ADVOKATGRUPPEN

Kort om Persondata

Advokat Eva Kaya

AARHUS
Åboulevarden 31, 8000 Aarhus C
70 10 13 30 / aarhus@advokatgruppen.dk

HORSENS
Emil Møllers Gade 41 B, 1., 8700 Horsens
70 10 13 30 / horsens@advokatgruppen.dk

FREDERICIA
Danmarksgade 8, 7000 Fredericia
70 10 13 30 / fredericia@advokatgruppen.dk

Persondata – kun en oversigt

Dette minikursus er beregnet for DMs/Gafsams/MLs/SHPs medlemmer, dvs. mindre og mellemstore virksomheder, hvis erhvervsaktiviteter primært består i salg og service af landbrugs-, entreprenør og have/park-maskiner.

Kurset giver alene et overblik over persondataforordningen.

En del områder indenfor persondata er stadig uafklarede; pt. afventer vi en del vejledninger og en ny persondatalov, se fx.

http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/plan_for_vejledninger_om_forordningen.pdf

Persondata – Hvad er det?

Eksempel : Facebook

- Hvad med dine persondata?

  - Mod at bruge Facebook har du accepteret, at en hvilken som helst virksomhed i verden får lov til at bruge oplysninger om, hvem du er, hvem du kender, hvem du taler med, hvad du foretager dig, hvor du færdes, og hvad du interesserer dig for, i reklameøjemed.

Persondata – Hvad er det?

Eksempel : Facebook

- Har den viden om dig så nogen værdi?
  - Ja - i 2016 var Facebooks indtægter fra salg af annoncer til brugerne 179 milliarder kroner.

Kilde: Artikel i Zetland fra 15. juni 2017, *"Snart har Facebook to milliarder brugere. Her er, hvad vi siger ja til (hint: ikke småting)".*

Persondataforordningen

- Anvendelsesområde: Erhvervsmæssig brug af persondata
- Ikrafttræden : Den 25. maj 2018
- Medfører persondataforordningen nye pligter?
  - Ja, men bygger videre på allerede gældende persondatalov.

Styr på virksomhedens persondata

- Hvilke persondata har din virksomhed?

A. Følsomme data:
- Race eller etnisk oprindelse
- Seksuelle forhold
- Politisk, religiøs eller filosofisk overbevisning
- Fagforeningsmæssigt tilhørsforhold *
- Biometrisk data med formål om identifikation
- Helbredsoplysninger *
- Oplysninger om børne- eller straffeattest *
- * persondata som ofte er registreret i en virksomhed – i forbindelse med ansatte og udbud

Styr på virksomhedens persondata

- Hvilke persondata har din virksomhed?

B. Ikke-følsomme data:

- Oplysninger om fysiske leverandørers og kunders identitet, adresse, køb, salg
- Bemærk afgrænsningen: Kundekartoteket i en virksomhed er en erhvervshemmelighed, men er ikke en følsom oplysning efter persondataloven eller persondataforordningen.
  - Hvad med markedsandele og prispolitik, som er ret følsomt?
  - Kunders kreditkortoplysninger?
- Persondata om medarbejdere, som er ikke-følsomme data

Styr på virksomhedens persondata

- Hvor er virksomhedens persondata?
  - Server
    - Egen server eller andres?
    - Hvor er den fysisk beliggende?
  - Hvad med data i printer/scanner/fax/kopimaskine?
  - Cloud-løsning
    - Hvor er data fysisk, hvis de lagres i skyen?

Styr på virksomhedens persondata

- Bliver virksomhedens persondata overført?
  - Til andre virksomheder (hosting eller cloud-løsning)?
  - Til udlandet?
  - Hvis data ikke ligger på virksomhedens egen server i EU, kan databehandleraftale og samtykke være nødvendigt…

Styr på virksomhedens persondata

- Den nuværende persondatalov fra år 2000 fastlægger allerede en del forpligtelser for de virksomheder, som har eller indsamler persondata.

- Persondataforordningen, som træder i kraft i maj 2018, bygger i vid udstrækning videre på indholdet i persondataloven.

