Persondataforordning

Igennem det sidste år er der skrevet meget om den kommende Persondataforordning, som træder i kraft den 25. maj 2018 som afløser for de nuværende regler fra 1995. Nu skal virksomhederne have styr på, hvordan de håndterer persondata, ellers vanker der bøder op til 4 pct. af den globale omsætning.

”Til forskel fra den nuværende danske Persondatalov, så er den nye EU-forordning en hel del skrappere. Tidligere var det sjældent, der blev uddelt bøder, og den typiske bøde var op til 10.000 kroner, men nu er det beløb sat markant op. Det er dog næppe bøder i 20 millionerkronersklassen, vi kommer til at se blandt danske SMV’er. Men en bøde på 100.000 kroner er også voldsom for en mindre virksomhed, ” siger Jeppe Rosenmejer, chefkonsulent og jurist i SMVdanmark.

Han understreger, at vi udover større bøder også kan forvente, og at der vil komme et skærpet tilsyn med overholdelse af reglerne. Målet med EU-forordningen er at ensrette reglerne for persondata inden for EU.

De nye regler
Ændringen i reglerne medfører også, at virksomhederne bliver pålagt et større dokumentationskrav.

Eksempelvis skal alle virksomheder have skriftlige retningslinjer for, hvordan de håndterer persondata og sikrer, at data ikke falder i de forkerte hænder.

”Det er ikke længere nok blot at overholde reglerne, nu skal det også kunne dokumenteres. Som virksomhed skal man udarbejde politikker, der beskriver, hvordan man vil sikre sig, at virksomheden lever op til reglerne. Og man skal dokumentere, at man har indhentet de nødvendige samtykker og overholdt sin oplysningsforpligtigelse,” siger Jeppe Rosenmejer, chefkonsulent og jurist i SMVdanmark.

Sikkerhed og databrud
Et af de helt store fokuspunkter i de nye regler er øget opmærksomhed på sikkerheden.

”Når vi taler datasikkerhed, er det vigtigt at være klar over, at det ikke alene er i forhold til omverden i form af hackerangreb, phishing, men også internt i virksomheden, så der ikke er fri adgang for alle ansatte til alle data. Det kan være nødvendigt for mange virksomheder at ændre procedure for, hvordan man begrænser adgangen,” siger Jeppe Rosenmejer.

Han understreger, at det kun er personer med en saglig og legitim interesse, der må have adgang til oplysningerne i virksomheden.

Det er vigtigt, at du forud for udfyldelsen har lavet en grundig gennemgang af, hvilke data du har liggende på personer (ansatte og kunder), og hvordan de opbevares, ellers kan dokumenterne ikke udfyldes korrekt.

7 gode råd
I de følgende 7 steps har vi udarbejdet en arbejdsgang, der kan hjælpe dig med at få et overblik over, hvilke persondata du har, samt hvilke forholdsregler du som minimum skal tage dig.

Step 1) Hvilke data gælder reglerne for?
Inden du finder ud af, hvad du skal gøre, er det vigtigt at vide, hvornår reglerne overhovedet gælder.

Persondataloven beskytter kun personoplysninger, dvs. alle oplysninger der kan være med til at identificere en fysisk person. Men personoplysninger fortolkes meget bredt. Det er altså ikke kun de umiddelbare oplysninger, som navn, adresse, cpr.nr., personlige mailadresser, men også oplysninger om digitale fodspor i form af adgangskort, internetlogning, cookies på hjemmesider og lignende.

Normalt er oplysninger, der udelukkende vedrører virksomheder, for eksempel cvr.nr., hovedtelefonnummer, hoved-email-adresse, ikke omfattet af persondataloven.

Step 2) Hvilke data har jeg?
Herefter skal du finde ud af, hvilke data din virksomhed har liggende, og om det er ”almindelige” personoplysninger, som eksempelvis telefonnummer, adresse, email, eller om det er ”følsomme” oplysninger.

Følsomme oplysninger er:
- politisk orientering
- seksuel orientering
- religion
- helbredsoplysninger
- tilhørsforhold til en fagforening

Særligt om CPR-numre
CPR-numre er ikke en ’følsom oplysning’ i juridisk forstand, men en ’kritisk oplysning’, der også skal behandles varsomt. I modsætning til ’følsomme oplysninger’ kan man i visse tilfælde behandle CPR-numre uden samtykke.

Step 3) Behandlingsadgang
En af grundstenene i behandlingen af persondata er, at man *kun* må behandle oplysninger, der er nødvendige. Du skal have et *sagligt* og *legitimt* formål med at behandle oplysningerne og må ikke have oplysninger liggende, fordi de er ”rare” at have. Unødvendige oplysninger skal slettes!

Når du indsamler og behandler oplysninger, skal du være opmærksom på, om typen af data kræver et samtykke, eller om der er en anden lovparagraf, der giver dig ret til at foretage behandlingen.

