MP ADVOKATER

DATABESKYTTELSESPOLITIK

Version 1.1

/MP Advokater, 2025

1. SELSKABET

Selskabet er:

MP Advokater ApS
CVR-nummer: 39424010
Jernbanegade 22 A, 1. tv.
DK – 8400 Ebeltoft
Danmark
(Benævnt: ”MP Advokater”)

T: 86343822
E: info@mpadvokater.dk
W: www.mpadvokater.dk

2. ANSVAR

2.1 MP Advokater skal i medfør af databeskyttelsesloven og EU’s forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (nr. 2016/679), beskytte fortroligheden, integriteten og tilgængeligheden af de oplysninger her de personoplysninger, som MP Advokater er i besiddelse af. Det omfatter oplysninger fra klienter, samarbejdspartnere, diverse leverandører medarbejdere o. Lign.

2.2 Beskyttelse af persondata er derfor en høj prioritet hos os.

3. TYPER AF PERSONDATA:

KLIENTER:

- Almindelige persondata (f.eks. navn, adresse, e-mail, fødselsdato, køn, fotomateriale, lokation, mv.)
- CPR-nummer
- Lokalitetsdata, navn, reg.nr., medarbejder mobil.nr.
- Bankinformationer, herunder bank- og formueopgørelser
- Trafikdata om brug af internettet
- Lokalisationsdata fra internettet, mobil, GPS eller kamera
- Transaktionsdata
- Unikke numre på netværksenheder
- Kontaktinformation, rapportadgang
- E-mails

- Regnskab
- Arbejdsgiverbetalt mobiltelefon, navn, adresse, tlf. nr., e-mail, opkaldshistorik, anonymiserede tlf. nr. på modtager af opkald, tro- og loveerklæringer
- Kvalitetsstyring
- Skadehåndtering

4. FORMÅL

4.1 Formålet MP Advokaters behandling af persondata, er at varetage opgaven overfor kunden, herunder bl.a. at vi med respekt for gældende regler og lovgivning, kan udføre det opdrag, vi som advokater har påtaget os overfor klienten, eller er blevet tildelt som hverv ved retten, eller andre opgaver vi som advokater har påtaget os, f.eks. overfor øvrige offentlige instanser mv. bl.a. vedrører dette:

KLIENTER:

- Alm. advokatvirksomhed
- Hvidvask
- Forbedring af rådgivning og tjenesteydelser
- Tilpasning af kommunikation både intern og for samarbejdspartnere, overfor dig
- Direkte markedsføringsaktiviteter
- Optimering af hjemmeside
- Gennemførelse af en aftale eller foranstaltninger efter din anmodning herom
- Administration af din relation til MP Advokater
- Opfyldelse af lovkrav
- Retskrav

Levering af den aftalte ydelse, efterlevelse af lovgivning bl.a. hvidvaskreglerne, efterlevelse af advokatetiske regler herunder habilitetsregler mv., som led i kvalitetsstyring herunder udvikling af MP Advokaters forretningsområder og de ydelser vi leverer samt som led i fakturering etc.

5. DINE RETTIGHEDER

5.1 MP Advokater, har i medfør lov og forordning nævnt under pkt. 1.1, en række forpligtelser til at varetage dine rettigheder.

5.2 Retten til **indsigt** betyder at du har ret til at få oplyst hvilke oplysninger MP Advokater, behandler om dig, herunder også hvordan behandlingen foregår samt overfor hvem. MP Advokater vil derfor, ved din anmodning herom, som udgangspunkt skulle meddele dig, hvilke oplysninger der bliver behandlet om dig.

Din rettighed hertil, er dog i praksis begrænset bl.a. i MP Advokaters advokatetiske og retsplejemæssige forpligtelser bl.a. i forbindelse med tavshedspligt, og varetagelsen af det frie forsvar mv.

5.3 Retten til **berigtigelse** betyder at du som registreret har ret til at få berigtiget manglende, eller forkerte oplysninger i forbindelse med sagsbehandlingen.

5.4 Retten til at blive **glemt** betyder, at du som registreret har ret til at få slettet persondata om dig selv.

Denne ret begrænses dog af en interesseafvejning med MP Advokaters forpligtigelse til at opbevare dine data i arkiveringsmæssig henseende.

