JANUAR 2018

Den nye databeskyttelsesforordning
Start jeres compliance-tjek med disse 6 trin

INSIGHT

KROMANN
REUMERT

Den nye databeskyttelsesforordning
Start jeres compliance-tjek med disse 6 trin

Den nye databeskyttelsesforordning træder i kraft den 25. maj 2018. Den lange frist giver virksomheder gode muligheder for at sikre, at de kan overholde forordningens regler. Forordningen skærper på en række områder de nugældende krav. Virksomheder bør derfor allerede nu forberede, hvordan de nye regler efterleves og dermed opnå en så smidig overgang som mulig. Med disse seks trin kommer I godt i gang.

Hvorfor er persondata compliance vigtigt?

Med den nye forordning om databeskyttelse træder væsentlige skærpede regler i kraft, herunder nye krav til blandt andet datasikkerhed og dokumentation samt sanktioner. Hvor bødeniveauet for overtrædelser i Danmark p.t. ligger på 3.000-10.000 kr. – med en enkelt historisk bøde på 25.000 kr. – vil der i fremtiden gælde et bødeniveau på helt op til 20 mio. euro eller 4 % af den samlede globale koncernomsætning, hvis det beløb er højere. Fremadrettet kan det derfor blive dyrt ikke at overholde de persondataretlige regler. Derudover kan overtrædelse af reglerne få andre negative konsekvenser for din virksomhed, blandt andet erstatningskrav, skade på virksomhedens renommé samt brud på tilliden til virksomheden.

Hvordan bliver din virksomhed compliant?

Mange virksomheder behandler, opbevarer og videregiver store mængder af persondata uden at have taget stilling til interne eller eksterne processer. Begrebet compliance opfattes tit som en uhåndgribelig størrelse, og det kan være svært at gennemskue, om en virksomhed er compliant. Og hvis virksomheden ikke er compliant, hvad er det så egentlig, virksomheden bør starte med?

Der er ingen *"one size fits all"*-løsning for persondata-compliance, men de fleste virksomheder kan komme godt i gang med de seks trin, vi har skitseret i nedenstående model.

1. AFGRÆNSNING OG FORBEREDELSE → 2. ANALYSE AF DATASTRØMME → 3. COMPLIANCE-ANALYSE → 4. HANDLINGSPLAN → 5. IMPLEMENTERING → 6. VEDLIGEHOLDELSE

1. Afgrænsning og forberedelse: Hvad gælder for virksomheden?

Det første og vigtigste trin er at informere ledelsen om, dels hvor vigtigt det er at overholde databeskyttelsesforordningen, og dels hvilke konsekvenser de nye regler kan få for virksomheden.

I bør derfor afholde et indledende møde, hvor I sammensætter et krydsfunktionelt team, der består af repræsentanter fra blandt andet virksomhedens juridiske afdeling, økonomi, risk management/compliance, IT, virksomhedens fremtidige Data Protection Officer (DPO) og evt. andre medarbejdere, der kan hjælpe med at afdække virksomhedens datastrømme.

I forberedelsesfasen bør I også danne jer et overblik over de love, regler og standarder, som skal efterleves for at blive compliant med den nye databeskyttelsesforordning.

På nuværende tidspunkt vil dette billede ikke være fuldendt, idet der fortsat mangler fortolkningsbidrag til flere af forordningens bestemmelser, men dette trin vil bidrage til forståelsen af, hvor kort eller lang vejen til persondata-compliance er.

1. AFGRÆNSNING OG FORBEREDELSE → 2. ANALYSE AF DATASTRØMME → 3. COMPLIANCE-ANALYSE → 4. HANDLINGSPLAN → 5. IMPLEMENTERING → 6. VEDLIGEHOLDELSE

2. Analyse af datastrømme: Hvilke oplysninger har vi og hvor?

Det næste trin går ud på at få et overblik over virksomhedens datastrømme – den såkaldte *data mapping* – for bl.a. at forstå:

- Hvilke kategorier af persondata indsamles og behandles?
- Hvilke registrerede personer vedrører dataene?
- Hvilke systemer bruges til behandling af data?

