PLESNER PERSONDATA TEAM
3 år med GDPR

25. maj 2021

PLESNER

INDHOLDSFORTEGNELSE

EN UVELKOMMEN GÆST

***Michael Hopp**, partner*

For 14 måneder siden ramte corona-pandemien Danmark.

Samfundet blev lukket ned, og medarbejdere blev hjemsendt og afskediget. Teknologien blev for en stund vores livline, og erhvervslivet og den offentlige sektor gennemgik digitale tranformationer, da hjemmearbejdspladser skulle implementeres natten over. En udvikling der betød, at mange stod tilbage med ubesvarede spørgsmål om sikkerhed og håndtering af personoplysninger.

Sideløbende blev nye teknologiske idéer og initiativer fremført - alle med håbet om at kunne bekæmpe pandemien. Forskellige apps blev udviklet til bl.a. kontaktsporing og symptomverificering. Tiltag der kunne være afgørende i kampen mod covid-19, men som samtidig kunne være på kollisionskurs med privatliv og databeskyttelse.

Nu står vi godt et år senere på treårsdagen for GDPR, hvor hverdagen og normaliteten så småt er ved at indfinde sig under de nye betingelser. Det seneste år har i den grad sat digitaliseringen på dagsordenen - vi deler og afgiver data som aldrig før, og derfor synes GDPR også mere aktuel end nogensinde før.

Hos Plesner Persondata Team står vi fortsat klar til at hjælpe med at løse de mest komplicerede juridiske udfordringer - også selvom de er ledsaget af en uvelkommen gæst.

Rigtig god læselyst!

EN NY VIRKELIGHED

Også i den juridske verden

JURIDISK STATUS

***Michael Hopp**, partner*
***Jesper Husmer Vang**, senior counsel*

Siden vores seneste nyhedsbrev i maj 2020 er den altoverskyggende nyhed, at EU-domstolen den 16. juli 2020 afsagde dom i den såkaldte Schrems II-sag. Afgørelsen og den efterfølgende vejledning fra tilsynsmyndighederne vil få stor betydning for både private virksomheders og offentlige myndigheders mulighed for at overføre personoplysninger til lande udenfor EU/EØS, herunder f.eks. ved brug af cloudtjenester.

HVAD HANDLEDE SAGEN OM?

Sagen startede i 2013, da Max Schrems - i forlængelse af Edward Snowdens afsløringer af amerikansk masseovervågning - klagede til det irske datatilsyn (DPC) over Facebook Irlands overførsel af hans persondata til Facebook Inc. i USA. Overførslen var baseret på den daværende "Safe Harbor-ordning", der betød, at amerikanske virksomheder omfattet af ordningen blev anset for at være beliggende i et 'sikkert tredjeland'.

Baggrunden for klagen var, at Schrems mente, at USA's lovgivning om indsamling af data til brug for national sikkerhed mv. gjorde, at de amerikanske virksomheder, der var tilsluttet Safe Harbor-ordningen, ikke kunne sikre et beskyttelsesniveau for persondata, som levede op til kravene i europæisk databeskyttelseslovgivning.

De irske domstole forelagde sagen for EU-Domstolen, som i oktober 2015 erklærede Safe Harbor-ordningen ugyldig. I dommen fastlagde EU-Domstolen samtidig, at niveauet for beskyttelse af personoplysninger i et 'sikkert tredjeland' i det væsentlige skal svare til niveauet for beskyttelse af personoplysninger i EU - man anvendte formuleringen "essentially equivalent".

I 2016 blev Safe Harbor-ordningen erstattet af den tilsvarende Privacy Shield-ordning, som efter EU-Kommissionens opfattelse rettede op på manglerne i Safe Harbor ordningen, bl.a. i kraft af stærkere tilsyns- og håndhævelsesmekanismer, herunder en uafhængig Privacy Shield-ombudsmand.

I forlængelse af EU-Domstolens afgørelse valgte Max Schrems at omformulere den oprindelige klage til det irske datatilsyn, da Facebook - nu på baggrund af tilrettede standardkontraktbestemmelser (også kaldet "SCC") - fortsat overførte personoplysninger til USA. Schrems mente ikke, at de tilrettede SCC gav ham en beskyttelse som inden for EU-området, særligt på grund af den nævnte lempelige amerikanske lovgivning om myndighedernes adgang til indsamling af persondata.

Det irske datatilsyn vurderede ved behandlingen af den nye klage, at der var et større og mere systematisk problem med SCC, hvorfor DPC valgte at indbringe sagen for den irske landsret, så sagen kunne forelægges præjudicielt for EU-Domstolen.

VÆSENTLIGE KONKLUSIONER FRA EU-DOMSTOLEN

1. EU-domstolen fastslog i dommen, at der ved overførsel af personoplysninger til lande udenfor EU/EØS samlet set skal opnås et niveau for beskyttelse (af de registreredes rettigheder og frihedsrettigheder), "der i det væsentlige svarer til det niveau, der er sikret i Den Europæiske Union ved denne forordning, sammenholdt med Den Europæiske Unions charter om grundlæggende rettigheder."

   Det skal med andre ord sikres, at beskyttelsesniveauet i det pågældende tredjeland er "essentially equivalent" med det niveau man har i EU.

   Ovennævnte beskyttelsesniveau skal opnås, både når Kommissionen godkender sikre tredjelande i medfør af GDPR artikel 45, og når der overføres personoplysninger på grundlag af "fornødne garantier" efter GDPR artikel 46, herunder f.eks. ved anvendelse af Kommissionens standardkontraktbestemmelser (SCC) og bindende virksomhedsregler (BCR).

   Kravet om "essentially equivalent" gælder dog ikke ved overførsler baseret på de særlige undtagelser i artikel 49.

2. Efter en gennemgang af amerikansk lovgivning - specifikt FISA Act Section 702 og Executive Order 12,333 - konkluderede EU-domstolen, at Kommissionens afgørelse efter GDPR artikel 45 i forhold til den såkaldte Privacy Shield-ordning ikke sikrer

et beskyttelsesniveau, der er "essentially equivalent" med beskyttelsesniveauet i EU.

På denne baggrund valgte EU-domstolen at annullere Privacy Shield-ordningen. Ved sin afgørelse lagde EU-domstolen vægt på, at ovennævnte amerikanske lovgivning var uklar og disproportional, ligesom der manglede effektive retsmidler for de berørte personer. Dette er i strid med artikel 47 og 52 i Den Europæiske Unions Charter om Grundlæggende Rettigheder.

3. SCC er fortsat generelt gyldige som overførselsgrundlag, jf. GDPR artikel 46.

   Brug af SCC kræver dog - som nævnt ovenfor - at der kan opnås et beskyttelsesniveau, der er "essentially equivalent" med beskyttelsesniveauet i EU. Ved vurderingen heraf må parterne se på deres aftale (SCC) samt reglerne om myndighedsadgang til oplysninger i det pågældende tredjeland.