Ved ønske om sletning må MP Advokater dog ikke videre behandle dine oplysninger.

5.5 Hvis der i forbindelse med sagen er tildelt MP Advokater særskilt samtykke til behandling af persondata, kan dette til enhver tid **tilbagekaldes**.

Man skal dog være opmærksom på at tilbagekaldelse, kan medfører et retstab, idet MP Advokater derved ikke længere må behandle oplysningerne.

5.6 Retten til **dataportabilitet** betyder, at du som registeret har ret til at få overført/tilbageleveret dine data din data, i et maskinlæsbart, struktureret almindeligt anvendt system, hvis dette ønskes.

5.7 Retten til at gøre **indsigelse** mod databehandlingen, betyder at du som registreret har ret til at gøre indsigelser med behandlingen af persondata om dig.

Dog begrænses af interesseafvejning med om behandlingen er nødvendig for at udføre en opgave i samfundets interesser, eller hvis behandlingen er nødvendig for at forfølge en berettiget interesse og hensynet til den registrerede ikke overstiger disse interesser.

5.8 Retten til **dataminimering** betyder, at du i følgende tilfælde har ret til at begrænse behandlingen af persondataoplysninger:

Hvis rigtigheden af persondata bestrides af den registrerede, men kun i perioder indtil den dataansvarlige har haft mulighed for at fastslå, om persondata er korrekte.

Hvis behandlingen er ulovlig, og den registrerede modsætter sig sletning af persondata og i stedet anmoder om, at anvendelsen heraf begrænses.

Hvis den dataansvarlige ikke længere har brug for persondata til behandlingen. Dette følger dog også af MP Advokaters pligt til dataminimering.

Hvis den registrerede har gjort indsigelser mod behandlingen, men kun i perioder mens det kontrolleres, om den dataansvarliges legitime interesser går forud for den registreredes legitime interesser (undersøgelse af interesseafvejning).

BEHANDLINGSREGLER - GENERELT

6. PRINCIPPER FOR VORES DATABEHANDLING

6.1 MP Advokater indsamler og behandler kun oplysninger som findes nødvendige og relevante i forhold til de aftalte **formål** med rådgivningen.

6.2 For at sikrer **dataminimering**, indsamler vi kun i fornødent og formålsforeneligt omfang oplysninger hos: klienter og leverandører og samarbejdspartnere, samt oplysninger fra vores hjemmeside (cookies mv.) m.fl. om oplysninger, hvor indsamlingen er foreneligt med opgavens formål.

6.3 De oplysninger, som vi indsamler, kan stamme direkte fra klienten, tredjemand, andre implicerede personer, kunder i øvrigt, retterne og andre offentlige myndigheder.

6.4 MP Advokater sørger for løbende at ajourføre de data som vi måtte have indsamlet, dette for at sikre **rigtigheden** af de indsamlede og behandlede oplysninger.

6.5 Opbevaring, sker ud fra en konkret vurdering fra sag til sag. MP Advokater sørger for at der sker korrekt **opbevaringsbegrænsning** af de indsamlede data. Det betyder at vi forud for en sag og løbende, sikrer at der på sagen alene ligger de nødvendige data, og der ligges forud og løbende med sagsbehandlingen, en plan for hvilke data der løbende skal udskilles og destrueres, samt en plan for hvornår sagen endeligt skal destrueres.
I forbindelse med sagens afslutning, vil der altid være et arkiveringshensyn, dette for at sikrer lovpligtige krav om opbevaring f.eks. iht. rådgiveransvar samt under hensyntagen til sagens karakter o. Lign. Ofte vil der blive arbejdet med en 5 års grænse, men konkret og i særlige tilfælde kan denne grænse være højere.

6.6 **Datasikkerhed** betyder meget for MP Advokater, og vi bestræber os derfor på, altid at være på forkanten med vore processer. Vi stiller derfor høje krav til vores samarbejdspartnere på området, såvel til os selv. Vi sikrer dette ved løbende at foretage tilstrækkelig evaluering, samt holder os ajour med udviklingen på området.

