**Advokatpartnerselskab**
Kalvebod Brygge 39-41
DK - 1560 København V
Telefon: +45 33 300 200
Fax: +45 33 300 299
www.lundelmersandager.dk
CVR nr. 32 28 39 34

**Torsten Hylleberg**
Advokat
thy@lundelmersandager.dk
Sagsnr. 130.035

# PERSONDATA POLITIK

**Lund Elmer Sandager Advokatpartnerselskab**

Dato: 18. maj 2018

## 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:

Lund Elmer Sandager Advokatpartnerselskab
CVR-nummer: 32283934
Kalvebod Brygge 39 – 41
DK - 1560 København V
Danmark
(Herefter benævnt "LES")

T: + 45 33 300 200
info@les.dk
W: www.les.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.

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

- Navn
- Pasnummer
- Lønindkomst
- Adresse
- Investeringer
- CVR-registrering (enkeltmandsvirksomheder)
- cpr-nr.
- Folkekirkemedlemsskab
- Tingbogen
- Telefonnummer
- Statsborgerskab
- Bilbogen
- E-mail
- Reklamebeskyttelse
- Livsforsikring
- Ægteskabelig status
- Forældre

- Køn
- Børn
- Fødselssted
- Pensionsoplysninger
- Daginstitution
- Skatteoplysninger
- Værnepligt
- Boligform
- Sociale problemer
- Gæld til det offentlige
- Biler
- Lokaliseringsoplysninger
- Lån i pengeinstitut
- Arbejdsplads
- Straffeoplysninger Realkreditlån
- Fagforening
- Sygdomsbehandling
- Værdipapirbeholdning
- A-kasse
- Tidsregistrering

- IP-adresse
- Regnskab
- Bank- og formueopgørelser
- Oplysninger i forbindelse med byggesager

## 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

- Advokatvirksomhed
- Hvidvask
- Forbedring af vores rådgivning og andre tjenesteydelser.
- Tilpasning af vores kommunikation og markedsføring til dig
- Tilpasning af samarbejdspartneres kommunikation og markedsføring til dig
- Direkte markedsføringsaktiviteter.
- Statistik og tilpasning af vores ydelser.
- Optimering af hjemmesiden.
- Gennemførelse af en aftale eller foranstaltninger efter din anmodning herom.
- Administration af din relation til os
- Opfyldelse af lovkrav

- Retskrav

## 6 KILDER

6.1 Persondata indsamles direkte fra dig, modparter, tredjeparter, offentlige myndigheder, banker, forsikringsselskaber, revisorer, domstolene, andre rådgivere, tidligere arbejdsgivere, kollegaer, klienter, dine it-enheder som smartphone, tablet eller computer og fra de transaktioner, som du gennemfører hos os.

## 7 DEN REGISTREREDES RETTIGHEDER

7.1 Håndtering af begæringer fra den registrerede

7.1.1 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.

7.2 Indsigtsretten

7.2.1 Den registrerede har – som udgangspunkt - 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 at få udleveret en udskrift eller en kopi af Persondata.

7.2.2 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.

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

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

7.2.5 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.

7.2.6 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 (medmindre vi fx har foretaget indberetning til Hvidvasksekretariatet i SØIK i medfør af hvidvaskloven, er meddelt forsvarerpålæg efter retsplejeloven mv.).

7.3 <u>Dataportabilitet</u>

7.3.1 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 os.

7.3.2 Den registrerede har desuden ret til selv at transmittere disse oplysninger til en anden dataansvarlig uden hindring fra os, når behandlingen er baseret på samtykke eller en kontrakt, 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.

7.3.3 Adgangen til dataportabilitet – som navnlig kan være relevant ved advokatskifte – omfatter kun oplysninger, den registrerede selv har givet, og vil kun omfatte behandlinger, der foretages automatisk, og som baserer sig på et samtykke eller en kontrakt med den registrerede.

7.3.4 Dataportabilitet giver den registrerede mulighed for at overføre og videreanvende egne oplysninger til egne formål og på tværs af forskellige tjenester. Denne ret gør det nemmere for den registrerede at flytte, kopiere eller transmittere Persondata fra ét IT-miljø til et andet uden besvær.

7.4 Ret til berigtigelse

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

7.4.2 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.

7.4.3 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.

7.5 Retten til at blive glemt

7.5.1 Den registrerede har efter databeskyttelsesforordningens artikel 17 i visse tilfælde ret til uden unødig forsinkelse at få Persondata om sig selv registreret hos LES slettet. LES har i så fald pligt til uden unødig forsinkelse at slette Persondata.

7.5.2 Den registrerede kan blandt andet kræve sig slettet, hvis Persondata ikke længere er nødvendige til at opfylde de formål, hvortil de blev indsamlet, hvis den registreredes legitime interesser i at gøre indsigelse mod behandlingen overstiger den dataansvarliges legitime interesser i at opbevare Persondata, eller hvis Persondata er blevet behandlet ulovligt.

7.5.3 I tråd med betingelserne kan der efter artikel 17, stk. 3, ikke 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.

7.5.4 Det er vores vurdering, at "Retten til at blive glemt" sjældent vil være relevant i forhold til vores sagsbehandling. Den kan dog eksempelvis tænkes anvendt, hvis Persondataene oprindeligt slet ikke har været nødvendige for sagens behandling, og derfor slet ikke burde være 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 oplysninger for at kunne imødegå et eventuelt retskrav fra klienter (fx en klage- eller ansvarssag) eller for at kunne opfylde vores advokatetiske forpligtelse vedrørende interessekonflikttjek.

7.5.5 Hvis advokatvirksomheden efter artikel 17 er forpligtet til at slette Persondata, som har været overladt til andre dataansvarlige eller databehandlere, skal vi instruere vore(s) databehandler(e) om at slette oplysningerne, samt underrette de andre dataansvarlige, som behandler Persondata, om, at den registrerede har anmodet om at få slettet alle link til eller kopier eller gengivelser af de pågældende Persondata, jf. artikel 19.

7.6 <u>Ret til indsigelse – samt ret til ikke at være genstand for automatiserede afgørelser</u>

7.6.1 Det følger af databeskyttelsesforordningens artikel 21, at den registrerede til enhver tid har ret til at gøre indsigelse mod behandling af Persondata om vedkommende, 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 interesse, eller hvis behandlingen er nødvendig for at forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse.

7.6.2 Hvis den registrerede gør 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.

7.6.3 Det er vores vurdering, at denne bestemmelse kun i begrænset omfang vil komme i spil i forhold til vores sagsbehandling, fordi vores sagsbehandling 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.

7.6.4 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.

7.6.5 Som supplement 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.

7.6.6 Et praktisk eksempel på profilering kunne være, at klienten afkrydser et spørgeskema, og at vi på basis af dette træffer en afgørelse om, hvorvidt sagen bør opretholdes/videreføres. Hvis bestemmelsen skal finde anvendelse, kræver det dog, at der ikke involveres medarbejdere fra LES i en sådan beslutningsproces.

7.6.7 Også denne bestemmelse indeholder en række undtagelser, jf. artikel 22, stk. 2. Den registreredes ret gælder blandt andet 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.

7.7 <u>Ret til begrænsning af behandlingsaktiviteterne</u>

7.7.1 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.

7.7.2 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.

7.7.3 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.

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

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

## 8 BEHANDLINGSPRINCIPPER

### 8.1 Behandlingsprincipper

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

8.1.2 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.

8.1.3 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.

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

8.1.5 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.

8.1.6 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.

8.2 Risikoanalyse

8.2.1 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.

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

8.3 Konsekvensanalyser vedrørende databeskyttelse (DPIA)

8.3.1 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.

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

8.3.3 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

8.3.4 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.

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

8.3.6 Vi vil dog foretage en konsekvensanalyse, såfremt vi påbegynder – i stort omfang - fx i en specialistfunktion med mange advokater hovedsageligt at arbejde med personfølsomme oplysninger.

8.3.7 Gennemføres en konsekvensanalyse, vil resultatet af analysen blive taget i betragtning, når der skal træffes passende foranstaltninger med henblik på at påvise, at vores behandling af Persondata overholder databeskyttelsesforordningen. Hvis det fremgår af en konsekvensanalyse vedrørende databeskyttelse, at vores behandlingsaktiviteter indebærer en høj risiko, som vi ikke kan begrænse ved passende foranstaltninger med hensyn til tilgængelig teknologi og gennemførelsesomkostninger, vil vi høre tilsynsmyndigheden forud for behandlingen.

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

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

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

8.4.3 Datatilsynet har også i sin "Vejledning om databeskyttelsesrådgivere" udtalt, at virksomheder, der behandler Persondata som en biaktivitet, ikke er forpligtede til at udpege en databeskyttelsesrådgiver, og at en enkelt advokats behandling af klientoplysninger skal anses som en sådan biaktivitet. Vores behandling af Persondata anses som en biaktivitet.