   Hvis reglerne om myndighedsadgang i et tredjeland forringer den beskyttelse af de registrerede, der forsøges opnået ved hjælp af SCC, skal der træffes supplerende foranstaltninger, således at beskyttelsen af de registrerede bringes op på et niveau, som er "essentially equivalent". Ved vurderingen heraf kan man tage udgangspunkt i de 4 Essentielle Europæiske Garantier, som de europæiske data datatilsyn (EDPB) har genbeskrevet i den nye vejledning - den kan læses her.

4. Dataeksportøren skal forud for hver enkelt overførsel - sag for sag - undersøge, om national lovgivning i tredjelandet forringer den beskyttelse, som forsøges tilvejebragt ved hjælp af SCC. Denne undersøgelse/analyse skal foretages i overensstemmelse med punkt 3 ovenfor.

   Viser analysen, at der ikke kan opnås et beskyttelsesniveau, der er "essentially equivalent", skal man som dataeksportør implementere supplerende foranstaltninger, som samlet set bringer beskyttelsen op på "essentially equivalent".

5. Kan beskyttelsesniveauet "essentially equivalent" ikke opnås i praksis - heller ikke med supplerende foranstaltninger - skal dataeksportøren undlade at påbegynde overførslen, alternativt bringe en igangværende overførsel til ophør.

HVAD KAN SUPPLERENDE FORANSTALTNINGER BESTÅ I?

De europæiske datatilsyn (EDPB) er i et udkast til anbefalinger fra den 10. november 2020 kommet med forslag til, hvilke supplerende foranstaltninger, der vil kunne benyttes for at forsøge at opnå et beskyttelsesniveau, som er "essentially equivalent". Anbefalingerne - der stadig kun foreligger i udkast - kan læses her.

EDPB beskriver tre typer af foranstaltninger:

- Tekniske foranstaltninger
  - Kryptering - både under transport og ved opbevaring
  - Pseudonymisering
  - Opbevaring af "nøgler"
- Kontraktuelle foranstaltninger
  - Forpligte importør til at oplyse om "access requests"
  - Styrke adgang til kontrol med importør
  - Forpligte importør til at informere om lovændringer
- Organisatoriske foranstaltninger
  - Fastsætte procedurer for håndtering af tredjelandsoverførsler (i koncern)
  - Fastsætte procedurer til sikring af at der ikke overføres mere end højst nødvendigt

Ved valget af foranstaltninger er det afgørende, om den valgte foranstaltning set fra de registreredes synsvinkel effektivt kan garantere et beskyttelsesniveau, der er "essentially equivalent". Hvorvidt en eller flere supplerende foranstaltninger er effektive vil være en dynamisk vurdering. En foranstaltning, der i en sammenhæng kan være effektiv, vil måske ikke være det i en anden sammenhæng.

Ifølge EDPB vil kontraktuelle og organisatoriske foranstaltninger generelt ikke kunne stå alene. Dette giver god mening, da hverken kontraktuelle eller organisatoriske foranstaltninger binder en myndighed i et tredjeland. Man vil således altid være nødt til at anvende tekniske foranstaltninger, hvis man kommer frem til, at man ikke kan opnå et beskyttelsesniveau, der er "essentially equivalent", når SCC'erne sammenholdes med lovgivningen i et givent tredjeland.

EDPB opstiller en række scenarier, hvor EDPB vurderer, om (tilgængelige) tekniske foranstaltninger henholdsvis vil og ikke vil være effektive.

I den forbindelse er det formentlig eksempel 6, der har givet anledning til flest hovedbrud. I eksemplet anfører EDPB, at man ikke har været i stand til at identificere tekniske foranstaltninger, der vil være effektive i forhold til en situation, hvor der sker overførsel af personoplysninger til en cloud leverandør eller andre databehandlere i et tredjeland, der har brug for adgang til oplysninger i klar tekst. Dette er situationen for eksempelvis Office365 løsninger.

EDPB kan således ikke se, at kendte forretningsmodeller inden for cloud mv. muliggør effektive foranstaltninger på nuværende tidspunkt.

KAN MAN ANLÆGGE EN RISIKOBASERET TILGANG?

Det har været diskuteret, om man ved vurderingen af lovgivning i tredjelande og behovet for supplerende foranstaltninger kan anlægge en risikobaseret tilgang og således f.eks. lægge vægt på oplysningernes karakter og sandsynligheden for, at de overførte oplysninger vil være af interesse for myndighederne i et tredjeland.

En sådan risikobaseret tilgang synes imidlertid at være blevet afvist af EU-domstolen i dommes præmis 171. Hér anfører EU-domstolen således følgende: *"Domstolen har allerede fastslået, at videregivelse af personoplysninger til en tredjemand såsom en offentlig myndighed udgør et indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, uanset hvad de videregivne oplysninger efterfølgende bruges til. Det samme gælder opbevaring af personoplysninger og de offentlige myndigheders adgang hertil med henblik på brug heraf, uanset om de pågældende oplysninger vedrørende privatlivet er følsomme oplysninger, eller om indgrebet har medført eventuelle ubehageligheder for de berørte […]."*

> *Hvis man stadig overfører oplysninger til USA baseret på Privacy Shield-ordningen, skal man straks finde et andet overførselsgrundlag, hvis muligt, eller bringe overførslen til ophør*

Hvis man læser høringssvarene til EDPB's anbefalinger, vil man dog kunne se, at der i mange af høringssvarene plæderes for en risikobaseret tilgang.

Da vi endelig har til gode at se de endelige anbefalinger fra EDPB, er det svært at sige, om en risikobaseret tilgang vil vinde gehør hos EDPB.

HVAD BØR MAN GØRE NU?

Hvis man stadig overfører oplysninger til USA baseret på Privacy Shield-ordningen, skal man straks finde et andet overførselsgrundlag, hvis muligt, eller bringe overførslen til ophør.

Ved brug af SCC'er skal alle overførsler til tredjelande analyseres nærmere. Der skal i den forbindelse foretages en konkret analyse og fastsættes supplerende foranstaltninger, hvis analysen viser, at der er behov derfor.

Når man som dataeksportør skal foretage en vurdering af, om der lovligt kan overføres personoplysninger til lande uden for EU, kan der f.eks. tages udgangspunkt i følgende:

1. Afdæk alle tredjelandsoverførsler samt overførselsgrundlagene for overførslerne.

   Husk i den forbindelse, at en overførsel både kan ske ved fysisk overførsel af oplysninger, men også ved fjernadgang til oplysninger, herunder f.eks. i forbindelse med support.

   Det er ligeledes vigtigt, at man får styr på hele kæden af databehandlere og underdatabehandlere.

