ver. 27.06.2018

PERSONDATAPOLITIK

NT ADVOKATER

NT Advokatpartnerselskab · Østbanegade 55 · 2100 København Ø · Danmark
Tlf: 35 44 70 00 · Fax: 35 44 70 01 · www.ntadvokater.dk · nt@ntadvokater.dk · CVR nr.: 35 40 74 48

1 ANSVAR

1.1 Beskyttelse af dine Persondata har vores højeste prioritet, uanset om disse data handler om dig, dine transaktioner, dine produkter/gods eller dine serviceydelser.

1.2 Vi behandler Persondata og har derfor vedtaget denne Persondata Politik, der beskriver, hvordan vi behandler dine Persondata.

2 SELSKAB

2.1 Selskabet er:

NT Advokatpartnerselskab
CVR-nummer: 35407448
Østbanegade 55, 4.
DK - 2100 København Ø
Danmark
(Herefter benævnt "NT Advokater")

T: + 45 35 44 70 00
E: nt@ntadvokater.dk
W: www.ntadvokater.dk

3 PERSONDATA

3.1 Det er vigtigt for os, at dine Persondata opbevares sikkert og fortroligt. Vi har procedurer for indsamling, opbevaring, sletning, opdatering og videregivelse af Persondata for at hindre uautoriseret adgang til dine Persondata og for at opfylde gældende lovgivning.

3.2 Vi sikrer fair og transparent databehandling. Når vi beder dig om at stille dine Persondata til rådighed for os, oplyser vi dig om, hvilke Persondata vi behandler om dig og til hvilket formål. Du modtager oplysning herom på tidspunktet for indsamling af dine Persondata. Vi indsamler ikke oplysninger som ikke er relevante for sagen. Indsamles unødig oplysninger, slettes oplysninger omgående.

3.3 Nedenstående retningslinjer beskriver hvilke typer af Persondata, vi indsamler, hvordan vi behandler disse Persondata, og hvem du kan kontakte, såfremt du har spørgsmål eller kommentarer til denne Persondata Politik.

4 TYPER AF PERSONDATA

KLIENTER

- Almindelige Persondata (f.eks. navn og/eller brugernavn, adresse, e-mail, fødselsdato, køn, profilbillede, lokalisation, m.v.)
- CPR-nummer
- Lokalisationsdata, navn, reg.nr., medarbejder mobil-nr.
- Bankinformationer
- Trafikdata om brug af internettet
- Lokalisationsdata fra internettet, mobil, GPS eller kamera
- Transaktionsdata
- Unikke numre på netværksenheder
- Kontaktinformation, rapportadgang, kontaktinformationer
- Newsletter
- CRM System, navne, adresse, tlf. nr., e-mail, interesseområder
- E-mails
- Regnskab
- Bank- og formueopgørelser
- Oplysninger i forbindelse med byggesager og lignende indhentes fra CVR Registeret, tinglysning.dk, CPR. Registeret, OIS.dk og weblager.dk

MEDARBEJDERE

- Stamdata, almindelige Persondata (f.eks. navn og/eller brugernavn, adresse, e-mail, fødselsdato, køn, profilbillede, lokalisation, m.v.)

- CPR-nummer
- Persondata om nær familie
- Persondata om uddannelse
- Udtalelser
- Tidligere beskæftigelse
- Nuværende stilling
- Arbejdsopgaver
- Arbejdstider og andre tjenstlige forhold
- Persondata om løn og skat, almindelige personlige data (fx navn og / eller bruger- navn, adresse, e-mail, fødselsdato, køn, placering osv.), CPR-nummer, Persondata om kontonummer, hvortil løn skal betales (NEMKONTO)
- Persondata om sygefravær og sygdom og andet fravær fra arbejde
- Pensionsoplysninger, navn, adresse, tlf. nr., e- mail, cpr.nr., navn på ægtefælle, navn på børn
- Trafikdata om brug af internettet
- Transaktionsdata
- Unikke numre på netværksenheder
- E-mails
- Sociale Persondata
- Sygdomsrelaterede Persondata, lægeerklæring, Navne, adresse, tlf. nr., e- mail, fraværsperiode, opbevaring til andre formål end rapportering vedrørende dagpenge, Danmarks Statistik, m.v.
- Uddannelsesdata

- Tidsregistrering
- Fratrædelsessamtaler, adfærdsdata, information om andre ansatte
- Straffeattest
- Lønstatistik (Danmark Statistik), almindelige personlige data (fx navn og / eller brugernavn, adresse, e- mail, fødselsdato, køn, placering osv.), CPR-nummer, Persondata om løn og skat, Persondata om fravær/sygdom
- MUS/PU Samtaler, almindelige personlige data (fx navn og / eller bruger- navn), uddannelsesoplysninger, performanceoplysninger, herunder adgang til medarbejdernes omsætning og tidsregistrering, adfærdsdata, information om andre ansatte
- Ansøgninger, almindelige personlige data (fx navn og / eller bruger- navn, adresse, e-mail, fødselsdato, køn, profilbillede, placering osv.), CPR-nummer, Persondata om løn og skat, uddannelsesoplysninger, erhvervserfaring, anbefalinger, referencer
- Personlighedstest, navne, adresse, tlf. nr., e- mail, personlige karakteristika
- Rekruttering, Almindelige personlige data (fx navn og / eller bruger- navn, adresse, e-mail, fødselsdato, køn, profilbillede, placering osv.), personlige karakteristika, CPR-nummer, Persondata om løn, uddannelsesoplysninger.
- Billeder af ansatte – markedsføring
- Arbejdsgiverbetalt mobil telefon, navn, adresse, tlf. nr., e- mail, opkaldshistorik, anonymiserede tlf. nr. på modtager af opkald, tro- & love erklæring
- Kvalitetsstyring
- Skadeshåndtering
- Whistleblower, navn, adresse, tlf. nr., e- mail, data om manglende overholdelse af NT Advokater' regelsæt, politikker, m.v.
- E-boks, mails fra offentlige myndigheder, CPR-nummer, navn, adresse, helbredsoplysninger, trafikbøder, rets udskrifter, arbejdsskader
- Medarbejdersignatur (det er kun administrator der har adgang)

5 FORMÅL

5.1 Vi indsamler og opbevarer dine Persondata til bestemte formål eller andre lovlige forretningsmæssige formål.

5.2 Dine Persondata indsamles og anvendes til:

KLIENTER

- Alm. advokatvirksomhed
- Hvidvask
- Forbedring af NT Advokater' rådgivning og andre tjenesteydelser.
- Tilpasning af NT Advokater' kommunikation og markedsføring til dig
- Tilpasning af samarbejdspartneres kommunikation og markedsføring til dig
- Direkte markedsføringsaktiviteter.
- Statistik og tilpasning af NT Advokater' ydelser.
- Optimering af hjemmesiden.
- Gennemførelse af en aftale eller foranstaltninger efter din anmodning herom.
- Administration af din relation til NT Advokater
- Opfyldelse af lovkrav
- Retskrav

MEDARBEJDERE

- Gennemførelse af en ansættelsesaftale
- Administration af din relation til os
- Opfyldelse af lovkrav

- Retskrav

6 DEN REGISTREREDES RETTIGHEDER

6.1 Håndtering af begæringer fra den registrerede

6.1.1 Vores håndtering af de registreredes rettigheder er centraliseret. Den ansvarlige vil dog sjældent være tilstrækkeligt inde i den enkelte sag til at kunne bedømme, om den registreredes anmodning kan/bør imødekommes helt eller delvist. Besvarelsen vil derfor ske efter dialog med den relevante sagsbehandler, som kan redegøre for de hensyn, der taler for henholdsvis imod, at en anmodning/indsigelse imødekommes.

6.2 Indsigtsretten

6.2.1 Den registrerede har i henhold til databeskyttelsesforordningens artikel 15 ret til at få bekræftet, om der behandles Persondata om den pågældende, og vil i givet fald få adgang til Persondata (der skal udleveres en kopi af Persondata).

6.2.2 Derudover har den registrerede ret til at modtage følgende information:

- formålene med behandlingen
- de berørte kategorier af Persondata
- de modtagere eller kategorier af modtagere, som Persondata er eller vil blive videregivet til, navnlig modtagere i tredjelande eller internationale organisationer
- om muligt det påtænkte tidsrum, hvor Persondata vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til fastlæggelse af dette tidsrum
- retten til at anmode den dataansvarlige om berigtigelse eller sletning af Persondata eller begrænsning af behandling af Persondata vedrørende den registrerede eller til at gøre indsigelse mod en sådan behandling
- retten til at indgive en klage til en tilsynsmyndighed
- enhver tilgængelig information om, hvorfra Persondata stammer, hvis de ikke indsamles hos den registrerede

6.2.3 Den registrerede har endvidere ret til at få oplysninger om fornødne garantier, hvis vi har overdraget Persondata til tredjelande.

6.2.4 For at kunne opfylde en indsigtsbegæring på behørig vis skal vi herefter gennemsøge alle systemer – herunder alle databaser samt alt hardware og alle flytbare medier – og også gennemsøge alt fysisk materiale, der indgår i et register, og udlevere de Persondata, der er registreret om den pågældende

6.2.5 Efter databeskyttelsesloven gælder retten til indsigt ikke, hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv.

6.2.6 Det er vores vurdering, at dette bl.a. vil omfatte oplysninger omfattet af vores tavshedspligt. Indsigtsretten vil derfor ikke have en selvstændig betydning, så længe der begæres om indsigt i Persondata, som er underlagt tavshedspligt. Klientens begæring om indsigt i egne oplysninger vil derimod som udgangspunkt ikke være begrænset (med mindre vi f.eks. har foretaget indberetning til SØIK om overtrædelse af hvidvaskloven, m.v.).

6.3 Dataportabilitet

6.3.1 Den registrerede har efter databeskyttelsesforordningens artikel 20 desuden ret til i et struktureret, almindeligt anvendt og maskinlæsbart format at modtage Persondata om sig selv, som den pågældende selv har givet til NT Advokater.

6.3.2 Den registrerede har desuden ret til selv at transmittere disse oplysninger til en anden dataansvarlig uden hindring fra NT Advokater, når behandlingen er baseret på samtykke og behandlingen foretages automatisk. Hvis den registrerede udøver denne ret til dataportabilitet, har den registrerede også ret til at få transmitteret Persondata direkte fra en dataansvarlig til en anden, hvis det er teknisk muligt.

6.3.3 Adgangen til dataportabilitet omfatter kun oplysninger, den registrerede selv har givet, og vil kun omfatte behandlinger, der foretages automatisk. Adgangen til dataportabilitet vil desuden være særdeles begrænset, såfremt vi baserer vores behandlingshjemmel på andet grundlag end samtykke.

6.3.4 Det er vores vurdering, at retten til dataportabilitet kun kan gøres gældende i meget begrænset omfang i forhold til vores klientoplysninger.

6.4 Ret til berigtigelse

6.4.1 I henhold til databeskyttelsesforordningens artikel 16 har den registrerede ret til at få urigtige Persondata om sig selv berigtiget af den dataansvarlige uden unødig forsinkelse. Under hensyntagen til formålene med behandlingen har den registrerede desuden ret til få fuldstændiggjort ufuldstændige Persondata, bl.a. ved at fremlægge en supplerende erklæring.

6.4.2 Denne ret supplerer vores egen grundlæggende forpligtelse til kontinuerligt at sikre os, at der alene behandles korrekte og ajourførte oplysninger, jf. artikel 5, stk. 1, litra d.

6.4.3 Retten til berigtigelse angår dog alene objektive Persondata, og ikke subjektive vurderinger. At vi måtte have vurderet, at klienten ikke har et juridisk grundlagt for at føre en sag, er eksempelvis ikke en personoplysning, der kan kræves berigtiget, blot fordi klienten ikke er enig. Vores vurdering af et bevis skal heller ikke berigtiges, fordi modparten ikke måtte være enig i vores udlægning.

