8 skridt...
Bliv klar til de nye persondataregler

EU's persondataforordning er blevet endeligt vedtaget, og de nye regler træder fuldt ud i kraft i alle EU-medlemsstater inklusiv Danmark den 25. maj 2018. Forordningen har et meget bredt anvendelsesområde og får store konsekvenser for danske virksomheder og myndigheder, der fremover skal leve op til en række strammere krav for håndtering af persondata.

Plesners Persondata Team giver her 8 gode råd til, hvordan jeres organisation bør tage fat på arbejdet med at leve op til persondataforordningen.

1. Få overblik over data

Først og fremmest skal I finde ud af, hvad det er for nogle persondata, som jeres organisation skal beskytte. Den indledende del af arbejdet foregår ved at klassificere og kortlægge organisationens persondata. Der skal skabes et samlet overblik over alle typer personrelaterede oplysninger - eksempelvis om kontaktpersoner i sælgernes CRM-systemer, emailadresser og telefonnumre i forbindelse med konkurrencer samt persondata om medarbejdere og kunder.

Overblikket over data skal afklare:

- Hvilke data har organisationen?
- Hvor kommer data fra?
- Hvor længe gemmes data?
- Hvem deles data med?

Den mest effektive måde rent praktisk at skabe overblikket er ved, at it-afdelingen og alle de relevante dele af organisationen sætter sig sammen og finder ud af, hvilke former for data virksomheden ligger inde med - det gælder både lokalt på egne computere og servere samt hos cloud- og outsourcingpartnere.

2. Få overblik over reglerne

Når jeres organisations data er kortlagt og klassificeret, er næste skridt at afklare, hvilke bestemmelser i persondataforordningen der vil være relevante for jeres organisation.

Målet for organisationen skal være at overholde de relevante regler - hverken mere eller mindre. Det kan få alvorlige konsekvenser i form af bøder og tab af omdømme hos kunder og andre interessenter, hvis reglerne ikke efterleves. Omvendt bør organisationen ikke bruge ressourcer på at overholde krav, som man hverken er forpligtet til eller af anden årsag har interesse i at overholde.

Det gælder helt basalt om at sætte sig ned og gennemgå, hvilke bestemmelser i forordningen der er relevante for jeres organisation.

3. Se på den nuværende måde at gøre tingene på

Da den ny persondataforordning generelt indfører en række skærpelser af reglerne, skal de fleste organisationer ændre på deres nuværende måde at gøre tingene på.

Skab et samlet overblik over hvordan jeres nuværende praksis overholder reglerne i dag. Find ud af præcis på hvilke områder I allerede lever op til reglerne, og om der er nogle alvorlige mangler, som kræver umiddelbar handling fra jeres side.

4. Beskriv organisationens kontrolmål

Når jeres organisation har fået overblik over den nuværende praksis for opbevaring, brug, sletning og deling af persondata, så er næste skridt at se på den løbende overholdelse af forordningen. Det skal gøres ved at beskrive de målsætninger, som organisationen skal leve op til med de nye regler.

Med udgangspunkt i persondataforordningen skal I formulere en række konkrete målsætninger, som er relevante for jeres organisation. Kontrolmålene kan eksempelvis være, at der skal iværksættes processer og kontroller til at sikre, at man overholder slettefrister for data. Eller det kan være et kontrolmål om, at I systematisk skal sikre jer, at alle har samtykket, når organisationen indsamler mailadresser til markedsføringsformål.

I første omgang handler det ikke om at tage stilling til, hvordan I konkret vil opfylde de enkelte målsætninger. Når I har et samlet overblik over alle kravene og jeres kontrolmål, vil I have bedre mulighed for at designe de løsninger, hvor enkelte processer eller kontroller bidrager til at opfylde flere af jeres opstillede kontrolmål.

5. Foretag en risikovurdering

Persondataforordningen fokuserer på, at organisationer skal gøre, hvad der er nødvendigt for at nedbringe risikoen for de registrerede personer til et acceptabelt niveau. Det betyder, at man ikke er forpligtet til at opretholde foranstaltninger, hvis det ikke er nødvendigt for at nedbringe en risiko for de registrerede, eller hvis implementeringen af foranstaltningen er uforholdsmæssigt omkostningstung i forhold til den effekt for beskyttelsen af den registrerede, der kan opnås ved at implementere den pågældende foranstaltning. Risiko handler her ikke kun om almindelig sikkerhed, men også om, hvorvidt man overtræder de almindelige krav i forordningen - altså eksempelvis kravene til saglighed, opbevaringsperiode, oplysningspligt osv.