Dette gælder både lokal indsamling og behandling samt behandling hos tredjeparter, f.eks. cloud- og outsourcing-partnere.

Start med at stille jer selv de vigtige spørgsmål:

- Hvor kommer personoplysningerne fra?
- Hvor opbevares oplysningerne?

Øvelsen går ud på at forsøge at følge dataene i deres "levetid". F.eks. vil nogle oplysninger om medarbejdere være indsamlet fra job-
ansøgninger, og nogle oplysninger vil først blive slettet efter ansættelsesforholdets ophør.

Hvor opbevarer I persondata?

I forhold til hvor oplysningerne opbevares kan dette være i rekrutteringssystemet, HR-systemet, personalemapper, mail- og arkiveringssystemet, lønsystemet, virksomhedens intranet og eksterne hjemmesider, whistleblowerordning mv. Oplysninger om kunder findes som oftest i kundedatabaser, mail- og arkiveringssystemer, CRM-systemer, mailinglister mv. Det er også vigtigt, at I tager højde for tredjepartssystemer og opbevaringsløsninger samt evt. intern brug – plejer medarbejderne for eksempel at gemme oplysninger på computerens skrivebord eller i private mapper, og er der lavet interne kundelister eller lignende, som ikke deles med andre afdelinger?

Hvordan er datastrømmene?

For at skabe overblik over datastrømmene kræver det en del viden om de interne processer, hvorfor det kan være oplagt at afholde workshops med de relevante medarbejdere, herunder medarbejdere fra IT, HR, juridisk afdeling og compliance, salg og marketing osv., med persondata-compliance og datastrømme som emne. Som forberedelse til workshoppen bør I udarbejde en spørgeguide til medarbejderne, som kan afklare, hvilke informationer I skal bruge for at kunne fastlægge datastrømmene. Denne proces kan også gennemføres som en til en-interviews med nøglemedarbejdere eller tilrettelægges på en anden måde, så den tilpasses virksomhedens organisation og de ressourcer, der er til rådighed.

Resultatet af en datastrømsanalyse bør være en oversigt over virksomhedens datastrømme, herunder de systemer virksomheden anvender, og indholdet af systemerne, både hvad angår de registrerede personer og de typer af oplysninger, der behandles. Oversigten kan derefter bruges som basis for den efterfølgende compliance-analyse.

3. Compliance-analyse: Overholder vi de gældende regler – og hvad med de nye?

Det første spørgsmål, der skal stilles under compliance-analysen, er, om virksomhedens behandling af data er lovlig i forhold til nugældende regler. Dernæst bør I se på, hvad der skal til for at overholde de nye regler i databeskyttelsesforordningen. Vi guider dig igennem en række områder, som har væsentlig betydning for, om behandlingen af persondata er lovlig.

Overholder I de grundlæggende behandlingsregler og dokumentationskrav?

Der skal foretages en vurdering af, om virksomhedens nuværende persondataretlige compliance- og interne regler overholder de grundlæggende krav i persondatalovens § 5, som stiller en række betingelser til, hvornår behandling af persondata er lovlig. Disse betingelser går igen i databeskyttelsesforordningen. Behandlingen skal f.eks. være lovlig og rimelig for at overholde kravet om god databehandlingsskik. Behandlingen af persondata må kun foretages på baggrund af et sagligt og legitimt formål, som angives udtrykkeligt, og der må kun indhentes relevante og tilstrækkelige oplysninger. Behandlingen er også underlagt proportionalitetsprincippet, hvilket betyder, at behandlingen kun må finde sted, hvis den er nødvendig i forhold til formålet, og samme resultat ikke kan opnås med mindre indgribende midler. Der påhviler også den dataansvarlige en slette- og berigtigelsespligt, da personoplysninger, som ikke længere tjener til deres formål, skal slettes, og ukorrekte oplysninger skal korrigeres.