- Man får en bedre forståelse af persondataregulering, hvis man læser Datatilsynets gennemgang af 12 spørgsmål om persondata, se: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/12_spoergsmaal_-_GDPR.pdf

Styr på virksomhedens persondata

- Når man har fået styr på, hvilke persondata, virksomheden har liggende, er det relevant at finde ud af, hvad virksomheden skal overholde i forbindelse med sine persondata.

- Den vigtigste bestemmelse er **persondataforordningens artikel 5**.

Hovedforpligtelserne i forordningen

Artikel 5, stk. 1.

Personoplysninger skal:

a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede ("lovlighed, rimelighed og gennemsigtighed").

b) indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål ("formålsbegrænsning").

c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles ("dataminimering").

d) være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges ("rigtighed").

e) opbevares op 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 personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder ("opbevaringsbegrænsning").

f) Behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger ("integritet og fortrolighed").

Artikel 5, stk . 2.

Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (ansvarlighed).

Artikel 5, stk. 1, litra a

a) Lovlighed, rimelighed og gennemsigtighed

- Samtykke
  - Frivilligt, specifikt, informeret, utvetydigt ja.
  - Ugyldigt, hvis ikke ved indhentelse af samtykke er oplyst, at et samtykke kan tilbagetrækkes.
  - Samtykket skal kunne bevises (skriftlighed).

- Kontrakt
  - Hvis persondata indsamlet som led i kontrakt(indgåelse).

Artikel 5, stk. 1, litra b-c

b) Formål

- Der skal altid være et legitimt formål for at have persondata
  - Formålet skal oplyses til den registrerede.
  - Data må kun anvendes/opbevares til det angivne formål.

c) Dataminimering

- Kun persondata relevante for formålet.
- Kun i relevant tidsrum
- fx makulering af ansøgning fra ikke-ansat ansøger til stilling

Artikel 5, stk. 1, litra d-e

d) Korrekte data

- Pligt til at sørge for at registrerede persondata er korrekte.
- Pligten modsvares af den registreredes rettigheder til indsigt, ændringer af ukorrekte data, sletning af data mv.

e) Opbevaringstid

- Persondata skal ikke opbevares længere end formålet tilsiger.
- Husk dog også andre forpligtelser, fx. opbevaring i min 5 år iht. bogføringslov

Artikel 5, stk. 1, litra f)

f) Behandling af persondata

- Beskyttelse af data mod uautoriseret adgang.
- Beskyttelse af data mod ulovlig brug.
  - Begge er både internt (adgangsbegrænsning mv) og eksternt (hacking mv)
- Beskyttelse mod tab, tilintetgørelse eller skade på data.

Artikel 5, stk. 1, litra a-f

- En virksomhed skal altså sørge for, at dens persondata indsamles og behandles i overensstemmelse med principperne i artikel 5.

- Dette søges opretholdt ved:
  - at kræve at virksomheden kan påvise overholdelse, og
  - at tildele de personer, hvis data er registreret, rettigheder.

Registreredes rettigheder

- Først gennemgås kort de rettigheder, som forordningen (art. 13-23) tildeler de personer, hvis data er registeret (*de registrerede*).

- Langt de fleste af de registreredes rettigheder i persondataforordningen er allerede fastlagt i den nuværende persondatalov.

Registreredes rettigheder

- Retten til at modtage oplysning om en behandling af sine personoplysninger (oplysningspligt)
- Retten til at indsigt i sine personoplysninger.
- Retten til at få urigtige personoplysninger berigtiget.
- Retten til at få sine personoplysninger slettet *
- Retten til at gøre indsigelse mod at personoplysninger anvendes til direkte markedsføring.
- Retten til at flytte sine personoplysninger (dataportabilitet)*

Registreredes rettigheder

- Retten til at modtage oplysning om en behandling af sine personoplysninger (oplysningspligt)
  - At der skal gives oplysninger om den dataansvarliges identitet og kontaktoplysninger, formålene med behandlingen mv. er ikke nyt; findes oftest i ”persondatapolitik” afsnit på hjemmeside.
- Retten til indsigt i sine personoplysninger
  - Information om den registreredes rettigheder på anmodning.

