten til berigtigelse (artikel 16)

Den registreredes ret til at få rettet urigtige eller forkerte oplysninger om sig selv går hånd i hånd med princippet om rigtighed, jf. afsnit 5.1. Fra tid til anden kan der dog være uenighed om, hvorvidt oplysningerne er urigtige, eller om oplysningerne blot er udtryk for en anden subjektiv eller faglig vurdering.[59] I retssager kommer man ofte ud for, at parterne er uenige om eksempelvis indholdet af en sagkyndig erklæring eller rigtigheden af en skønsmands forklaring. I sådanne situationer skal oplysningerne selvsagt ikke ukritisk berigtiges, selvom man modtager en anmodning fra den registrerede herom. I stedet bør man notere den registreredes synspunkter på sagen eller tilføje den registreredes oplysninger 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. Det kan for eksempel være modparten eller retten.[60]

6.5. Retten til sletning (artikel 17)

En registreret har som udgangspunkt ret til at få slettet personoplysninger om sig selv. Rettigheden går hånd i hånd med den dataansvarliges pligt til efter princippet om opbevaringsbegrænsning at

[58] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, bilag B, side 56-59.
[59] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 30.
[60] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 30-33.

slette personoplysninger, når det ikke længere er nødvendigt at gemme dem, jf. afsnit 5.1. Det betyder også, at du af egen drift skal slette personoplysninger. Opstil derfor nogle sletteprocedurer og slettefrister, som du følger, når du behandler personoplysninger.

Advokater har en pligt til opbevaring af sagsakter. Det følger af de advokatetiske regler, at efter afslutning af en sag skal sagens akter, herunder elektroniske data, opbevares i en passende periode.[61] Hvad der forstås ved passende periode afhænger af den konkrete sag og af akternes karakter. Advokatrådet anbefaler, at der bliver taget udgangspunkt i en opbevaringsperiode på fem år fra afslutning af sagen, selvom der kan være oplysninger, der bør opbevares længere. En 5-årig opbevaringsperiode har blandt andet støtte i bogføringslovens § 10 om opbevaring af regnskabsmateriale i 5 år fra udgangen af det regnskabsår, materialet vedrører. Endvidere følger det af hvidvasklovens § 30 om opbevaring af oplysninger indhentet efter hvidvaskloven, at oplysningerne skal opbevares i 5 år fra klientforholdets ophør. [62]

Interessekonfliktreglerne kan tale for, at personoplysninger gemmes i en vis periode også efter sagens afslutning, således at der kan foretages effektivt konflikttjek, hvis det måtte blive aktuelt. Efter Advokatrådets opfattelse må en advokat således have ret til at gemme oplysninger om en registreret, som advokaten tidligere har haft som klient, således at der kan foretages effektivt konflikttjek. Imidlertid bør advokaten begrænse sig til at gemme de personoplysninger, som er nødvendige for at kunne foretage et effektivt konflikttjek. Øvrige personoplysninger bør slettes, medmindre der efter andre regler er pligt til at gemme dem.

I praksis opererer mange advokater af hensyn til rådgiveransvaret med en opbevaringsperiode på op til 10 år fra afslutningen af sagen. En 10-årig opbevaringsperiode har blandt andet støtte i den absolutte forældelsesfrist på 10 år efter forældelsesloven. Hensynet til både klienten og advokaten kan tale for at opbevare oplysningerne efter sagens afslutning – også udover 5 år – så det kan dokumenteres, hvilken rådgivning der er givet, og baggrunden herfor i tilfælde af en eventuel klage eller et sagsanlæg. Der gælder endvidere ingen absolut forældelsesfrist for indgivelse af klage til Advokatnævnet.[63]

Men det er tvivlsomt, om alle oplysninger blot under henvisning til forældelsesloven kan opbevares i 10 år efter sagens afslutning. Det må altid – både advokatetisk og persondataretligt – bero på en konkret vurdering, hvor længe sagens akter skal gemmes. Personoplysninger skal slettes, når det ikke længere er nødvendigt at have dem af hensyn til opfyldelse af de formål, som de blev indsamlet til. Det følger endvidere af princippet om dataminimering, jf. afsnit 5.1 ovenfor.