8.4.4 Vi behandler ikke Persondata i større omfang, hvor der er en høj risiko for datasubjektet

*8.4.5* Advokatsamfundet anfører i vejledning om advokaters behandling af Persondata (file://dafs01/da_tshomesr2$/datbj/Downloads/2018%20Vejledning%20Person-data_Master%20(4).pdf ) følgende vedrørende forsvarsadvokater:

*"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 Persondata ikke er forsvarsadvokatens kerneaktivitet"*

8.4.6 Vi har derfor valgt ikke at udpege en databeskyttelsesrådgiver (DPO).

8.4.7 Som følge af princippet om ansvarlighed, har vi – uanset om vi agerer som dataansvarlig eller databehandler - udpeget en person i vores organisation, der har som ansvarsområde at foretage de vurderinger og den rådgivning, der sædvanligvis vil blive varetaget af en databeskyttelsesrådgiver. Denne Persondataansvarlige har ansvaret for og skal håndtere databeskyttelsesspørgsmål.

8.5 Videregivelse til andre tjenester

8.5.1 Der videregives ikke Persondata til sociale netværk.

8.6 Anden videregivelse

8.6.1 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.

8.7 Profilering

8.7.1 Vi anvender ikke dine Persondata til profilering.

8.8 Generelle tekniske foranstaltninger

8.8.1 Datatilsynets IT-sikkerhedstekster danner udgangspunkt for de overvejelser og vurderinger, som vi har foretaget efter databeskyttelsesforordningen vedrørende generelle tekniske og sikkerhedsmæssige foranstaltninger.

8.8.2 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 sagsbehandlere har adgang til alle sager. Vi har vurderet, at dette findes nødvendigt, da alle medarbejdere i virksomheden er involverede i sagerne.

8.8.3 Medarbejdere, der håndterer Persondata, har fået instruktion og oplæring i, hvad de må gøre med Persondata, og hvordan de skal beskytte Persondata.

8.8.4 Der anvendes adgangskode for at få adgang til pc'er og andet elektronisk udstyr med Persondata. Kun de personer, der skal have adgang, får en adgangskode 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. Kontrol af tildelte koder bør foretages mindst en gang hvert halve år.

8.8.5 Følsomme Persondata eller fortrolige oplysninger i sager eller vedrørende klienter, som findes på papir – fx i kartoteker og ringbind – vil blive opbevaret aflåst, når de ikke er i brug.

8.8.6 Når fysiske dokumenter smides ud, anvendes der makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til Persondata.

8.8.7 Det vil blive registreret, 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.

8.8.8 Vi har udpeget en ekstern leverandør, der kan overvåge sådanne forgæves adgangsforsøg. Under hensyntagen til den teknologiske udvikling vil vi anskaffe programmel, der kan afklare, hvem der har forsøgt at skaffe sig adgang til Persondata.

8.8.9 Hvis Persondata lagres på en USB-nøgle, vil Persondata blive beskyttet. Det kan ske enten ved at låse USB-nøglen med en kode, eller ved at opbevare USB-nøglen i en aflåst skuffe eller skab. Tilsvarende gælder ved opbevaring af Persondata på andre bærbare datamedier, herunder bærbare PC'er og smartphones.

8.8.10 Elektroniske medier, der kobles til internettet, vil have en opdateret firewall og viruskontrol installeret.

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

8.8.12 Hvis der benyttes hjemmesideformularer, hvor følsomme Persondata eller personnummer kan indtastes og fremsendes, vil der blive anvendt kryptering.

8.8.13 Systemer, applikationer mv., der ikke anvendes, vil løbende blive slettet.

8.8.14 Der må ikke ske sammenblanding af arbejdsrelaterede oplysninger og private oplysninger på samme medie. Dog kan der forekomme private e-mails i vores mail-system.

8.8.15 Hvis følsomme Persondata eller personnumre sendes med e-mail via internettet, vil sådanne e-mails blive krypteret i den udtrækning, dette er praktisk muligt. Vi tilstræber i videst muligt omfang at udelade de sidste 4 cifre i cpr. Vurderes det dog, at de sidste 4 cifre i cpr.nr. er strengt nødvendigt, foretages der en kryptering af den e-mail

8.8.16 I forbindelse med reparation og service af dataudstyr, der indeholder Persondata, og når datamedier skal sælges eller kasseres, vil der blive truffet fornødne foranstaltninger, så oplysninger ikke kan komme til uvedkommendes kendskab.

8.8.17 I de situationer, hvor en computer indleveres til reparation, og hvor der på computeren ligger Persondata, vil det ved aftale og kontrol blive sikret, at reparatører ikke uretmæssigt tilgår Persondata. Det kan fx være ved brug af fortrolighedserklæringer.

8.8.18 Ved brug af en ekstern databehandler til håndtering af Persondata, skal der underskrives en skriftlig databehandleraftale mellem LES 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.

8.8.19 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.

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

8.9 <u>Implementering i organisationen</u>

8.9.1 Vi har udarbejdet leveregler, som gælder sideløbende med denne Persondatapolitik.

8.10 Back-up

8.10.1 Vi 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.

8.10.2 Vi foretager følgende typer af backup:

- 1) backup 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.

- 2) backup klon. Denne backup-strategi skaber en perfekt kopi af hver enhed på netværket.

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

8.10.3 Alle backup data og filer overskrives med intervaller på 30 dage. Det er ikke teknisk muligt at gennemføre sletning af enkelte filer på en foretagen backup, inden sådan overskrivning sker. Det vil sige, at har du anmodet os om sletning af dine Persondata, vil sådanne Persondata blive slettet i live miljø, jf. nedenfor, men vil forblive på backup indtil den specifikke backup efter 30 dage er overskrevet. Vi 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 backup, såfremt dine data er blevet slettet i henhold til din "ret til at blive glemt".

## 9 GENERELLE BEHANDLINGSREGLER

9.1 Overordnet

9.1.1 Generelle Behandlingsregler 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. Generelle Behandlingsregler er derudover udtryk for, hvordan vi opfylder dokumentationskravene i databeskyttelsesforordningen.

9.1.2 Hertil hører også fagspecifikke guidelines målrettet særlige sagsområder – herunder:

- Insolvens

- Inkasso
- Strafferet
- Familieret
- Ejendomshandler
- M & A – (due diligence processer)
- Erstatnings- og Forsikringsret (herunder personskade)
- Ansættelsesret

9.1.3 Med udspring i nærværende Generelle Behandlingsregler tager de fagspecifikke behandlingsregler fat i problemstillinger, der navnlig viser sig på de pågældende fagspecifikke områder.

9.2 Dataansvarlig

9.2.1 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, hvordan Persondata behandles, til hvilket formål Persondata behandles, og hvor længe Persondata skal opbevares.

9.2.2 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, fx i forbindelse med behandling af konkursboer.

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

*"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".*

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

9.2.5 For så vidt angår fx en 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.

9.2.6 Tilsvarende kan det overvejes, om vi er databehandler, hvis vi administrerer en ejendom, men udelukkende opkræver leje og indgår lejekontrakter på udlejers vegne uden selvstændig stillingtagen til kontraktbetingelserne mv. Hvis vi til gengæld også udfærdiger lejekontrakter og vurderer lejeres eventuelle misligholdelse samt behandler udsættelsessager, må vi snarere vurderes at være dataansvarlig.

9.2.7 Vores Persondatapolitik tager i det følgende udgangspunkt i, at vi er dataansvarlig for vores sagsbehandling.

9.3 <u>Databehandler</u>

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

9.3.2 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.

9.3.3 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.

9.3.4 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.

9.3.5 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.

9.3.6 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 (fx. indsamle, registrere, opbevare, videregive eller slette) Persondata efter instruks fra os som dataansvarlig.

9.3.7 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 fx 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 (fx 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.

9.3.8 Spørgsmålet er med andre ord, om vi alene er interesseret i at modtage det færdige produkt (fx 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.

9.3.9 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.

9.3.10 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.

9.4 <u>Databehandleraftale</u>

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

9.4.2 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.

9.4.3 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.

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

9.5 Overførsel til tredjelande

9.5.1 Ved brug af en databehandler, indhentelse af responsum fra en advokat uden for EU/EØS eller ved kommunikation med modparter vil vi vurdere, om overførslen 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.

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

9.5.3 Overførsel 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 Standardmodel Klausulaftaler, eller
- at der er et tilstrækkeligt beskyttelsesniveau fastsat ved godkendte bindende virksomhedsregler

9.5.4 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

9.6 Databehandlere

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

9.6.2 Databehandling foretages inden for den Europæiske Union.

9.6.3 Databehandleren handler alene efter instruks fra os.

9.6.4 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.

9.7 Behandlingshjemmel

9.7.1 Vi må kun behandle Persondata – herunder indsamle Persondata – hvis der er en hjemmel til behandlingen.

9.7.2 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. Til gengæld vil vi inden for vores opdrag som udgangspunkt have hjemmel til at behandle alle de Persondata, der er nødvendige til brug for løsning af opdraget.

9.7.3 Øvrige relevante hjemler til at behandle Persondata følger navnlig af databeskyttelsesforordningens artikel 6, stk. 1, litra a-c og litra f, samt af artikel 9, stk. 2, litra a og f. 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.