Registreredes rettigheder

- Retten til at få urigtige personoplysninger berigtiget
  - Bemærk at underretning om berigtigelse skal ske til modtagere af persondata.
  - Ved uenighed om indhold / behandling af persondata kan den registrerede forlange, at data kun opbevares, medmindre der er givet samtykke til andet.

- Retten til at få sine personoplysninger slettet *
  - Ret til sletning er nyt.
  - Sletning bør ikke ske, før reklamationstid, og evt. garantiperiode er udløbet!
  - Sletning bør ikke ske, før bogføringsreglerne overholdt!

Registreredes rettigheder

- Retten til at gøre indsigelse mod at personoplysninger anvendes, bl.a. til direkte markedsføring
  - Reglerne om forbud mod spam, mod uanmodet henvendelse, robinson-listen mv. gælder stadig.
  - Før anvendelse skal den registrerede oplyses om sin ret til at gøre indsigelse mod anvendelse af data til direkte, lovlig markedsføring.
    - Bemærk at indirekte markedsføring ikke er omhandlet.

- Retten til at flytte sine personoplysninger(dataportabilitet) *
  - Ret til at få udskrift af sine egne persondata.
  - Ret til at få flyttet sine data over til en anden dataansvarlig, hvis muligt.

Overholdelse af forordningen

- Udover tildeling af rettigheder kræver forordningen, at en virksomhed kan påvise, at forordningen overholdes.

- Dette kan påvises på forskellige måder, med en kombination af tiltag. Der er ikke – slet ikke endnu – nogen enkelt måde, der 100% sikkert opfylder alle kravene.

- I det følgende gennemgås kort de tiltag, som forordningen foreslår og i nogle tilfælde kræver.

Overholdelse af forordningen

Standardindstillinger i virksomhedens IT (art. 25)

- Der er ikke krav om ny IT.
- Hvis det nuværende IT kan ændre standardindstillinger, bør virksomheden sørge for dataminimering, kun at indsamle og gemme data iht. formål, slette efter fx. 6 år efter seneste databehandling og indstille så registreredes rettigheder kan overholdes (ændring af ukorrekte data, udskrift af data mv.).
- Hvis virksomhedens nuværende IT ikke kan ændre standardindstillinger, må virksomheden bruge andre tiltag for at opfylde forordningen.
- Ved nyanskaffelse af IT bør IT-leverandøren afkræves, at persondataregulering i Danmark bliver overholdt.

Overholdelse af forordningen

Fortegnelse over behandlingsaktiviteter (art. 30)

- Hver virksomhed skal føre en intern fortegnelse – som Datatilsynet kan bede om en udskrift af ved eftersyn.
- Fortegnelsen over virksomhedens databehandling virker enormt omfattende, men se venligst Justitsministeriets forslag til fortegnelse for personaledata på de næste sider (fra betænkningens side 461 ff).
- Der er tale om en fortegnelse, der deles op i kategorier (personale, kunder, leverandører, (ejere, hvis straffeattester v. udbud)) og som laves en gang og herefter kan justeres årligt, hvis der er ændringer.

Eksempel på en fortegnelse over behandlingsaktiviteter ved HR

Dataansvarlig	**Myndighedens/virksomhedens navn, CVR-nr. og kontaktoplysninger** *(adresse, hjemmeside, telefonnummer og e-mail)*	Københavns Kommune Økonomiforvaltningen Rådhuset 1599 København V CVR:
	Den fælles dataansvarlige samt dennes kontaktoplysninger *(adresse, hjemmeside, telefonnummer og e-mail)*	-
	Den dataansvarliges repræsentant samt dennes kontaktoplysninger *(adresse, hjemmeside, telefonnummer og e-mail)* *(Offentlige myndigheder er ikke omfattet, jf. artikel 27, stk. 2, litra b)*	-
	Myndighedens/ virksomhedens databeskyttelsesrådgiver samt dennes kontaktoplysninger *(adresse, hjemmeside, telefonnummer og e-mail)*	DPO, Anders Andersen Kongestien XXX, 1111 Kongsted www.hjemmeside.dk + 45 88 88 88 88 dpo@andersandersen.dk