Den nye databeskyttelsesforordning indeholder et nyt krav om dokumentation. I skal kunne bevise, at I overholder ovenstående krav til behandling af personoplysninger.

I bør derfor aktivt tage stilling til, hvordan formålet med en given behandling begrænses, hvordan datamængden minimiseres, hvordan regelmæssig ajourføring og den nødvendige sletning håndteres, samt hvilke tiltag der skal sikre beskyttelse mod ulovlig behandling og tab af data.

Start allerede nu:
- Vurder formålene med behandlingen
- Se på de indsamlede datamængder i forhold til relevante formål og vurder, om dataene er nødvendige
- Ryd op i oplysninger, der er forældede, irrelevante eller ikke længere tjener et formål
- Dokumentér overholdelse af grundlæggende principper, f.eks. ved at udarbejde retningslinjer om indsamling og behandling af data eller lignende.

Har I fået samtykke til behandlingen af persondata?

I Danmark gælder der altid krav om et "udtrykkeligt" samtykke til behandling af personoplysninger, hvis behandlingen er samtykkebaseret. Med "udtrykkeligt" menes, at samtykket kræver en aktivhandling for den registrerede person, f.eks. i form af en underskrift eller en elektronisk accept. Stiltiende eller indirekte tilslutning til behandling af oplysninger er ikke tilstrækkelig. Samme krav er ikke nødvendigvis gældende i andre EU-lande, for så vidt angår almindelige, ikke-følsomme oplysninger (navn, kontaktoplysninger mv.), men behandling af følsomme oplysninger, såsom helbredsoplysninger, kræver et udtrykkeligt samtykke.

Med den nye databeskyttelsesforordning er kravene til samtykke blevet skærpet i forhold til databeskyttelsesdirektivet. I Danmark vil virksomhederne dog ikke opleve det som en skærpelse af reglerne – forudsat naturligvis, at der i forvejen anvendes gyldige samtykketekster. Et gyldigt samtykke skal være frivilligt, specifikt og informeret. Forordningen har herudover særlig fokus på, at samtykketekster skal være forståelige, klare og lettilgængelige i formen, samtidig med at et samtykke skal adskilles fra den øvrige tekst i en kontrakt, betingelser mv.

Opfyldelsen af en kontrakt må kun betinges af samtykket, hvis behandlingen af de oplysninger, den registrerede giver samtykke til, rent faktisk er nødvendig. Det nye er dog, at virksomheden også skal oplyse den registrerede om, at samtykke kan tilbagekaldes, og det skal være let at foretage tilbagekaldelsen.

Overholder I de nye samtykkeregler?

I kan med fordel allerede nu have fokus på de nye samtykkeregler, så de samtykker, der indhentes fremadrettet, er langtidsholdbare og gælder efter den nye forordning. Opdater derfor de samtykketekster, I anvender i dag. Viser det sig, at de tidligere indhentede samtykker ikke er gyldige efter den nye databeskyttelsesforordning, bør I vurdere, om dataene kan behandles uden samtykke. Hvis det ikke er muligt, skal nye samtykker indhentes for at sikre compliance fremadrettet.

Hvilke sikkerhedsforanstaltninger har I til beskyttelse af persondata?

Sørg for at kortlægge, hvilke sikkerhedsforanstaltninger I har taget for at beskytte personoplysninger, så I herefter kan redegøre for, om disse er passende i teknisk eller organisatorisk henseende. Sikkerhedsforanstaltninger kan bl.a. være begrænset adgang, passwords, firewall, pseudonymisering, kryptering af følsomme oplysninger osv. Forordningen har på dette område tilføjet visse nye begreber, såsom databeskyttelse gennem design (data protection by design) og databeskyttelse gennem standardindstillinger (data protection by default).

Data protection by design kræver, at design af systemer, der skal håndtere persondata, fremadrettet er særligt indrettet til at tage højde for databeskyttelse, mens data protection by default indeholder et princip om, at de mest begrænsende standardindstillinger skal anvendes som udgangspunkt for håndtering af persondata.