---

[61] AER pkt. 10.
[62] Lars Økjær Jørgensen og Martin Lavesen, De advokatetiske regler, 2. udgave, side 91-93.
[63] Retsplejelovens § 147 b, stk. 2, og § 18 i bekendtgørelse nr. 20 af 17. januar 2008 om Advokatnævnets og kredsbestyrelsernes virksomhed ved behandling af klage over advokater mv. samt Advokatnævnets sagsnr. 2014-1152.

Eksempel på sagstyper, som efter en konkret vurdering kan begrunde længere opbevaring end 5 år:

- Retsskabende dokumenter – for eksempel testamente, lejekontrakt mv.

- Konkursboer, dødsboer eller andre sager, hvor der kan ske genoptagelse.

- Dødsbo, hvor skifte af længstlevendes bo kan ske flere årtier efter, men hvor det kan være relevant at se i skifte efter førstafdøde.

- Lejefastsættelse, hvor man skal have dokumentation for udviklingen i lejens størrelse over årrække.

Modtager du en anmodning fra en registreret om sletning af personoplysninger, må du tage stilling til, om anmodningen om sletning er berettiget, 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).

"Den registreredes ret til sletning får […] som udgangspunkt kun praktisk betydning i de tilfælde, hvor en registreret anmoder om sletning før det tidspunkt, hvor oplysningerne om den registrerede skulle have været slettet som følge af de slettefrister, som du selv har opstillet i forhold til den pågældende behandling."[64]

I en række situationer har man ikke pligt til at imødekomme en anmodning om sletning, jf. artikel 17, stk. 3. Af relevans for advokater er situationen, hvor (fortsat) behandling er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares, eller hvis den fortsatte behandling af personoplysningerne er nødvendig for at opfylde en retlig forpligtelse, jf. artikel 17, stk. 3, litra b og e.

6.6. Andre rettigheder (artikel 18-22)

Forordningen indeholder i artikel 18-22 en række andre rettigheder for den registrerede. For en nærmere gennemgang kan henvises til Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 37-50.

På dette sted skal dog nævnes, at retten til dataportabilitet, som følger af artikel 20, kan tænkes at få betydning for advokatens pligt til ved udtræden at aflevere sagens akter til en ny advokat.[65]

[64] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 35.
[65] AER pkt. 11 og Lars Økjær Jørgensen og Martin Lavesen, De advokatetiske regler, 2. udgave, side 95.

> Den registrerede har ret til at modtage personoplysninger om sig selv i et struktureret, almindeligt anvendt og maskinlæsbart format og har ret til at transmittere oplysningerne til en anden myndighed eller virksomhed. Den registrerede kan også bede om at få oplysningerne sendt direkte fra den dataansvarlige til en anden myndighed eller virksomhed.[66]

I praksis kunne retten til dataportabilitet betyde, at eksempelvis 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.[67]

7. Databeskyttelsesrådgiveren (DPO'en)

Som en nyskabelse er der i forordningen 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.[68]

I de fleste tilfælde skal private virksomheder ikke udpege en databeskyttelsesrådgiver. Udgangspunktet vil være, at advokater ikke har pligt til at udpege en databeskyttelsesrådgiver.[69] 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*.[70] Det er Advokatrådets opfattelse, at forsvarsadvokater som udgangspunkt ikke er omfattet af reglerne om databeskyttelsesrådgivere, selvom forsvarsadvokater behandler mange oplysninger om strafbare forhold. Det skyldes efter rådets opfattelse, at behandling af personoplysninger ikke er forsvarsadvokatens kerneaktivitet.[71]

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.[72]

---

[66] Datatilsynets vejledning om databeskyttelsesforordningen, oktober 2017, side 14.
[67] Datatilsynets vejledning om de registreredes rettigheder, marts 2018, side 40-43.
[68] Datatilsynets vejledning om databeskyttelsesrådgivere, december 2017, side 5.
[69] Betænkning nr. 1565/2017 om databeskyttelsesforordningen, side 564 og 568, og præambelbetragtning 91.
[70] Artikel 37.
[71] Datatilsynets vejledning om databeskyttelsesrådgivere, december 2017, side 6.
[72] Datatilsynets vejledning om databeskyttelsesrådgivere, december 2017, side 12.