9.7.4 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.

9.7.5 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.

9.7.6 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.

9.8 Generelle principper - sagsbehandlingen

9.8.1 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. Det vil som det klare udgangspunkt være langt mere hensigtsmæssigt, at advokatvirksomheden baserer sagsbehandling på en anden behandlingshjemmel – eksempelvis i bestemmelserne om opfyldelse af en kontrakt og/eller fastlæggelsen af et retskrav (artikel 6, stk. 1, litra b-c, og artikel 9, stk. 2, litra f). Samtykke kan nemlig tilbagekaldes og giver i øvrigt heller ikke selvstændig mening ved siden af opdraget/aftalen om bistand.

9.8.2 Samtykke vil dog være relevant, hvis advokatvirksomheden ønsker at markedsføre sig på grundlag af den konkrete sag. Advokatnævnet har udtalt, at der skal indhentes et udtrykkeligt samtykke fra klienten til at lave nyheder til hjemmesider og sociale medier, fordi mange ud fra sagsfremstillingen vil kunne genkende klienten. Dette gælder også, selvom alle navne og adresser mv. er anonymiseret. Genkendelse kan give anledning til personlige kommentarer fra pågældendes venskabs- og bekendtskabskreds, som måske ikke er tilstrækkelig opmærksom på anonymisering.

9.8.3 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.

9.8.4 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 LES være opmærksomme på de særlige regler, der gælder for overførsel af Persondata til tredjelande.

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

9.8.6 Vi vil som udgangspunkt undgå at basere vores behandling af Persondata på et samtykke fra klienten. Samtykke giver ikke selvstændig mening ved siden af opdraget/aftalen om bistand. Samtykke vil dog blive indhentet, såfremt vi ønsker at markedsføre os på grundlag af den konkrete sag. Advokatnævnet har udtalt, at der skal indhentes et udtrykkeligt samtykke fra klienten til at lave nyheder til hjemmesider og sociale medier, fordi mange ud fra sagsfremstillingen vil kunne genkende klienten. Dette gælder også, selvom alle navne og adresser mv. er anonymiseret. Genkendelse kan give anledning til personlige kommentarer fra pågældendes venskabs- og bekendtskabskreds, som måske ikke er tilstrækkelig opmærksom på anonymisering.

9.9 Oplysningspligt - klient

9.9.1 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. Det forudsætter en konkret vurdering og stillingtagen.

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

9.9.3 I velkomstbrevet henvises der til vores Persondatapolitik, hvori følgende er beskrevet:

- 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.

9.9.4 For de tilfælde, hvor vores behandling alene er baseret på en interesseafvejning eller udførelse af opgaver i samfundets interesse – eller hvor der er tale om behandling af Persondata med henblik på direkte markedsføring - fremgår det dog 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. I sådanne tilfælde vil vi sende særskilt oplysning om behandlingen til klienten.

9.10 Oplysningspligt - modparter

9.10.1 Så længe behandling af Persondata vedrørende modparten ligger inden for det, som er nødvendigt af hensyn til at løse opdraget, og så længe oplysningerne er omfattet af advokatens tavshedspligt, har vi ikke en oplysningsforpligtelse overfor modparten.

9.10.2 Såfremt behandlingen af Persondata vedrørende modparten ikke ligger inden for det, som er nødvendigt af hensyn til at løse opdraget, og oplysningerne ikke er omfattet af advokatens tavshedspligt, vil vi opfylde vores oplysningsforpligtelse direkte overfor modparten eller modpartens advokat.

*9.10.3* Advokatsamfundet har i vejledning om advokaters behandling af Persondata anført følgende vedrørende opfyldelse af oplysningspligten over for modparten:

”*Modtager du Persondata om modparten direkte fra denne, skal du naturligvis være opmærksom på forbuddet mod henvendelse direkte til modparten, hvor denne er repræsenteret ved advokat…..*

*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…..*

*Af afgørende betydning for at fravige forbuddet mod direkte henvendelse til modparten er efter rådets opfattelse, at oplysningspligten alene kan opfyldes ved, at 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 Persondata 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."*

9.11 Oplysningspligt – tredjeparter, dog ikke modparten

9.12 Begrebet tredjemand defineres i databeskyttelsesforordningen som:

*"En anden fysisk eller juridisk person, offentlig myndighed eller institution eller ethvert andet organ end den registrerede, den dataansvarlige, databehandleren og de personer under den dataansvarliges eller databehandlerens direkte myndighed, der er beføjet til at behandle Persondata".*

9.12.1 Tredjeparter kan f.eks. være vidner, familiemedlemmer, naboer, arbejdsgiver, kolleger, virksomheders ansatte mv., samt bipersoner, herunder skønsmænd, læger, sagsbehandlere, revisorer, konsulenter m.v.

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

9.12.3 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.

9.12.4 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 Datatilsynets praksis fortolket således, 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.

9.12.5 Det betyder eksempelvis, at vi ved opkøb af en ejendom ikke nødvendigvis skal underrette alle de enkelte lejere om, at vi registrerer Persondata om deres navn og lejekontrakt. Underretningspligten vil afhænge af karakteren af Persondata. I en klagesag med sensitive oplysninger, vil vi overveje oplysningspligten opfyldt i det omfang vores tavshedspligt ikke påbyder, at oplysningerne holdes fortroligt.

9.12.6 Oplysningspligten vil da konkret blive opfyldt ved, at vi i en autosignatur indsætter et link til denne Persondatapolitik.

9.12.7 Se i øvrigt Advokatsamfundets vejledning om advokaters behandling af Persondata: file://dafs01/da_tshomesr2$/datbj/Downloads/2018%20Vejledning%20Persondata_Master%20(2).pdf

9.13 Hvidvask

9.13.1 I tillæg til reglerne i databeskyttelsesforordningen og databeskyttelsesloven, findes der særregler om behandling af Persondata i relation til indhentelse og kontrol af Persondata i relation til lov om hvidvask (lov nr. 651 af 8. juni 2017).

9.13.2 Advokatsamfundet har i sin vejledning "Vejledning til Hvidvaskloven 2017" fastsat nærmere regler for behandling af Persondata indhentet og behandlet i relation til hvidvask. Vi har i denne forbindelse udarbejdet interne retningslinjer for behandling af hvidvask oplysninger.

9.13.3 Vi skal i medfør af hvidvaskloven opbevare følgende Persondata i fem år fra klientforholdets ophør. Dette vedrører:

- Persondata indhentet i forbindelse med opfyldelse af kravene om kunde-kendskabsprocedurer 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.

9.13.4 Vi skal inden etablering af en forretningsforbindelse med en klient og inden gennemførelse af en enkeltstående transaktion for fysiske personer informere klienten om, hvad LES er forpligtet til at foretage os vedrørende de Persondata, som vi indhenter efter hvidvaskloven. Informationen vil blive givet ved, at vi udleverer en af advokatvirksomheden udarbejdet generel politik herom. Oplysningspligten efter databeskyttelsesforordningen gælder således også i forhold til de Persondata, som advokatvirksomheden indhenter i medfør af hvidvaskloven.

9.13.5 Oplysningerne vil altid blive givet direkte til klienten og vil desuden kunne findes på vores hjemmeside.

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

9.13.7 Persondata indhentet i relation til hvidvask vil blive opbevaret separat fra de enkelte sager.

9.13.8 Persondata indsamlet og behandlet til opfyldelse af hvidvaskloven skal opbevares i fem år fra klientforholdets ophør, hvorefter de skal slettes. Bestemmelsen om sletning må dog fortolkes sådan, at oplysninger, der – udover til brug ved opfyldelsen af hvidvasklovens krav – tillige er indhentet som en nødvendig del af advokatens bistand til klienten, ikke skal slettes, medmindre der i øvrigt gælder en sletningsforpligtelse. Det omfatter eksempelvis cpr. nr., der tillige er indhentet til brug for berigtigelse af en ejendomshandel.

9.13.9 Den tidsmæssige ramme i sletningsreglen fortolkes i øvrigt stramt. Det betyder, at der løbende – og som minimum månedsvis – skal foretages sletning af alle de oplysninger, der er registreret mere end 5 år efter fra klientforholdets ophør.

9.14 <u>Løbende indsamling og videregivelse af oplysninger</u>

9.14.1 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.

9.14.2 Når der indsamles Persondata på sagen, skal vi navnlig være opmærksom 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.

9.14.3 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.

9.14.4 Vi vurderer, at dette princip også er vigtigt i forhold til at begrænse yderligere udbredelse af Persondata. Eksempelvis forudsætter de processuelle regler, der gælder for retssager, voldgift mv., at alle aktører i sagen har kendskab til alle Persondata, der indgår heri. Domstolene vil derfor også forudsætte, at advokater alene inddrager Persondata – herunder oplysninger om tredjeparter – som er relevante for den anlagte sag.

9.14.5 I udvekslingen af Persondata vil vi generelt være opmærksomme på kommunikationsformen. Datatilsynet anbefaler, at følsomme Persondata og oplysninger om personnummer, der sendes med e-mail, beskyttes med kryptering.

