

Quick guide i person-databeskyttelse

I maj 2018 vil Danmark og resten af EU få en ny fælles forordning, der regulerer, hvordan virksomheder skal behandle personoplysninger. En nyhed i denne databeskyttelses-forordning er de strafferetlige sanktioner en virksomhed kan blive idømt, hvis den overtræder reglerne. Dette har fået mange virksomheder til at overveje, hvordan de håndterer og beskytter personlige data. Her er en simpel guide i databeskyttelse rettet mod mindre virksomheder.



Databeskyttelse - de 4 kritiske

1. Indsaml ikke flere personlige data end nødvendigt.
2. Indsaml kun data til et forudbestemt formål.
3. Gem ikke data længere end nødvendigt.
4. Sørg for, at du har belæg for at indsamle data.



Hvad er persondata?

Persondata er alle de oplysninger, der kan knyttes til en fysisk person, som er i live. Typiske persondata er cpr-nummer, navn, adresse, telefonnummer og e-mail adresse. Også billeder af personer kan klassificeres som persondata. Ja, selv lydoptagelser, der er gemt elektronisk, kan være persondata, selvom der ikke er nævnt navne i optagelsen. Et cvr-nummer er ofte ikke persondata, men afhængig af forretningsaktiviteten og den juridiske form, så kan det være persondata alligevel. Det samme omkring registreringsnummeret på en bil som også kan være persondata, hvis det er muligt, at forbinde nummeret til en fysisk person. Hvis registreringsnummeret på en bil, der bruges af flere, oftest ikke vurderes som persondata.



GDPR - hvad betyder det

Databeskyttelsesforordningen forkortes almindeligvis til GDPR, som er en forkortelse for General Data Protection Regulation. Databeskyttelsesforordningen træder i kraft den **25. maj 2018** og erstatter på det tidspunkt den nuværende danske databeskyttelseslov. -



Compliance Partners

Religion, seksuelt liv og etnisk oprindelse

Den nye databeskyttelsesforordningen skelner mellem "almindelig" persondata og følsomme persondata. Følsomme data er dem, der afslører race eller etnisk oprindelse, politiske meninger, religiøse eller filosofiske overbevisninger, medlemskab af fagforeninger samt personoplysninger vedrørende sundhed og/eller sexliv. Sundhedsoplysninger kan være informationer i forbindelse med sygeorlov, graviditet og lægebesøg. Normalt er det forbudt at håndtere sådanne persondata, men der er undtagelser fra forbuddet. Disse følsomme persondata skal beskyttes mere end anden persondata.



NYT I FORORDNINGEN

I den nye databeskyttelsesforordning opfattes genetiske data også som følsomme persondata. Det samme gælder biometriske data, der bruges til at identificere en person.

Er det virkelig nyt?

Det faktum at vi i maj 2018 får en ny forordning, der regulerer hvordan man indsamler og bruger persondata, har tiltrukket sig meget opmærksomhed. Men faktisk har vi haft lovgivning på området i rigtig mange år. Der er blot blevet strammet og sammenkørt indenfor EU. I grunden indeholder forordningen de samme regler og principper som dagens lovgivning, men der er nyheder.

Hvornår må persondata indsamles?



I forordningen står der at "Persondata må kun indsamles til særlige, udtrykkelige og legitime formål og ikke behandles senere på en måde, der er uforenelig med disse formål". Således kan data indsamlet til et bestemt formål ikke anvendes til helt andre formål. Eksempelvis kan et firma udstyre deres biler med GPS-udstyr, der bruges til elektroniske kørebøger, for at forenkle dokumentationen til SKAT. Arbejdsgivere må dog ikke bruge data som GPS'en indsamler til at kontrollere, hvor lange pauser medarbejderne tager. I forordningen står der også, at du have belæg for at håndtere persondata. Der er et par forskellige "retsgrundlag", som virksomheder kan bruge. De vigtigste er:

RETSFORPLIGTELSE

I nogle tilfælde er virksomheder forpligtet til at registrere personoplysninger, f.eks i forbindelse med regnskabspligten i regnskabsloven.



KONTRAKTER / AFTALER

Ansættelseskontrakter, kundeaftaler/leveringsaftaler og leverandøraftaler er eksempler på kontrakter/aftaler, der kræver, at virksomheder registrerer og håndterer personoplysninger (men kun de oplysninger, der er nødvendige for at overholde aftalen).



SAMTYKKE

Der er også den mulighed at man beder personen om lov til at registrere oplysninger om ham / hende. Det kaldes for at få et samtykke. Et samtykke er i overensstemmelse med forordningen "enhver frivillig, specifik, informeret og utvetydig udtryk for vilje, hvorved den registrerede enten ved en erklæring eller ved en klar positiv særbehandling, giver tilladelse til registrering af persondata vedrørende ham eller hende." På lidt enklere dansk: det skal klart og tydeligt fremgå, hvilke persondata der indsamles for at man kan give en godkendelse. Det skal også fremgå, at man har ret til at tilbagekalde sit samtykke og hvordan.