8. Dokumentationskrav mv.

Med forordningen erstattes den nuværende anmeldelsesordning, hvorefter visse behandlinger af personoplysninger skal anmeldes til Datatilsynet, med et nyt krav om, at den dataansvarlige skal føre interne *fortegnelser* over sin behandling af personoplysninger.[73] Dette er en væsentlig ændring sammenlignet med de nugældende regler.

Selvom forordningen indeholder en undtagelse til kravet om at føre fortegnelser, hvis virksomheden beskæftiger under 250 personer, forventes fortegnelseskravet at komme til at omfatte langt de fleste advokater. Det skyldes, at undtagelsen blandt andet 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.[74]

I praksis betyder fortegnelseskravet, at du skal føre en skriftlig fortegnelse over de behandlingsaktiviteter i din virksomhed, som du er dataansvarlig for. Kravene til det nærmere indhold af fortegnelsen følger af forordningens artikel 30, stk. 1 og 2. Benytter du en databehandler, eller er du (undtagelsesvis) selv databehandler, er du også omfattet af kravet.[75]

Formålet med fortegnelsen er at kunne dokumentere, hvordan databeskyttelsesreglerne efterleves. Kravet har en tæt sammenhæng med princippet om ansvarlighed, jf. afsnit 5.1. Fortegnelsen skal derfor også foreligge skriftligt og elektronisk og skal stilles til rådighed for Datatilsynet, hvis tilsynet anmoder herom.[76] I øvrigt er fortegnelsen intern og ikke omfattet af for eksempel indsigtsretten. Du kan finde et eksempel på en fortegnelse i betænkning 1565/2017 om databeskyttelsesforordningen, side 461-464. Datatilsynet har endvidere offentliggjort en vejledning om fortegnelse, hvor der er et eksempel på en fortegnelse.[77]

9. Behandlingssikkerhed

Det påhviler den dataansvarlige at foretage en *risikovurdering* med henblik på at fastsætte et passende sikkerhedsniveau vedrørende behandling af personoplysninger.[78] Meget taler for at anbefale skriftlighed, så det kan dokumenteres over for Datatilsynet, eksempelvis ved sikkerhedsbrud, at håndteringen af personoplysninger ikke var tilfældig, men derimod udtryk for overvejelser omkring behandlingssikkerheden. Hvis behandlingen medfører høj risiko for den

[73] Forordningen artikel 30.
[74] Datatilsynets vejledning om fortegnelse, januar 2018, side 13-15
[75] Forordningen artikel 30, stk. 2.
[76] Forordningen artikel 30, stk. 3 og 4.
[77] Datatilsynets vejledning om fortegnelse, januar 2018, side 17.
[78] Forordningen artikel 32.

registreredes rettigheder, herunder hvis du påbegynder anvendelse af en ny type teknologi i forbindelse med behandlingen af personoplysninger, er der pligt til også at gennemføre en *konsekvensanalyse* (DPIA).[79] Det vil efter Advokatrådets opfattelse som udgangspunkt ikke være nødvendigt for advokater at gennemføre en konsekvensanalyse.

Risikovurderingen indebærer, at du bør overveje, om din behandling af personoplysninger sker på et passende sikkerhedsniveau, som tager hensyn til de risici, der er forbundet med behandlingen, og som tager højde for, hvilken type personoplysninger der behandles. Sikkerhedsniveauet skal altså ofte være højere, når der behandles eksempelvis følsomme oplysninger, personnumre eller oplysninger om eksempelvis strafbare forhold.