9.15 Sletning - hvornår

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

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

9.15.3 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 ophørt, hvorefter de 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 vil blive overvejet, 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 eller lignende, 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).

- Kontaktinformation vil blive slettet løbende. E-mails, som kan have betydning for fastlæggelse af et retskrav, skal gemmes i 5 år og herefter slettes, medmindre retskrav er rejst mod eller tænkes rejst af os.

- Særlige overvejelser skal foretages, 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, idet et bo skal genoptages med efterudlodning, hvis der dukker nye aktiver op. Vi vil 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.

- De advokatetiske regler om interessekonflikter kan endvidere betyde, at vi selv efter sletning af sagens akter (f.eks. 10 år efter afslutning) kan have behov for at gemme visse stamoplysninger om klient og modpart samt grundlæggende oplysninger om sagens karakter og genstand. Har vi fx rådgivet en part i forbindelse med indgåelsen af en ejeraftale, kan vi ikke repræsentere en anden part i en tvist om samme ejeraftale, uanset om der måtte være gået mere end 10 år, når tvisten opstår.

9.15.4 Såvel hensynene som skæringstidspunkterne er forskellige.

9.15.5 Sletningsreglerne betyder også, 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.

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

9.16 Sletning - hvordan

9.16.1 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, mobiltelefoner, tablets, USB-nøgler mv., samt backup.

9.16.2 For at lette sletningsproceduren har vi instrueret vores medarbejdere om, at alt fysisk materiale, hvor det er praktisk gennemførligt, scannes til den elektroniske sag, og dernæst makuleres eller tilbagesendes til klienten.

9.16.3 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.

9.16.4 Derved kan den samlede sag til sin tid (efter endt opbevaringsperiode) i det hele blive slettet fra vores sagsstyringssystem.

9.16.5 I tilfælde, hvor alle Persondata om en klient – og ikke kun en konkret sag – skal slettes, vil den elektroniske formular med klientens stamoplysninger blive slettet fra vores sagsstyringssystem, ligesom de hertil hørende registreringer vedrørende klienten i alle øvrige systemer vil blive slettet. Der skal dog ved denne sletning være fokus på reglerne om interessekonflikter, som kan betyde, at visse stamoplysninger gemmes længere.

9.16.6 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.

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

9.17 Sletning - backup

9.17.1 Det må antages, at der ikke skal ske sletning af indhold i vores tidligere generationer af en backup (sikkerhedskopi). Dette skyldes, at vi selvstændigt for sikkerhedskopier har fastsat en procedure for løbende sletning/overskrivning af de gamle sikkerhedskopier, så Persondata, der er slettet i et IT-system, automatisk forsvinder fra sikkerhedskopier, når disse slettes eller over skrives.

9.17.2 Forpligtelsen til at slette Persondata forudsætter også, at vi, hvis vi bliver nødt til at tage en backup i brug, ved ibrugtagningen sørger for at slette de Persondata, der i mellemtiden er blevet slettet i henhold til den generelle slettepolitik eller efter en konkret indsigelse.

9.18 IP-adresser og browserindstillinger

9.18.1 I forbindelse med hvert besøg på les.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 vi 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.

9.19 Nyhedsbrev

9.19.1 Hvis du tilmelder dig LES' nyhedsbreve, registreres dine Persondata direkte hos os. Udsendelse af nyhedsbreve vil blive baseret på et samtykke, medmindre udsendelsen har hjemmel i markedsføringslovens § 10, stk. 2. Ønsker du ikke længere at modtage nyhedsbreve fra os, kan du afmelde dig ved at logge ind på din profil og dér redigere dine Persondata.

9.20 Anonymisering

9.20.1 Vi anvender anonymisering af data fra klienter for statiske og forskningsmæssige formål, samt for at kunne forbedre systemer, processor og produkter.

9.20.2 Vi anonymiserer således, at muligheden for at identificere enkeltpersoner i et datasæt fjernes. Der foretages således en uigenkaldelig anonymisering, således at Persondata bliver gjort anonyme på en sådan måde, at personen ikke længere kan identificeres. Fx navn, adresse eller personnummer erstattet af en kode, et løbenummer el.lign., der ikke længere kan føres tilbage til de oprindelige individuelle Persondata. Koder tildeles tilfældigt og kan ikke føres tilbage ved brug af lister, nøgler el.lign., der viser sammenhængen mellem løbenummer og de egentlige identifikationsoplysninger. Dette betyder også, at Persondata, som foreligger i form af billede, personens stemme, fingeraftryk eller genetiske kendetegn, slettes i forbindelse med anonymiseringen.

## 10 FAGSPECIFIKKE SAGSBEHANDLINGSREGLER INSOLVENS

10.1 I forbindelse med vores behandling af insolvenssager gælder vores Generelle Behandlingsregler, jf. pkt. 9 ovenfor. I tillæg hertil gælder følgende fagspecifikke sagsbehandlingsregler for vores behandling af insolvenssager.

10.2 I forbindelse med sagsbehandlingen i Insolvens modtages en lang række Persondata, herunder stamdata (almindelige Persondata som fx navn, adresse, e-mail, fødselsdato, køn, lokalisation, m.v.), billeder, følsomme oplysninger, cpr.nr. og oplysninger om strafbare og sociale forhold.

10.3 Personoplysninger, der behandles i Insolvens, herunder modtages, indsamles, bruges, videregives og opbevares, må som udgangspunkt alene bruges med insolvens behandling for øje. Skal oplysningerne anvendes til anden behandling hos os, vil behandlingshjemmel og behandlingsprincipper særskilt blive vurderet for disse nye formål. Vi kan videreanvende Persondata til andre legitime formål, hvis der er tale om formål, der ikke er uforenelige med det oprindelige formål.

10.4 Behandlingen vil altid ske efter et need-to-know princip.

10.5 Vi vil løbende vurdere, om der er hjemmel til at behandle og videregive de modtagne Persondata, herunder om der er hjemmel til behandling og videregivelse af cpr.nr., følsomme oplysninger, oplysninger om strafbare forhold og lovovertrædelser. Vi har gennemført passende procedurer herfor.

10.6 Vi vil begrænse behandling og videregivelse af oplysninger mest muligt, særligt for så vidt angår behandling og videregivelse af følsomme oplysninger, cpr.nr. samt oplysninger om strafbare forhold og lovovertrædelser. På formularer, fx åbningsstatus, boopgørelser eller andre formularer med rubrikker, der forudsætter cpr.nr. indsat, skal

disse oplysninger som udgangspunkt fjernes, inden de oversendes til myndigheder eller parter, der ikke har hjemmel til at behandle sådanne oplysninger. Anvendelse af cpr.nr. vil derudover søges minimeret.

10.7 Oprindelige Persondata

- Oprindelige Persondata er de Persondata, som var indsamlet eller behandlet inden konkursdekretet afsigelse (”Oprindelig Persondata”).

- Videregivelse eller overdragelse til os af Oprindelige Persondata fra konkursbo, hvor vi agerer som kurator, anses som almindelig succession.

- Videregivelsen eller overdragelsen af Oprindelige Persondata udløser ikke i sig selv en oplysningspligt.

- Kurator kan behandle Oprindelige Persondata i henhold til det formål, som var gældende for disse Persondata på tidspunktet for boets indhentelse af de pågældende Persondata.

- Behandling skal i øvrigt ske i henhold til de personpolitikker, som var gældende på tidspunktet for indhentelse af de Oprindelige Persondata.

- Oprindelige Persondata opbevares elektronisk adskilt fra andre Persondata i vores sagsstyringssystem, herunder særskilt fra Efterfølgende Persondata, se forklaring nedenfor.

10.8 Efterfølgende Persondata

- Efterfølgende Persondata er de Persondata, som indsamles eller behandles af kurator efter konkursdekretets afsigelse, herunder de Oprindelige Persondata, som efterfølgende inddrages i behandlingen af konkursboet (”Efterfølgende Persondata”).

- Kurator skal foretage en konkret vurdering af om opbevaring af hver enkelt type af Persondata, som kurator modtager som led i bo-behandlingen, er lovlig.

- Opbevaring kræver et behandlingsgrundlag. Som udgangspunkt kan disse Persondata behandles med hjemmel i interesseafvejningsreglen eller for, at retskrav kan fastlægges, gøres gældende eller forsvares. Det er dog et krav, at behandlingen ligger indenfor sædvanligt arbejdsområde for kurator.

- Behandlingen af disse regler sker i øvrigt i henhold til vores Generelle Behandlingsregler.

- Efterfølgende Persondata opbevares i vores sagsstyringssystem særskilt fra Oprindelige Persondata.

10.9 Gennemgang af e-mails fra ledelse/ansatte i konkursbo

- Kurators gennemgang af e-mails fra ledelse/ansatte i konkursboet anses som en selvstændig behandling.

- For ikke-følsomme Persondata anvendes interesseafvejningsreglen som behandlingsgrundlag. For følsomme Persondata kan behandling ske med henvisning til, at behandlingen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares.