INTERESSEAFVEJNING

Sidste mulighed er at håndtere persondata på grundlag af såkaldt afvejning af interesser, hvis virksomheden kan påvise, at dens interesse i brugen af oplysningerne opvejer den enkeltes ret til privatlivets fred. Ifølge lov om persondata, der gælder på tidspunktet for denne folders udgivelse, kan virksomheder som grundlag herfor i mange tilfælde anvende persondata til markedsførings og direct-mail. OBS! Du må ikke sende direkte mail til nogen, der har sagt nej til det.





Giv bedre og mere information ...

Når du indsamler oplysninger om en person, skal du informere den pågældende person. Forordningen indeholder en lang liste over ting, der skal oplyses om, men meget kort skal du nævne:

- At du indsamler personoplysninger.
- Til hvilket formålet du indsamler personoplysninger.
- Hvorfor du gør det.

Hvis du skal videregive oplysningerne til andre, er det også vigtigt at du oplyser det med det samme.

Tænk også på !

Der kan være krav i anden lovgivning, der kræver, at data skal gemmes i et vist tidsrum, f.eks. til regnskabs- og arkiveringsformål.



... og gem mindre

En af de vigtigste regler i forordningen er, at du ikke må gemme persondata i for lang tid. Når data ikke længere er nødvendige til det formål, som de engang blev indsamlet til, skal de slettes. For et firma betyder det for eksempel, at oplysninger om personer, der ikke længere er kunder skal slettes fra it-systemer, arkiver m.m. Når persondata-forordningen gælder, er praksis, at persondata om en tidligere kunde normalt kan bruges til markedsføringsformål i et år efter kundeforholdet er udløbet. I nogle tilfælde er en virksomhed i forbindelse med et salg nødsaget til at gemme visse persondata oplysninger for at kunne opfylde garantiforpligtelser indtil garantien er udløbet.



Få styr på sikkerheden!

Det er vigtigere nu end nogensinde at sørge for at beskytte de persondata, der håndteres, så de ikke bliver stjålet eller slettet eller ændret. Et nyt krav i forordningen er, at hvis virksomheden bliver bekendt med at den har "lækket" en "persondata oplysning" så skal hændelsen rapporteres til Datatilsynet. En sådan hændelse kan f.eks. være en tabt usb-stik med persondata, en forkert adgang til data på en af virksomhedens servere eller at en medarbejder har fået uautoriseret adgang til personlige data på andre medarbejdere. Et tip er at gennemgå beskyttelsen af personoplysninger i dine it-systemer.



Må du gemme oplysninger om dine kunders interesser?

I et CRM kundesystem kan du registrere flere oplysninger om kunderne end dem, der er behov for i relation til opfyldes af en kontrakt med din kunde.

- Spiller kunden golf?
- Hvor mange børn har kunden?
- Navn på kundens kone og børn
- Sygdomme i kundens familie
- Sidste ferie rejsemål m.m.

For at registrere denne type oplysninger er det normalt nødvendigt at få kundens samtykke på at du må gemme den type data og hvorfor du gemmer dem. Dette samtykke skal gemmes og kunden skal have mulighed for at tilbagekalde det. Du skal også sikre dig, at dataene er relevante for kundeforholdet ellers har du ikke ret til, at registrere dem.



Styr på detaljerne!

Ifølge forordningen er alle virksomheder (og andre organisationer) forpligtet til at lave en fortegnelse eller beskrivelse således, at man kan få et overblik over hvordan virksomheden håndterer persondata samt følsomme persondata. Den skal bl.a. indholde følgende:

- Hvem der internt ansvarlig for de forskellige data kartoteker / oplysninger
- Hvem der er ansvarlig for de forskellige it-systemer
- Hvad it-systemerne bruges til
- Hvilke typer persondata gemmes / opbevares
- Hvilke typer opgaver persondata bruges til
- Hvilket retsgrundlag giver virksomheden ret til at håndterer og gemme dataene?

Million bøder, hvis du er ligeglad

En nyhed i databeskyttelsesforordningen er, at Datatilsynet kan beslutte, at en virksomhed, der ikke overholder forskrifterne i forordningen, skal betale en administrativ straf, som er en form for bøde. Straffen kan være op til 20 mio. EUR eller fire procent af firmaets globale årlige omsætning.

LÆS MERE OM DATABESKYTTELSE

I denne folder nævner vi nogle af de vigtigste emner i den nye databeskyttelses forordning. Vi adresserer dog ikke nogen krav og anbefalinger, der kan være relevante, når persondata indsamles og håndteres.

Et godt sted at fortsætte med at læse om den kommende forordning er på:
www.compliance-partners.dk



Risikoen for bøder har gjort, at virksomheder er mere opmærksomme på at beskytte persondata.

Det er positivt.



Compliance Partners

Telefon: +45 69 1356 69

www.compliance-partners.dk

info@compliance-partners.dk