2. Vurder lovgivningen i de relevante tredjelande samt påvirkningen af beskyttelsesniveauet.

   Reglerne om myndighedsadgang i tredjelandene skal holdes op i mod GDPR og Den Europæiske Unions charter om grundlæggende rettigheder. Der kan også med fordel tages udgangspunkt i de 4 Essentielle Europæiske garantier, der er omtalt ovenfor.

3. Hvis vurderingen under punkt 2 viser, at lovgivningen i et tredjeland forringer den beskyttelse, som SCC er tiltænkt at tilvejebringe, skal der implementeres supplerende foranstaltninger. EDPB's anbefalinger vil kunne give inspiration til, hvad man kan gøre og om det er "effektivt".

4. Tilpas eventuelle databehandleraftaler, bl.a. i forhold til myndighedsadgang. Lever databehandleraftalen f.eks. op til GDPR artikel 28, stk. 3.

5. Vær opmærksom på, at Kommissionen har offentliggjort et nyt udkast til SCC. Når disse er endelig vedtaget, vil man have et år til at udskifte gamle SCC med den nye.

6. Følg løbende op på dine vurderinger. Lovgivningen i et tredjeland kan f.eks. ændre sig.

VIL VI SE LØSNINGER FRA INDUSTRIEN?

Det er vores oplevelse, at industrien allerede er i gang med at forsøge at løse de udfordringer, der er opstået i kølvandet på Schrems II.

Vi har således allerede set cloud leverandører, der har indarbejdet yderligere kontraktuelle foranstaltninger i deres aftaler mv. Disse kontraktuelle foranstaltninger vil dog ikke i sig selv være tilstrækkelige, da de som nævnt ovenfor ikke binder myndighederne i tredjelande. De er derfor ikke "effektive" i forhold til at opnå et beskyttelsesniveau, der er "essentially equivalent".

Det er vores vurdering, at vi først vil se reelle brugbare løsninger på bagkant af EDPB's offentliggørelse af de endelige anbefalinger, som er på trapperne i juni 2021.

Vi ved pt. ikke, hvor det ender, men vi har stor tiltro til, at de mange dygtige og innovative medarbejdere, der arbejder hos cloud leverandører mv., vil komme op med smarte løsninger, der muliggør, at europæiske virksomheder og myndigheder kan benytte de teknologier, som vi har vænnet os til, og i overensstemmelse med de europæiske regler om databeskyttelse.

PLESNER GDPR MASTER CLASS

Tirsdag den 29. juni 2021 afholder Plesner GDPR Master Class om overførsel af personoplysninger til tredjelande, hvor vi vil give vores deltagere en grundig indføring i mulighederne for at overføre personoplysninger til tredjelande.

Vi vil derfor bruge en hel dag på at gennemgå kapitel V i GDPR - og derigennem give deltagerne både det fulde overblik, men også alle detaljerne i de enkelte typer af overførselsgrundlag.

Du kan læse mere om Plesner GDPR Master Class her.

MØD ÉN AF VORES EKSPERTER

***Peter Østerby Mønsted**, advokat, director*
***Specialer:** Persondataret, ePrivacy og operationel compliance*

Mit navn er Peter Østerby Mønsted, og jeg er director i Plesners persondatateam.

Min juridiske karriere tog sin spæde begyndelse tilbage i 2009, hvor jeg startede som student på et mindre advokatkontor i København. Efter at have fået smag for det juridiske erhverv, byttede jeg for en stund København ud med Sydney, da jeg studerede et år på University of New South Wales.

I februar 2012 startede jeg som Legal Intern hos Plesner, og siden da har jeg trofast fuldt karriere-rangstien her. Oprindeligt beskæftigede jeg mig med kontrakts- og selskabsret, inden jeg blev fuldblods persondatajurist.

Jeg synes, at persondata og databeskyttelse er interessant, fordi det vedrører os alle. Vi lever i en digitaliseret verden, med et stadig stigende brug af data.

Der er ingen tvivl om, at udviklingen kun går imod en mere og mere digital verden - og på den rejse handler det i høj grad om fortsat at sikre borgernes tillid. GDPR er derfor et område, hvis eksistensberettigelse og relevans er fortsat.

I mit virke som director værdsætter jeg de mange klientrelationer. Jeg bestræber mig på at skabe et rum, hvor tonen er uformel, men fagligheden høj. Jeg sætter pris på at være i øjenhøjde med klienterne, hvor vi kan diskutere og drøfte forskellige persondataretlige problemstillinger og derigennem finde de bedste løsninger.

> *Der er ingen tvivl om, at udviklingen kun går imod en mere og mere digital verden - og på den rejse handler det i høj grad om fortsat at borgernes tillid*

KRAV OM WHISTLE-BLOWERORDNINGER FOR MYNDIGHEDER OG VIRKSOMHEDER

***Michael Hopp**, partner*
***Jacob Falsner**, senior counsel*

Forslaget til lov om beskyttelse af whistleblowere forventes vedtaget den 3. juni 2021. Med loven skal en bred kreds af myndigheder og virksomheder etablere en whistleblowerordning senest den 17. december 2021.

Loven implementerer det såkaldte "whistleblowerdirektiv" (Direktiv 2019/1937) om beskyttelse af personer, der indberetter overtrædelser af (udvalgte dele af) EU-retten.

Rationalet bag direktivet er, at ved at beskytte whistleblowere og ved at stille krav til selve whistleblowerordningen, så opnås en styrket håndhævelse af EU-retten, da flere whistleblowere vil stå frem.

Loven forventes at træde i kraft den 17. december 2021 og vil indebære, at alle offentlige og private virksomheder med mindst 50 ansatte skal etablere en whistleblowerordning med virkning fra denne dato. Fristen for private arbejdsgivere med mellem 50 og 249 ansatte er dog først den 17. december 2023. Ved opgørelsen af antal "ansatte" medregnes alle arbejdsgiverens arbejdstagere uanset beskæftigelsesgrad.

ANVENDELSESOMRÅDET

Udover indberetninger om overtrædelse af udvalgte dele af EU-retten, er det i Danmark besluttet at udvide beskyttelsen til også at omfatte whistleblowere, der indberetter om "alvorlige lovovertrædelser eller øvrige alvorlige forhold", som har offentlighedens interesse i at blive afdækket (f.eks. misbrug af økonomiske midler, tyveri, svig, bedrageri, bestikkelse og enhver form for sexchikane).

En arbejdsgiver, der qua antallet af ansatte falder inden for loven, og som i forvejen er omfattet af en lovpligtig whistleblowerordning, eksempelvis i medfør af § 75a i lov om finansiel virksomhed, skal indrette sin whistleblowerordning, så den opfylder begge regelsæt.

