Persondataforordningen

Nye regler om persondata

PLESNER

Personoplysninger

Personoplysninger er defineret som: *"Enhver form for information om en identificeret eller identificerbar fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliserings-data, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet."*

Persondataforordningen

Europa-Parlamentets og Rådets forordning (EU) 2016 / 679 af 27. april 2016

Nye regler om persondata

EU har vedtaget nye regler for, hvordan virksomheder, offentlige myndigheder og andre skal håndtere persondata. Den nye persondataforordning finder anvendelse fra den 25. maj 2018 og skærper kravene til, hvordan f.eks. en virksomhed indsamler, registrerer og bruger kunde-oplysninger.

De nye regler gælder for håndtering af alle typer af person-oplysninger og dermed for såvel kunde- som medarbejder-oplysninger. I praksis betyder det, at enhver personrelateret information om kunder, medarbejdere, jobansøgere osv. er omfattet af reglerne. Det gælder alt lige fra helt basale informationer som f.eks. emailadresser og telefonnumre til følsomme personoplysninger om f.eks. helbredsmæssige forhold og medlemskab af en fagforening.

Samtidig bliver sanktionerne for ikke at overholde reglerne øget markant med risiko for bøder på helt op til 20 mio. euro eller 4 % af en virksomheds årlige globale omsætning.

Overholder I reglerne i dag?

Generelt er der øget fokus på virksomhedernes beskyttelse af persondata fra myndighedernes side, men også fra de berørte personers side. Det giver sig bl.a. udslag i en langt større mediebevågenhed, og vi ser nu sager om over-trædelse af persondataloven som forsidestof.

Uanset om jeres virksomhed indtil nu har haft fokus på at overholde persondatalovgivningen eller ej - så er det med den nye persondataforordning afgørende, at I får overblik over reglerne og jeres håndtering af personoplysninger.

De grundlæggende regler

De grundlæggende regler om persondata indebærer, at det enkelte individ har en række rettigheder og skal beskyttes mod uberettiget behandling af dets personlige oplysninger. Det betyder, at enhver virksomhed/myndighed mv., der indsamler, opbevarer og anvender personrelaterede oplysninger, skal leve op til nogle grundlæggende principper for behandling af persondata. Principperne er de samme efter de nuværende regler som efter de kommende regler i persondataforordningen:

1. Persondata må kun behandles på en lovlig, rimelig og gennemsigtig måde
2. Persondata må kun indsamles til specifikke, klare og saglige formål - og må ikke senere anvendes til andre formål, som er uforenelige med de oprindelige formål
3. De oplysninger, der behandles, skal være relevante og tilstrækkelige og må ikke omfatte mere, end hvad der kræves til opfyldelse af formålet med behandlingen – der gælder et strengt princip om 'need to know' (i modsætning til 'nice to know')
4. Der skal ske ajourføring af persondata, og der skal ske kontrol af, at der ikke behandles urigtige og vildledende oplysninger
5. Persondata må kun behandles, herunder opbevares, så længe det er nødvendigt for at forfølge et sagligt formål
6. Persondata skal sikres mod ulovlig brug, tab eller utilsigtet sletning eller skade

Som noget helt nyt, er det et grundlæggende krav, at I som virksomhed/myndighed skal kunne dokumentere, at reglerne overholdes.

Herudover gælder der skærpede forholdsregler og hensyn, hvis I håndterer såkaldte 'følsomme persondata', som eksempelvis oplysninger om race, religion, helbred og politisk tilhørsforhold. Der kan - særligt i de organisationer, der håndterer mange følsomme persondata - også være krav om at udpege en databeskyttelsesrådgiver, en såkaldt Data Protection Officer (DPO).