6.5 Retten til at blive glemt

6.5.1 Den registrerede har efter databeskyttelsesforordningens artikel 17 ret til at få Persondata om sig selv slettet af os uden unødig forsinkelse. Modtager vi en berettiget anmodning herom, har vi i så fald pligt til at slette Persondata uden unødig forsinkelse.

6.5.2 Dog er retten begrænset sådan, at der ikke kan kræves sletning, hvis behandlingen er nødvendig for at overholde en retlig forpligtelse, eller for at retskrav kan fastlægges, gøres gældende eller forsvares, jf. artikel 17, stk. 3, litra b og e.

6.5.3 Det er vores vurdering, at "retten til at blive glemt" kun meget sjældent vil komme i spil i forhold til vores sagsbehandling. Den kan eksempelvis tænkes anvendt, hvis Persondata oprindeligt slet ikke har været nødvendige for sagens behandling, og derfor slet ikke burde have indgået i sagen, eller hvis Persondata utvivlsomt ikke længere er nødvendige for sagens behandling. I så fald vil pligten til at slette Persondata også følge af den grundlæggende forpligtelse til kun at behandle nødvendige oplysninger, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra c. "Retten til at blive glemt" finder dog ikke anvendelse, såfremt (og så længe) vi opbevarer sådanne Persondata for at kunne modgå et eventuelt retskrav fra klienter.

6.5.4 Hvis vi er forpligtet til at slette Persondata efter artikel 17, som har været overladt til andre dataansvarlige eller databehandlere, skal vi underrette sådanne dataansvarlige eller databehandlere, som behandler Persondata, om, at den registrerede har anmodet om at få slettet alle link til eller kopier eller gengivelser af de pågældende Persondata.

6.6 Ret til indsigelse – også mod automatiserede afgørelser

6.6.1 Det følger af databeskyttelsesforordningens artikel 21, at den registrerede til enhver tid har ret til at gøre indsigelse mod behandling af sine Persondata, hvis behandlingen – herunder profilering – er baseret på artikel 6, stk. 1, litra e eller f. Disse bestemmelser omhandler adgangen til at behandle almindelige Persondata, hvis behandlingen er nødvendig for at udføre en opgave i samfundets interesser, eller hvis behandlingen er nødvendig for at forfølge en berettiget interesse og hensynet til den registrerede ikke overstiger denne interesse.

6.6.2 Hvis der gøres indsigelse, må vi ikke længere behandle de pågældende Persondata, medmindre vi kan påvise vægtige legitime grunde til behandlingen, der går forud for den registreredes interesser, eller hvis behandlingen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares.

6.6.3 Det er vores vurdering, at denne bestemmelse kun begrænset vil komme i spil i forhold til vores sagsbehandling, fordi sagsbehandlingen i vidt omfang kan knyttes op på hjemlen vedrørende fastlæggelsen af et retskrav, ligesom vi – hvis behandlingen i øvrigt opfylder de grundlæggende behandlingsregler – oftest vil kunne påvise vægtige legitime grunde til, at oplysningerne indgår i sagsbehandlingen.

6.6.4 Bestemmelsen i artikel 21 forudsætter, at den registrerede gøres udtrykkeligt opmærksom på sin ret til at gøre indsigelse, og at dette skal ske senest på tidspunktet for den første kommunikation. Endvidere skal oplysningen herom meddeles klart og holdes adskilt fra de andre oplysninger.

6.6.5 Supplerende til artikel 21, har den registrerede i henhold til artikel 22 ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende.

6.6.6 Også denne bestemmelse indeholder en række undtagelser, jf. artikel 22, stk. 2. Blandt andet gælder retten ikke, hvis afgørelsen er nødvendig for indgåelse eller opfyldelse af en kontrakt mellem den registrerede og en dataansvarlig, hvis behandlingen har hjemmel i lov, eller hvis behandlingen er baseret på den registreredes udtrykkelige samtykke.

6.6.7 Artikel 22 forudsætter dog generelt, at automatiserede afgørelser ikke baseres på særlige kategorier af Persondata, jf. artikel 9, stk. 1, medmindre der er givet udtrykkeligt samtykke hertil, og der er indført passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser.

6.7 <u>Ret til dataminimering.</u>

6.7.1 I henhold til databeskyttelsesforordningens artikel 18 har den registrerede ret til at få begrænset behandlingen af Persondata, hvis:

- rigtigheden af Persondata bestrides af den registrerede, men kun i perioden indtil den dataansvarlige har haft mulighed for at fastslå, om Persondata er korrekte

- behandlingen er ulovlig, og den registrerede modsætter sig sletning af Persondata og i stedet anmoder om, at anvendelsen heraf begrænses

- den dataansvarlige ikke længere har brug for Persondata til behandlingen, men de er nødvendige for, at et retskrav kan fastlægges, gøres gældende eller forsvares

- den registrerede har gjort indsigelse mod behandlingen i medfør af artikel 21, stk. 1, men kun i perioden mens det kontrolleres, om den dataansvarliges legitime interesser går forud for den registreredes legitime interesser.

6.7.2 Retten udgør dermed et alternativt (og mindre) indgreb i sagsbehandlingen sammenlignet med den registreredes ret til at gøre indsigelse efter artikel 21 og 22, og den registreredes "ret til at blive glemt" efter artikel 17.

6.7.3 Det følger af bestemmelsens stk. 2, at hvis en behandling er blevet begrænset, må sådanne Persondata, bortset fra opbevaring, stadig behandles blandt andet, hvis den registrerede giver samtykke hertil, eller hvis behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

6.7.4 Bestemmelsen vil efter vores vurdering kun få begrænset betydning for vores adgang til at behandle Persondata i vores sagsbehandling.

6.7.5 Bestemmelsen supplerer desuden i vidt omfang vores egen selvstændige forpligtelse til kontinuerligt at sikre overholdelse af de grundlæggende rettigheder for den registrerede.

7 BEHANDLINGSREGLER - GENERELT

7.1 Behandlingsprincipper

7.1.1 Vi vil behandle Persondata lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.

7.1.2 Vores behandling af Persondata er undergivet en formålsbegrænsning, hvilket vil sige, at Persondata skal indsamles til udtrykkeligt angivne og legitime formål. Persondata må ikke viderebehandles på en måde, der er uforenelig med disse formål.

7.1.3 Vi behandler Persondata ud fra et princip om dataminimering, hvilket vil sige, at Persondata skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles,

7.1.4 Persondata skal behandles ud fra et princip om rigtighed, hvilket vil sige, at de skal være korrekte og om nødvendigt ajourførte,

7.1.5 Vi behandler Persondata ud fra et princip om opbevaringsbegrænsning, hvilket vil sige, at Persondata skal 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 Persondata behandles, og

7.1.6 Persondata skal behandles ud fra et princip om integritet og fortrolighed, hvilket vil sige, at de skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for Persondata, herunder skal de beskyttes mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske og organisatoriske foranstaltninger

7.2 Risikoanalyse

7.2.1 Vi skal i forbindelse med vores sagsbehandling gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, som konkret er forbundet med vores behandling af Persondata.

7.2.2 Vi har gennemført en risikoanalyse, som ligger til grund for denne Persondatapolitik.

7.3 Konsekvensanalyser vedrørende databeskyttelse (DPIA)

7.3.1 Databeskyttelsesforordningens artikel 35 indeholder et krav om, at hvis en behandling – navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål – sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal den dataansvarlige forud for behandlingen foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af Persondata.

7.3.2 Pligten til at foretage en konsekvensanalyse gælder alene i særlige tilfælde, hvor der kan konstateres en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

7.3.3 Konsekvensanalyser skal navnlig gennemføres, når der foretages:

a) behandling i stort omfang af følsomme oplysninger eller af Persondata vedrørende straffedomme og lovovertrædelser, eller

b) systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, og som er grundlag for afgørelser, der har retsvirkning for den fysiske person eller på tilsvarende vis betydeligt påvirker den fysiske person

c) systematisk overvågning af et offentligt tilgængeligt område i stort omfang

7.3.4 Det er vores vurdering, at vi i udgangspunktet sjældent vil foretage behandlinger, der opfylder et af ovennævnte kriterier. Det må derfor antages, at reglerne om konsekvensanalyse vil have et forholdsvis begrænset anvendelsesområde i relation til vores behandling af Persondata om klienter.

7.3.5 Vurderingen finder bl.a. støtte i databeskyttelsesforordningens præambel. Ifølge betragtning 91, bør behandling af Persondata ikke anses for omfattende af reglerne om konsekvensanalyse, hvis der er tale om en læges, en sundhedspersons eller en advokats behandling af Persondata om patienter eller klienter.

7.3.6 Gennemføres en konsekvensanalyse alligevel, vil resultatet af analysen tages i betragtning, når vi skal træffe passende foranstaltninger for at imødegå en eventuel forhøjet risiko for fysiske personers rettigheder og frihedsrettigheder.

7.4 <u>Databeskyttelsesrådgiver (DPO)</u>

7.4.1 Pligten til at udpege en databeskyttelsesrådgiver forudsætter efter databeskyttelsesforordningens artikel 37, at behandling af Persondata indgår som vores "kerneaktivitet".

7.4.2 Det er ikke vores kerneaktivitet at behandle Persondata i et stort omfang eller at foretage regelmæssig og systematisk overvågning af personer i stort omfang.

7.4.3 Datatilsynet har i sin "Vejledning om databeskyttelsesrådgivere" udtalt, at virksomheder, der behandler Persondata som en biaktivitet, ikke er forpligtede til at udpege en databeskyttelsesrådgiver.

7.4.4 Vores behandling af Persondata, anses som en biaktivitet.

7.4.5 Med den type sager, som vi behandler, har vi vurderet, at det ikke findes nødvendigt at udpege en databeskyttelsesrådgiver.

7.5 Videregivelse til andre tjenester

7.5.1 Der videregives ikke Persondata til sociale netværk.

7.6 Anden videregivelse

7.6.1 Såfremt vi modtager henvendelse fra politi (eller anden lignende offentlig myndighed) eller retsvæsen om udlevering af Persondata, vil vi foretage udlevering af dine Persondata i overensstemmelse med gældende lovgivning.

7.7 Profilering

7.7.1 Vi anvender ikke dine Persondata til profilering.

7.8 Generelle tekniske foranstaltninger

7.8.1 Datatilsynets IT-sikkerhedstekster, jf. nedenfor, danner udgangspunkt for de overvejelser og vurderinger, som vi skal foretage efter databeskyttelsesforordningen:

7.8.2 Vi skal beskrive, hvordan vi teknisk og organisatorisk har gennemført foranstaltninger til at sikre de Persondata, som vi behandler, og dermed i praksis hvordan vi har implementeret pkt. 2-12 nedenfor. Beskrivelsen kan være særlige retningslinjer, der indgår i vores uddybende sikkerhedsregler, i en it-sikkerhedspolitik eller som en del af vores information til medarbejderne.

7.8.3 Adgang til Persondata skal begrænses til personer, der har et sagligt behov for adgang til Persondata. Det skal være så få personer som muligt, dog med behørigt hensyn til driften – der skal være et tilstrækkeligt antal medarbejdere til at sikre driften af de pågældende opgaver ved sygdom, ferier, personaleudskiftning m.v. Der foreligger et skøn hos virksomheden. Alle medarbejdere har adgang til alle sager. NT Advokater har vurderet, at dette er nødvendigt, da alle medarbejdere i virksomheden skal have mulighed for at foretage ekspeditioner i sagerne.

7.8.4 Alle medarbejdere, der håndterer Persondata, har fået instruktion og oplæring i, hvad de må gøre med Persondata, og hvordan de skal beskytte Persondata.

7.8.5 Persondata på papir – f.eks. i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug.

7.8.6 Når dokumenter (papirer, kartotekskort mv.) med Persondata smides ud, skal der anvendes makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til Persondata.