INTERN WHISTLEBLOWERORDNING

Ifølge loven påhviler der alene en pligt for arbejdsgiveren til at etablere en intern whistleblowerordning, der skal gøre det muligt for ansatte at foretage indberetning. Arbejdsgiveren kan dog udvide kredsen af personer, der kan indberette under ordningen, til også at omfatte eksempelvis tidligere ansatte, bestyrelsesmedlemmer, leverandører og samarbejdspartnere. Loven omfatter dog kun indberetninger, der vedrører arbejdsrelaterede forhold.

Med loven etableres der også en ekstern, offentlig whistleblowerordning, som skal drives af Datatilsynet. Whistlebloweren beslutter selv, om indberetningen skal ske via den interne eller den eksterne ordning. Det er dog givet, at hvis en arbejdsgiver etablerer en snæver intern whistleblowerordning, så vil det føre til flere indberetninger til den eksterne ordning. Vedtages lovforslaget i dets nuværende form, er der bl.a. lagt op til, at Datatilsynet skal håndtere indberetninger om sexchikane vedrørende to ansatte på en arbejdsplads!

SAGSBEHANDLINGEN

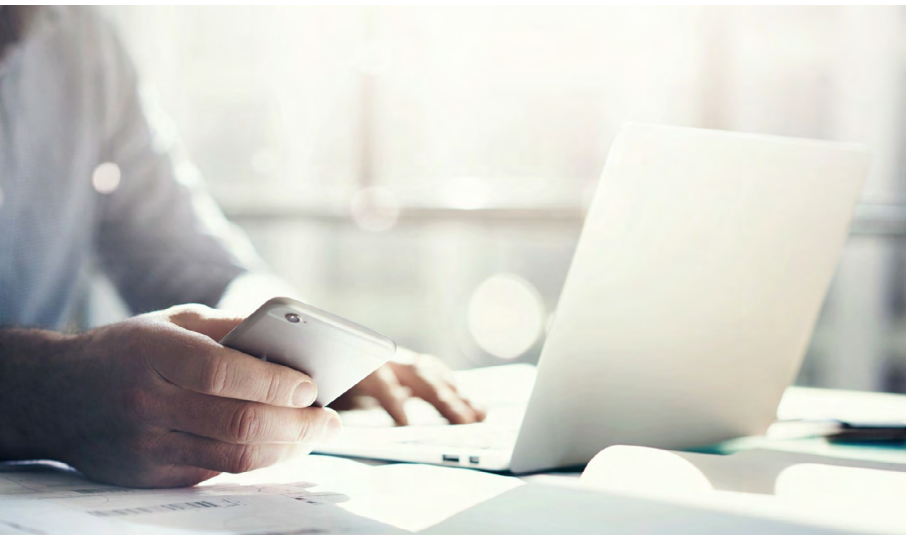
Arbejdsgiveren skal fastsætte procedurer for modtagelse og behandling af indberetninger i whistleblowerordningen, herunder udpege en upartisk whistleblowerenhed, der kan håndtere indberetninger under ordningen. Enheden kan eksempelvis bestå af HR- eller compliance-medarbejdere, men det er også muligt at outsource opgaven til ekstern tredjepart, f.eks. advokater.

Whistleblowerenheden har bl.a. til opgave at modtage indberetninger og forestå kontakt med whistlebloweren. Man skal bl.a. sikre, at der kvitteres for indberetningen senest 7 dage efter modtagelsen, at der sker opfølgning på indberetninger samt gives feedback til whistlebloweren.

Arbejdsgiveren skal opbevare skriftlig dokumentation for etableringen og for procedurerne for whistleblowerordningen. Arbejdsgiveren bl.a. udarbejde en procedure - en vejledning - vedrørende whistleblowerordningen, herunder hvad der kan indberettes om, hvem der kan indberette under ordningen osv.

Arbejdsgiveren beslutter selv, om det skal være muligt at indberette skriftlig eller mundtligt

eller begge dele, og hvorvidt arbejdsgiveren ønsker at give mulighed for anonyme indberetninger. En adgang til at indberette mundtligt afføder bl.a. en pligt for arbejdsgiveren til afholde et fysisk møde med whistlebloweren, hvis personen beder om det.



BESKYTTELSEN AF WHISTLEBLOWEREN

En whistleblower, der i god tro indberetter under whistleblowerordningen, er under nærmere betingelser sikret en særlig beskyttelse. Blandt andet anses whistlebloweren ikke for at for at have tilsidesat sin tavshedspligt.

En whistleblower, der udsættes for repressalier som følge af indberetningen, har ret til en godtgørelse, og afskedigelse af en whistleblower kan underkendes. Loven introducerer endvidere en særlig bevisbyrderegel, hvorefter arbejdsgiveren skal bevise at en ulempe, som en whistleblower er påført efter at have foretaget en indberetning, ikke udgør repressalier som følge af indberetningen.

DELING AF RESSOURCER

Det er lovens udgangspunkt, at alle arbejdsgivere med eget CVR-nummer, som omfattes af loven, skal oprette en selvstændig whistleblowerordning for at sikre "let tilgængelighed" og "nærhed". Dog kan private arbejdsgivere med 50-249 ansatte dele ressourcer med hensyn til modtagelse af indberetninger og undersøgelser i forbindelse hermed, hvilket omvendt betyder at arbejdsgivere med mere end 249 ansatte ikke kan indgå i en fælles intern indberetningskanal.

Det er dog fortsat muligt for koncernforbundne arbejdsgivere at outsource sine individuelle whistleblowerordninger til samme eksterne tredjepart.

PLESNERS LØSNING

Plesner tilbyder en færdig whistleblowerordning, der lever op til lovkravene inden for de enkelte områder. Ordningen tager også højde for de krav, der følger af lov om whistleblowere. Der er samtidig mulighed for at udvide ordningens anvendelsesområde, og eksempelvis give samarbejdspartnere eller kunder mulighed for at indberette.

Indberetninger til whistleblowerordningen screenes af Plesner i forhold til, om indberetningen falder inden for ordningen. Før indberetningen sendes videre til kunden, kontrollerer vi, at den ikke sendes til personer, der er berørt af indberetningen.

Whistleblowerordningen er en brugervenlig og sikker løsning, der giver mulighed for fuld anonymitet og skaber rammen for, at man effektivt og fortroligt kan håndtere indberetningerne.

Plesner rådgiver også om alle juridiske aspekter vedrørende whistleblowerordninger, og bistår med alt lige fra etableringen af en whistleblowerordning frem til afdækningen af forhold indberettet under ordningen, eventuelt i form af en advokatundersøgelse med inddragelse af specialeområder i Plesner.

Såfremt du ønsker at høre nærmere om Plesners løsning, er du velkommen til at kontakte advokat, partner Michael Hopp eller advokat Jacob Falsner.