Rettigheder for den registrerede

Den registrerede person har en række grundlæggende rettigheder i relation til de persondata, som en virksomhed/myndighed mv. har registreret om dem:

- Personen skal - uden at spørge - modtage information om, hvordan håndteringen af personens oplysninger finder sted og til hvilke formål osv.
- Personen har ret til at få detaljeret indsigt i, hvilke persondata der opbevares , hvad de bruges til m.m.
- Personen har ret til at få korrigeret, slettet og begrænset brugen af data
- Personen har i nogle tilfælde ret til at få en kopi af data afgivet af personen selv i et almindeligt, læsbart format
- Personen har ret til at protestere mod nogle former for automatisk afgørelse, herunder profilering

Bøder og erstatning

Persondataforordningen indfører hårdere sanktioner for overtrædelse af reglerne på op til 2 - 4 % af virksomhedens årlige globale omsætning. Man kan også blive pålagt at betale erstatning og godtgørelse for tort.

Regler der skal overholdes

Det er vigtigt, at man som dataansvarlig spørger sig selv, om man overholder de nuværende regler. Ved at gennemgå nedenstående liste, får I et hurtigt overblik over jeres complianceniveau på persondataområdet:

Overholder I de velkendte grundlæggende principper

Persondatareglerne stiller en række krav, som jeres organisation skal opfylde. Kort fortalt, så stiller persondataforordningen krav om, at I overholder de førnævnte 6 principper og har et klart overblik over alle persondata, samt hvad de præcist bliver brugt til. Dette omfatter også en sikring af, at I opfylder oplysningspligten og har et juridisk grundlag for anvendelsen af persondata.

Kan I overholde det nye princip om accountability

Derudover skal I overholde det nye begreb, som persondataforordningen indfører: 'Accountability' eller 'ansvarlighed' - som bliver et nyt grundlæggende princip. Det betyder i praksis, at I skal kunne dokumentere, at I lever op til reglernes indhold, f.eks. ved at kunne fremlægge datastrømsanalyser, politikker, forretningsgange og kontroller. Selvom I overholder persondatereglerne i praksis, så vil alene det, at I ikke kan fremvise dokumentation, kunne være en overtrædelse af forordningen.

Har I styr på jeres sikkerhed og processerne omkring persondatasikkerheden

I skal også implementere de nødvendige tekniske og organisatoriske tiltag, der sikrer en passende grad af beskyttelse af de persondata, I behandler. Sikkerhedsniveauet skal vurderes i forhold til risikoen og typen af persondata, der behandles.

Husk risikoanalysen

Der skal gennemføres en risikoanalyse af alle nye behandlinger af persondata - og i de tilfælde, hvor der er en høj risiko for de berørte personer, skal der udarbejdes en formel og grundig konsekvensanalyse.

Husk, at med 'høj risiko' tænkes der ikke bare på klassisk datasikkerhed, men på overholdelse af hele persondataforordningen. Et element i risikoanalysen kan derfor f.eks. være risikoen for, at persondata bruges til et andet, ulovligt formål, end det formål oplysningerne blev indsamlet til.

Har I en plan for, hvordan I håndterer en sikkerhedsbrist

I har pligt til at oplyse om en sikkerhedsbrist, hvis I opdager, at persondata kan være blevet kompromitteret. I skal informere Datatilsynet om sikkerhedsbristen uden unødig forsinkelse og senest 72 timer efter, at sikkerhedsbristen er blevet opdaget. I skal også informere om sikkerhedsbristen til de personer, hvis data kan være blevet kompromitteret - medmindre I kan bevise, at sikkerhedsbristen ikke udgør en væsentlig risiko for de berørte personer.

Har I styr på jeres databehandlere

Hvis jeres organisation bruger eksterne firmaer til at håndtere persondata, eller hvis jeres organisation håndterer data for andre, gælder en række forpligtelser. Der skal bl.a. være indgået en formel, skriftlig kontrakt, der sætter rammerne for databehandlingen - en databehandleraftale - og databehandleren må udelukkende behandle data efter klare og dokumenterede instrukser fra den dataansvarlige.

Har I et overblik over, om I overfører persondata til tredjelande

Hvis I overfører data indeholdende persondata til lande uden for EU/EØS, gælder der særlige krav. I skal sikre, at de persondata, der bliver overført til et tredjeland, har en tilstrækkelig grad af beskyttelse - i praksis svarende til den beskyttelse, som persondataforordningen giver. Der findes en række forskellige juridiske overførselsgrundlag, der kan sikre denne beskyttelse.