7.8.7 Der skal anvendes adgangskode for at få adgang til pc'er og andet elektronisk udstyr med Persondata. Kun de personer, der skal have adgang, må få en kode og da kun til de systemet, den pågældende har brug for at anvende. De personer, der har adgangskode, må ikke overlade koden til andre eller lade den ligge, så andre kan se den. Ændring af valgte koder skal foretages mindst en gang hvert tredje måned.

7.8.8 Det skal registreres, hvis der konstateres forgæves forsøg på at få adgang til it-systemer med Persondata. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg, skal der blokeres for yderligere forsøg.

7.8.9 Fortages der ikke ændring af adgangskoden, lukkes der dermed for adgangen til systemet.

7.8.10 Hvis Persondata lagres på en USB-nøgle, skal Persondata beskyttes. Der kan f.eks. bruges en USB-nøgle med adgangskode og kryptering. Ellers skal USB-nøglen opbevares i aflåst skuffe eller skab. Tilsvarende gælder ved opbevaring af Persondata på andre bærbare datamedier. Der er ingen persondata tilgængelig på medarbejdernes bærbare computeres skrivebord.

7.8.11 PC'er koblet til internettet skal have en opdateret firewall og viruskontrol installeret.

7.8.12 Ved opkobling til wifi, hvortil der er fri adgang, sikrer vi passende sikkerhedsmæssige foranstaltninger under hensyntagen til det aktuelle teknologiske udviklingstrin på it-området.

7.8.13 Hvis der benyttes hjemmesideformularer, hvor følsomme Persondata eller personnummer kan indtastes og fremsendes, anvender vi kryptering.

7.8.14 Hvis følsomme Persondata eller personnummer sendes med e-mail via internettet, skal sådanne e-mails krypteres. Vi tilstræber i videst muligt omfang at udelade de sidste 4 cifre i CPR. Vurderes det dog, at de sidste 4 cifre i cpr. er strengt nødvendigt, foretages der en kryptering af mailen.

7.8.15 I forbindelse med reparation og service af dataudstyr, der indeholder Persondata, er de fornødne foranstaltninger truffet ved, at der ikke ligger persondata, så oplysninger ikke kan komme til uvedkommendes kendskab.

7.8.16 I de situationer, hvor en computer indleveres til reparation, og hvor der på computeren ligger Persondata, skal der etableres flere koder til forskellige sektioner af data. En reparatør vil eksempelvis ikke have behov for at kunne tilgå Persondata, der måtte ligge på computeren. En sådan ordning med flere koder vil kunne hjælpe, men ikke fjerne risikoen for misbrug af Persondata. Herudover bør det også ved aftale og kontrol sikres, at reparatører ikke uretmæssigt tilgår Persondata. Det kan f.eks. være ved brug af fortrolighedserklæringer.

7.8.17 Ved brug af en ekstern databehandler til håndtering af Persondata, skal der underskrives en skriftlig databehandleraftale mellem vi og databehandleren. Det gælder eksempelvis, når der anvendes et eksternt dokumentarkiv eller hvis der anvendes cloud-systemer i forbindelse med klientbehandlingen – herunder kommunikation med klienten.

7.8.18 Vi beskytter dine Persondata og har interne regler om informationssikkerhed. Vi har vedtaget interne regler om informationssikkerhed, som indeholder instrukser og foranstaltninger, der beskytter dine Persondata mod at blive tilintetgjort, gå tabt eller blive ændret, mod uautoriseret offentliggørelse, og mod at uvedkommende får adgang eller kendskab til dem.

7.8.19 NT Advokater vil sørge for, at de indsamlede Persondata behandles varsomt og beskyttes i henhold til gældende sikkerhedsstandarder.

7.8.20 Vi har strenge sikkerhedsprocedurer for indsamling, opbevaring og overførsel af Persondata for at hindre uautoriseret adgang og for at overholde gældende lovgivning. Vores sikkerhed kontrolleres jævnligt. De Persondata og personlige Persondata, du giver os, gemmes på vores egen eller på en af vores databehandlerens servere.

7.8.21 Vi har truffet de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger for at beskytte dine Personligoplysninger mod utilsigtet eller ulovlig destruktion, tab eller ændring og mod uautoriseret offentliggørelse, misbrug eller anden handling i strid med gældende lovgivning.

7.8.22 Vi gemmer og behandler dine personlige data på it-systemer med kontrolleret og begrænset adgang. Systemerne er placeret på servere i sikrede lokaler.

7.8.23 Vi bruger industristandarder som firewalls og autentificeringsbeskyttelse for at beskytte dine Persondata.

7.8.24 Hvis du sender Persondata til os via e-mail, skal du være opmærksom på, at afsendelse til os ikke er sikker, såfremt dine e-mails ikke er krypteret.

7.8.25 Alle data overført mellem klient (browser og webapp) og server(er) krypteres efter HTTPS-protokollen.

7.8.26 Vi har fuld adgang til alle dine Persondata, der er opbevaret i vore database(r) og på vores server(e). Data vil alene blive tilgået på "need to know" basis.

7.9 Implementering i organisationen

7.9.1 NT Advokater har udarbejdet leveregler, som gælder sideløbende med denne Persondatapolitik.

7.10 Back-up

7.10.1 NT Advokater tager back-up af alle databaser og filer på fællesdrev hver nat. Back-up´en opbevares dels på en intern server, dels på et eksternt datacenter.

7.10.2 Vi foretager følgende typer af backup:

- 1) back-up rullende. Med denne metode, tages der dagligt backup af alle fil og data opdateringer og oprettes en sikkerhedskopi af alle de nye data. Dette skaber en historie af ændringer, således at muligheden for at genvinde tabte data forøges (denne back-up går dagligt tilbage).

- 2) back-up klon. Denne back-up-strategi skaber en perfekt kopi af hver enhed på netværket (denne back-up går 7 dage tilbage)

- 3) backup offsite. Denne back-up sikrer mod tab af data, hvis back-up opbevares on site. Alle data og filer sikkerhedskopieres og backup opbevares offsite.

7.10.3 Alle back-up data og filer overskrives med intervaller på 30 dage. Det er ikke teknisk muligt at gennemføre sletning af enkelte filer på en foretagen back-up inden sådan overskrivning sker. Det vil sige, at har du anmodet NT Advokater om sletning af dine Persondata, vil sådanne Persondata blive slettet i live miljø, jf. nedenfor, men vil forblive på backup indtil den specifikke back-up efter 30 dage er overskrevet. NT Advokater har dog indført interne processer og procedurer til at sikre, at dine Persondata ikke genintroduceres som live data ved at genindlæse data og filer fra en back-up såfremt dine data er blevet slettet i henhold til

din "ret til at blive glemt". Vi genindlæser i forhold til sletteregler. Den person der ønsker at blive slettet, bliver slettet.

8 BEHANDLINGSREGLER - KLIENTER

8.1 Overordnet

8.1.1 Behandlingsregler – klienter er tænkt som de generelle principper, som vi skal anvende i forbindelse med sagsbehandling for klienter og er dermed en gennemgang af de spørgsmål, som vi generelt i vores sagsbehandling skal forholde os til. Behandlingsregler – klienter er derudover udtryk for, hvordan vi opfylder dokumentationskravene i databeskyttelsesforordningen.

8.1.2 Medarbejderne er instrueret i, at der skal foretages dataminimering af mails, der er tilgængelige i Outlook.:

8.2 Dataansvarlig

8.2.1 Vi arbejder som altovervejende udgangspunktet selvstændigt i relation til klienten og tredjeparter. Vi vurderer selvstændigt, om der er grundlag for at indsamle/behandle Persondata, hvilke Persondata, der er relevante og nødvendige, og hvor længe Persondata skal opbevares.

8.2.2 I henhold til de advokatetiske regler er vi også i et vist omfang forpligtet til at vurdere processen uafhængigt af klienten. Derudover skal vi i visse tilfælde også opfylde bevismæssige forpligtelser for tredjemand, f.eks. i forbindelse med behandling af konkursboer.

8.2.3 Datatilsynet har i "Vejledning om dataansvarlige og databehandlere" givet 2 eksempler vedrørende advokaters arbejde (eksempel 15 og 16), som illustrerer grænsefladen:

"Yder advokaten rådgivning/bistand til en sag (i eksemplet en erstatningssag), er advokaten selvstændig dataansvarlig, fordi advokatvirksomheden træffer selvstændige beslutninger om, hvilke oplysninger der skal indsamles, slettes, videregives mv. Behandlingen af oplysninger sker ikke efter instruks eller godkendelse fra klienten, og i lyset af retsplejelovens regler og de advokatetiske regler er det ifølge Datatilsynet også tvivlsomt, i hvilket omfang advokaten ville have mulighed for at følge en detaljeret instruks".

8.2.4 Består vores ydelse derimod i at administrere en ordning eller forpligtelse, som klienten har (i eksemplet en whistleblower-ordning), er vi databehandler. I dette tilfælde vil opgaven væ-

re bundet af aftale (instruksen) fra klienten, og behandling vil være ekspeditionspræget, ligesom den ikke er udtryk for klassisk advokatvirksomhed.

8.2.5 I en udtalelse fra 2000 har Datatilsynet i tråd med ovennævnte vurderet,

> "(…) at en overladelse af oplysninger fra [inkassofirmaets] kunder (den dataansvarlige) til [inkassofirmaet] til brug for databehandling i en konkret arbejdsopgave ikke er i strid med behandlingsreglerne i PDL § 11, stk. 2. Inkassofirmaet er således alene databehandler for kunden, og må ikke behandle oplysningerne selvstændigt eller uden instruktion fra den dataansvarlige".

8.2.6 For så vidt angår M&A-proces skal det også konkret vurderes, om vi er dataansvarlig eller databehandler. Ydes der udelukkende bistand i form af administration af et datarum, taler det for, at vi er databehandler.

8.3 Databehandler

8.3.1 Inddrages tredjeparter i sagsbehandlingen skal vi vurdere, om sådanne tredjeparter får status som databehandlere eller selvstændige dataansvarlige.

8.3.2 Et eksempel på overgivelse af Persondata til en tredjepart er den situation, hvor vi anmoder en anden advokat om bistand til løsning af en klients sag. I dette tilfælde skal det iagttages, om der er hjemmel til at overdrage sådanne Persondata til en selvstændig tredjepart.

8.3.3 Modtager vi Persondata fra andre advokater, skal vi selvstændigt vurdere, om opgaven indebærer, at vi får en rolle som databehandler eller som selvstændig dataansvarlig. Dette skal afklares, inden behandlingen af de konkrete Persondata påbegyndes.

8.3.4 Det skal i overvejelsen holdes for øje, at den dataansvarlige er den, som bestemmer, med hvilke formål Persondata må behandles (formålet), og hvordan Persondata må behandles (hjælpemidlerne), herunder af hvem Persondata må behandles.

8.3.5 En databehandler behandler til gengæld udelukkende Persondata på vegne af den dataansvarlige. Databehandleren bestemmer i modsætning til den dataansvarlige hverken hvordan, eller til hvilket formål, der må behandles Persondata.

8.3.6 Der vil derfor kun foreligge en databehandlerkonstruktion, hvis en aftale eller en del af en aftale mellem os og en anden part (en databehandler) går ud på, at den anden part skal behandle (f.eks. indsamle, registrere, opbevare, videregive eller slette) Persondata efter instruks fra os som dataansvarlig.

8.3.7 Hvis aftalen mellem os og den anden part først og fremmest drejer sig om levering af en anden ydelse end ren administration/behandling af Persondata – hvis der f.eks. skal udarbejdes en juridisk vurdering af en bestemt problemstilling, hvor vi ikke har behov for at give en instruks om den konkrete behandling af Persondata – vil den anden part ikke være databehandler for os. Dette gælder også, selvom vi videregiver Persondata (f.eks. navn og adresse), som er nødvendige for, at denne anden part kan levere sin hovedydelse i form af eksempelvis juridisk rådgivning, og at tredjeparten leverer denne ydelse bestilt af os.