- Personen skal ikke oplyses om, at behandlingen finder sted, eller til hvilket formål behandlingen sker, da behandlingen vil være omfattet af vores tavshedspligt.

- Kurator skal iagttage gældende regler om brevhemmelighed.

- Ved anden gennemgang af e-mails end til brug for gennemgang af konkursboet som kurator, skal kurator vurdere formål og behandlingsgrundlag på ny samt iagttage oplysningspligten over for personen.

10.10 Videregivelse af Persondata til potentielle købere

- Kurator skal altid iagttage proportionalitetsprincippet, det vil sige, at der ikke må videregives flere Persondata end påkrævet for at kunne opfylde formålet med virksomhedsoverdragelsen.

- For ikke-følsomme Persondata anvendes interesseafvejningsreglen som behandlingsgrundlag. Følsomme Persondata må ikke overdrages uden samtykke fra personen.

- Ved salg af hele boet, eller den del af boet som Persondata vedrører, gælder reglen om succession. Køber indtræder således i boets hidtidige retsstilling. Der skal være tale om salg af en selvstændig del af konkursboet, som kan stå alene, de overdragne aktiviteter skal videreføres og alle rettigheder og forpligtelser i forhold til de overdragne aktiviteter skal overdrages til køber (grenspaltning).

- Ved overdragelse af et enkeltstående aktiv finder reglerne om succession ikke anvendelse. Ikke-følsomme Persondata kan overdrages med henvisning til interesseafvejningsreglen, for så vidt overdragelsen har relevans for driften af det overdragne enkeltstående aktiv. Køber skal dog opfylde sin oplysningsforpligtelse og selvstændigt have et behandlingsgrundlag for at kunne databehandle.

- Særlige regler for videregivelse til brug for markedsføring (Robinson listen) samt salg af kundedatabaser.

10.11 Hosting af Persondata hos 3. part eller brug af cloud leverandør

- Hosting provider vil agere som databehandler.

- Der skal indgås en databehandleraftale med hosting provider, medmindre aftalen allerede er indgået med os, og konkursboet er indtrådt i denne databehandleraftale. Ofte vil kurator indgå en særskilt aftale med hosting provider om at få adgang til data.

10.12 Sletning

- Oprindelige Persondata og Efterfølgende Persondata opbevares i 10 år fra konkursboets afslutning. Opbevaring i denne periode sker med henvisning til opfyldelse af lovkrav (regnskabsmæssige krav), mulighed for at retskrav kan fastlægges, gøres gældende eller forsvares, dokumentation over for skifteretten, mulighed for kurator at kunne afgive forklaring, dokumentation i tilfælde af genoptagelse af konkursboet.

- Kreditorlister opbevares af kurator, så længe der er mulighed for, at der skal ske fordeling af midler i henhold til kreditorlisten.

10.12.1 Gendannelse af data slettet inden konkurs

- Gendannelse af ikke-følsomme Persondata slettet inden konkursen i boet kan ske med hjemmel i interesseafvejningsreglen, såfremt gendannelsen er begrundet i kuratorens pligt til at varetage konkursboets interesser.

- Gendannelse af følsomme Persondata kan alene ske, såfremt dette er nødvendigt for, at retskrav kan fastlægges, gøres gældende eller forsvares. Er dette ikke tilfældet, må følsomme Persondata ikke gendannes.

- Vurderingen er konkret i hvert enkelt tilfælde og er en afvejning af de modsatrettede hensyn. Begrundelsen skal dokumenteres skriftligt. Særligt skal det begrundes, om der

er konkrete holdepunkter for at antage, at der er slettede Persondata, som er af betydning for bo behandlingen.

## 11 FAGSPECIFIKKE SAGSBEHANDLINGSREGLER INKASSO

11.1 I forbindelse med vores behandling af inkassosager gælder vores Generelle Behandlingsregler, jf. pkt. 9 ovenfor. I tillæg hertil gælder følgende fagspecifikke sagsbehandlingsregler for vores behandling af inkassosager.

11.2 Databehandler

11.2.1 Som anført ovenfor vil vi agere som databehandler i de situationer, hvor vores ydelser består i at administrere en ordning eller forpligtelse. I dette tilfælde vil opgaven være bundet af aftale (instruksen) fra klienten, og behandling vil være ekspeditionspræget, ligesom den ikke er udtryk for klassisk advokatvirksomhed.

11.2.2 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".*

11.2.3 For inkassobehandlingen vil vi derfor som udgangspunkt agere som databehandler i henhold til en databehandleraftale indgået med klienten.

11.2.4 Vi vil dog også agere som selvstændigt dataansvarlig for de oplysninger, som vi vil opbevare for at sikre sig med et eventuelt rådgiveransvar. Sådanne oplysninger vil blive opbevaret og slettet i henhold til vores almindelige behandlingsregler, som er angivet ovenfor i pkt. 9.

11.3 Behandlingsregler

11.3.1 I forbindelse med sagsbehandlingen i Inkasso modtages en lang række Persondata, herunder stamdata (almindelige Persondata som fx navn, adresse, e-mail, fødselsdato, køn, lokalisation, m.v.), billeder, følsomme oplysninger, cpr.nr. og oplysninger om strafbare og sociale forhold.

11.3.2 Personoplysninger, der behandles i Inkasso, herunder modtages, indsamles, bruges, videregives og opbevares, må som udgangspunkt alene bruges med inkassobehandling for øje. Skal oplysningerne anvendes til anden behandling hos os, vil behandlingshjemmel og behandlingsprincipper særskilt blive vurderet for disse nye formål. Vi kan videreanvende Persondata til andre legitime formål, hvis der er tale om formål, der ikke er uforenelige med det oprindelige formål.

11.3.3 Behandlingen vil altid ske efter et need-to-know princip.

11.3.4 Vi vil løbende vurdere, om der er hjemmel til at behandle og videregive de modtagne Persondata, herunder om der er hjemmel til behandling og videregivelse af cpr.nr., følsomme oplysninger, oplysninger om strafbare forhold og lovovertrædelser. Vi har gennemført passende procedurer herfor.

11.3.5 Vi vil begrænse behandling og videregivelse af oplysninger mest muligt, særligt for så vidt angår behandling og videregivelse af følsomme oplysninger, cpr.nr. samt oplysninger om strafbare forhold og lovovertrædelser. På formularer, fx åbningsstatus, boopgørelser eller andre formularer med rubrikker, der forudsætter cpr.nr. indsat, skal disse oplysninger som udgangspunkt fjernes, inden de oversendes til myndigheder eller parter, der ikke har hjemmel til at behandle sådanne oplysninger. Anvendelse af cpr.nr. vil derudover søges minimeret.

11.3.6 Persondata opbevares i 10 år fra sagens afslutning. Opbevaring i denne periode sker med henvisning til mulighed for, at et retskrav kan fastlægges, gøres gældende eller forsvares. Efter 10 år slettes elektroniske og fysiske Persondata vedrørende en konkret inkassosag.

## 12 FAGSPECIFIKKE SAGSBEHANDLINGSREGLER STRAFFERET

12.1 I forbindelse med vores behandling af strafferetssager gælder vores Generelle Behandlingsregler, jf. pkt. 9 ovenfor. I tillæg hertil gælder følgende fagspecifikke sagsbehandlingsregler for vores behandling af strafferetssager.

12.2 Behandlingsregler

12.2.1 I forbindelse med sagsbehandlingen i Strafferet modtages en lang række Persondata, herunder stamdata (almindelige Persondata som fx navn, adresse, e-mail, fødselsdato, køn, lokalisation, m.v.), billeder, følsomme oplysninger, cpr.nr. og oplysninger om strafbare og sociale forhold.

12.2.2 Personoplysninger, der behandles i Strafferet, herunder modtages, indsamles, bruges, videregives og opbevares, må som udgangspunkt alene bruges med denne behandling for øje. Skal oplysningerne anvendes til anden behandling hos os, vil behandlingshjemmel og behandlingsprincipper særskilt blive vurderet for disse nye formål. Vi kan videreanvende Persondata til andre legitime formål, hvis der er tale om formål, der ikke er uforenelige med det oprindelige formål.

12.2.3 Behandlingen vil altid ske efter et need-to-know princip.

12.2.4 Vi vil løbende vurdere, om der er hjemmel til at behandle og videregive de modtagne Persondata, herunder om der er hjemmel til behandling og videregivelse af cpr.nr., følsomme oplysninger, oplysninger om strafbare forhold og lovovertrædelser. Vi har gennemført passende procedurer herfor.

12.2.5 Vi vil begrænse behandling og videregivelse af oplysninger mest muligt, særligt for så vidt angår behandling og videregivelse af følsomme oplysninger, cpr.nr. samt oplysninger om strafbare forhold og lovovertrædelser. På formularer, fx åbningsstatus, boopgørelser eller andre formularer med rubrikker, der forudsætter cpr.nr. indsat, skal disse oplysninger som udgangspunkt fjernes, inden de oversendes til myndigheder eller parter, der ikke har hjemmel til at behandle sådanne oplysninger. Anvendelse af cpr.nr. vil derudover søges minimeret.