Justitsministeriets Betænkning nr. 1565 af 24.05.2017, s. 461-464

Formål (-ene)	**Behandlingens eller behandlingernes formål** *(et samlet, logisk sammenhængende formål med en behandling eller en række af behandlinger, som hermed angives som ét formål ud af alle samlede formål hos den dataansvarlige)*	Personaleadministration
Kategorierne af registrerede og kategorierne af personoplysningerne	**Kategori af registrerede personer** *(eksempelvis borger/kunder, partsrepræsentanter nuværende eller tidligere ansatte, andre virksomheder, andre myndigheder mv.)*	Der behandles oplysninger om følgende kategorier af registrerede personer: a) Ansøgere b) Ansatte c) Tidligere ansatte d) Pårørende e) Borger der henvender sig til Københavns Kommune f) Politikere

Justitsministeriets Betænkning nr. 1565 af 24.05.2017, s. 461-464

	Oplysninger, som behandles om de registrerede personer *(afkryds og beskriv de typer af oplysninger, som er omfattet af behandlingsaktiviteterne)*	Oplysninger, som indgår i den specifikke behandling. Beskriv:	
		Identifikationsoplysninger	X
		Oplysninger vedrørende ansættelsesforholdet til brug for administration, herunder stilling og tjenestested, lønforhold, oplysninger af relevans for lønindeholdelse, personalepapirer, uddannelse og sygefravær.	X
		Race, eller etnisk oprindelse	
		Politisk, religiøs eller filosofisk overbevisning	
		Fagforeningsmæssigt tilhørsforhold	X
		Helbredsoplysninger herunder genetisk data	X
		Biometrisk data med henblik på identifikation	X
		Seksuelle forhold	
		Strafbare forhold	X

Justitsministeriets Betænkning nr. 1565 af 24.05.2017, s. 461-464

Modtagerne af personoplysningerne	**Kategorier af modtagere som oplysninger er eller vil blive videregivet til herunder modtagere i tredjelande og internationale organisationer (eksempelvis andre myndigheder, virksomheder, borger/ kunder mv.)**	**1. Offentlige myndigheder (så vidt muligt myndighedens navn, f.eks. SKAT)** **2. Banker** **3. Kreditbureauer**
Tredjelande og internationale organisationer	Oplysninger om overførelse af personoplysninger til tredjelande eller internationale organisationer (eksempelvis databehandleres placering i tredjelande, databehandlers brug af cloudløsninger placeret i tredjelande)	Nej (Angivelse af virksomhed/ samarbejdspartner, hvis denne er placeret i tredjeland)
Sletning	Tidspunkt for sletning af oplysninger (de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger)	Oplysninger om tidligere ansatte slettes senest X år efter afslutningen af den journalperiode, hvor personalesagen er afsluttet. Oplysninger om ansøgere slettes senest X måneder efter afslutningen af den journalperiode, hvor sagen er afsluttet. Oplysninger overføres løbende til Rigsarkivet efter arkivlovens regler og Statens Arkivers bestemmelser herom.

Tekniske og organisatoriske sikkerhedsforanstaltninger	**Beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger** *(hvis muligt skal der gives en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, jf. artikel 32, stk. 1)*	Behandling af personoplysninger i forbindelse med HR-arbejde sker i overensstemmelse med interne retningslinjer, som bl.a. fastsætter rammerne for autorisation- og adgangsstyring og logning. Personoplysninger opbevares i pseudonymiseret og i kryptret form og transmitteres krypteret. Fysisk materiale opbevares aflåst. Der anvendes følgende sikkerhedsstandarder: ISOXXXXX.