8.3.8 Spørgsmålet er med andre ord, om vi alene er interesseret i at modtage det færdige produkt (f.eks. en rapport, som giver svar på en bestemt problemformulering) men ikke ønsker at blande os i, med hvilke delformål og hjælpemidler dette opnås. Fraværet af en instruks i denne sammenhæng taler for, at hovedydelsen drejer sig om andet end behandling af Persondata som databehandler.

8.3.9 Er der ikke tale om en databehandlerkonstruktion, vil den part, som modtager oplysningerne fra os, herefter være dataansvarlig for den efterfølgende behandling af Persondata hos parten selv.

8.3.10 Som ovenfor anført skal det ved videregivelse til en selvstændig dataansvarlig i det hele sikres, at der er hjemmel til videregivelsen, ligesom den modtagende part skal sikre sig opfyldelse af sin oplysningspligt.

8.4 Databehandleraftale

8.4.1 Hvis vi er dataansvarlige og har vurderet, at der foreligger en databehandlerkonstruktion, skal der udarbejdes en databehandleraftale.

8.4.2 Databehandleraftalen skal indgås mellem os (den dataansvarlige) og den anden part (databehandleren), og skal leve op til databeskyttelsesforordningens krav til databehandleraftaler, jf. forordningens artikel 28, stk. 3. Det indebærer, at der skal udarbejdes en kontrakt eller andet retligt dokument, som er bindende for databehandleren. Det er desuden et krav, at databehandleraftalen er skriftlig, herunder elektronisk.

8.4.3 Databeskyttelsesforordningen fastsætter herudover en del specifikke krav til indholdet af databehandleraftalen. Aftalen skal bl.a. indeholde oplysninger om genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af Persondata, kategorierne af registrerede og vores forpligtelser og rettigheder som dataansvarlig samt de pligter, som databehandleren har i forhold til at varetage opgaven. Kravene er specifikt beskrevet i databeskyttelsesforordningens artikel 28, stk. 3, litra a-h.

8.4.4 Agerer vi som databehandler for klienten, skal der indgås en databehandleraftale med klienten.

8.5 Overførsel til tredjelande

8.5.1 Ved brug af en databehandler, indhentelse af responsum fra en advokat uden for EU/EØS eller ved kommunikation med modparter skal vi være opmærksomme på, om overladelsen af Persondata til en databehandler eller videregivelsen af Persondata til en anden dataansvarlig uden for EU/EØS vil indebære, at der sker behandling uden for EU/EØS.

8.5.2 Databeskyttelsesforordningen forudsætter, at der ikke sker behandling af Persondata i lande med ringere Persondatabeskyttelse end databeskyttelsesniveauet i EU, jf. databeskyttelsesforordningens artikel 44-49.

8.5.3 Overladelse til lande uden for EU/EØS kræver som udgangspunktet (artikel 44-47):

- at EU-Kommissionen har godkendt landet (herunder Privacy Shield for USA),
- at vi og tredjeparten har indgået en aftale ved brug af EU-Kommissionens standard model klausuler, eller
- at der er et tilstrækkeligt beskyttelsesniveau fastsat ved godkendte bindende virksomhedsregler

8.5.4 Herudover kan enkelte overførsler finde sted, hvis

- der foreligger et samtykke
- overførslen er påkrævet for opfyldelse af en kontrakt eller
- overførslen er påkrævet for, at et retskrav kan fastlægges, gøres gældende eller forsvares

8.5.5 Uanset hjemmelsgrundlaget forudsætter en overførsel, at fire grundlæggende garantier altid er opfyldt, jf. Datatilsynets "Vejledning om overførsel af Persondata til tredjelande":

- Myndigheder i tredjelandes adgang til og brug af Persondata hidrørende fra EU skal ske på grundlag af klare, præcise og tilgængelige regler.

- Myndigheder i tredjelandes adgang til og brug af Persondata hidrørende fra EU skal være nødvendig og proportional (der skal være balance mellem formålet (national sikkerhed) og indgrebet i de registreredes ret til beskyttelse af deres privatliv).

- Der skal være en uafhængig og effektiv tilsynsmyndighed i tredjelandet.

- Der skal være tilgængelige og effektive rets midler for de registrerede i tredjelandet.

8.6 Databehandlere - oversigt

8.6.1 Vi anvender eksterne virksomheder til at foretage den tekniske drift af NT Advokater. Denne virksomhed fungerer som databehandler i forhold til de Persondata, som vi er dataansvarlig for.

8.6.2 Databehandling foretages inden for den Europæiske Union.

8.6.3 Databehandleren handler alene efter instruks fra os.

8.6.4 Vi benytter følgende databehandlere:

Databehandler	**Lokalisation**	**Aftaletype**
EG	Danmark	Databehandleraftale
Simple Solution P/S	Danmark	Databehandleraftale
Konica	Danmark	Databehandleraftale
Telia (Unosoft)	Danmark	Databehandleraftale
Flexya	Danmark	Databehandleraftale
City Call Center	Danmark	Databehandleraftale
Sylvester Hvid Online	Danmark	Databehandleraftale
Fotograf Birgitte Røddik	Danmark	Databehandleraftale

8.6.5 Databehandleren har truffet de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at Persondata hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at Persondata kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med reglerne om Persondata. På din anmodning - og mod betaling af databehandlerens til enhver tid gældende timetakster for sådant arbejde - giver databehandleren dig tilstrækkelige oplysninger til, at databehandleren kan påvise, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger er truffet.

8.7 Behandlingshjemmel

8.7.1 Vores hjemmel til at behandle Persondata ligger først og fremmest i opdraget fra klienten. Til gengæld vil vi inden for dette opdrag i udgangspunktet have hjemmel til at behandle de nødvendige oplysninger til brug for løsning af opdraget. Det følger navnlig af databeskyttelsesforordningens artikel 6, stk. 1, litra a-c og litra f, samt af artikel 9, stk. 2, litra a og f.

8.7.2 Disse bestemmelser omhandler adgang til at behandle Persondata, (i) hvis der foreligger et samtykke, (ii) hvis behandlingen er nødvendig for at opfylde en kontrakt, (iii) hvis behandlingen er nødvendig for at overholde en retlig forpligtelse , (iv) nødvendig for at opfylde væsentlige interesser, der overstiger den registreredes interesser, eller (v) nødvendig for at et retskrav kan fastlægges, gøres gældende eller forsvares.

8.7.3 For så vidt angår navnlig personnumre kan vi behandle oplysninger om personnumre, (i) når det følger af lovgivningen, (ii) hvis der foreligger et samtykke, eller (iii) hvis det er nødvendigt med henblik på fastlæggelsen af et retskrav, jf. databeskyttelseslovens § 11, jf. § 7.

8.7.4 Det er vores vurdering, at den behandling af Persondata vi foretager i relation til et opdrag fra en klient, i vidt omfang vil være hjemlet i de anførte bestemmelser.

8.7.5 Vi vil nøje overveje i den enkelte sag, hvad opdraget omfatter, når Persondata behandles, så den enkelte advokat undlader at behandle – herunder registrere og gemme – Persondata, som ikke er relevante for sagen. Vi skal derfor i alle sammenhænge forholde os til rammerne for opdraget og sikre, at der ikke indsamles og behandles Persondata, som ikke er relevante. Navnlig er det vigtigt at sikre, at der ikke behandles Persondata om tredjemænd, som ikke er relevante for sagen.

8.8 Generelle principper - sagsbehandlingen

8.8.1 Ved opstart af sagen skal vi først og fremmest sikre os, at hjemmelsgrundlaget er klart – altså hvilke behandlinger af oplysninger, som opdraget forudsætter, og at vi har et lovligt behandlingsgrundlag herfor.

8.8.2 Dernæst skal vi tage stilling til vores forpligtelse om af egen drift til at underrette klienten om den behandling, vi foretager herunder om de særlige regler, der gælder for indhentning og opbevaring af Persondata til brug for hvidvaskkontrol.

8.8.3 Under processen skal vi løbende sikre os, at indsamling og videregivelse af Persondata sker i overensstemmelse med formålet, og vi skal løbende overveje vores forhold til eventuelle databehandlere. Inddrages et tredjeland i sagen, skal man vi være opmærksomme på de særlige regler, der gælder for overførsel af Persondata til tredjelande.

8.8.4 Når sagen er afsluttet, skal vi tage stilling til, hvor længe vi har behov for at opbevare oplysningerne, og hvornår de skal slettes.

8.8.5 Vi skal som udgangspunkt undgå at basere vores behandling af Persondata på et samtykke fra klienten. Samtykke kan nemlig tilbagekaldes og giver i øvrigt heller ikke selvstændig mening ved siden af opdraget/aftalen om bistand.

8.9 <u>Oplysningspligt - klient</u>

8.9.1 Oplysningspligten gælder både i forhold til klienten selv og i forhold til eventuelle tredjeparter, som forudsættes inddraget i sagsbehandlingen. Pligten til at underrette tredjeparter skal altid overvejes i forhold til vores tavshedspligt, men tavshedspligten kan næppe – som generelt princip – undtage fra en oplysningsforpligtelse i alle sammenhænge. Det forudsætter en konkret vurdering og stillingtagen.

8.9.2 I forhold til klienten opfyldes oplysningspligten ved at sende et link til vores persondatapolitikken i det velkomstbrev, som beskriver betingelserne for samarbejdet.

8.9.3 I velkomstbrevet henvises der til Persondatapolitikken:

- Vores behandling – herunder elektronisk og fysisk behandling/opbevaring og eventuelt anvendelse af cloud-system og sagsbehandlingssystem.

- Andre relevante aktører – modparter/myndigheder/vidner/skønsmænd – der vil blive inddraget, samt også evt. ekstern bogholder og it-support.

- Opbevaringsperiode efter afslutning – herunder hvidvaskrav og klientkontokrav.

- Rettigheder og mulighed for klage samt muligheden for at tilbagekalde samtykket, hvis behandlingen skal baseres på et samtykke. For så vidt angår personens rettigheder fremgår det af databeskyttelsesforordningens artikel 21 om den registreredes ret til at gøre indsigelse, at den registrerede skal gøres udtrykkeligt opmærksom på denne rettighed, og at dette skal ske senest på tidspunktet for den første kommunikation, jf. artikel 21, stk. 4. Oplysningen skal meddeles klart og adskilt fra andre oplysninger.

- Hver klient modtager et link til vores Persondatapolitik og som der herefter blot kan henvises til i bekræftelsesbrevet. Persondatapolitik vedrørende hvidvask vedlægges.

8.10 Oplysningspligt - tredjeparter

8.10.1 Tredjeparter kan f.eks. udgøre vidner, familiemedlemmer, naboer, arbejdsgiver, kolleger mv., samt bipersoner, herunder skønsmænd, læger, sagsbehandlere mv.

8.10.2 Det fremgår af databeskyttelsesforordningens artikel 14, stk. 5, litra d, at oplysningspligten ikke gælder, hvis Persondata skal forblive fortrolige som følge af tavshedspligt.

8.10.3 Så længe behandling af Persondata vedrørende tredjeparter, ligger inde for opdraget, og så længe oplysningerne er omfattet af vores tavshedspligt, har vi ikke en oplysningsforpligtelse overfor sådanne tredjeparter.

8.10.4 Oplysningspligten indtræder dog i det øjeblik, der ikke længere er et hensyn at tage til tavshedspligten. Vi overvejer løbende, i hvilket omfang man kan undlade at give oplysning med henvisning til sin tavshedspligt.