7. VIDEREGIVELSE AF PERSONDATA

7.1 MP Advokater, videregiver kun oplysninger dersom vi har hjemmel hertil. Det klare udgangspunkt er således, at MP Advokater, ikke videregiver oplysninger, men der vil naturligvis være flere situationer, hvor dette ikke kan undgås, f.eks. kan nævnes personoplysningers videreoverdragelse til domstolsbehandling i forbindelse med en retssag.

7.2 MP Advokater, kan også være i en situation hvor vi som advokater er forpligtet til udlevering af personoplysninger, f.eks. i forbindelse med varetagelse af hvidvasklovgivningen mv.

7.3 MP Advokater, overfører ikke persondataret til andre lande, uden for EU/EØS

8. TEKNISKE FORANSTALTNINGER

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

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

8.3 Adgang til Persondata skal begrænses til personer, der har et sagligt behov for adgang til Persondata. Det skal være så få personer som muligt, dog med behørigt hensyn til driften – der skal være et tilstrækkeligt antal medarbejdere til at sikre driften af de pågældende opgaver ved sygdom, ferier, personaleudskiftning m.v.

Der foreligger et skøn hos virksomheden. MP Advokater har vurderet, at dette er nødvendigt, da alle medarbejdere i virksomheden skal have mulighed for at foretage ekspeditioner i sagerne.

Alle medarbejdere har således adgang til alle sager.

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

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

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

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

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

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

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

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

8.12 Hvis følsomme Persondata eller personnummer sendes med e-mail via internettet, skal sådanne e-mails krypteres. MP advokater anvender "Fusemail TLS/Encrypt-smart" via Advosys.

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

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

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

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

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

8.18 Vi har strenge sikkerhedsprocedurer for indsamling, opbevaring og overførsel af Persona-ta for at hindre uautoriseret adgang og for at overholde gældende lovgivning. De Persondata og personlige Persondata, du giver os, gemmes på vores egen eller på en af vores databehandlerens servere.

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

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

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

8.22 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.

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

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

8.25 Alle backup data og filer overskrives i passende intervaller.

9. ORGANISATORISKE FORANSTALTNINGER

9.1 MP Advokater har udarbejdet et sæt leveregler, som gælder sideløbende med denne persondatapolitik.

BEHANDLINGSREGLER – KLIENTER

10. OVERORDNET

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

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

11. MP ADVOKATER SOM DATABEHANDLER

11.1 MP Advokater er i langt de fleste tilfælde dataansvarlig, hvilket betyder at MP Advokater i langt de fleste tilfælde selv skønner hvordan de angivne oplysninger bruges til f.eks. en retssag etc.

11.2 I andre og langt de færreste tilfælde er MP Advokater databehandler, hvor vi handler efter instruks. Det kan f.eks. være i for de tilfælde, hvor MP Advokater varetager en Whistleblower ordning for andre virksomheder etc.

12. DATABEHANDLERE OG DATABEHANDLERAFTALE

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

12.2 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.

12.3 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.

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

12.5 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 da-tabehandleraftalen er skriftlig, herunder elektronisk.

12.6 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 data-beskyttelsesforordningens artikel 28, stk. 3, litra a-h.

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

12.8 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.

13. BEHANDLINGSHJEMMEL

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

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

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

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

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

14. GENERELLE PRINCIPPER – SAGSBEHANDLINGEN

14.1 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.

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

14.3 Under processen skal vi løbende sikre os, at indsamling og videregivelse af Persondata sker i overensstemmelse med formålet, og vi skal løbende overveje vores forhold til eventuelle

databehandlere. Inddrages et tredjeland i sagen, skal man vi være opmærksomme på de særlige regler, der gælder for overførsel af Persondata til tredjelande.

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

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

15. OPLYSNINGSPLIGT

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

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

15.3 I velkomstbrevet henvises der til Persondatapolitikken:

- Vores behandling – herunder elektronisk og fysisk behandling/opbevaring og eventuelt anvendelse af cloud-system og sagsbehandlingssystem.
- Andre relevante aktører – modparter/myndigheder/vidner/skønsmænd – der vil blive inddraget, samt også evt. ekstern bogholder og it-support.
- Opbevaringsperiode efter afslutning – herunder hvidvaskrav og klientkontokrav.