Persondataretligt skal både den fysiske og den elektroniske behandling af personoplysninger leve op til et passende sikkerhedsniveau. Advokatetisk er der tillige krav om, at opbevaring af sagsakter skal ske på en sikker og hensigtsmæssig måde.[80] Det gælder opbevaringen af såvel fysiske som elektroniske sager. En sløset omgang med personoplysninger vil også kunne udgøre en tilsidesættelse af tavshedspligten.[81]

Risikoen for, at uvedkommende får adgang til personoplysninger, skal begrænses, og denne risikobegrænsning kan ske dels ved organisatoriske foranstaltninger og dels ved tekniske foranstaltninger. Du skal tænke over, hvordan du bedst muligt kan sikre de personoplysninger, som du er blevet betroet. Det hænger endvidere sammen med pligten til at handle forsvarligt, jf. artikel 5, stk. 2.

I praksis betyder kravet om behandlingssikkerhed, at du bør indføre nogle rutiner for ansvarlig behandling af personoplysninger. Du skal tage stilling til, om filer skal krypteres ved for eksempel at forsyne dem med adgangskoder, eller om meddelelser måske bør sendes til modtagerens e-boks i stedet for at benytte almindelig e-mail. Det kan også være en god idé at gøre det til en rutine at logge af din computer, når du forlader den, eller sikre at systemet automatisk logger af efter en inaktiv periode. Det er endvidere vigtigt, at man sørger for løbende at udskifte adgangskoder til diverse systemer. Ved at begrænse, hvem der har adgang til at se elektroniske sager, kan du desuden mindske risikoen for, at der sker databrud, ligesom du sikrer dig, at personoplysninger kun bliver delt med de personer i din virksomhed, som rent faktisk skal beskæftige sig med sagen.

I bund og grund afviger disse rutiner ikke væsentligt fra, hvordan du allerede i dag skal agere. Du vil for eksempel aldrig forlade kontoret som den sidste medarbejder uden at låse døren, ligesom du heller ikke lader fysiske sagsmapper ligge og flyde i receptionen, så uvedkommende kan få indblik i

[79] Forordningen artikel 35 og Datatilsynets vejledning om konsekvensanalyse, marts 2018.
[80] AER pkt. 10 og Lars Økjær Jørgensen og Martin Lavesen, De advokatetiske regler, 2. udgave, side 90.
[81] AER pkt. 5 og Lars Økjær Jørgensen og Martin Lavesen, De advokatetiske regler, 2. udgave, side 47-49.

indholdet. Tankegangen må være, at alle personoplysninger – uanset om de behandles fysisk eller elektronisk – skal håndteres forsvarligt.

En stor del af kommunikationen i dag finder sted ved brug af e-mails mv. Hvis klienten eksempelvis korresponderer med advokaten via sin private e-mailadresse, vil korrespondancen som udgangspunkt ikke blive betragtet som sikker. Ifølge Datatilsynet svarer korrespondance via almindelig e-mail til, at man sender et åbent postkort. Brugen af "almindelig e-mail" skal i denne sammenhæng forstås som brugen af e-mail uden kryptering eller andre sikkerhedstiltag. Ved brug af almindelig e-mail er der derfor generelt en risiko for, at oplysningerne undervejs læses eller ændres af uvedkommende, eller at parterne i kommunikationen ikke er dem, de udgiver sig for.[82] Følsomme personoplysninger om klienten, oplysninger om strafbare forhold eller personnumre – det kan eksempelvis være i straffesager, personskadesager mv. – bør slet ikke sendes over det åbne internet. Hvis advokatens e-mailkorrespondance med klienten kommer til uvedkommendes kendskab, er det sandsynligvis advokaten, der bærer ansvaret. Tænk i den forbindelse også på din tavshedspligt. Hvis en e-mail for eksempel bliver sendt til en forkert modtager, vil det potentielt kunne være både et brud på tavshedspligten og et databrud efter forordningen.

Datatilsynet har offentliggjort en række krav og anbefalinger, som tilsynet lægger vægt på i forhold til overførsel af personoplysninger via internettet i den private sektor.[83] Datatilsynet anbefaler, at private virksomheder anvender kryptering, når e-mail eller et vedhæftet dokument hertil indeholder cpr-numre eller følsomme personoplysninger. Det er endnu uvist, om Datatilsynets anbefalinger vil blive ændret som følge af de nye databeskyttelsesregler.