Du kan også læse mere om Plesners løsning her.

UDVALGTE AFGØRELSER

Udvalgte afgørelser fra Datatilsynet
Periode: *Fra 25. maj 2020 og frem*

SAGER VEDRØRENDE GRUND-PRINCIPPERNE I ART. 5

27. juli 2020: *Arp-Hansen Hotel Group politianmeldt for manglende sletning*

Datatilsynet har i forlængelse af et tilsynsbesøg hos Arp-Hansen Hotel Group politianmeldt og indstillet virksomheden til en bøde på 1.100.000 kr. for manglende sletning af ca. 500.000 kundeprofiler. Datatilsynet kunne under tilsynsbesøget konstatere, at et bookingsystem indeholdt personoplysninger, som efter Arp-Hansens egne fastsatte slettefrister burde være slette flere år tidligere.

Sagen illustrerer endnu engang vigtigheden af overholdelse af det grundlæggende princip om opbevaringsbegrænsning i GDPR, art. 5.1.e. Sagen er i øvrigt den sidste af tre slettetilsyn, der blev afholdt i efteråret 2018. De to øvrige sager - Taxa 4X35 og IdeDesign - er også endt med bødeindstillinger.

3. november 2020: *Alvorlig kritik af Rejsekort A/S' behandling af personoplysninger på forkert behandlingsgrundlag*

På baggrund af en klage udtalte Datatilsynet bl.a. alvorlig kritik af Rejsekort A/S for at have benyttet samtykke som behandlingsgrundlag, når dette grundlag ikke kunne anses for det mest hensigtsmæssige. Dette var ikke i overensstemmelse med GDPR artikel 5.1.a. om lovlighed, rimelighed og gennemsigtighed.

Datatilsynet lagde i den forbindelse bl.a. til grund, at Rejsekort havde tilrettelagt sin behandling af personoplysninger således, at der skulle ske skift af behandlingsgrundlaget, hvis samtykket blev trukket tilbage, idet Rejsekort fortsat ville behandle oplysninger om klager i medfør af forordningens artikel 6, stk. 1. Rejsekort ville således efter det oplyste anvende artikel 6, stk. 1, litra b, c og f, vedrørende klagers aftaleindgåelse, rejsedata, træk/indbetalinger på i kortet forbindelse med klagers benyttelse af sit rejsekort.

Herudover udtalte tilsynet, at en dataansvarlig som altovervejende udgangspunkt ikke bør skifte behandlingsgrundlag, efter behandlingen af personoplysninger er påbegyndt, og at et skift af behandlingsgrundlag anses som særlig problematisk, når behandlingen sker på baggrund af et samtykke, da et samtykke efter databeskyttelsesforordningen er et udtryk for, at de registrerede gives et reelt valg og kontrol over, hvordan deres oplysninger behandles.

Datatilsynet udtalte endvidere alvorlig kritik af, at Rejsekort ikke slettede oplysningerne om aftaleindgåelse og rejsedata, da klager trak sit samtykke tilbage, jf. databeskyttelsesforordningens artikel 17, stk. 1, litra b, jf. artikel 6. Rejsekort fik samtidig et påbud om at slette oplysningerne.

Sagen viser, at det er meget vigtigt, at man gør sig grundige overvejelser om sit behandlingsgrundlag, inden en behandling påbegyndes. Samtykke bør heller ikke benyttes som behandlingshjemmel, hvis man kan finde et andet passende hjemmelsgrundlag.

10. februar 2021: *Regionale lægevagters optagelse af telefonsamtaler*

Datatilsynet udtalte på baggrund af en klage alvorlig kritik af Lægevagten Region Syddanmark for at have opbevaret optagelser af telefonsamtaler, som var mere end 5 år gamle. Regionen fik ligeledes et påbud om at slette.

I sagen mente Regionen, at optagelserne var del af patientjournalen, hvorfor optagelserne skulle opbevares i 10 år fra seneste kontakt.

Efter en forelæggelse for Sundhedsministeriet afviste Datatilsynet, at optagelserne var en del af patientjournalen, hvor de almindendelige regler i GDPR artikel 5.1.e. fandt anvendelse.

I den forbindelse fandt Datatilsynet, at opbevaring i op til 5 år var ok, idet 5 år var den absolutte frist for indgivelse af klager over Lægevagten.

Afgørelsen er bl.a. interessant idet den viser, at Datatilsynet er villig til at acceptere relativt lange opbevaringsfrister for optagne telefonsamtaler, når optagelserne sker til dokumentationsformål.

Det bemærkes i den forbindelse, at Datatilsynet - i tilsynets vejledning om optagelse af telefonsamtaler fra november 2020 - lægger op til en maksimal opbevaringsperiode på 6 måneder.

SAGER VEDRØRENDE ANMODNINGER FRA DE REGISTRERede

20. august 2020: *Klage over manglende insigt*

I en klagesag udtalte Datatilsynet, at det var i overensstemmelse med databeskyttelsesreglerne, at forsikringsselskabet, Velliv, ikke gav en tidligere kunde indsigt i alle oplysninger, som forsikringsselskabet behandlede om vedkommende.

Registrerede har efter GDPR art. 15 ret til at få indsigt i personoplysninger, som behandles om vedkommende. Datatilsynet udtalte i sagen, at navne og stillingsbetegnelser på medarbejdere og en lægekonsulent som klart udgangspunkt ikke udgjorde en personoplysning om klager, hvorfor disse oplysninger ikke var omfattet af indsigtsretten.

Velliv kunne endvidere undtage en korrespondance med en advokat efter DBL § 22.1 samt et internt arbejdsdokument med en juridisk vurdering af en potentiel retssag, idet dokumentet ikke indeholdt faktiske personoplysninger, som ikke allerede var udleveret til klageren.

Sagen illustrerer, at der kan gøres undtagelse til indsigtsretten i særlige tilfælde, men også at adgangen til at gøre undtagelse er begrænset.

SAGER VEDRØRENDE PERSONDATASIKKERHED OG BRUD

11. juni 2020: *Utilstrækkelig sikkerhed ved levering af inkassobreve*

Datatilsynet har i forlængelse af en klagesag vedrørende levering af inkassobreve fra Alektum, udtalt kritik af at Alektums databehandler, RoestNielsen, ikke levede op til kravene i GDPR art. 32 om et passende sikkerhedsniveau. RoestNielsens leveringsmetode ved levering af inkassobreve var ikke i overensstemmelse med instruksen fra den dataansvarlige.

Datatilsynet lagde ved afgørelsen vægt på, at inkassobreve ikke blev afleveret i postkasse, uagtet at vedkommende havde postkasse. Der blev endvidere lagt vægt på den store risiko for at brevene ville gå tabt i et eventuelt uvejr, og at uvedkommende kunne tilgå brevene.