16. OPLYSNINGSPLIGT – TREDJEPARTER

16.1 I velkomstbrevet henvises der til Persondatapolitikken:
Tredjeparter kan f.eks. udgøre vidner, familiemedlemmer, naboer, arbejdsgiver, kolleger mv., samt bipersoner, herunder skønsmænd, læger, sagsbehandlere mv.

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

16.3 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.

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

16.5 Det følger af databeskyttelsesforordningens artikel 14, stk. 5, litra b, at oplysningspligten ikke gælder, hvis det vil kræve en uforholdsmæssig stor indsats at opfylde den. Denne undtagelse er i praksis fortolket sådan, at oplysningsforpligtelsen bl.a. ikke omfatter bipersoner. Det kan være navne på læger og diverse øvrige behandlere, samt navne på diverse konsulenter, kolleger, naboer og andre, der måtte indgå i beskrivelsen af sagen, men hvor det eksempelvis er funktionen og ikke personen, der er relevant, og hvor selve personidentiteten ingen

betydning har for sagen og heller ikke vil få nogen betydning. Undtagelsen forudsætter dog, at der alene indgår kontaktoplysninger og tilsvarende almindelige Persondata om den/de pågældende.

17. HVIDVASK

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

- Persondata indhentet i forbindelse med opfyldelse af kravene om kundekendskabsprocedurer i henhold til hvidvaskloven
- Identitets- og kontroloplysninger
- Kopi af foreviste legitimationsdokumenter
- Dokumentation for og registreringer af transaktioner, der gennemføres
- Dokumenter og registreringer vedrørende undersøgelser gennemført i henhold til hvidvasklovens § 25, stk. 1 og 2.

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

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

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

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

18. LØBENDE INDSAMLING OG VIDEREGIVELSE AF OPLYSNINGER

18.1 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.

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

18.3 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.

19. SLETNING

19.1 Ved afslutning af en sag har vi i princippet ikke længere behov for at behandle Persondata når opdraget er løst.

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

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

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

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

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

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

19.4 Såvel hensynene som skæringstidspunkterne er forskellige.

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

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

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

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

19.9 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.

20. IP-ADRESSER OG BROWSERINDSTILLINGER

20.1 I forbindelse med hvert besøg på vores hjemmeside registreres din computers anvendte IP-adresse og browserindstillinger. Din IP-adresse er adressen på den computer du anvender til

at besøge mpadvokater.dk. Browserindstillinger er for eksempel den browser type du anvender, browser sprog, tidszone mv. IP-adressen og browserindstillinger registreres for at sikre, at der altid kan findes tilbage til den anvendte computer, såfremt der måtte ske misbrug eller ulovligheder. IP-adressen benyttes desuden til at fastslå din omtrentlige lokalisation (på by-niveau).

21. COOKIES

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

21.2 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.

21.3 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.

21.4 Vi bruger cookies til:

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

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

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

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

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

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

21.6 Ved at bruge mpadvokater.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.

22. ÆNDRING AF PERSONDATAPOLITIK

22.1 MP Advokater kan til enhver tid og uden varsel ændre denne Persondatapolitik med virkning for fremtiden. Ved sådanne ændringer sker der orientering af MP Advokater' brugere i

forbindelse med brugernes login på MP Advokater. MP Advokater' nye Persondatapolitik vil herefter være gældende for din brug af MP Advokater.

23. KONTAKT

23.1 Såfremt du har spørgsmål eller ønsker at gøre brug af dine rettigheder, kan vi kontaktes på:

MP Advokater ApS
Jernbanegade 22, 8400 Ebeltoft
T: 86343822
CVR. 39424010
MP@mpadvokater.dk

24. KLAGE

24.1 Ønsker du at klage over MP Advokaters behandling af dine personoplysninger, kan du fremsende en e-mail med beskrivelse af baggrunden for din klage. Vi vil da behandle klagen og vende tilbage.

24.2 Du kan også klage til Datatilsynet, læs mere herom på www.datatilsynet.dk