12.2.6 Vi modtager sagsakter med Persondata fra Politiet på krypteret USB-nøgle. Efter sagens afslutning, afleveres USB-nøglen tilbage til retten efter aftale mellem Domstolsstyrelsen og Anklagemyndigheden.

12.2.7 Det vil løbende blive vurderet, om Persondata har relevans i relation til opdraget. Modtagne elektroniske dokumenter opbevares særskilt i vores sagsstyringssystem i 3-6 mdr. efter en sags afslutning af hensyn til, at klienten vil kunne kontakte os vedrørende spørgsmål til afsoning, m.v. I denne periode vil vi have behov for at kunne behandle og opbevare de modtagne elektroniske dokumenter.

12.2.8 Fysiske dokumenter opbevares i 3-6 mdr. efter samme princip som angivet ovenfor. Derefter makuleres fysiske dokumenter, da sagens oplysninger er arkiveret på vores sagsstyringssystem.

12.2.9 Persondata opbevares i 10 år fra sagens afslutning. Opbevaring i denne periode sker med henvisning til mulighed for, at et retskrav kan fastlægges, gøres gældende eller forsvares. Efter 10 år slettes elektroniske Persondata vedrørende en konkret strafferetlig sag.

## 13 FAGSPECIFIKKE SAGSBEHANDLINGSREGLER FAMILIERET

13.1 I forbindelse med vores behandling af familieretsager gælder vores Generelle Behandlingsregler, jf. pkt. 9 ovenfor. I tillæg hertil gælder følgende fagspecifikke sagsbehandlingsregler for vores behandling af familieretsager.

13.2 Behandling

13.2.1 I forbindelse med sagsbehandlingen i Strafferet modtages en lang række Persondata, herunder stamdata (almindelige Persondata som fx navn, adresse, e-mail, fødselsdato, køn, lokalisation, m.v.), billeder, følsomme oplysninger, cpr.nr. og oplysninger om strafbare og sociale forhold.

13.2.2 Personoplysninger, der behandles i Strafferet, herunder modtages, indsamles, bruges, videregives og opbevares, må som udgangspunkt alene bruges med denne behandling for øje. Skal oplysningerne anvendes til anden behandling hos os, vil behandlingshjemmel og behandlingsprincipper særskilt blive vurderet for disse nye formål. Vi kan videreanvende Persondata til andre legitime formål, hvis der er tale om formål, der ikke er uforenelige med det oprindelige formål.

13.2.3 Behandlingen vil altid ske efter et need-to-know princip.

13.2.4 Vivil løbende vurdere, om der er hjemmel til at behandle og videregive de modtagne Persondata, herunder om der er hjemmel til behandling og videregivelse af cpr.nr., følsomme oplysninger, oplysninger om strafbare forhold og lovovertrædelser. Vi har gennemført passende procedurer herfor.

13.2.5 Vi vil begrænse behandling og videregivelse af oplysninger mest muligt, særligt for så vidt angår behandling og videregivelse af følsomme oplysninger, cpr.nr. samt oplysninger om strafbare forhold og lovovertrædelser. På formularer, fx åbningsstatus, boopgørelser eller andre formularer med rubrikker, der forudsætter cpr.nr. indsat, skal disse oplysninger som udgangspunkt fjernes, inden de oversendes til myndigheder eller parter, der ikke har hjemmel til at behandle sådanne oplysninger. Anvendelse af cpr.nr. vil derudover søges minimeret, fx angivelse af arvingers og testatorers cpr.nr. udelades, hvor det er praktisk muligt, således at cpr.nr. alene anføres på genparten til notaren. Er der en efterlevende ægtefælle, vil cpr.nr. blive slettet på testamentet, inden dokumenterne sendes til boets øvrige arvinger.

13.2.6 Persondata opbevares i 10 år fra sagens afslutning (kopi af underskrift af testamente). Opbevaring i denne periode sker med henvisning til mulighed for, at et retskrav kan fastlægges, gøres gældende eller forsvares. Originalen sendes retur til klienten efter, at testamentet er blevet underskrevet. Efter 10 år slettes elektroniske og fysiske Persondata vedrørende en konkret sag.

## 14 FAGSPECIFIKKE SAGSBEHANDLINGSREGLER EJENDOMSHANDLER

14.1 I forbindelse med vores behandling af sager om ejendomshandler gælder vores Generelle Behandlingsregler, jf. pkt. 9 ovenfor. I tillæg hertil gælder følgende fagspecifikke sagsbehandlingsregler for vores behandling af sager om ejendomshandler.

14.2 Behandling

14.2.1 I forbindelse med sagsbehandlingen i en ejendomshandel modtages en lang række Persondata, herunder stamdata (almindelige Persondata som fx navn, adresse, e-mail, fødselsdato, køn, lokalisation, m.v.), billeder, følsomme oplysninger og cpr.nr. Eksempler på dokumenter, der indeholder Persondata, kan være købs-, salgs, eller finansieringsaftaler, hvor køber og sælgers navn, adresse og cpr.nr. fremgår samt oversigter over betaling af ejendomsskatter. Det kan forekomme, at en ejendomsmægler opretter et datarum i forbindelse med en transaktion, hvor vi kan få adgang til data og herunder Persondata. Vi anvender data, der har relevans for transaktionen.

14.2.2 Personoplysninger, der behandles i Ejendomsret, herunder modtages, indsamles, bruges, videregives og opbevares, må som udgangspunkt alene bruges med denne behandling for øje. Skal oplysningerne anvendes til anden behandling hos os, vil behandlingshjemmel og behandlingsprincipper særskilt blive vurderet for disse nye formål. Vi kan videreanvende Persondata til andre legitime formål, hvis der er tale om formål, der ikke er uforenelige med det oprindelige formål.

14.2.3 Behandlingen vil altid ske efter et need-to-know princip.

14.2.4 Vi vil løbende vurdere, om der er hjemmel til at behandle og videregive de modtagne Persondata, herunder om der er hjemmel til behandling og videregivelse af cpr.nr. og andre følsomme oplysninger. Vi har gennemført passende procedurer herfor.

14.2.5 Vi vil begrænse behandling og videregivelse af oplysninger mest muligt, særligt for så vidt angår behandling og videregivelse af følsomme oplysninger og cpr.nr. På formularer, der forudsætter cpr.nr. indsat, skal disse oplysninger som udgangspunkt fjernes, inden de oversendes til myndigheder eller parter, der ikke har hjemmel til at behandle sådanne oplysninger. Anvendelse af cpr.nr. vil derudover søges minimeret, fx angivelse på en købs- eller salgsaftale.

14.2.6 Persondata opbevares i 10 år fra sagens afslutning. Opbevaring i denne periode sker med henvisning til mulighed for, at et retskrav kan fastlægges, gøres gældende eller forsvares. Efter udløb af den 10-årige periode vil vi sende originale dokumenter retur til klienten. Efter 10 år slettes elektroniske og fysiske Persondata vedrørende en konkret sag.

## 15 FAGSPECIFIKKE SAGSBEHANDLINGSREGLER EJENDOMSASMINISTRATION

15.1 I forbindelse med vores behandling af sager om ejendomsadministration gælder vores Generelle Behandlingsregler, jf. pkt. 9 ovenfor. I tillæg hertil gælder følgende fagspecifikke sagsbehandlingsregler for vores behandling af sager om ejendomsadministration.

15.2 Databehandler

15.2.1 Som anført ovenfor vil vi agere som databehandler i de situationer, hvor vores ydelser består i at administrere en ordning eller forpligtelse. I dette tilfælde vil opgaven være bundet af aftale (instruksen) fra klienten, og behandling vil være ekspeditionspræget, ligesom den ikke er udtryk for klassisk advokatvirksomhed.

15.2.2 Vi vil typisk agere som databehandler, hvis vi administrerer en ejendom, men udelukkende opkræver leje og indgår lejekontrakter på udlejers vegne uden selvstændig stillingtagen til kontraktbetingelserne mv. Hvis vi til gengæld også udfærdiger lejekontrakter og vurderer lejeres eventuelle misligholdelse samt behandler udsættelsessager, må vi snarere vurderes at være dataansvarlig. Dette gælder både for administration af lejligheder i andelsboligforeninger og ejerforeninger, som administration af lejligheder i udligningsejendomme (investeringsejendomme).

15.2.3 Det vil derfor konkret blive bedømt ud fra opdraget, om vi agerer som databehandler eller dataansvarlig. Agerer vi som databehandler, vil vi indgå en databehandleraftale med klienten.

15.3 Behandling

15.3.1 I forbindelse med sagsbehandlingen i Ejendomsadministrationen modtages en lang række Persondata, herunder stamdata (almindelige Persondata som fx navn, adresse, e-mail, fødselsdato, køn, lokalisation, m.v.), billeder, følsomme oplysninger, helbredsoplysninger og cpr.nr. Dataflowet foretages ved hard copy og behandles herefter elektronisk via e-mail eller i vores ejendomsadministrationssystem.