Jeres organisation skal foretage en grundig risikovurdering. Det er vigtigt at være opmærksom på, at I er forpligtet til at dokumentere, hvordan I har overvejet relevante risici - og især kunne dokumentere overvejelserne om de risici, som jeres organisation vælger ikke at fokusere på. Grundspørgsmålet for risikovurderingen er: Hvor alvorlig er situationen for de registrerede personer, hvis det går galt? Altså eksempelvis hvis den dataansvarlige ikke overholder reglerne om oplysningspligt ved indsamling af persondata.

I skal have for øje, at optimal indsats og maksimal indsats ikke er det samme. Højeste prioritet i forhold til risikovurderingen vil ofte være de følsomme personoplysninger som eksempelvis helbredsoplysninger om personer i virksomhedens CRM-system. Risikovurderingen skal ikke kun give svar på, hvor organisationen bør sætte ind, men også til dels i hvilken rækkefølge dette bør ske. For de fleste større organisationer vil det være både nyttigt og nødvendigt at prioritere indsatsområderne, så der sikres fokus på områder med størst eksponering.

6. Design jeres løsning

Når organisationen har fået overblik over det nuværende omfang af persondata og processerne og kontrollerne til fremtidig styring af data - samt et overblik over hvor I ikke lever op til forordningen - er næste skridt at få klargjort, hvordan jeres organisation kommer på plads med afhjælpningen af de forskellige mangler.

I skal udforme løsninger, der både tager højde for jeres konkrete mangler i forhold til aktuelle behandlinger, eksempelvis udarbejdelse af nye persondatapolitikker,

og jeres mangler i forhold til opfyldelse af kontrolmål, dvs. processer der sikrer den fremtidige overholdelse. I denne fase er jeres organisation klar til at designe og dimensionere løsningerne, så de er i overensstemmelse med jeres risikoanalyse.

Det er afgørende, at I er opmærksomme på, at alt skal dokumenteres - om end i varierende detaljeringsgrad. Det er jeres ansvar at kunne svare og fremlægge dokumentation, hvis I bliver udsat for kontrol. Dokumentationen skal være på plads, inden myndighederne kontakter jer. Mangel på tilstrækkelig dokumentation er i sig selv en overtrædelse af reglerne.

7. Implementér hele vejen rundt

Næste skridt er den konkrete implementering af jeres plan for at kunne efterleve persondataforordningen. Denne implementering bør følge organisationens normale processer for gennemførelse af forandringer. Det er vigtigt ikke at undervurdere de organisatoriske og psykologiske faktorer - og behovet for forandringsledelse, der vil være nødvendigt i de fleste organisationer.

De nye persondataregler får konsekvenser for mange medarbejdere. Eksempelvis vil mange ikke tænke over, at når de modtager et CV til en jobansøgning, så håndterer de persondata. En central del af implementeringen er derfor også at sikre, at alle relevante medarbejdere er opmærksomme på de særlige regler og procedurer, der fremover gælder. Jeres arbejde med at implementere vil typisk kræve intern uddannelse af alle medarbejdere, der har at gøre med persondata.

8. Følg op

En succesfuld implementering er ingen garanti for, at jeres organisation fremadrettet overholder reglerne. Hvis I ikke skal risikere, at jeres plan og implementering langsomt skal glide tilbage til tidligere arbejdsgange og processer, eller at ændring af eksisterende aktiviteter og igangsættelsen af nye aktiviteter ikke sker lovligt, så er det afgørende med opfølgning.

Det sidste skridt er derfor at planlægge, hvordan I løbende følger op på jeres implementering. I bør fastlægge, hvordan og hvornår I følger op på, om reglerne og organisationens processer nu også bliver overholdt i praksis. Gennemfør eksempelvis en grundig opfølgning efter en periode på tre til seks måneder.

Kontakt

Michael Hopp
advokat, partner

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