Oplysningernes karakter udgjorde i sagen en skærpende omstændighed, idet der var tale om oplysninger om inkasso og gæld, og da eksponering af sådanne oplysninger kan indebære alvorlige krænkelser for de berørte borgerne, herunder konsekvenser for de registreredes integritet og omdømme. Det talte dog som formildende omstændighed, at der var tale om en enkeltstående hændelse, og at det var en enkelt konsulent, der handlede i strid med retningslinjerne.

Sagen illustrerer, at det, som dataansvarlig, er vigtigt at få givet klare instruktioner til sine databehandlere, da dette kan betyde, at Datatilsynet vælger at rette sit fokus mod databehandleren i tilfælde af f.eks. brud på persondatasikkerheden.

12. juni 2020: *Utilstrækkelige sikkerhedsforanstaltninger hos Region Syddanmark*

Datatilsynet har i forlængelse af en anmeldelse om brud på persondatasikkerheden udtalt alvorlig kritik af Region Syddanmarks behandling af personoplysninger. I sagen havde alle regionens ansatte igennem en årrække haft adgang til et netværksdrev, hvor der lå fortrolige og følsomme personoplysninger om mange borgere.

Ud over at udtale kritik meddelte Datatilsynet samtidig Region Syddanmark et påbud om at underrette de registrerede om bruddet på persondatasikkerheden. Henset til det store antal ansatte med adgang (potentiel adgang for 30.000 medarbejdere til mere end 800.000 borgeres personoplysninger) og karakteren af personoplysningerne (bl.a. oplysninger af fortrolig karakter) vurderede Datatilsynet, at det udgjorde en høj risiko for de registreredes rettigheder.

Datatilsynet udtalte i sagen, at *"når den dataansvarlige ikke har kunne fastslå, om en potentiel adgang er udnyttet eller ej, er det ikke nok at lukke adgangen, men nødvendigt også at underrette de registrerede, fordi risikoen for dem er vurderet som høj."*

I sagen understreger Datatilsynet på ny, at tilsynet har en klar forventning om, at man underetter de registrerede om brud på persondatasikkerheden, hvis man har kompromitteret fortrolige og/eller følsomme personoplysninger. Underretning kan kun undlades, hvis det kan dokumenteres, at bruddet konkret ikke har haft en betydning for de registreredes rettigheder og frihedsrettigheder, herunder via af kontrol af en log eller lignende.

18. juni 2020: *Uautoriseret adgang til videoovervågning i Salling*

Datatilsynet har i en sag, hvor en ansat gav en tidligere kollega mulighed for at gennemgå tv-overvågningsbilleder, fundet, at Salling havde implementeret passende tekniske og organisatoriske foranstaltninger, jf. artikel 32. Datatilsynet udtalte dog kritik af, at Salling først efter 10 dage anmeldte sikkerhedsbruddet til Datatilsynet.

Datatilsynet kom i afgørelsen frem til, at Salling ikke kunne anses for ansvarlig for den pågældende hændelse og udtalte, at "medarbejderen foretog indtil flere handlinger, som lå udover, hvad der med rimelighed kunne forventes, at Salling skulle have været forberedt på eller truffet foranstaltninger med henblik på at undgå."

Ved afgørelsen lagde Datatilsynet bl.a. vægt på Sallings e-learning, politikker, skiltning, fortrolighedsaftaler og medarbejderhåndbøger.

30. juni 2020: *Lejre Kommune politianmeldt for mangende behandlingssikkerhed*

Datatilsynet har i forlængelse af en anmeldelse om brud på persondatasikkerheden politianmeldt og indstillet Lejre Kommune til en bøde på 50.000 kr. for ikke at overholde sin forpligtelse til at gennemføre passende sikkerhedsforanstaltninger. Datatilsynet udtalte samtidig alvorlig kritik af, at Lejre Kommune ikke levede op kravet om underretning af de registrerede i forbindelse med bruddet på persondatasikkerheden.

Af sagen fremgik det, at Lejre Kommunes afdeling, Center for Børn og Unge, havde haft en fast praksis, hvorefter mødereferater indeholdende personoplysninger af særdeles følsom og beskyttelsesværdig karakter, herunder om borgere under 18 år, blev uploadet på kommunens medarbejderportal. På medarbejderportalen var der potentiel adgang til oplysningerne for en stor del af kommunens ansatte, uanset om de pågældende medarbejdere arbejdede med den type af sager.

Datatilsynet udtalte bl.a., at: *"Det er vores generelle opfattelse, at kommuners behandling af oplysninger af fortrolig karakter som minimum skal beskyttes med adgangskontrol. Som udgangspunkt er det kun medarbejdere med et arbejdsbetinget behov, som bør have adgang til oplysningerne."*

Efter vores vurdering illustrerer sagen, at Datatilsynet er tilbøjelige til at indstille til bøde, når man ikke har styr på hel basal behandlingssikkerhed (her adgangskontrol). Man har set noget tilsvarende i sagerne, hvor Datatilsynet har politianmeldt Gladsaxe og Hørsholm Kommune.

4. august 2020: *PrivatBo politianmeldt for videregivelse af lejeres fortrolige oplysninger*

I forlængelse af et brud på persondatasikkerheden har Datatilsynet politianmeldt og indstillet PrivatBo til en bøde på 150.000 kr. for videregivelse af lejeres fortrolige oplysninger ved uddeling af tilbudsmateriale på 424 USB-nøgler.

Datatilsynet udtalte i anledning af politianmeldelsen bl.a.: "I en sag som den pågældende er det vores vurdering, at PrivatBo som minimum burde have gennemgået tilbudsmaterialet, før det blev udleveret til andre. Vi hæfter os i den forbindelse særligt ved, at der var risiko for at videregive oplysninger af fortrolig karakter til bl.a. naboer, og at dette kunne indebære et betydeligt ubehag for de pågældende lejere, herunder for tab af omdømme."

Samtidig udtalte Datatilsynet alvorlig kritik af, at PrivatBo utilsigtet havde udleverede en oversigt med oplysninger af økonomisk karakter om lejere til beboere i en anden ejendom end den, som var omfattet af den i sagen omhandlede tilbudspligt.

Som i ovennævnte sag med Lejre Kommune var der også i denne sag mangel på helt basale sikkerhedsforanstaltninger, idet man ikke havde gennemgået tilbudsmaterialet, inden det blev delt med beboerne.

2. november 2020: *Kritik af Randers Kommune for utilsigtet videregivelse samt manglende anmeldelse til Datatilsynet og underretning af den registrede*

I forbindelse med opsigelse af en medarbejder kom Randers Kommune til at sende opsigelsen til en forkert modtager.

Opsigelsen indeholdte bl.a. oplysninger om den ansattes helbredsmæssige forhold og fagforeningsmæssige forhold.