15.3.2 Ved behandling af Persondata i Ejendomsadministrationen kan sagsbehandlingen opdeles i to kategorier: Investeringsejendomme og Foreninger.

15.3.3 **Investeringsejendomme.** På vegne af ejeren, sender vi kontrakt til underskrivelse hos lejer, hvorefter dokumentet opbevares hos os. Lejekontrakten er selvstændigt udfærdiget af os (baseret på visse basis oplysninger fra ejeren). Ligesom vi selvstændigt vurderer lejeres eventuelle misligholdelse samt behandler udsættelsessager. Vi vil derfor i overvejende tilfælde anses for at være dataansvarlig.

15.3.4 **Foreninger.** Sælger (ejeren) af andelsboligen/ejerlejligheden sender informationer til os, som udarbejder dokumenter ved brug af disse informationer. I nogle tilfælde fremsender sælger også kopi af kørekort eller sygesikringskort. Ved salg af lejligheder i en ejerforening, indhenter vi fuldmagt. Vi vil i langt overvejende tilfælde selvstændigt udarbejde dokumenter, og vi vil derfor i overvejende tilfælde anses for at være dataansvarlig.

15.3.5 Vi anvender E-signatur i forbindelse med underskrift mellem parterne. Det er sælger, køber og tegningsberettiget i en given forening, der forestår underskrivelsen af handlen. Underskrifterne slettes efter to måneder hos E-signatur. Ved anvendelsen af E-signatur, sendes der ikke cpr.nr. eller andre Persondata end de Persondata, der er indeholdt i de underskrevne dokumenter.

15.3.6 Personoplysninger, der behandles i Ejendomsadministrationen, herunder modtages, indsamles, bruges, videregives og opbevares, må som udgangspunkt alene bruges med denne behandling for øje. Skal oplysningerne anvendes til anden behandling hos os, vil behandlingshjemmel og behandlingsprincipper særskilt blive vurderet for disse nye formål. Vi kan videreanvende Persondata til andre legitime formål, hvis der er tale om formål, der ikke er uforenelige med det oprindelige formål.

15.3.7 Behandlingen vil altid ske efter et need-to-know princip.

15.3.8 Vi vil løbende vurdere, om der er hjemmel til at behandle og videregive de modtagne Persondata, herunder om der er hjemmel til behandling og videregivelse af følsomme oplysninger og cpr.nr. Vi har gennemført passende procedurer herfor.

15.3.9 Vi vil begrænse behandling og videregivelse af oplysninger mest muligt, særligt for så vidt angår behandling og videregivelse af følsomme oplysninger og cpr.nr. Anvendelse af følsomme oplysninger og cpr.nr. vil derudover søges minimeret.

15.3.10 Persondata opbevares i 10 år fra en sags afslutning. Opbevaring i denne periode sker med henvisning til mulighed for, at et retskrav kan fastlægges, gøres gældende eller forsvares. Efter 10 år slettes elektroniske og fysiske Persondata vedrørende en konkret sag.

## 16 FAGSPECIFIKKE SAGSBEHANDLINGSREGLER ANSÆTTELSESRET

16.1 I forbindelse med vores behandling af ansættelsesretssager gælder vores Generelle Behandlingsregler, jf. pkt. 9 ovenfor. I tillæg hertil gælder følgende fagspecifikke sagsbehandlingsregler for vores behandling af ansættelsesretssager.

16.2 Behandling

16.2.1 I forbindelse med sagsbehandlingen i en ansættelsesretlig sag modtages en lang række Persondata, herunder stamdata (almindelige Persondata som fx navn, adresse, e-mail, fødselsdato, køn, lokalisation, m.v.), billeder, følsomme oplysninger, helbredsoplysninger, fagforeningsmæssige oplysninger og cpr.nr. Dokumenter, der indsamles, kan være ansættelseskontrakter, hvor den ansattes navn, adresse og cpr.nr. fremgår samt lønoversigter.

16.2.2 Personoplysninger, der behandles i Ansættelsesret, herunder modtages, indsamles, bruges, videregives og opbevares, må som udgangspunkt alene bruges med denne behandling for øje. Skal oplysningerne anvendes til anden behandling hos os, vil behandlingshjemmel og behandlingsprincipper særskilt blive vurderet for disse nye formål. Vi kan videreanvende Persondata til andre legitime formål, hvis der er tale om formål, der ikke er uforenelige med det oprindelige formål.

16.2.3 Behandlingen vil altid ske efter et need-to-know princip.

16.2.4 Vi vil løbende vurdere, om der er hjemmel til at behandle og videregive de modtagne Persondata, herunder om der er hjemmel til behandling og videregivelse af

cpr.nr. og andre følsomme oplysninger. Vi har gennemført passende procedurer herfor.

16.2.5 Vi vil begrænse behandling og videregivelse af oplysninger mest muligt, særligt for så vidt angår behandling og videregivelse af følsomme oplysninger og cpr.nr. På formularer, der forudsætter cpr.nr. indsat, skal disse oplysninger som udgangspunkt fjernes, inden de oversendes til myndigheder eller parter, der ikke har hjemmel til at behandle sådanne oplysninger. Anvendelse af cpr.nr. vil derudover søges minimeret, fx angivelse på ansættelseskontrakter.

16.2.6 Persondata opbevares i 10 år fra sagens afslutning. Opbevaring i denne periode sker med henvisning til mulighed for, at et retskrav kan fastlægges, gøres gældende eller forsvares. Efter udløb af den 10-årige periode vil vi sende originale dokumenter retur til klienten. Efter 10 år slettes elektroniske og fysiske Persondata vedrørende en konkret sag.

## 17 FAGSPECIFIKKE SAGSBEHANDLINGSREGLER ERSTATNINGS- OG FORSIKRINGSRET (HERUNDER PERSONSKADE)

17.1 I forbindelse med vores behandling af erstatnings- og forsikringssager (herunder personskade) gælder vores Generelle Behandlingsregler, jf. pkt. 9 ovenfor. I tillæg hertil gælder følgende fagspecifikke sagsbehandlingsregler for vores behandling af erstatnings- og forsikringssager (herunder personskade).

17.2 Som hovedregel behandler vi ikke personskadesager. I særtilfælde, kan vi dog håndtere personskadesager.

17.3 <u>Behandling</u>

17.3.1 I forbindelse med sagsbehandlingen i erstatnings- og forsikringssager (herunder personskade) modtages en lang række Persondata, herunder stamdata (almindelige Persondata som fx navn, adresse, e-mail, fødselsdato, køn, lokalisation, m.v.), billeder, følsomme oplysninger, helbredsoplysninger og cpr.nr.

17.3.2 Personoplysninger, der behandles i en forsikringssag (fx personskadesag), herunder modtages, indsamles, bruges, videregives og opbevares, må som udgangspunkt alene bruges med denne behandling for øje. Skal oplysningerne anvendes til anden behandling hos os, vil behandlingshjemmel og behandlingsprincipper særskilt blive vurderet

for disse nye formål. Vi kan videreanvende Persondata til andre legitime formål, hvis der er tale om formål, der ikke er uforenelige med det oprindelige formål.

17.3.3 Behandlingen vil altid ske efter et need-to-know princip.

17.3.4 Vi vil løbende vurdere, om der er hjemmel til at behandle og videregive de modtagne Persondata, herunder om der er hjemmel til behandling og videregivelse af følsomme oplysninger og cpr.nr. Vi har gennemført passende procedurer herfor.

17.3.5 Vi vil begrænse behandling og videregivelse af oplysninger mest muligt, særligt for så vidt angår behandling og videregivelse af følsomme oplysninger og cpr.nr. Anvendelse af cpr.nr. og helbredsoplysninger vil derudover søges minimeret.

17.3.6 Persondata opbevares i 30 år fra sagens afslutning. Opbevaring i denne periode sker med henvisning til mulighed for, at et retskrav kan fastlægges, gøres gældende eller forsvares. Efter 30 år slettes elektroniske og fysiske Persondata vedrørende en konkret sag.

## 18 FAGSPECIFIKKE SAGSBEHANDLINGSREGLER M&A – (DUE DILIGENCE)

18.1 I forbindelse med at vi agerer som datarum i forbindelse med M&A (due diligence) gælder vores Generelle Behandlingsregler, jf. pkt. 9 ovenfor. I tillæg hertil gælder følgende fagspecifikke sagsbehandlingsregler for vores behandling af M&A (due diligence).

18.2 Databehandler

18.2.1 Som anført ovenfor vil vi agere som databehandler i de situationer, hvor vores ydelser består i at administrere en ordning eller forpligtelse. I dette tilfælde vil opgaven være bundet af aftale (instruksen) fra klienten, og behandling vil være ekspeditionspræget, ligesom den ikke er udtryk for klassisk advokatvirksomhed.

18.2.2 Hvis der alene ydes bistand i en M&A proces, vil vi agere som databehandler. I en sådan situation skal der indgås en databehandleraftale med klienten, og vi agerer da efter instruks fra klienten.