Advokater skal underrette modparten med samtidig kopi, når der sendes processtof til retten.[84] Af praktiske grunde sendes processkrifter og andet ofte pr. e-mail til retten og modpartens advokat. Med den digitale behandling af civile sager (minretssag.dk) er det alene nødvendigt at sende *stævningen* (og bilag) særskilt til modparten. *Efterfølgende processkrifter mv*. er der ikke behov for at sende særskilt til modparten, idet modparten vil få besked om dette materiale og adgang hertil på minretssag.dk samtidig med retten. Selvom det ikke er et krav, vælger mange dog fortsat (ofte af kollegiale grunde) at orientere modparten pr. e-mail samtidig med, at man lægger materiale ud på portalen. Men hvis man ikke anvender kryptering, er der en vis risiko for, at personoplysninger omfattet af orienteringen til modparten kan komme i de forkerte hænder.

Advokatnævnet fandt i kendelse af 25. april 2017, at indklagede ikke havde tilsidesat god advokatskik ved at sende fortrolige og følsomme personoplysninger til en kommune fra sin almindelige e-mail. Advokatnævnet lagde herved vægt på, at det ikke er et lovkrav – men alene en

---

[82] https://www.datatilsynet.dk/borger/sikkerhed/fortrolige-personoplysninger-i-e-mails/
[83] https://www.datatilsynet.dk/erhverv/internettet/krav-og-anbefalinger-ifm-overfoersel-af-personoplysninger-via-internettet/
[84] AER pkt. 18.3.

anbefaling – at private virksomheder sender sådanne oplysninger krypteret.[85] I den konkrete sag var det således ikke i strid med god advokatskik at sende følsomme personoplysninger pr. e-mail. Med den nye forordning sættes der imidlertid fokus på databeskyttelse som en grundlæggende rettighed, og med den hastige teknologiske udvikling, som til stadighed skaber nye udfordringer for så vidt angår beskyttelse af personoplysninger, er der behov for at have større fokus på omgangen med og beskyttelse af personoplysninger. Tiden må vise, om Advokatnævnet fremadrettet vil forholde sig anderledes i forhold til brugen af almindelig e-mail ved kommunikation af følsomme personoplysninger. Advokatrådet finder dog, at advokater i lyset af den nye databeskyttelsesforordning og anbefalingen om kryptering fra Datatilsynet bør begrænse brugen af ukrypteret e-mailkorrespondance. Særligt, hvis materialet indeholder cpr-numre og følsomme personoplysninger.

Der findes på nuværende tidspunkt ikke regler eller retningslinjer for, hvad der udgør et passende sikkerhedsniveau, og dette må derfor bero på en konkret vurdering. [86] Det sikkerhedsniveau, som, du mener, er passende for din virksomhed, er ikke nødvendigvis passende for en anden. Dermed er det også sagt, at behandlingssikkerheden ikke kan sættes på formel. Der findes mange produkter og løsninger på markedet, som det kan være en dyr fornøjelse at benytte sig af. Du bør nøje overveje, hvad der er den rette løsning for din virksomhed, og det er ikke sikkert, at du behøver hjælp for at leve op til kravene til behandlingssikkerhed. Dertil kommer, at behandlingssikkerhed langt hen ad vejen også er et driftsanliggende, hvilket det ikke er tanken, at denne vejledning skal berøre. Datatilsynet vil senere offentliggøre en vejledning om behandlingssikkerhed, hvor der forventeligt vil være yderligere hjælp at hente. I forordningen er endvidere oplistet en række eksempler på sikkerhedsforanstaltninger, der kan komme på tale at benytte.[87]