Det er som udgangspunkt jer selv, der bestemmer, hvilke sikkerhedstiltag I vil anvende til at beskytte dataene. Har I dog anmeldt en databehandling til Datatilsynet, kan der være tilknyttet særlige vilkår til behandlingen, herunder også i forhold til datasikkerhed. F.eks. har Datatilsynet udarbejdet standardvilkår til behandling af følsomme oplysninger som led i personaleadministration, og der gælder også særlige sikkerhedskrav til anvendelse af cloud-baserede løsninger.

Disse krav skal I naturligvis overholde, og kravene bør indgå i jeres vurdering af, hvilke tiltag der er passende til en given persondatabehandling, selv om behandlingen ikke er anmeldt til Datatilsynet.

Offentlige myndigheder er underlagt sikkerhedsbekendtgørelsen (nr. 528 af 15. juni 2000 med senere ændringer), som stiller en række krav til bl.a. logning, adgangskontrol mv. Bekendtgørelsen gælder ikke for private virksomheder, men der kan hentes inspiration derfra. Herudover kan det være en god idé at se på evt. branchestandarder og kutymer samt ISO-certificeringer, f.eks. ISO 27001.

Kravet om iværksættelse af passende sikkerhedsforanstaltninger er en dynamisk størrelse, som skal afspejle den gældende viden og teknologiske udvikling. I kan derfor ikke nøjes med at foretage vurderingen en gang for alle. Selv om den nye forordning ikke tilføjer så meget nyt til de nuværende regler om sikkerhedsforanstaltninger, er disse et vigtigt element i kravene til databehandlingen, som bl.a. skal forebygge mulige sikkerhedsbrud.

Hvordan håndterer I de registrerede personers rettigheder?

Begynd med at gennemgå de eksisterende procedurer, som I bruger til at sikre, at I opfylder jeres oplysningspligt, håndtering af indsigtsbegæringer og diverse henvendelser om f.eks. sletning eller berigtigelse af data. Sammenhold så disse procedurer med de eksisterende regler, og lav tilpasninger, hvor det måtte være nødvendigt.

Når den nye databeskyttelsesforordning træder i kraft er jeres oplysningspligt udvidet. Det vil sige, at de registrerede personer har ret til at vide, hvordan deres oplysninger behandles, og informationen skal være tilgængelig på en klar og forståelig måde.

I den nye forordning bliver der også stillet krav om ret til dataportabilitet (dvs. at den registrerede person under visse omstændigheder har ret til at få udleveret oplysninger om sig selv i *"et struktureret, almindeligt anvendt og maskinlæsbart format"* – formentlig på USB-stik eller lignende), begrænsning af behandling, "retten til at blive glemt" inklusiv sletning af data hos tredjeparter osv. I bør derfor skabe jer et overblik over, hvilke tiltage der er nødvendige i denne henseende, og begynde at tilpasse de procedurer, som skal ændres for, at alle de rettigheder, som de registrerede personer er tillagt efter forordningen, bliver respekteret fremadrettet.

Opfylder I de nye dokumentationskrav?

Databeskyttelsesforordningen kommer som nævnt ovenfor til at betyde, at virksomheder bliver underlagt en dokumentationspligt. Det betyder, at I ikke kun skal overholde den nye forordning. I skal også kunne bevise, at I har iværksat de nødvendige foranstaltninger for at sikre, at I overholder forordningens regler.

Som led i dokumentationskravet bør I implementere passende procedurer, forholdsregler m.v. Her kan I overveje følgende procedurer/dokumenter:

- Generel IT-politik
- Politikker eller retningslinjer for håndtering af personoplysninger – helst pr. type (f.eks. medarbejderdata, kundedata osv.) – som tager stilling til indsamling, løbende behandling, sletning, blokering mv.
- Procedure for håndtering af opfyldelse af oplysningspligt
- Politik for håndtering af indsigtsbegæringer, som bør kunne læses af tredjeparter
- Politik for håndtering af de registreredes øvrige rettigheder
- Håndtering af internationale dataoverførsler
- Procedure for håndtering af sikkerhedsbrud, herunder også pligten til anmeldelse til Datatilsynet fra den 25. maj 2018
- Håndtering af databehandleraftaler – hvornår skal disse indgås, standardordlyd mv.
- Vejledning om brug af cloud-baserede løsninger og/eller ydelser fra IT-leverandører i øvrigt
- Privatlivspolitik til virksomhedens hjemmeside osv.