Justitsministeriets Betænkning nr. 1565 af 24.05.2017, s. 461-464

Overholdelse af forordningen

Behandlingssikkerhed (art. 32)

- Hvad ligger i behandlingssikkerhed?
  - Der må ikke komme nogle uautoriserede ind til persondata (internt eller udefra via hacking).
  - Data må ikke slippe ud.
  - Indsamling og anvendelse af data skal ske på en sikker måde.
  - Data må ikke mistes/tilintetgøres/skades.
- Anmeldelse af sikkerhedsnedbrud (hacking m.v).

Overholdelse af forordningen

Behandlingssikkerhed (art. 32)

- Organisatorisk
  - F.eks. kan hver medarbejder kun få adgang til persondata, som har relevans for udførelsen af deres arbejde, sælgere adgang til kundeoplysninger, men ikke til medarbejderdata.
  - F.eks. har kun bogholder og ejer adgang til virksomhedens følsomme persondata.
  - Informere om aldrig at trykke på ukendte links, uanset lokkemaden!

Overholdelse af forordningen

Behandlingssikkerhed (art. 32)

- IT
  - Dobbelte passwords.
  - Pseudonymisering/kryptering ikke nødvendig ved almindelig personaleadministration af følsomme oplysninger.
- Dobbelte netværk (ex. standardkontor som alarm, varmestyring, gæstewifi, labelprinter på et netværk, alle virksomhedsdata, scanner/printer/fax på lukket, kabelnetværk) – afventer input fra Bjarne
- Firewalls, virustjek.
  - ALTID jævnligt udføre back up
  - ALDRIG acceptere at ens back up slettes efter fx tre måneder

Overholdelse af forordningen

Behandlingssikkerhed (art. 32)

- Anmeldelse af hacking m.v.
  - Inden 72 timer til Datatilsynet (eller tilsvarende myndighed).
  - Evt. informere de registrerede.

Overholdelse af forordningen

Konsekvensanalyse (art. 35)

- Gælder for virksomheder, som behandler høj-risiko persondata, særligt:
  - En systematisk, omfattende og automatisk vurdering af personlige forhold,
  - der har betydelig indvirkning på den pågældende person.
  - Behandling i et stort omfang af følsomme oplysninger.
  - Systematisk overvågning af et offentligt tilgængeligt område i et stort
  - omfang.
- DMs medlemmer pålægges pt. ikke at udføre en konsekvensanalyse.

Overholdelse af forordningen

Databeskyttelsesrådgiver (art. 37)

Kræves i virksomheder, som har følgende tre karakteristika:

- Behandling af personoplysninger er virksomhedens kerneaktivitet
- Personoplysninger behandles i et stort omfang, og
- Behandlingsaktiviteten består i regelmæssig og systematisk overvågning af personer eller behandlingen vedrører følsomme oplysninger.
- DMs medlemmer skal pt. ikke have en databeskyttelsesrådgiver.

Overholdelse af forordningen

Adfærdskodeks (art. 40)

- Udarbejdelse og overholdelse af et kodeks om persondata er ikke en pligt, MEN..
  - Det ville være en god ide at få de persondataregler, som skal overholdes af DMs medlemmer, skrevet ned.
  - Det ville være med til at øge medarbejderes opmærksomhed, forståelse og overholdelse af persondatareglerne.
  - Og ikke mindst skal virksomheden kunne påvise overholdelse af persondatareglerne: et kodeks, som medarbejderne er blevet informeret om og overholder, er et meget velegnet element til at påvise overholdelse af virksomhedens forpligtelser i henhold til forordningen.
- DM kan evt. udarbejde et kodeks, tilpasset medlemmernes virksomhedstyper, som medlemmerne kan anvende.

Overholdelse af forordningen

Certificering (art. 43)

- Certificering er også et velegnet element til at påvise overholdelse af virksomhedens forpligtelser i henhold til forordningen.
- Der er endnu ikke nogen certificeringsordninger på plads.
- Certificering af persondatabehandling er ikke et krav.

Overholdelse af forordningen

- Som nævnt er der endnu uafklarede områder i forordningen, og vejledninger til forordningen og en ny persondatalov afventes.