Hvad gør I nu?

1. Nedsæt en projektgruppe

Det er vigtigt, at I indledningsvist får nedsat en projektgruppe, f.eks. med interessenter fra jura, IT og evt. IT-sikkerhed. Alt efter hvor stor jeres virksomhed er, kan det også være en god idé at få en erfaren projektleder tilknyttet. Projektgruppen kan med fordel udarbejde en kortfattet præsentation til ledelsen, da det er helt afgørende, at virksomhedens ledelse bakker op om projektet.

2. Få overblik over data

I skal finde ud af, hvad det er for nogle persondata, som jeres virksomhed skal beskytte. Den indledende del af arbejdet foregår ved at kortlægge virksomhedens persondata. Der skal med andre ord skabes et samlet overblik over alle typer personrelaterede oplysninger - f.eks kundeoplysninger, kontaktpersoner i jeres CRM-systemer, herunder emailadresser samt telefonnumre i forbindelse med konkurrencer og persondata om medarbejdere.

Overblikket over persondata skal afklare:

- Hvilke persondata har organisationen?
- Hvor kommer persondata fra?
- Hvad bruges persondata til?
- Hvor længe gemmes persondata?
- Hvem overlades/videregives persondata til?

Det kræver ofte en indsats fra både IT-afdelingen og alle de dele af virksomheden, som behandler persondata, hvis man skal have et nogenlunde komplet overblik over den behandling af persondata, der rent faktisk finder sted i virksomheden.

Husk, at overblikket skal omfatte både persondata, der lagres internt, og persondata, der lagres hos cloud- og outsourcingleverandører.

3. Hvilke regler er relevante for jer

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

Målet er 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 der ikke bruges ressourcer på at overholde krav, som I hverken er forpligtet til eller af anden årsag har interesse i at overholde.

4. Se på den nuværende praksis

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

Skab et samlet overblik over, om jeres nuværende praksis overholder reglerne i dag, og om der er nogle alvorlige mangler, som kræver umiddelbar handling fra jeres side.

5. Beskriv organisationens kontrolmål

Når I har fået overblik over den nuværende praksis for indsamling, opbevaring, brug, sletning, deling osv. af persondata, så er næste skridt at se på, hvordan I kan overholde reglerne i forordningen.

Med udgangspunkt i persondataforordningen skal I formulere en række kontrolmål, som er relevante for jeres organisation, f.eks. at der iværksættes processer og kontroller til at sikre overholdelse af slettefrister for persondata. Eller f.eks. et kontrolmål om, at I systematisk skal sikre jer, at alle kunder har afgivet samtykke, når virksomheden indsamler emailadresser til markedsføringsformål.

I første omgang handler det derfor ikke om at tage stilling til, hvordan I vil opfylde de enkelte kontrolmål, men om at have et samlet overblik over netop kontrolmålene. På den måde vil I have bedre mulighed for at designe de løsninger, hvor enkelte processer eller kontroller bidrager til at opfylde flere af jeres opstillede kontrolmål.

6. Foretag en risikovurdering

Persondataforordningen fokuserer på, at virksomheder skal gøre, hvad der er nødvendigt for at nedbringe risikoen for de registrerede personers oplysninger 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 beskyttelse 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 - eksempelvis kravene til saglighed, opbevaringsperiode, oplysningspligt osv.

Jeres virksomhed skal foretage en grundig risikovurdering. Det er vigtigt at være opmærksom på, at I skal kunne dokumentere, hvordan I har overvejet relevante risici, herunder de risici som jeres virksomhed vælger *ikke* at fokusere på.

Grundspørgsmålet for risikovurderingen er: Hvor alvorlig er situationen for de registrerede personer, hvis vi ikke overholder reglerne? Risikovurderingen går altså meget længere end den almindelige risikovurdering i forhold til IT-sikkerhed.