Har I overblik over tredjeparter, der behandler data på jeres vegne?

Virksomheder må kun gøre brug af databehandlere, hvis der indgås en skriftlig databehandleraftale mellem parterne med et nærmere bestemt indhold.

I bør derfor vurdere, hvilke tredjeparter I anvender til at behandle data på jeres vegne, gennemgå de eksisterende aftaler og indsætte de nødvendige bestemmelser om f.eks. databeskyttelse, hvis disse mangler.

Det er vigtigt, at I tager højde for potentiel behandling på jeres vegne, f.eks. hvis en tredjepart kan få adgang til jeres data, og hvis der i nødstilfælde skal foretages backup af systemerne. Den nye forordning stil-ler yderligere krav til indholdet af en databehandleraftale, herunder at karakteren, typen af oplysninger, kategorier af registrerede mv. fremgår af aftalen.

I bør derfor som udgangspunkt opdatere alle jeres databehandleraftaler senest den 25. maj 2018.

Derudover bør i overveje at indsætte en bestemmelse om ansvar i aftalen, da virksomheden som dataansvarlig og aftaleparten som databehandler nu hæfter solidarisk for ulovlig behandling, der foretages af databehandleren. Dette er en væsentlig ændring i forhold til nuværende regler, hvor I som dataansvarlige ifalder alt ansvar for de handlinger databehandleren foretager på jeres vegne.

Overfører I data til udlandet?

Overførsel af persondata til andre EU-lande kræver ikke særlige forholdsregler. Overførsel af persondata til lande uden for EU, må der-imod kun ske, hvis der er sikret et tilstrækkeligt beskyttelsesniveau for overførslen. I bør tage stilling til, om I overfører persondata til lande uden for EU og i så fald på hvilket grundlag. Den hurtigste og mest fortrukne løsning er at anvende EU-Kommissionens standardkontrakter, som ikke kræver Datatilsynets tilladelse, hvis ordlyden anvendes uændret. Ved overførsler til USA kan det være relevant at anvende den nye Privacy Shield-aftale, som netop er blevet godkendt af EU-Kommissionen , og som de amerikanske virksomheder, som ønsker denne certificering, kan tilslutte sig fra den 1. august 2016. Andre grundlag kan anvendes, såsom Binding Corporate Rules inden for en koncern eller ved at indhente udtrykkeligt samtykke fra den registrerede person. I bør under alle omstændigheder sikre, at overførsler allerede i dag sker på lovligt grundlag.

Udarbejd en compliance-rapport

Med afsæt i den gennemarbejdede analyse over jeres datastrømme og en vurdering af, om jeres nuværende behandling af persondata er lovlig, kan I lave en egentlig compliance-analyse, hvor det kortlæg-ges, hvilke foranstaltninger I skal foretage for at overholde persondataloven i dag og den kommende databeskyttelsesforordning pr. 25. maj 2018. Resultatet bør være en compliance-rapport, som også til dels kan fungere som den fremtidige, nødvendige dokumentation for, at I behandler persondata ansvarligt.

1. AFGRÆNSNING OG FORBEREDELSE | 2. ANALYSE AF DATASTRØMME | 3. COMPLIANCE-ANALYSE | **4. HANDLINGSPLAN** | 5. IMPLEMENTERING | 6. VEDLIGEHOLDELSE

4. Handlingsplan: Hvilke tiltag er nødvendige for at overholde reglerne?

I har nu kortlagt alle relevante oplysninger om jeres datastrømme og interne politikker samt på det grundlag foretaget en udredning af, hvilke tiltag der er nødvendige for at overholde de gældende regler og være klar til den kommende databeskyttelsesforordning. Nu mangler I blot at omsætte compliance-rapporten til handling. Det kan I gøre ved at udarbejde en konkret handlingsplan, som evt. munder ud i virksomhedens nye compliance-politik. Handlingsplanen bør være realistisk og tage stilling til, hvilke områder I vil prioritere.