8.10.5 Det følger af databeskyttelsesforordningens artikel 14, stk. 5, litra b, at oplysningspligten ikke gælder, hvis det vil kræve en uforholdsmæssig stor indsats at opfylde den. Denne undtagelse er i praksis fortolket sådan, at oplysningsforpligtelsen bl.a. ikke omfatter bipersoner. Det kan være navne på læger og diverse øvrige behandlere, samt navne på diverse konsulenter, kolleger, naboer og andre, der måtte indgå i beskrivelsen af sagen, men hvor det eksempelvis er funktionen og ikke personen, der er relevant, og hvor selve personidentiteten ingen betydning har for sagen og heller ikke vil få nogen betydning. Undtagelsen forudsætter dog, at der alene indgår kontaktoplysninger og tilsvarende almindelige Persondata om den/de pågældende.

8.11 Hvidvask

8.11.1 Vi skal i medfør af hvidvaskloven opbevare følgende Persondata i fem år fra klientforholdets ophør:

- Persondata indhentet i forbindelse med opfyldelse af kravene om kundekendskabsprocedurer i henhold til hvidvaskloven

- Identitets- og kontroloplysninger

- Kopi af foreviste legitimationsdokumenter

- Dokumentation for og registreringer af transaktioner, der gennemføres

- Dokumenter og registreringer vedrørende undersøgelser gennemført i henhold til hvidvasklovens § 25, stk. 1 og 2.

8.11.2 Vi skal inden etablering af en forretningsforbindelse med en klient og inden gennemførelse af en enkeltstående transaktion for fysiske personer informere klienten om vores regler for behandling af Persondata, som er indhentet efter hvidvaskloven ved at udlevere vores Persondatapolitik om hvidvask oplysninger.

8.11.3 Oplysningerne skal gives direkte til klienten, f.eks. som et vedhæftet dokument til velkomstbrev (og ikke alene ved henvisning til en angivelse på vores hjemmeside).

8.11.4 Reelle ejere skal ikke informeres om vores behandling af Persondata i henhold til hvidvaskloven.

8.11.5 Oplysninger indhentet i relation til hvidvask skal opbevares separat fra de enkelte sager ved angivelse på hvidvaskkortet.

8.12 Løbende indsamling og videregivelse af oplysninger

8.12.1 Formålet er at løse klientens sag – at løse sit opdrag. Vi skal derfor i vores ageren sikre os, at der kun sker indsamling og videregivelse af Persondata i det omfang, indsamlingen/videregivelsen ligger inden for det, som er nødvendigt for at løse klientens sag.

8.12.2 Når der indsamles Persondata på sagen, skal vi navnlig være opmærksomme på, om materialet indeholder Persondata om tredjeparter, som ikke ved, at man behandler Persondata om de pågældende. Det kan udløse pligten til af egen drift at give oplysning til de pågældende om den behandling, der finder sted.

8.12.3 Det er vigtigt, at vi samtidig overvejer nødvendigheden af, at der indgår Persondata om den pågældende tredjemand i sagen. Hvis ikke det er nødvendigt, bør personoplysningen

slettes med det samme. Derved undgår man også at skulle forholde sig til oplysningspligt mv.

8.13 Sletning - hvornår

8.13.1 Ved afslutning af en sag har vi i princippet ikke længere behov for at behandle Persondata. Opdraget er løst.

8.13.2 En række andre hensyn samt særregler indebærer dog, at Persondata ikke bør eller ikke må slettes førend, der er gået et vist antal år.

8.13.3 Det skal konkret overvejes hvor længe Persondata opbevares, inden de slettes.

- Bogføringsreglerne indebærer, at Persondata knyttet til en betaling skal opbevares i 5 år + løbende kalenderår efter regnskabsårets afslutning.

- Hvidvaskreglerne indebærer, at oplysninger indsamlet til opfyldelse af hvidvaskreglerne skal opbevares i 5 år fra klientforholdet er afsluttet, hvorefter de straks skal slettes.

- Hensynet til at vi kan varetage vores interesser ved et muligt rådgiveransvar kan indebære, at sagen bør opbevares i 10 år efter afslutningen af sagen.

- Det kan overvejes, om sager vedrørende erstatning eller godtgørelse i anledning af personskade og for fordringer på erstatning for skade forvoldt ved forurening af luft, vand, jord eller undergrund eller ved forstyrrelser ved støj, rystelser el.lign, bør opbevares i mere end 10 år fra sagens afslutning, eller om materialet skal tilbagesendes til klienten, som herefter må vende tilbage, i fald der senere måtte opstå et grundlag for genoptagelse af sagen.

- Stamdata for klienten bør – for at sikre logisk synergi til også den tidsmæssige opbevaring af sagerne – opbevares i 10 år fra klientforholdets afslutning (de konkrete hvidvaskoplysninger skal dog slettes efter 5 år).

- Særlige overvejelser skal tages, hvor Persondata ikke kan opbevares af andre, og hvor der på et senere tidspunkt end 10 år fra sagens afslutning kan vise sig et behov for at genskabe Persondata. Et eksempel herpå er opbevaring af kreditorlister i konkursboer. vi må i sådanne tilfælde konkret vurdere, om der er behov for en længere opbevaringsfrist end i andre tilfælde, og da tage konkret stilling til, hvilke Persondata, som kan og bør opbevares ud over den 10 årige periode.

8.13.4 Såvel hensynene som skæringstidspunkterne er forskellige.

8.13.5 Korrekt sletning kræver derfor, at vi kortlægger vores behov og forpligtelser, der sikrer behørig sletning alt afhængig af formålet med den enkelte registrering.

8.13.6 Det kan betyde, at Persondata indsamlet i henhold til hvidvaskreglerne slettes hurtigere end den konkret afsluttede sag. Vi kan således finde det nødvendigt at opbevare selve sagen af hensyn til at kunne imødegå en mulig indsigelse om rådgiveransvar. En sådan passiv opbevaring betyder dog ikke, at selve klientforholdet fortsat må anses for aktivt.

8.13.7 Som generel politik (og med mindre andet er angivet i denne Persondatapolitik) skal alle Persondata data vedrørende en specifik sag slettes 10 år efter sagens afslutning. Alle oplysninger vedrørende en klient skal slettes 10 år efter klientforholdets ophør

8.14 Sletning - hvordan

8.14.1 Det fremgår af IT-sikkerhedstekst ST3 fra Datatilsynet vedrørende sletning af Persondata, at sletning af Persondata i praksis betyder, at Persondata uigenkaldeligt fjernes fra alle lagringsmedier, hvorpå de har været lagret, og at Persondata på ingen måde kan genskabes. Man skal i den forbindelse være opmærksom på alle lagringsmedier – herunder også flytbare medier i form af bærbare computere, USB-nøgler mv., samt back-up.

8.14.2 For at lette sletningsproceduren skal alt fysisk materiale scannes til den elektroniske sag, og dernæst makuleres eller tilbagesendes til klienten.

8.14.3 Derudover skal al korrespondance mv. fra Outlook overføres til den elektroniske sag og slettes i det hele fra Outlook, ligesom alle redegørelser/præsentationer mv. på diverse bærbare medier og lokale drev skal overføres til den elektroniske sag og slettes i øvrigt.

8.14.4 Derved kan den samlede sag til sin tid (efter endt opbevaringsperiode) i det hele blive slettet fra det elektroniske sagssystem.

8.14.5 I tilfælde hvor alle Persondata om en klient – og ikke kun en konkret sag – skal slettes, skal den elektroniske formular med klientens stamoplysninger slettes fra Advopro, ligesom de hertil hørende registreringer vedrørende klienten i alle øvrige systemer skal slettes.

8.14.6 Persondata kan som et alternativ anonymiseres fuldstændigt med den virkning, at de ikke længere kan henføres til en bestemt person. I givet fald finder reguleringen om Persondata slet ikke anvendelse, og fuldstændig anonymisering er derfor et alternativ til sletning. Det er dog vigtigt at holde sig for øje, at anonymisering – som et alternativ til sletning – forudsætter, at man sletter alle spor, der kan lede til den person, oplysningen vedrører. Det er som oftest en meget vanskelig øvelse.

8.14.7 Efter sletning/anonymisering vil vi foretage behørigt krydstjek i form af søgninger på navn/cpr-nr. mv. vedrørende klienten henholdsvis sagen for at sikre, at der ikke kommer noget frem.

8.15 IP-adresser og browserindstillinger

8.15.1 I forbindelse med hvert besøg på nt.dk registreres din computers anvendte IP-adresse og browserindstillinger. Din IP-adresse er adressen på den computer du anvender til at besøge les.dk. Browserindstillinger er for eksempel den browser type du anvender, browser sprog, tidszone mv. IP-adressen og browserindstillinger registreres for at sikre, at nt.dk altid kan finde tilbage til den anvendte computer, såfremt der måtte ske misbrug eller ulovligheder i forbindelse med besøget på eller anvendelsen af les.dk. IP-adressen benyttes desuden til at fastslå din omtrentlige lokalisation (på by-niveau).

8.16 Demografiske Persondata

8.16.1 I forbindelse med at du foretager opslag af Persondata, herunder personlige Persondata, på nt.dk logger vi din demografiske placering. Disse Persondata vil blive offentliggjort sammen med de Persondata, du har slået op på din profil.

9 BEHANDLINGSREGLER - ANSATTE

9.1 Behandlingshjemmel

9.1.1 Vi behandler personaleoplysninger med følgende behandlingshjemmel:

- Medarbejderen har givet sit samtykke til behandling af sine Persondata til et eller flere specifikke formål.

- Behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som medarbejderen er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på medarbejderens anmodning forud for indgåelse af en kontrakt.

- Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler os.

- Behandling er nødvendig for at beskytte medarbejderens eller en anden fysisk persons vitale interesser.

- Behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som vi har fået pålagt.

- Behandling er nødvendig for, at vi eller en tredjemand kan forfølge en legitim interesse, medmindre medarbejderens interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af Persondata, går forud herfor.

9.2 Behandling af Persondata forud for ansættelsen

9.2.1 Vi vil forud for en ansættelse af en medarbejder behandle en række almindelige Persondata om medarbejderen.

9.2.2 Vi modtager visse Persondata direkte fra ansøgeren, f.eks. en ansøgning, et CV, fotos, eksamensbeviser, udtalelser fra tidligere arbejdsgivere og referencer.

9.2.3 Derudover indhenter vi af egen drift Persondata om ansøgeren. Det kan f.eks. være offentligt tilgængelige Persondata på LinkedIn, Facebook eller Persondata, der indhentes via en almindelig søgning på internettet.

9.2.4 Grundlaget for behandling af sådanne almindelige Persondata, der behandles med det formål at udvælge en medarbejder til ansættelse hos os, er databeskyttelsesforordningen artikel 6, stk. 1, litra a, om gennemførelse af foranstaltninger forud for indgåelse af en kontrakt, samt interesseafvejningsreglen i artikel 6, stk. 1, litra f.

9.2.5 Billeder, der er vedlagt en ansøgning, kan behandles til ansættelsesprocessen, hvis der foreligger et samtykke hertil. Hvis billeder anvendes til andre videregående formål end ansættelsesprocessen, kræves der også samtykke til denne anvendelse.

9.2.6 Vi vil forud for ansættelse af en medarbejder også i visse tilfælde have behov for at behandle følsomme Persondata om en ansøger.

9.2.7 Hvis vi indsamler Persondata om dig hos din nuværende eller tidligere arbejdsgivere via referenceindhentning, beder vi om dit samtykke hertil først. Konkret bliver du bedt om at underskrive en samtykkeerklæring, som du efterfølgende selv får en kopi af. Hvis ikke du giver samtykke, indhenter vi ikke referenceoplysninger.