Datatilsynet udtalte kritik af, at Randers Kommune ikke havde levet op til GDPR artikel 32. I den forbindelse lagde tilsynet vægt på, at kommunen ikke havde ført passende kvalitetskontrol af indholdet af det fremsendte dokument samt kontrol af, at dokumentet blev fremsendt til rette modtager.

I forhold til spørgsmålet om anmeldelse til Datatilsynet udtalte tilsynet, at der skulle have været foretaget anmeldelse til tilsynet, selvom brevet alene var blevet sendt til en forkert modtager inden for kommunen. Tilsynet lagde i den sammenhæng vægt på, at der henset til dokumentets fortrolige personalemæssige karakter, og at dokumentet indeholdte oplysninger om klagers helbred og fagforeningsmæssige tilhørsforhold – havde været en særlig risiko for tab af omdømme og fortrolighed for klager i forbindelse med, at opsigelsen blev sendt til en anden medarbejder på arbejdspladsen.

Det konkrete brud adskilte sig således fra et konkret eksempel til Datatilsynets vejledning om anmeldelse af brud på persondatasikkerheden, som kommunen havde henvist til.

Endelig udtalte Datatilsynet kritik af, at kommunen først 2 måneder efter bruddet foretog en mundtlig underretning af den registrerede.

16. februar 2021: *Kritik af Vejen Kommune for offentliggørelse af personnummer*

På baggrund af en klage udtalte Datatilsynet kritik af, at Vejen Kommune - i forbindelse med offentliggørelse af et høringssvar - der var indsendt af en borger via digital post, ved en fejl kom til at offentliggøre borgerens personnummer, som fremgik af signaturbeviset.

Datatilsynet udtalte i den sammenhæng, at offentlige myndigheder, der modtager eller udarbejder materiale med henblik på offentliggørelse, og hvor materialet ofte indeholder personoplysninger, eksempelvis vedhæftet eller i form af metadata, skal gennemføre kontrolforanstaltninger med henblik på at undgå utilsigtet offentliggørelse af personoplysninger.

Efter tilsynets opfattelse indebærer sådanne kontrolforanstaltninger som minimum en forudgående proces for at gennemgå materialet med henblik på at slette eller anonymisere personoplysninger, der ikke skal offentliggøres. Alt efter personoplysningernes karakter og omfang vil det - efter tilsynets opfattelse - normalt også være en passende sikkerhedsforanstaltning at gennemføre en supplerende forudgående manuel eller teknisk kontrol af, om oplysningerne rent faktisk er blevet slettet eller anonymiseret som tiltænkt.

Det bemærkes, at Vejen Kommune allerede havde en teknisk løsning på plads, således at hjemmesiden løbende blev screenet for utilsigtet offentliggjorte oplysninger. Datatilsynet bemærkede i den forbindelse, at det ville kunne nedbringe risikoen for de registrerede betragteligt, at hvis løsningen blev anvendt forud for offentliggørelser i stedet for på bagkant.

SAGER OM BRUG AF DATABEHANDLERE

18. juni 2020: *MaCom's videregivelse af opgavebesvarelser*

Datatilsynet har i en afgørelse - i en sag hvor tre gymnasier havde anmeldt et brud på persondatasikkerheden til tilsynet - udtalt alvorlig kritik af MaCom, idet MaCom, som databehandler, havde videregivet dele af elevernes opgavebesvarelser til forskere fra Datalogisk Institut ved Københavns Universitet til brug for udvikling af plagiatprogrammer. MaCom havde således handlet uden for instruks i strid med GDPR art. 28.3.

I afgørelsen forholdt Datatilsynet sig også til begrebet "personoplysninger", herunder bl.a. ved at henvise til EU-domstolens afgørelser i Nowak-sagen (C 434/16) og i Breyer-sagen (C-582/14).

Sagen illustrerer bl.a. vigtigheden af, at man, som databehandler, holder sig inden for den instruks, som man har modtaget fra den dataansvarlige. Handler man uden for instruks, bliver man selvstændig dataansvarlig, og den dataansvarlige har et brud på persondatasikkerheden.

18. juni 2020: *Alvorlig kritik af behandling af oplysninger om opsagt medarbejder*

Datatilsynet har på baggrund af en klagesag udtalt alvorlig kritik af, NCC's sendte personoplysninger om en opsagt medarbejder til flere af virksomhedens ansatte. NCC begrundede behandlingen med uro på arbejdspladen grundet en verserende sag om organisationsfjendtlig adfærd ved Arbejdsretten.

I den forbindelse fandt Datatilsynet, at NCC ikke havde godtgjort at have en legitim interesse i at orientere flere af virksomhedens ansatte om afskedigelsen og den opsagte medarbejders tidligere ansættelsesforhold. Datatilsynet fandt endvidere, at NCC i den pågældende situation ikke lovligt kunne behandle oplysninger om den opsagte medarbejders fagforeningsmæssige tilhørsforhold.

Sagen er ikke den første af sin art, og den illustrerer, at man som arbejdsgiver skal passe på med at lade sig friste af at orientere medarbejdere om sager, der dækkes i pressen mv. Man må godt orientere i et vist omfang, men man skal overveje sin hjemmel grundigt. Følsomme personoplysninger vil som udgangspunkt aldrig kunne deles.

8. juli 2020: *Fingreaftryk som adgangskontrol*

Datatilsynet har på baggrund af en klage vurderet, at det ikke var i strid med databeskyttelsesreglerne, at en virksomhed behandlede oplysninger om fingeraftryk med henblik på entydig identifikation af virksomhedens medarbejdere.

Virksomheden havde under sagen godtgjort, at kontrolforanstaltningen var afgørende for fødevaresikkerheden, herunder virksomhedens eksportmuligheder, at uvedkommende ikke fik adgang til produktionen, og at det kunne identificeres, hvem der har deltaget i produktionen. Brug af nøglebrikker kunne ikke give tilstrækkelig sikkerhed for identifikation, idet nøglebrikker kan stjæles, ombyttes mv. - både ubevidst og bevidst.

Sagen er forud for Datatilsynets afgørelse behandlet på et møde i Datarådet og kontrolforanstaltningen var forud for implementeringen varslet i henhold til DA/LO-aftalen om kontrolforanstaltninger.

Identifikationsløsningen fungerede ved, at en beregnet værdi af den ansattes fingeraftryk blev matchet op imod en database med de tilsvarende værdier, således at der kunne ske en entydig identifikation af, hvilken medarbejder, der tilgik og forlod arbejdspladsen. Behandling af biometriske data med det formål entydigt at identificere en fysisk person er omfattet af forbuddet i GDPR art. 9.1. Datatilsynet finder dog, at behandlingen af personoplysninger omfattet af forbuddet i art. 9.1 kan ske inden for rammerne af DBL § 12.1, når behandlingen sker som led i en kontrolforanstaltning indført i henhold til DA/LO-aftalen om kontrolforanstaltninger.