Behandlingen af personfølsomme oplysninger må KUN ske på baggrund af et samtykke. Behandlingen af andre oplysninger kan også ske som opfyldelse af en aftale eller efter en interesseafvejning, hvor behandlingen af oplysningen vejer tungere end den registreredes interesse i at undgå behandlingen.

Hvis du behandler en oplysning på baggrund af et samtykke, skal du kunne dokumentere at have fået samtykket.

Step 4) Oplysningsforpligtelse
Første gang du behandler en persons oplysninger, er du forpligtiget til skriftligt at oplyse personen om formålet med behandlingen og personens rettigheder.

Personens rettigheder er blandt andet:

- retten til at tilbagekalde et samtykke
- retten til indsigt i, hvilke oplysninger virksomheden har på vedkommende
- retten til at få berigtiget og slettet oplysninger (populært kaldet ”retten til at blive glemt”).

Husk at gemme dokumentationen på at have levet op til oplysningsforpligtelsen ved eksempelvis at gemme den afsendte mail.

Hvor opbevares data, og hvem har adgang til dem?
Når du har fået overblik over, hvilke persondata du ligger inde med, skal du finde ud af, hvor de er placeret. Er de placeret på en intern eller ekstern server, individuelle drev eller fællesdrev, i mail, i papirform mv? Dette er vigtigt, for at du senere kan finde ud af, hvordan du skal håndtere dem i forhold til sikkerheden.

Det er kun personer med en *saglig* og *legitim* interesse, der må have adgang til oplysningerne, og det er kun nødvendige persondata, du må opbevare. Så du kan blive nødt til at strukturere dit IT-system anderledes og indføre adgangsbegrænsninger i forhold til, hvem der har adgang til hvilke oplysninger.

Step 6) Dokumentation og politikker
I forhold til tidligere skal du nu i langt højere grad kunne dokumentere, at du overholder reglerne. Du skal desuden løbende sikre dig dokumentation for overholdelse af loven, eksempelvis dokumentation for indhentelse af samtykke og overholdelse af din oplysningsforpligtelse.

Derfor skal du udarbejde politikker, der beskriver, hvordan virksomheden sikrer sig, at den lever op til reglerne:

- Hvilke data har du?
- Hvor opbevares data?
- Hvem har adgang til data?
- Hvilken ret har du til at behandle oplysningerne (hjemmel)?
- Hvordan opfylder du din oplysningsforpligtelse?
- Hvornår skal data slettes?
- Hvordan er sikkerheden omkring dine data?
- Hvad gør du i tilfælde af databrud (hvor du mister nogle oplysninger)?

Det kan være en god ide at udarbejde flere forskellige politikker, alt efter hvilke oplysninger det drejer sig om, eksempelvis én for personaleoplysninger og én for kundeoplysninger.

Step 7) Hvordan håndterer jeg sikkerhed og databrud?
Virksomheden skal i forhold til omverdenen sikre sig imod hackerangreb, phishing og ved at have en opdateret IT-sikkerhed med firewall, antivirus-programmer, mulighed for kryptering af e-mails etc.

Er en ekstern partner involveret i opbevaring eller behandling af data, skal du huske at have en databehandleraftale med dem, så du sikrer dig, at de også overholder de nye regler. Eksterne partnere er eksempelvis involveret, hvis du opbevarer data i en cloud-løsning eller bruger et eksternt lønbureau.

Men virksomheden skal også sikre sig internt i virksomheden, så der ikke er fri adgang for alle ansatte til alle oplysninger. Det kan derfor blive nødvendigt at ændre procedurer for, hvordan man gør tingene i virksomheden. Det kan være nødvendigt at opsætte nye regler for, hvordan man håndterer oplysninger, og hvor man må gemme oplysninger samt begrænse adgangen til visse oplysninger. Sidstnævnte kan eksempelvis ske ved at låse fysiske dokumenter inde og sikre visse dele af IT-systemet med et kodeord.

Skulle der ske et databrud, hvor du mister data til uvedkommende, er det vigtigt, at der er beskrevet en procedure i sikkerhedspolitikken, så der er styr på hvem, der skal gøre hvad og hvornår.
Ved databrud skal Datatilsynet informeres indenfor 72 timer!

Særligt for dofk medlemmer - dokumenter til virksomheden

Som medlem af dofk, kan du på www.dofk.dk/medlemsområde finde og downloade forskellige skriftlige retningslinjer for håndtering af persondata.

Alle dokumenterne ligger i Word format og der er markeret med GULT, der hvor du som virksomhed skal indsætte egen tekst.

Det er vigtigt, at du forud for udfyldelsen har lavet en grundig gennemgang af, hvilke data du har liggende på personer og kunder, og hvordan de opbevares. Ellers kan dokumenterne ikke udfyldes korrekt.

Udover dokumenterne skal du også udarbejde et kontrolskema for de enkelte procedurer i virksomheden.

Læs også ”Huskeliste”, hvor vi har prøvet at sætte det i skema som du skal have liggende eller udlevere til din ansatte. Der er en henvisning til de dokumenter du kan bruge.