- Alligevel er der en del, som en virksomhed allerede kan gøre nu for at kunne overholde – og kunne påvise overholdelse af – persondataforordningen fra 25. maj 2018.

Hvad gør man i praksis?

Få styr på:

- 1. Hvilke data virksomheden har, herunder
  - Hvilke ikke-følsomme data for hhv. ansatte, kunder og samarbejdspartnere,
  - Hvilke følsomme data for hhv. ansatte, kunder og samarbejdspartnere,
  - Få slettet forældede data – og unødvendige data.
- 2. Lav herefter en fortegnelse over persondata (se side 26-30).

Hvad gør man i praksis?

Få styr på:

- 3. Hvilke data virksomheden indsamler:
  - Indsamles data til brug for kontraktindgåelse / som del af gennemførsel af aftale?
  - Hvis dette ikke er tilfældet, får virksomheden indhentet et skriftligt samtykke før indsamling?
  - Følsomme data kræver samtykke – indhent samtykkeerklæringer og gem dem.
- 4. Sørg herefter for at virksomhedens IT-indstillinger begrænser indsamling af persondata ifht. hvad der er brug efter aftalens formål eller samtykke samt at indstillingerne giver adgang til korrektion, sletning og udprintning af data.

Hvad gør man i praksis?

Få styr på:

- 5. Hvor virksomhedens data er og hvordan de sikres
    - Er IT-systemet forsvarligt sikret, både udefra og indefra?
    - Er adgang til data forsvarligt sikret, både udefra og indefra?
    - Der bør tages jævnlig back up, som gemmes, indtil næste back up er taget.
- 6. Sørg for at få lavet en oversigt over virksomhedens tiltag for at sikre sine persondata (IT-sikkerhed og organisatorisk).

Hvad gør man i praksis?

Få styr på:

- 7. Bliver virksomhedens persondata overført?
  - Hvor sker overførslen til? Cloudløsning?
  - Hvorfor sker overførslen – skal andre end virksomheden selv behandle virksomhedens persondata? I så fald kræves en særlig, skriftlig aftale med databehandleren.
  - Overførsel indenfor EU er typisk OK, men udenfor er ikke uden specifikt samtykke. Er der givet samtykke til overførslen?

Hvad gør man i praksis?

Få lavet eller gennemgået:

- 8. Persondatainformation (hvorfor indsamles data, hvad bruges det til, overføres data, registreredes rettigheder osv.) til kunder og samarbejdspartnere og læg informationen på virksomhedens hjemmeside.

- 9. Virksomhedens interne persondatapolitik (inklusiv persondatainformation til medarbejdere), gerne med afsæt i det adfærdskodeks, som DM får udarbejdet og gennemgå det med medarbejderne og gem det et tilgængeligt sted.

Hvad gør man i praksis?

Få samlet og gemt:

- 10. Informationen om gennemgang af punkterne 2)-9) og dokumenterne iht. punkt 2), 3), 6), 8), 9) og evt. 7) for at kunne dokumentere virksomhedens bestræbelser på at opfylde kravene skal gemmes samlet, hvis nu Datatilsynet skulle spørge om noget.

Hvad gør man i praksis?

- Gennemførsel af punkt 1)-10) kan bruges til:
  - En grundig oprydning i gamle data, det kan øge IT-kapaciteten,
  - Gennemførsel af ny, mindre datatunge arbejdsgange,
  - Sikre mod hacking og tab af data, og
  - Overholdelse af persondatabeskyttelsesforordningen.

AARHUS
Åboulevarden 31, 8000 Aarhus C
70 10 13 30 / aarhus@advokatgruppen.dk

HORSENS
Emil Møllers Gade 41 B, 1., 8700 Horsens
70 10 13 30 / horsens@advokatgruppen.dk

FREDERICIA
Danmarksgade 8, 7000 Fredericia
70 10 13 30 / fredericia@advokatgruppen.dk

ADVOKATGRUPPEN
RET LIGETIL. SIDEN 1987.