Sker der brud på persondatasikkerheden, skal du som dataansvarlig som hovedregel uden unødig forsinkelse og senest 72 timer efter at være blevet bekendt med bruddet, anmelde bruddet til Datatilsynet. I visse situationer skal du også orientere de berørte registrerede.[88] Hvis reglerne om anmeldelse af brud på persondatasikkerheden og underretning til de berørte registrerede ikke overholdes, har Datatilsynet mulighed for at sanktionere dette. Det er derfor Advokatrådets anbefaling, at du har procedurer for hurtig og korrekt håndtering af eventuelle databrud. For flere oplysninger om anmeldelse ved brud på persondatasikkerheden kan der henvises til Datatilsynets vejledning om samme.[89]

---

[85] Advokatnævnets sagsnr. 2016-2165.
[86] Betænkning nr. 1565/2017 om databeskyttelsesforordningen, side 486-489, indeholder et eksempel på en 4-trinsraket, der kan benyttes af den dataansvarlige.
[87] Eksemplerne er selvsagt ikke udtømmende.
[88] Forordningen artikel 33 og 34
[89] Datatilsynets vejledning om håndtering af brud på persondatasikkerheden, februar 2018, og Artikel 29-gruppens Guidelines on Personal data Breach Notification under Regulation 2016/679 (WP 250 rev 01)

10. Tilsyn og sanktioner

Datatilsynet fører tilsyn med, at advokater overholder forordningen 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. Der lægges i lovforslaget op til, at dette videreføres, jf. lovens § 29.

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

Med forordningen er der umiddelbart udsigt til væsentlige bøder for overtrædelser af forordningen. Hidtil har overtrædelser af persondataloven givet anledning til, at Datatilsynet har udtalt kritik, og i visse – grove – tilfælde har domstolene tilkendt registrerede en godtgørelse for tort. For manglende efterlevelse af pligterne efter forordningen kan der straffes med bøder på op til 10 millioner euro eller 2 procent af virksomhedens samlede globale årlige omsætning. For manglende efterlevelse af de registreredes rettigheder (afsnit 6), de grundlæggende principper for behandling (afsnit 5.1), reglerne for overførsel af persondata til lande uden for EU eller afgørelser fra Datatilsynet kan der straffes med bøder på op til 20 millioner euro eller 4 procent af dens samlede globale årlige omsætning. Tiden må vise, hvordan reglerne vil blive administreret i praksis, og hvor bødeniveauet kommer til at ligge. Tiden må også vise, om visse overtrædelsestilfælde i første omgang vil udløse påbud fra Datatilsynet.

11. Tjekliste

- Find ud af, om du er dataansvarlig (eller databehandler).
- Undersøg, hvilken type personoplysninger du behandler.
- Find ud af, hvad formålet/formålene med behandlingen er, og om principperne for behandling er overholdt.
- Find ud af, hvad der er dit/dine behandlingsgrundlag.
- Undersøg, hvorfra du modtager personoplysninger.
- Undersøg, om du videregiver personoplysninger til andre og til hvem.
- Sørg for, at du opfylder de registreredes rettigheder, herunder ved at have procedurer, der sikrer din iagttagelse af din oplysningsforpligtelse, samt retningslinjer for imødekommelse af henvendelser fra de registrerede.
- Fastsæt slettefrister og sletteprocedurer.
- Sørg for, at du opfylder dokumentationskravet, herunder fortegnelseskravet.
- Foretag en risikovurdering og sørg for, at din behandling lever op til et passende organisatorisk og teknisk sikkerhedsniveau.
- Fastsæt en procedure for anmeldelse af sikkerhedsbrud.
- Skab opmærksomhed i din virksomhed om databeskyttelsesreglerne, herunder ved orientering og eventuel uddannelse.