9.2.8 Efter retsplejelovens regler kan en advokatfuldmægtig ikke autoriseres, hvis vedkommende er dømt for et kvalificeret strafbart forhold, hvis vedkommende har udvist kvalificeret strafværdig adfærd i en tidligere stilling, eller hvis vedkommende har forfalden gæld på mere end 50.000 kr. til det offentlige. Beskikkelse som advokat kan også nægtes i disse situatio-

ner. Uanset at retterne ved autorisation af advokatfuldmægtige/advokater påser, om den pågældende bør nægtes autorisation af de ovenfor anførte grunde, vil vi i forbindelse med en ansættelsesproces af advokatfuldmægtige og advokater typisk behandle Persondata om dig fra Det Centrale Kriminalregister, ligesom der vil blive indhentet en attestation fra SKAT om, hvorvidt du har gæld til det offentlige.

9.2.9 Vi vil typisk anmode medarbejderen om selv at fremskaffe en straffeattest (privat straffeattest), men kan også selv indhente den med samtykke (privat straffeattest med samtykke). I begge situationer kræves der et samtykke fra dig til, at vi kan behandle Persondata. Det vil også typisk være relevant at indhente straffeattester på advokatbogholdere og andre betroede medarbejder. I det omfang vi anmoder en medarbejder om at fremskaffe sin straffeattest, vil vi blot se den, men ikke foretage en opbevaring. Såfremt vi anmoder medarbejderen om at indhente straffeattest, eller vi ved samtykke fra medarbejderen berettiges til at indhente straffeattesten, kræves der samtykke fra medarbejderen til, at vi kan behandle persondata.

9.2.10 Efter Hvidvasklovens skal vi screene særlige kategorier af medarbejdere. Dette indebærer blandt andet, at vi inden ansættelsen af dig sikrer, at du ikke er dømt for et strafbart forhold, der begrunder en nærliggende fare for misbrug af den pågældendes stilling, ligesom det sikres, at vi bliver bekendt med, såfremt due dømmes for et sådant forhold i løbet af din ansættelse. Der kan anlægges en risikovurdering, alt efter hvilken funktion du skal varetage hos os. Det vil f.eks. ikke være aktuelt for personer, der ikke varetager funktioner, der sikrer opfyldelse af hvidvaskloven. For personer, som ansættes i en stilling, hvor personen direkte eller indirekte kan misbruge stillingen til hvidvask eller finansiering af terrorisme, vil det altid være relevant med en nærmere undersøgelse af personen inden ansættelsen. Det vil bero på en konkret vurdering i forhold til, om en person direkte eller indirekte kan misbruge sin stilling til hvidvask eller finansiering af terrorisme.

9.2.11 Vi vil ikke indhente kreditoplysninger om jobansøgere, medmindre der er tale om ansættelse i en særligt betroet stilling. Det skal her vurderes, hvilke opgaver den pågældende medarbejder er befuldmægtiget til at udføre, og i hvilket omfang medarbejderen er underlagt rutinemæssige kontrolforanstaltninger, evt. fra overordnede. Vi vil indhente kreditoplysninger om personer, der søger stillinger som advokatbogholdere eller personer, der søger stillinger med mere overordnet økonomiansvar. Grundlaget for behandlingen vil kunne være interesseafvejningsreglen i databeskyttelsesforordningen artikel 6, stk. 1, litra f.

9.2.12 Vi vil i nogle situationer benytte os af personlighedstest i forbindelse med ansættelse af nye medarbejdere. Det gælder særligt, når der er tale om stillinger, der er særligt betroede. En sådan test kan i sagens natur alene gennemføres, hvis du samtykker til at blive testet. Uanset at resultatet af en personlighedstest kan betragtes som Persondata af mere privat karakter, betragter vi det som udgangspunkt som almindelige Persondata. En personlighedstest

kan dog også indeholde følsomme Persondata. I så fald kræves der et udtrykkeligt samtykke fra dig til vores behandling af Persondata.

9.2.13 Vi kan i helt særlige tilfælde anmode dig om Persondata om dit helbred. Det kan være relevant i de situationer, hvor en sygdom vil have væsentlig betydning for din evne til at varetage stillingen. Hvis det konkret vurderes nødvendigt med helbredsoplysninger, vil vi angive, hvilke sygdomme eller symptomer på sygdomme, der ønskes Persondata om. I givet fald vil oplysninger da blive indhentet med samtykke.

9.2.14 Hvis du ender med at blive ansat hos os, vil de Persondata, som vi har modtaget og behandlet i forbindelse med rekrutteringsprocessen, blive opbevaret på din personalesag gennem dit ansættelsesforhold og i en periode på 5 år fra ansættelsesforholdets ophør.

9.2.15 Hvis du får afslag på din ansøgning, vil vi hurtigst muligt – og som udgangspunkt senest 6 måneder efter, at du har modtaget afslaget – slette de Persondata, som vi har modtaget og behandlet i forbindelse med rekrutteringsprocessen. Vi vil dog samtidig anmode om dit samtykke til at opbevare dine Persondata fra ansættelsesprocessen i en periode på 3 år til brug for lignende ansættelsesprocesser til stillinger modsvarende den stilling, hvortil du søgte. Hvis vi skønner, at en jobansøger, der ikke er blevet ansat, vil indlede en sag efter ligebehandlingsloven eller forskelsbehandlingsloven, vil Persondata blive opbevaret i længere tid.

9.3 Behandling af Persondata om nuværende ansatte

9.3.1 Når et ansættelsesforhold er etableret, vil vi behandle en række yderligere almindelige Persondata. Det er dels Persondata, som du selv giver til os, f.eks. dit CPR-nr., adresseoplysninger, kontonummer m.v., ansættelsesaftalens beskrivelse af arbejdsopgaver, -tid, løn og lignende, Persondata om nærmeste pårørende samt Persondata om sygefravær og sygdomsperioder. Derudover indsamler vi selvstændigt Persondata om dig. Det kan f.eks. være Persondata om dig, der løbende registreres fra ledere og andre medarbejdere (herunder MUS-samtalereferater) samt fra samarbejdspartnere. Henvendelser og klager af enhver art fra øvrige medarbejdere eller klienter/samarbejdspartnere, ledelsens egen indsamling af Persondata i sociale medier og henvendelser fra offentlige myndigheder om medarbejderen m.v. vil også være omfattet.

9.3.2 Videregives Persondata til offentlige myndigheder, f.eks. til SKAT om A-skat eller lignende, er behandlingen nødvendig for at overholde den indeholdelses- og indberetningspligt, der påhviler os som arbejdsgiver, jf. skattelovgivningens bestemmelser herom.

9.3.3 Vi vil alene offentliggøre arbejdsrelaterede Persondata om ansatte på vores hjemmeside uden forudgående samtykke. Offentliggørelse af Persondata af mere personlig karakter, f.eks. et billede af den ansatte, vil alene blive offentliggjort med den ansattes samtykke.

9.3.4 Når et ansættelsesforhold er etableret, vil vi i visse situationer også skulle behandle følsomme Persondata om dig. Det kan f.eks. være helbredsoplysninger om dig, herunder Persondata om alkoholmisbrug og behandling af sådant misbrug, Persondata om medlemskab af en fagforening eller Persondata om strafbare forhold. Private forhold og udfaldet af personlighedstests behøver ikke nødvendigvis at indeholde følsomme Persondata.

9.3.5 Som udgangspunkt er det forbudt at behandle følsomme Persondata. Vi kan dog i visse tilfælde behandle følsomme Persondata om en medarbejder. Det kan navnlig være tilfældet, hvis den ansatte har givet sit udtrykkelige samtykke til, at vi kan foretage behandlingen. Uden samtykke vil vi behandle helbredsoplysninger i nødvendigt omfang i forbindelse med en aftale i henhold til § 56 i lov om sygedagpenge. Vi vil i sådanne situationer behandle følsomme helbredsoplysninger om kronisk sygdom mv. I tilfælde af opsigelse, hvor en tidligere medarbejders ret til på begæring at få oplysning om årsagen til afskedigelsen nødvendiggør registrering af Persondata herom, kan Persondata betragtes som følsomme, hvis de er præcise og gengiver konkrete faktiske forhold af social eller personlig karakter om medarbejderen. Hvis Persondata alene er holdt i vage og skønsmæssige termer, er de ikke nødvendigvis følsomme.

9.3.6 Behandling af Persondata om fagforeningsmæssige tilhørsforhold kan endvidere foretages, hvis behandlingen er nødvendig for overholdelsen af vores arbejdsretlige forpligtelser eller specifikke rettigheder, som omfatter alle former for forpligtelser og rettigheder, der hviler på et arbejdsretligt grundlag.

9.3.7 Derudover vil vi kun i begrænset omfang kunne registrere følsomme Persondata i et personaleregister. Der skal være tale om registrering, som er nødvendige for, at det kan fastlægges, om nogen har et retskrav. Det vil f.eks. kunne forekomme, at vi har behov for at registrere Persondata om et strafbart forhold i form af underslæb begået af en medarbejder, hvis dette er nødvendigt for at kunne gøre vores krav på erstatning gældende over for medarbejderen.

9.3.8 Også på områder, hvor der kan tænkes at eksistere et retskrav, f.eks. en medarbejders krav på erstatning som følge af en arbejdsskade, kan det være nødvendigt at foretage registreringer af følsomme Persondata til brug for en eventuel sag.

9.4 <u>Behandling af Persondata om tidligere ansatte, herunder om sletning</u>

9.4.1 Vi skal slette Persondata uden unødig forsinkelse. Det kan f.eks. være i den situation, hvor Persondata ikke længere er nødvendige til at opfylde de formål, hvortil de blev indsamlet eller på anden vis behandlet.

9.4.2 Persondata om fratrådte medarbejdere kan opbevares indtil 5 år efter ansættelsesforholdets ophør. Vi vil dog opbevare Persondata i længere tid, såfremt vi har brug for Persondata med henblik på, at retskrav kan fastlægges, gøres gældende eller forsvares, f.eks. ansættelsesretlig sag. I sådanne situationer kan Persondata blive gemt i så lang tid, som det er nødvendigt for at føre sagen. Tilsvarende kan gælde i forbindelse med arbejdsskader.

9.4.3 I forbindelse med en medarbejders fratræden, kan der også opstå spørgsmål om, hvornår vi må videregive de Persondata, som vi ligger inde med. Hvis vi efter anmodning fra en anden virksomhed, hvor medarbejderen har søgt ansættelse, videregiver referencer på medarbejderen, kan dette ske uden samtykke fra medarbejderen, hvis der er tale om almindelige Persondata. Følsomme Persondata må alene videregives med medarbejderens samtykke.

9.5 Information til personen

9.5.1 Vi skal, på det tidspunkt, hvor Persondata indsamles, give medarbejderen en række obligatoriske Persondata. Herudover skal der gives en række supplerende Persondata, der er nødvendige for at sikre en rimelig og gennemsigtig behandling. Hvis vi agter at viderebehandle Persondata til et andet formål end det, som de blev indsamlet til, skal den derfor give medarbejderen Persondata om det andet formål og andre relevante yderligere Persondata som f.eks. tidsrum, indsigt, sletning m.v. Hvis en medarbejder allerede er bekendt med Persondata, gælder oplysningspligten ikke.

9.5.2 I den anden situation skal vi, der indsamler Persondata om en medarbejder, hvor Persondata ikke er indsamlet hos medarbejderen, give medarbejderen en række obligatorisk Persondata. Herudover skal der gives en række supplerende Persondata, der er nødvendige for at sikre en rimelig og gennemsigtig behandling af medarbejderen. De obligatoriske og supplerende Persondata skal gives til medarbejderen inden for nærmere angivne frister.

9.5.3 Hvis vi agter at viderebehandle Persondata til et andet formål end det, som de blev indsamlet til, skal den forud for denne viderebehandling give den ansatte Persondata om det andet formål og andre relevante yderligere Persondata f.eks. om tidsrum, indsigt, sletning mv. Oplysningspligten gælder ikke i en række tilfælde, herunder hvis medarbejderen allerede er bekendt med Persondata.

9.5.4 Jobansøgere vil blive oplyst om, hvis vi kontrollerer dem i kreditoplysningsbureauer som f.eks. RKI, samt om en eventuel opbevaring af kreditoplysningerne, herunder i hvilke tilfælde Persondata opbevares.