1. AFGRÆNSNING OG FORBEREDELSE | 2. ANALYSE AF DATASTRØMME | 3. COMPLIANCE-ANALYSE | 4. HANDLINGSPLAN | **5. IMPLEMENTERING** | 6. VEDLIGEHOLDELSE

5. Implementering: Udarbejd politikker og uddan medarbejdere

Implementeringsfasen kan involvere udarbejdelsen af konkrete politikker, træning af medarbejdere, implementering af nye procedurer og sikkerhedstiltag. Det er afgørende, at I i denne fase gør opmærksom på persondata i virksomheden, og formidler det på en måde, så alle kan forholde sig til det, fremfor at det bliver en byrde eller noget kedeligt, der bare skal overstås.

1. AFGRÆNSNING OG FORBEREDELSE | 2. ANALYSE AF DATASTRØMME | 3. COMPLIANCE-ANALYSE | 4. HANDLINGSPLAN | 5. IMPLEMENTERING | **6. VEDLIGEHOLDELSE**

6. Vedligeholdelse: Opfølgning på handlingsplanen

Når I har gennemgået en compliance-undersøgelse, og alle nødvendige foranstaltninger er sat i værk, er det afgørende at I vedligeholder regelefterlevelsen ved hjælp af periodisk kontrol. Hvis I ikke var compliant tidligere, er mange interne mekanismer blevet sat i gang, og derfor er det især i starten vigtigt at være opmærksom på faldgruber. Lettilgængelige og forståelige guidelines og procedurer samt evt. opfølgende træning vil hjælpe medarbejderne til at vedligeholde de nye krav. I bør også gennemgå procedurerne efter ca. 1 år for at sikre, at de fungerer som tiltænkt og rent faktisk bliver anvendt.

Kromann Reumerts rådgivning

Kromann Reumerts forretningsgruppe for persondata rådgiver om alle juridiske aspekter af persondataretten inden for alle brancher, bl.a. den finansielle sektor, forsknings- og sundhedssektoren og telebranchen. Vi har over de senere år udvidet vores kompetencer og rådgivning inden for persondataretten ganske betragteligt. Vores erfarne og dygtige advokater har bistået med en række opgaver inden for persondataretlig compliance og yder værdifuld rådgivning, som tager højde for et vigtigt sammenspil mellem jura og praktisk anvendelige løsninger for vores klienter.

Kontakt

Tina Brøgger Sørensen
Partner

Dir. +45 38 77 44 08
Mob. +45 61 20 35 33
tib@kromannreumert.com

Daiga Grunte-Sonne
Director, Advokat

Dir. +45 38 77 41 18
Mob. +45 61 20 99 95
dso@kromannreumert.com

Mette Hansen Hølledig
Senioradvokat

Dir. +45 38 77 44 75
Mob. +45 24 86 00 14
mhd@kromannreumert.com

KROMANN REUMERT

Hos Kromann Reumert sætter vi standarden. Sammen. Vi leverer værdiskabende løsninger og rådgivning med engagement og nærvær. Det gør vi med fokus på værdierne kvalitet, forretningsforståelse, samarbejdsglæde og troværdighed. Vi er Danmarks førende advokatvirksomhed med kontorer i København, Aarhus og London.

KØBENHAVN Ø
SUNDKROGSGADE 5
DK-2100 KØBENHAVN Ø

AARHUS
RÅDHUSPLADSEN 3
DK-8000 AARHUS C

LONDON
65 ST. PAUL'S CHURCHYARD
LONDON EC4M 8AB

ADVOKATFIRMA
KROMANNREUMERT.COM
TLF. +45 70 12 12 11