Der blev under sagen lagt vægt på, at systemet ikke lagrer billeder af fingeraftrykket, men en unik værdi baseret på fingeraftrykket, ligesom det ikke er muligt at konvertere værdien tilbage til det konkrete fingeraftryk. Data i scanneren kan ikke bruges uden en kopi af databasen, da disse data er lagret på hovedkontoret i serverrum, hvor kun IT har adgang med separat kodesystem. Datatilsynet fandt derfor, at behandlingen sker i overensstemmelse med GDPR art. 32.1.

Sagen illustrerer bl.a., at der i DBL er taget højde for den danske model, således at foranstaltninger i overensstemmelse med aftaler mellem arbejdsmarkedets parter også vil have hjemmel i den databeskyttelsesretlige lovgivning.

KOMMENDE GDPR-AKTIVITETER

UDDANNELSE: PLESNER CERTIFIKAT I PERSONDATARET

Dag 1 og 2: Onsdag den 9. og torsdag den 10. juni 2021

Dag 3 og 4: Onsdag den 16. og torsdag den 17. juni 2021

Undervisningen foregår alle dage kl. 9.00-16.00 hos Plesner

UDDANNELSE: GDPR MASTER CLASS - OVERFØRSEL AF PERSON-OPLYSNINGER TIL TREDJELANDE

Tirsdag den 29. juni 2021, kl. 09.00-16.00

Undervisningen udbydes virtuelt igennem værktøjet GoToWebinar

KONFERENCE: DATABESKYTTELSESDAGEN 2021

Onsdag den 8. september 2021, kl. 8.30-16.30

Konferencen afholdes hos Dansk Industri

UDDANNELSE: PLESNER CERTIFIKAT I PERSONDATARET

Dag 1 og 2: Onsdag den 15. og torsdag den 16. september 2021

Dag 3 og 4: Onsdag den 29. og torsdag den 30. september 2021

Undervisningen foregår alle dage kl. 9.00-16.00 hos Plesner

UDDANNELSE: PLESNER CERTIFIKAT I PERSONDATARET

Dag 1 og 2: Onsdag den 10. og torsdag den 11. november 2021

Dag 3 og 4: Onsdag den 24. og torsdag den 25. november 2021

Undervisningen foregår alle dage kl. 9.00-16.00 hos Plesner

UDDANNELSE: PLESNER CERTIFIKAT I PERSONDATARET

Dag 1 og 2: Onsdag den 1. og torsdag den 2. december 2021

Dag 3 og 4: Tirsdag den 14. og onsdag den 15. december 2021

Undervisningen foregår alle dage kl. 9.00-16.00 hos Plesner

Se mere på www.plesner.com

LEGALHUB

LegalHub er et digitalt værktøj udviklet af Plesner Persondata Team med det formål at gøre dit arbejde med GDPR så enkelt som muligt.

INDHOLD

Med et abonnement til LegalHub får du adgang til direkte referencer mellem lovgivning og relevant materiale - helt ned på de enkelte bestemmelser. Ligeledes får du adgang til en række Plesner standardskabeloner, der nemt kan tilpasses dine specifikke behov. Du sparer dermed tid på udarbejdelsen af dokumenter og bliver hjulpet videre i løsningen af dine juridiske opgaver.

HOLD DIG OPDATERET

Med LegalHub får du eksklusiv adgang til at deltage i faglige webinarer hver 14. dag om de mest aktuelle emner inden for persondataretten. Vores juridiske eksperter formidler kompleks viden på en simpel og håndgribelig måde, og du får mulighed for at stille spørgsmål undervejs.

Det juridiske indhold på LegalHub opdateres løbende, og som en del af dit abonnement modtager du hver 14. dag et nyhedsbrev med direkte links til den nye viden, så du nemt og hurtigt kan holde dig opdateret.

FORDELE VED LEGALHUB

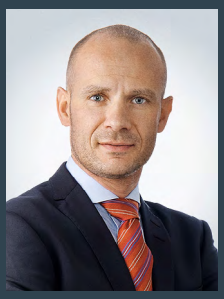
- Det juridiske indhold er koblet og samlet ét sted
- Du sparer tid på udarbejdelsen af juridiske dokumenter
- Du får adgang til faglige webinarer hver 14. dag
- Du bliver holdt opdateret på persondataretten

FÅ ADGANG TIL LEGALHUB

Læs mere og tilmeld dig på Plesner.com/LegalHub

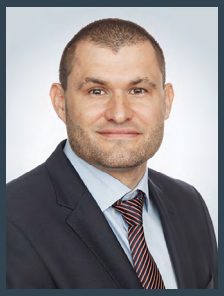
LEGALHUB
EN PLESNER-LØSNING

VORES EKSPERTER



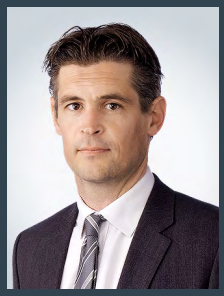
Michael Hopp
advokat, partner

mho@plesner.com
P: +45 36 94 13 06
M: +45 29 99 30 14



Jesper Husmer Vang
advokat, senior counsel

jhv@plesner.com
P: +45 36 94 14 58
M: +45 30 93 71 11



Jacob Falsner
advokat, senior councel

jfa@plesner.com
P: +45 36 94 11 80
M: +45 30 93 71 59

Peter Østerby Mønsted
advokat, director

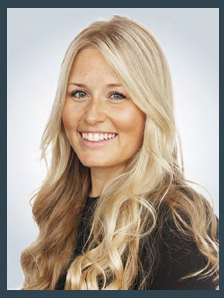
pom@plesner.com
P: +45 36 94 15 41
M: +45 30 93 71 32

Martin Nybye-Petersen
advokat, manager

mny@plesner.com
P: +45 36 94 15 21
M: +45 29 99 30 89

Maria Katrine Westphal-Rasmussen
advokat

mkw@plesner.com
P: +45 36 94 12 49
M: +45 29 99 30 18



Mille Selbach Rasmussen
advokat

mrn@plesner.com
P: +45 36 94 12 82
M: +45 30 93 71 71

HOLD DIG OPDATERET

Vi ønsker at dele vores viden og levere juridisk information af højeste kvalitet til vores klienter om persondata.

Gå ind på www.plesner.com/insigts for at blive tilmeldt "Plesner Insights", eller følg vores LinkedIn-gruppe "Plesner Persondata Team". Du kan læse mere om Plesner Persondata Team på plesner.com.

Plesner Advokatpartnerselskab | Amerika Plads 37 | DK-2100 Copenhagen | Tel +45 33 12 11 33 | www.plesner.com