9.6 E-mail

9.6.1 Vi stiller internetadgang og brug af e-mail til rådighed for medarbejderen. Medarbejderen har i den forbindelse fået tildelt en særlig e-mail konto.

9.6.2 Brug af e-mail i ikke arbejdsmæssig sammenhæng må kun ske i det omfang, det er foreneligt med den ansattes varetagelse af det daglige arbejde for NT Advokater, og under iagttagelse af disse retningslinjer. Ikke-arbejdsmæssig anvendelse bør således kun ske i meget begrænset omfang.

9.6.3 Vi tillader privat anvendelse af mail og internettet, der er til rådighed på arbejdspladsen. Det er vores holdning, at medarbejderne begrænser det private element til et rimeligt niveau. Det opfattes som et rimeligt niveau, at private mails er korte beskeder og svar, medens det mere omfattende hører privatlivet til.

9.6.4 Vi anser alt, hvad NT Advokaters it-udstyr anvendes til for vores ejendom, med mindre det tydeligt er mærket med angivelsen ”privat”. Det gælder også dine dokumenter og e-mails. Det betyder, at personlige mails sendt/modtaget via din arbejdsmail i princippet kan læses af andre.

9.6.5 Vi kan gennemgå disse Persondata for, at vi kan forfølge berettigede interesser - nemlig hensynet til drift, sikkerhed, genetablering og dokumentation samt hensynet til kontrol af brug - og at hensynet til de ansatte ikke overstiger disse interesser. Med henblik på at sikre overholdelse af retningslinjerne om IT-sikkerhed samt med henblik på at forebygge eller udbedre systemnedbrud kan de IT-ansvarlige åbne enhver e-mail og modtage eksekverbare filer.

9.6.6 I tilfælde af fravær, for eksempel pga. sygdom, ferie eller efter fratrædelse, kan vi give en kollega adgang til medarbejderens e-mail konto.

9.6.7 Vi vil ikke læse private e-mails. Hvis der ved en gennemgang af e-mails findes private e-mails uden relation til os, vil de pågældende e-mails ikke blive læst af andre end den retmæssige modtager. Vi vil ikke læse e-mails markeret med ”privat” med mindre det klart fremgår af omstændigheder, at en konkret e-mail – trods mærkningen – ikke er privat eller har et indhold, som kan være et brud på dine forpligtelser overfor os.

9.6.8 Ved din fratrædelse – frivilligt eller ufrivilligt – vil din e-mail konto hos NT Advokater kun blive holdt aktiv i en periode, der er så kort som mulig fra tidspunktet hvor du ikke længere har adgang til din personlige e-mail konto hos os. Periodens længde vil blive fastsat under hensyntagen til din stilling og funktion og kan højst udgøre 12 måneder. Du vil ikke blive orienteret om endelig nedlukning af din e-mail konto. Snarest muligt efter at du ikke længere kan få adgang til din personlige e-mail konto vil vi sætte et autosvar på e-mail kontoen med besked om din fratrædelse og eventuel anden relevant information. Den aktive e-mail konto vil herefter kun blive anvendt til modtagelse af e-mail, hvis der modtages private e-mails vil vi dog muligvis anvende e-mail kontoen til videre sendelse til din private e-mail konto. Persondata om din personlige e-mail adresse vil hurtigst muligt blive fjernet fra vores hjemmeside og andre offentligt tilgængelige informationssteder. Kun en enkelt – eller ganske få betroede medarbejdere vil herefter få adgang til din personlige e-mail konto.

9.6.9 E-mails skal slettes løbende. E-mails, som kan have betydning for fastlæggelse af et retskrav skal gemmes i 5 år og herefter slettes, med mindre retskrav er rejst mod, eller tænkes rejst. Såfremt en E-mail har generel interesse for et senere sammenligneligt projekt/opgave, kan den gemmes i anonymiseret form udover 5 år.

9.7 Internettet

9.7.1 Vi tillader privat anvendelse af mail og internettet, der er til rådighed på arbejdspladsen på et rimeligt niveau. Internetadgangen kan benyttes til søgning, der ikke strider imod almindelige etiske standarder. Særligt må internetadgangen ikke benyttes til besøg på hjemmesider, hvis indhold er af pornografisk, politisk, ekstremistisk eller diskriminerende karakter for så vidt angår race, køn, etnisksocial oprindelse eller religion. Tilsvarende må medarbejderen ikke ved brug af e-mail sende materiale af ovennævnte karakter.

9.7.2 Der foretages ikke en systematisk, generel kontrol af den enkelte medarbejders anvendelse af systemerne. Medarbejdernes færden på internettet og samtlige mails sendt til og fra hver enkelt medarbejder registreres i en central logfil. Hvis der er mistanke om misbrug, for eksempel afsendelse af private mails i stor stil, eller surfing på internettet i større omfang, forbeholder vi sig ret til at overvåge og gennemgå den enkelte medarbejders aktiviteter og lagrede data på it-systemet.

9.7.3 Tilmelding til særlige internetfaciliteter, såsom abonnementsservice eller portaler m.m. må kun finde sted efter aftale med NT Advokaters ledelse.

9.7.4 Vi anvender firewall/log, der er et systemteknisk værktøj, som bruges af den systemansvarlige i sikkerhedsmæssigt øjemed. De integrerede logningsfaciliteter er nødvendige af hensyn

til systemernes drift og vedligeholdelse samt sikkerhedsovervågning (systemlog). En systemlog kan indeholde Persondata.

9.7.5 En logning af medarbejderes brug af Internet, som foretages i form af en systemlog på en firewall eller en anden aktiv netværkskomponent, er at betragte som en systemlog. Loggen anvendes alene til systemmæssige formål.

9.7.6 Vi kan gennemgå brug af Internettet for tekniske og sikkerhedsmæssige hensyn og hensynet til kontrol af medarbejdernes brug af internettet.

9.8 Hjemmearbejdsplads

9.8.1 Vi har sikret, at ad hoc-arbejdspladser, f.eks. hjemmearbejdspladser for medarbejdere, der arbejder hjemmefra, overholder NT Advokaters IT-sikkerhedsregler, jf. nedenfor.

9.8.2 Hjemmearbejdspladserne skal opfylde følgende krav:

- Opkobling kan kun ske via en VPN forbindelse, der er installeret på den pågældende arbejdsstation,

- Der kan kun ske opkobling via fjernskrivebord, hvor forbindelsen er etableret via den installerede VPN.

9.9 Whistleblower

9.9.1 Vi har oprettet en whistleblower-ordning, hvor alle ansatte via en særlig, uafhængig og selvstændig kanal kan indberette overtrædelser eller potentielle overtrædelser af hvidvaskloven og regler udstedt i medfør heraf.

9.9.2 Indberetninger til ordningen kan foretages anonymt. Vi kan ikke spore den enkelte ansatte, som har foretaget indberetningen, f.eks. via IP-adresse.

9.9.3 Vi er forpligtet til ikke at udsætte en ansat for ufordelagtig behandling eller ufordelagtige følger, som følge af at den ansatte har foretaget en intern underretning om mistanke om hvidvask eller finansiering af terrorisme eller en underretning til SØIK.

9.9.4 Ordningen er anmeldt til Datatilsynet.

9.9.5 Ordningen er "uafhængig" af den daglige ledelse, og den udpegede modtager af indberetningerne er en ansat, der ikke er partner hos os.

9.9.6 Indberetning sker uden om de normale procedurer, eksempelvis uden om virksomhedens almindelige EDB-system hos os.

10 BEHANDLINGSOVERSIGT

10.1 Behandlingsoversigt for oplysninger om klienter / leverandører:

Dataansvarlig	**Advokatvirksomhedens navn, CVR-nr. og kontaktoplysninger**	NT Advokatpartnerselskab CVR-nr.: 35407448 Østbanegade 55, 4. DK-2100 København Ø Danmark T: + 45 35 44 70 00 E: nt@ntadvokater.dk W: www.ntadvokater.dk	
	Den fælles dataansvarlige samt dennes kontaktoplysninger	NT Advokatpartnerselskab CVR-nr.: 35407448 Østbanegade 55, 4. DK-2100 København Ø Danmark T: + 45 35 44 70 00 E: nt@ntadvokater.dk W: www.ntadvokater.dk	
	Den dataansvarliges repræsentant samt dennes kontaktoplysninger		
Formål (ene)	**Behandlingens eller behandlingernes formål**	At foretage almindelig advokatvirksomhed og dermed rådgive klienter i forbindelse med juridiske spørgsmål, tvister og retssager mm. Til brug for dette har vi behov for at behandle persondata, således at vi kan drive advokatvirksomhed på bedst mulig vis.	
Kategorierne af registrerede og kategorierne af Persondata	**Kategori af registrerede personer**	Der behandles oplysninger om følgende kategorier af registrerede personer:	
	Oplysninger, som behandles om de registrerede personer	Oplysninger, som indgår i den specifikke behandling:	
		Stamdata (navn, mobilnummer, adresse, køn, e-	X

		mail mm.)	
		Cpr-numre	X
		Bankoplysninger og formueopgørelser	X
		Transaktionsdata	X
		Regnskaber	X
Modtagerne af Persondata	**Kategorier af modtagere som oplysninger er eller vil blive videregivet til, herunder modtagere i tredjelande og internationale organisationer**	1. Offentlige myndigheder, herunder SKAT 2. Modparter 3. Domstole 4. Vidner 5. Politiet (strafferetlige sager)	
Tredjelande og internationale organisationer	**Oplysninger om overførelse af Persondata til tredjelande eller internationale organisationer**	Nej, der foretages ikke overførsel af data til tredjeland.	
Sletning	**Tidspunkt for sletning af oplysninger**	Vi overvejer konkret, hvor længe Persondata opbevares, inden de slettes. Hensynet til at vi kan varetage vores interesser ved et muligt rådgiveransvar kan indebære, at sagen bør opbevares i 10 år efter afslutning af sagen. Stamdata for klienten bør – for at sikre logisk synergi til også den tidsmæssige opbevaring af sagerne – opbevares i 10 år fra klientforholdets afslutning (de konkrete hvidvaskoplysninger skal dog slettes efter 5 år).	
Tekniske og organisatoriske sikkerhedsforanstaltninger	**Beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger**	Vi har gennemført en risikoanalyse, som ligger til grund for denne Persondatapolitik. Fysisk materiale opbevares i relevant omfang aflåst. Adgang til Persondata skal begrænses til personer, der har et sagligt behov for adgang til Persondata. Det skal være så få personer som muligt, dog med behørigt hensyn til driften – der skal være tilstrækkeligt antal medarbejdere til at sikre driften af de pågældende opgaver ved sygdom, ferier, personaleud-	

		skiftning m.v. Der foreligger et skøn hos virksomheden. Der skal anvendes adgangskode for at få adgang til pc´er og andet elektronisk udstyr med Persondata. Kun de personer, der skal have adgang, må få en kode, og da kun til de systemer, den pågældende har brug for at anvende. De personer, der har adgangskode, må ikke overlade koden til andre eller lade den ligge, så andre kan se den. Ændringen af valgte koder skal foretages mindst en gang hver tredje måned. Der anvendes følgende sikkerhedsstandarder: Firewall: Barracuda NextGeneration Firewall F18 med ATP. Antivirusprogram: Trend Micro Office Scan.