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 f.eks. helbredsoplysninger om personer i virksomhedens CRM-system. Risikovurderingen skal ikke kun give svar på, hvor I bør sætte ind, men også til dels i hvilken rækkefølge dette bør ske. For de fleste større virksomheder vil det være både nyttigt og nødvendigt at prioritere indsatsområderne, så der sikres fokus på områder med størst eksponering.

7. Design jeres løsning

Når I har fået overblikket over det nuværende omfang af jeres persondata, 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 virksomhed kommer på plads med at afhjælpe de forskellige mangler.

I skal udforme løsninger, der tager højde for jeres konkrete mangler i forhold til de *aktuelle* behandlinger, f.eks. udarbejdelse af nye persondatapolitikker. Samtidig skal løsningerne tage højde for jeres mangler i forhold til opfyldelse af kontrolmål, dvs. processer, der sikrer den *fremtidige* overholdelse af persondatareglerne. I denne fase er I 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 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.

8. Implementér hele vejen rundt

Næste skridt er den konkrete implementering af jeres plan for at kunne overholde persondatareglerne. Implementeringen bør følge virksomhedens normale processer for gennemførelse af forandringer. Det er vigtigt ikke at undervurdere de organisatoriske og psykologiske faktorer og behovet for forandringsledelse.

De nye persondataregler får konsekvenser for mange medarbejdere - også uden, at de måske selv er klar over det, f.eks. vil mange chefer 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 nye regler og procedurer. Jeres arbejde med at implementere vil typisk kræve intern uddannelse af alle medarbejdere, der er i berøring med persondata.

9. 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 glider tilbage til tidligere arbejdsgange og processer, eller at ændring af eksisterende aktiviteter og igangsættelse 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. Et godt råd er f.eks. at gennemføre en grundig opfølgning efter en periode på tre til seks måneder.

Vores team

Michael Hopp
Advokat, partner

- Har opbygget og er i dag ansvarlig for Plesners persondatateam
- Langvarig og dyb erfaring med teoretisk og praktisk persondataret - oparbejdet ved fokusering på området i mere end 15 år
- Bl.a. stået for gennemførsel af Binding Corporate Rules for LEGO

Kamilla Enevoldsen
Advokat

- Hos Plesner siden februar 2011
- Har ud over persondataret særlig erfaring med IT-ret
- Har i 2016 været udstationeret i 9 måneder hos Nordea i forbindelse med et persondata-complianceprojekt

Christian Nielsen
Advokat

- Hos Plesner siden juni 2013
- Specialist i persondata- og markedsføringsret
- Har været udstationeret hos Københavns Lufthavne
- Har i 2016 været udstationeret i 9 måneder hos Nordea i forbindelse med et persondata-complianceprojekt

Mads Toftgaard Nielsen
Advokatfuldmægtig

- Hos Plesner siden november 2015
- Inden da 3 års erfaring fra Datatilsynet - særlig erfaring med reglerne om overførsel til tredjelande

Phillip Giede Bøving
Legal Intern

- Hos Plesner siden september 2016
- Erfaring fra advokatbranchen samt fra e-handelsvirksomhed

Sara Reeh Lynge
Advokat

- Hos Plesner siden juli 2016
- Specialist i persondataret- og markedsføringsret
- Praktisk erfaring inden for persondata-compliance fra Tryg Forsikring, senest med ansvar for den juridiske vinkel af projektet til overholdelse af persondata-forordningen

Martin Hjørlund Nielsen
Advokat

- Hos Plesner siden februar 2015
- Specialist i persondataret
- 25 års erfaring fra international konsulentvirksomhed
- Erfaring som ansvarlig for 'information security compliance'
- Certificeret Prince 2 Practitioner (projektledelse)

Martin Nybye-Petersen
Advokatfuldmægtig

- Hos Plesner siden november 2015
- Inden da 3 års erfaring fra Datatilsynet – særlig erfaring med problemstillinger inden for den finansielle sektor og på det markedsføringsretlige område

Mille Selbach Rasmussen
Legal Intern

- Hos Plesner siden februar 2016
- Erfaring fra Datatilsynet

Mads Ehlers Falch
Legal Intern

- Hos Plesner siden marts 2016