Bilag 1: Oversigt over personoplysninger

Følsomhed

Almindelige personoplysninger (artikel 6):	**CPR-numre (artikel 87 og § 11)**	**Straffedomme og lovovertrædelser (artikel 10 og § 8)**	**Følsomme personoplysninger (artikel 9):**
Navn Adresse Telefonnummer Fødselsdato Økonomi Løn Skatteoplysninger Gæld Familieforhold Sociale forhold Bolig Bil Uddannelse Eksamen CV Ansættelsesdato Stilling Sygedage Tjenestelige forhold Arbejdsområde Arbejdstelefon IP-adresse			Race eller etnisk oprindelse Politisk, religiøs eller filosofisk overbevisning Fagforeningsmæssige tilhørsforhold Genetiske data Biometriske data mhp. entydig identifikation Helbredsoplysninger Seksuelle forhold eller orientering

Bilag 2: Eksempel på advokaten som databehandler

”Eksempel 15 – Advokatfirmaet, som administrerer en whistleblowerordning

Virksomheden X er ved lov pålagt at oprette en whistleblowerordning, hvor medarbejderne kan foretage anonyme indberetninger af ulovlige forhold mv.

Advokatfirma Y tilbyder at administrere virksomhedens whistleblowerordning ved at stille et system til rådighed, hvori medarbejderne kan foretage indberetninger. Advokatfirmet vil herefter modtage, opbevare og eventuelt videresende indberetningerne efter instruks fra virksomheden. Aftalen mellem parterne vedrører derfor behandling af personoplysninger.

Virksomheden X er som følge af den lovbestemte whistleblowerordning forpligtet til at foretage behandling af personoplysninger. Virksomheden er derfor afhængig af, at advokatfirmaet Y behandler oplysningerne på en bestemt måde (efter instruks), så virksomheden lever op til sine lovmæssige forpligtelser.

Advokatfirmaet Y vil i denne situation også umiddelbart kunne følge en instruks fra virksomheden, fordi behandlingen er mere ekspeditionspræget, lovbunden og ikke udtryk for klassisk advokatvirksomhed. I dette tilfælde vil overvægten af argumenter pege i retning af at anse advokatfirmaet Y som databehandler for de oplysninger, som firmaet behandler i forbindelse med sin administration af whistleblowerordningen for virksomheden X.”[90]

[90] Vejledning om dataansvarlige og databehandlere, november 2017, side 22

Bilag 3: Eksempel på advokaten som dataansvarlig

”Eksempel 16 – Advokatfirmaet, som bistår en eventvirksomhed med at få erstattet et økonomisk tab

Eventvirksomheden Z beder Advokatfirma X om hjælp til at få erstattet et tab, som virksomheden har lidt i forbindelse med et nyligt overstået event, hvor en gruppe berusede unge mennesker skubbede virksomhedens varevogn indeholdende blandt andet højtalere og rappellingudstyr i havnen.

Aftalen mellem parterne sigter på, at Advokatfirma X skal bistå eventvirksomheden med at få erstattet det økonomiske tab.

Advokatfirma X begynder herefter at behandle personoplysninger om blandt andre de unge mennesker til brug for erstatningssagen. Advokatfirmaet træffer selvstændige beslutninger om, hvilke oplysninger der skal indsamles, slettes, videregives mv. Behandlingen af oplysninger sker ikke efter instruks eller godkendelse fra eventvirksomheden.

I forhold til retsplejelovens regler og de advokatetiske regler er det desuden tvivlsomt, i hvilket omfang Advokatfirma X ville have mulighed for at følge en detaljeret instruks fra den dataansvarlige om, hvordan der skal behandles personoplysninger i en konkret sag, eller at oplysningerne skal slettes.

Der kan i situationer vedrørende advokatbistand og anden rådgivning argumenteres for forskellige delinger af ansvaret. I denne situation vil mest dog tale for at anse Advokatfirma X for at være en selvstændig dataansvarlig, fordi Eventvirksomheden X ikke henvendte sig til advokatfirmaet for at få behandlet, for eksempel opbevaret, personoplysninger. Aftalen mellem parterne må i denne situation anses for at vedrøre en anden ydelse (advokatbistand), hvor advokatfirmaet helt naturligt træffer egne beslutninger om udførelsen af en opgave, og advokatfirmaet vil som udgangspunkt ikke være undergivet en egentlig instruktionsbeføjelse fra eventvirksomheden om at behandle oplysningerne på en bestemt måde.”[91]

[91] Vejledning om dataansvarlige og databehandlere, november 2017, side 23