10.2 Behandlingsoversigt for personaleoplysninger:

Dataansvarlig	**Advokatvirksomhedens navn, CVR-nr. og kontaktoplysninger**	NT Advokatpartnerselskab CVR-nr.: 35 40 74 48 Østbanegade 55, 4. DK – 2100 København Ø Danmark T: +45 35 44 70 00 E: nt@ntadvokater.dk W: www.ntadvokater.dk
	Den fælles dataansvarlige samt dennes kontaktoplysninger	NT Advokatpartnerselskab CVR-nr.: 35 40 74 48 Østbanegade 55, 4. DK – 2100 København Ø Danmark T: +45 35 44 70 00 E: nt@ntadvokater.dk W: www.ntadvokater.dk

	Den dataansvarliges repræsentant samt dennes kontaktoplysninger (adresse, hjemmeside, telefonnummer og e-mail)		
Formål (ene)	**Behandlingens eller behandlingernes formål**	Vi har til formål at foretage behandling af persondata til brug for gennemførelse af en ansættelsesaftale. Derudover anvender vi persondata af hensyn til medarbejderens relation til vores virksomhed. Vi anvender persondata til opfyldelse af lovkrav.	
Kategorierne af registrerede og kategorierne af Persondata	**Kategori af registrerede personer**	Der behandles oplysninger om følgende kategorier af registrerede personer: a) Ansøgere b) Ansatte c) Tidligere ansatte	
	Oplysninger, som behandles om de registrerede personer	Oplysninger, som indgår i den specifikke behandling. Beskriv: a) Navn b) Adresse c) Fødselsdato	
		Identifikationsoplysninger	
		Oplysninger vedrørende ansættelsesforholdet til brug for administration, herunder stilling og tjenestested, lønforhold, oplysninger af relevans for lønindeholdelse, personalepapirer, uddannelse og sygefravær.	Stamdata (navn, adresse, e-mail, mobilnummer mm.) Cpr.nummer Uddannelse Udtalelser Tidligere beskæftigelse Løn Skatteoplysninger Bankoplysninger Sygefravær MUS samtaler Straffeattest Billeder af medarbejderen

			Informationer om E-boks.
		Race eller etnisk oprindelse	Nej
		Politisk, religiøs eller filosofisk overbevisning	Nej
		Fagforeningsmæssigt tilhørsforhold	Kan forekomme, se politikkens afsnit 9.3.4 og 9.3.6
		Helbredsoplysninger, herunder genetisk data	Kan forekomme, se politikkens 9.2.13 og 9.3.5
		Biometrisk data med henblik på identifikation	Nej
		Seksuelle forhold	Kan forekomme, se afsnit 4 vedr. informationer om nær familie og pårørende.
		Strafbare forhold	Kan forekomme, se afsnit 4, hvor der indhentes straffeattest.
Modtagerne af Persondata	**Kategorier af modtagere som oplysninger er eller vil blive videregivet til, herunder modtagere i tredjelande og internationale organisationer**	1. Offentlige myndigheder, herunder SKAT 2. Banker 3. Offentlige instanser 4. Borgerservice 5. Pensionsselskaber	
Tredjelande og internationale organisationer	**Oplysninger om overførelse af Persondata til tredjelande eller internationale organisationer**	Nej	
Sletning	**Tidspunkt for sletning af oplysninger**	Persondata om fratrådte medarbejdere kan opbevares indtil 5 år efter ansættelsesforholdets ophør. Vi vil dog opbevare Persondata i længere tid, såfremt vi har brug for Persondata med henblik på, at retskrav kan fastlægges, gøre gældende eller forsvares, f.eks. i en ansættelsesretlig sag. I sådanne situationer kan Persondata blive gemt i så lang tid, som det er nødvendigt for at føre sagen (se politikkens afsnit 9.4.2). Vi opbevarer dog kun personda-	

		ta på et "need to know" og foretager dataminimering, såfremt der ikke er yderligere behov for opbevaring heraf. Hvis du får afslag på din ansøgnin, vil vi hurtigst muligt – og som udgangspunkt senest 6 måneder efter, at du har modtaget afslaget – slette de Persondata, som vi har modtaget og behandlet i forbindelse med rekrutteringsprocessen. Vi vil dog samtidig anmode om dit samtykke til at opbevare dine Persondata fra ansættelsesprocessen i en periode på 3 år til brug for lignende ansættelsesprocesser til stillinger modsvarende den stilling, hvortil du søgte (se politikkens afsnit 9.2.15) Oplysninger om tidligere ansatte slettes senest X år efter afslutningen af den journalperiode, hvor personalesagen er afsluttet.
Tekniske og organisatoriske sikkerhedsforanstaltninger	**Beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger**	Vi har gennemført en risikoanalyse, som ligger til grund for denne Persondatapolitik. Fysisk materiale opbevares i relevant omfang aflåst. Adgang til Persondata skal begrænses til personer, der har et sagligt behov for adgang til Persondata. Det skal være så få personer som muligt, dog med behørigt hensyn til driften – der skal være et tilstrækkeligt antal medarbejdere til at sikre driften at de pågældende opgaver ved sygdom, ferier, personaleudskiftning m.v. Der foreligger et skøn hos virksomheden. Der skal anvendes adgangskode for at få adgang til pc´er og andet elektronisk udstyr med Persondata. Kun de personer, der skal have adgang, må få en kode og da kun til de systemer, den pågældende har brug for at anvende. De personer, der har adgangskode, må ikke overlade koden til andre eller lade din ligge, så andre kan se den. Ændring af valgte koder skal foretages mindst en gang hver tredje måned.

11 COOKIES

11.1 Vi indsamler på forskellig vis Persondata om dig i forbindelse med driften af nt.dk. Vi indhenter Persondata om dig på Hjemmesiden og ved din brug af nt.dk på to måder: Gennem såkaldte 'cookies' og gennem registrering og brug af nt.dk.

11.2 Hvis vi placerer cookies, bliver du informeret om anvendelsen og formålet med at indsamle data via cookies. Før vi placerer cookies på dit udstyr, beder vi om dit samtykke. Nødvendige cookies til sikring af funktionalitet og indstillinger kan dog anvendes uden dit samtykke.

11.3 Du kan få flere Persondata på vores hjemmeside om vores brug af cookies, og om hvordan du kan slette eller afvise dem. Hvis du vil tilbagekalde dit samtykke, så se vejledningen under vores cookie-politik.

11.4 Hvad er en cookie og lignende teknologier?

11.5 Cookies er små informationsenheder, som nt.dk placerer på din computers harddisk, på din tablet, eller på din smarttelefon. Cookies indeholder informationer, som nt.dk bruger til at effektivisere kommunikationen mellem dig og din web-browser. Cookien identificerer ikke dig som individuel bruger, men identificerer din computer.

11.6 Vi benytter lignende teknologier, der lagrer og læser information i browseren eller enheden, og som udnytter lokale enheder og lokal opbevaring, såsom HTML 5 cookies, Flash og andre metoder. Disse teknologier kan fungere på tværs af dine browsere. I visse tilfælde kan brugen af disse teknologier ikke styres af browseren, men kræver specielt værktøj. Vi bruger disse teknologier til at opbevare information, som anvendes til at sikre kvaliteten af vores services og til at opfange uregelmæssigheder i brugen af les.dk.

11.7 Når du besøger nt.dk første gang, modtager du automatisk en cookie. En cookie er en lille tekstfil, der lagres i din web browser, og som registrerer dig som unik bruger. Denne cookie identificerer vores webserver, når du besøger nt.dk, og registrerer anvendelsen heraf.

11.8 En cookie kan indeholde tekst, tal eller fx en dato, men der er ingen Persondata indeholdt i en cookie. Det er ikke et program og kan ikke indeholde virus.

11.9 Vi anvender cookies for at kunne tilpasse og oprette indhold og tjenester, der stemmer overens med dine interesser og ønsker. Vi anvender også cookies til at føre demografiske og brugerrelaterede statistikker, og dermed fastlægge nærmere, hvem der besøger nt.dk. Vi registrerer udelukkende anonyme informationer som IP-numre, antal bytes sendt og modtaget, Internethost, tid, browsertype, -version, og -sprog, osv.

11.10 Hvilke typer af cookies bruger vi og til hvilke formål?

11.11 Vi bruger cookies til

- Statistik, det vil sige til at måle trafikken på nt.dk, herunder antallet af besøg på nt.dk, hvilke domæner den besøgende kommer fra, hvilke sider de ser på nt.dk, og hvilket overordnet geografisk område brugeren befinder sig i.

- Forbedre funktionalitet, det vil sige til at forbedre funktionaliteten og optimere din oplevelse af nt.dk og hjælpe dig med at huske dit brugernavn og adgangskode, så du ikke behøver at logge igen, når du returnerer til nt.dk.

- Integrere med sociale medier, det vil sige til at give dig mulighed for at integrere med sociale medier, som for eksempel Facebook.

- At sikre kvaliteten af vores services og forhindre misbrug og uregelmæssigheder i forbindelse med brugen af vores services.

- Vise specifik markedsføring på nt.dk, som vi tror, at du vil finde interessant.

11.12 Adgang for tredjepart

11.12.1 Vi giver adgang for vores underleverandører til at få indsigt i indholdet af de cookies, som er sat af nt.dk. Denne Information må dog alene anvendes på vegne af os og må ikke anvendes til tredjepartens egne formål.

11.13 Tredjeparts-cookies

11.13.1 nt.dk anvender cookies fra følgende tredjeparter:

- Google Analytics: Anvendes kun på serverniveau og til statistiske formål. Du kan afvise cookies fra Google Analytics ved at klikke her: http://tools.google.com/dlpage/gaoptout

11.14 Sådan sletter du cookies

11.14.1 Du har altid mulighed for at slette cookies, der er gemt på din computer.

- Vejledning i at slette cookies i Microsoft Internet Explorer

- Vejledning i at slette cookies i Mozilla Firefox browser

- Vejledning i at slette cookies på Google Chrome browser
- Vejledning i at slette cookies på Opera browser
- Vejledning i at slette flash cookies - gælder alle browsere

11.15 Google Analytics

11.15.1 Vi bruger Google Analytics for at analysere, hvordan brugerne anvender nt.dk. De Persondata, som cookien indsamler om din brug (trafikdata, herunder din IP-adresse), sendes til og gemmes på Googles servere i USA.

11.15.2 Google Analytics sætter to typer cookies: (a) En persistent cookie der viser om brugeren er tilbagevendende, hvor brugeren kommer fra, hvilken søgemaskine der er brugt, keywords, etc., samt (b) sessionscookies som bruges til at vise, hvornår og hvor længe en bruger er på sitet. Sessionscookies udløber efter hver session, det vil sige, når du lukker din fane eller browser. Google sammenkører ikke din IP-adresse med andre Persondata, Google ligger inde med.

11.16 De fleste browsere tillader dig at slette cookies fra Google Analytics. Læs mere om Google Analytics brug af cookies.

11.16.1 Ved at bruge nt.dk giver du samtykke til, at vi benytter cookies som beskrevet. Hvis du ikke længere ønsker at give samtykke til brugen af cookies, skal du fravælge cookies ved at ændre indstillingerne i din browser.

12 ÆNDRING AF PERSONDATAPOLITIK

12.1 NT Advokater kan til enhver tid og uden varsel ændre denne Persondatapolitik med virkning for fremtiden. Ved sådanne ændringer sker der orientering af NT Advokater' brugere i forbindelse med brugernes login på NT Advokater. NT Advokater' nye Persondatapolitik vil herefter være gældende for din brug af NT Advokater.

13 HENVENDELSER

13.1 Hvis du har spørgsmål til nærværende Persondatapolitik, vores behandling af Persondata, berigtigelse eller dit forhold til os i øvrigt, er du velkommen til at rette henvendelse til os på

følgende adresse: NT Advokatpartnerselskab, CVR-nummer: 35407448, Østbanegade 55, 4., DK - 2100 København Ø, Danmark, T: + 45 35 44 70 00, E: nt@ntadvokater.dk, W: www.ntadvokater.dk

14 DATATILSYNET

14.1 Du har mulighed for at klage til Datatilsynet over NT Advokater' indsamling og behandling af dine Persondata:

DATATILSYNET
BORGERGADE 28, 5.
1300 KØBENHAVN K

TELEFON 3319 3200
MAIL: DT@DATATILSYNET.DK
WWW.DATATILSYNET.DK