18.2.3 Ydes der derimod juridisk rådgivning i forbindelse med M&A-processen, vil vi agere som dataansvarlig, og de under pkt. 18.1 og 18.3 angivne behandlingsregler vil da gælde.

18.3 Behandling

18.3.1 I forbindelse med sagsbehandlingen i en M&A proces modtages en lang række Persondata, herunder stamdata (almindelige Persondata som fx navn, adresse, e-mail, fødselsdato, køn, lokalisation, m.v.), billeder, følsomme oplysninger, helbredsoplysninger, fagforeningsmæssige oplysninger og cpr.nr. Dokumenter, der indsamles, kan være ansættelseskontrakter, CV og en lang række andre dokumenter relateret til M&A processen, hvoraf navn, adresse og cpr.nr. fremgår.

18.3.2 Personoplysninger, der behandles i en M&A proces, herunder modtages, indsamles, bruges, videregives og opbevares, må som udgangspunkt alene bruges med denne behandling for øje. Skal oplysningerne anvendes til anden behandling hos os, vil behandlingshjemmel og behandlingsprincipper særskilt blive vurderet for disse nye formål. Vi kan videreanvende Persondata til andre legitime formål, hvis der er tale om formål, der ikke er uforenelige med det oprindelige formål.

18.3.3 Behandlingen vil altid ske efter et need-to-know princip.

18.3.4 Vi vil løbende vurdere, om der er hjemmel til at behandle og videregive de modtagne Persondata, herunder om der er hjemmel til behandling og videregivelse af cpr.nr. og andre følsomme oplysninger. Vi har gennemført passende procedurer herfor.

18.3.5 Vi vil begrænse behandling og videregivelse af oplysninger mest muligt, særligt for så vidt angår behandling og videregivelse af følsomme oplysninger og cpr.nr. På formularer, der forudsætter cpr.nr. indsat, skal disse oplysninger som udgangspunkt fjernes, inden de oversendes til myndigheder eller parter, der ikke har hjemmel til at behandle sådanne oplysninger. Anvendelse af cpr.nr. vil derudover søges minimeret.

18.3.6 Persondata opbevares i 10 år fra sagens afslutning. Opbevaring i denne periode sker med henvisning til mulighed for, at et retskrav kan fastlægges, gøres gældende eller forsvares. Efter udløb af den 10-årige periode vil vi sende originale dokumenter retur til klienten. Efter 10 år slettes elektroniske og fysiske Persondata vedrørende en konkret sag.

## 19 FAGSPECIFIKKE SAGSBEHANDLINGSREGLER BESTYRELSESARBEJDE

19.1 I forbindelse med, at ansatte hos os udfører bestyrelsesarbejde, gælder vores Generelle Behandlingsregler, jf. pkt. 9 ovenfor. I tillæg hertil gælder følgende fagspecifikke sagsbehandlingsregler for vores behandling af i forbindelse med udførelse af bestyrelsesarbejde.

19.2 Behandling

19.2.1 I forbindelse med sagsbehandlingen i en M&A proces modtages en lang række Persondata, herunder stamdata (almindelige Persondata som fx navn, adresse, e-mail, fødselsdato, køn, lokalisation, m.v.), billeder, følsomme oplysninger, helbredsoplysninger, fagforeningsmæssige oplysninger og cpr.nr. Dokumenter, der indsamles, kan være fuldmagter til brug for generalforsamlinger, regnskaber, opgørelser, bestyrelsesprotokollater m.v..

19.2.2 Personoplysninger, der behandles i forbindelse med bestyrelsesarbejde, herunder modtages, indsamles, bruges, videregives og opbevares, må som udgangspunkt alene bruges med denne behandling for øje. Skal oplysningerne anvendes til anden behandling hos os, vil behandlingshjemmel og behandlingsprincipper særskilt blive vurderet for disse nye formål. Vi kan videreanvende Persondata til andre legitime formål, hvis der er tale om formål, der ikke er uforenelige med det oprindelige formål.

19.2.3 Behandlingen vil altid ske efter et need-to-know princip.

19.2.4 Vi vil løbende vurdere, om der er hjemmel til at behandle og videregive de modtagne Persondata, herunder om der er hjemmel til behandling og videregivelse af cpr.nr. og andre følsomme oplysninger. Vi har gennemført passende procedurer herfor.

19.2.5 Vi vil begrænse behandling og videregivelse af oplysninger mest muligt, særligt for så vidt angår behandling og videregivelse af følsomme oplysninger og cpr.nr. På formularer, der forudsætter cpr.nr. indsat, skal disse oplysninger som udgangspunkt fjernes, inden de oversendes til myndigheder eller parter, der ikke har hjemmel til at behandle sådanne oplysninger. Anvendelse af cpr.nr. vil derudover søges minimeret.

19.2.6 Persondata opbevares i 10 år fra sagens afslutning. Opbevaring i denne periode sker med henvisning til mulighed for, at et retskrav kan fastlægges, gøres gældende eller forsvares. Derudover kan Erhvervsstyrelsen foretage stikprøvekontrol, hvorfor opbevaring af data anses for nødvendig. Efter udløb af den 10-årige periode vil vi sende

originale dokumenter retur til klienten. Efter 10 år slettes elektroniske og fysiske Persondata vedrørende en konkret sag.

## 20 COOKIES

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

20.2 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.

20.3 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.

20.4 Hvad er en cookie og lignende teknologier?

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

20.6 Der er to typer af cookies - midlertidige cookies og permanente cookies. Midlertidige cookies er informationsenheder, som slettes, når du lukker din web-browser. Permanente cookies er informationsenheder, som bliver gemt på din computer, indtil de bliver slettet. Permanente cookies sletter sig selv efter en vis periode, men bliver fornyet, hver gang du besøger les.dk. les.dk anvender både midlertidige og permanente cookies.

20.7 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.

20.8 Når du besøger les.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 les.dk, og registrerer anvendelsen heraf.

20.9 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.

20.10 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 les.dk. Vi registrerer udelukkende anonyme informationer som IP-numre, antal bytes sendt og modtaget, Internethost, tid, browsertype, -version, og -sprog, osv.

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

20.12 Vi bruger cookies til:

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

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

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

- Kvalitetssikring, det vil sige til at sikre kvaliteten af vores services og forhindre misbrug og uregelmæssigheder i forbindelse med brugen af vores services.

- Målrettet markedsføring, det vil sige til at vise specifik markedsføring på les.dk, som vi tror, at du vil finde interessant.

20.13 Adgang for tredjepart

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

20.14 Tredjeparts-cookies

20.14.1 Vores hjemmeside anvender cookies fra følgende tredjeparter:

- Google Analytics: til statistiske formål. Du kan afvise cookies fra Google Analytics ved at klikke her: http://tools.google.com/dlpage/gaoptout
- Facebook: sættes af Facebook.
- Twitter: sættes af Twitter, hvis du interagerer med Twitter plugin eller allerede er logget på Twitter fra en anden kilde med det formål at interagere med dem.

20.15 Sådan afviser du brugen af cookies

20.15.1 De fleste browsere tillader dig at slette cookies fra din harddisk, blokere for alle cookies eller modtage en advarsel, før der gemmes en cookie. Du skal dog være opmærksom på, at der i så fald kan være services og funktioner, du ikke kan bruge, fordi de kræver cookies til at huske valg, du foretager. Vi håber, at du vil tillade de cookies vi sætter, da de hjælper os med at forbedre les.dk.

20.16 Sådan sletter du cookies

20.16.1 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

20.17 Google Analytics

20.17.1 les.dk bruger Google Analytics for at analysere, hvordan brugerne anvender les.dk. De Persondata, som cookien indsamler om din brug (trafikdata, herunder din IP-adresse), sendes til og gemmes på Googles servere i USA. Google bruger Persondata til at evaluere din brug af les.dk, udarbejde rapporter om aktiviteten på les.dk og yde

andre tjenester i tilknytning til aktiviteten på les.dk og brugen af internettet. Google kan også videregive Persondata til tredjemand, hvis loven kræver det, eller hvis tredjemand behandler Persondata på Googles vegne.

20.17.2 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, osv, 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.

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

20.18.1 Ved at bruge les.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.

## 21 ÆNDRING AF PERSONDATAPOLITIK

21.1 Vi kan til enhver tid og uden varsel ændre denne Persondatapolitik med virkning for fremtiden. Ved sådanne ændringer sker der orientering af vores brugere i forbindelse med brugernes login på les.dk. Vores nye Persondatapolitik vil herefter være gældende for din brug af les.dk.

## 22 HENVENDELSER

22.1 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:

Lund Elmer Sandager Advokatpartnerselskab
CVR-nummer: 32283934
Kalvebod Brygge 39 – 41
DK - 1560 København V
Danmark

T: + 45 33 300 200
info@les.dk
W: www.les.dk

## 23 DATATILSYNET

23.1 Du har mulighed for at klage til Datatilsynet over vores indsamling og behandling af dine Persondata:

Datatilsynet
Borgergade 28, 5.
1300 København K

Telefon 3319 3200
Mail: dt@datatilsynet.dk
www.datatilsynet.dk