

Sådan forbereder virksomhederne sig på persondataforordningen

Persondataforordningen vil stille en række nye krav til den måde, som danske virksomheder behandler personoplysninger på, og derfor bør man allerede nu begynde at kigge på, om virksomheden og dens processer er gearet til persondataforordningens komme.

Ledelsen skal søge for, at alle ansatte får regelsættet under huden for at undgå høje bøder

En af de mest markante ændringer ved at gå fra persondatalov til persondataforordning bliver det øgede fokus på regelhåndhævelse som følge af introduktion af et markant højere bødeniveau for overtrædelse.

For fremtiden vil ulovlige behandlinger af personoplysninger i værste fald kunne medføre bøder på op til 4 % af den årlige globale koncernomsætning. Med bødeniveauer i denne størrelsesorden kan manglende overholdelse af forordningens regler udgøre en reel forretningsrisiko.

Det er derfor vigtigt, at virksomhedens øverste ledelse får forankret og understreget vigtigheden af implementeringen af dette regelsæt i virksomheden, og at virksomhedens daglige ledelse formår at få persondatabeskyttelsen ind under huden på virksomhedens ansatte, så vigtigheden af regelefterlevelsen ikke kun lever på ledelsesplan, men derimod kommer til at gennemsyre alle niveauer og funktioner i virksomheden.

Få udpeget en Data Protection Officer, hvis kerneaktiviteterne består af behandling af personoplysninger

Som led i det øgede fokus på persondatabeskyttelse vil virksomheder, hvis kerneaktiviteter består af behandling af personoplysninger, eller som behandler følsomme personoplysninger i et væsentligt omfang, skulle udpege en såkaldt Data Protection Officer (DPO – også kaldet databeskyttelsesrådgiver). Som følsomme personoplysninger regnes blandt andet oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, oplysninger om helbredsmæssige forhold og seksuelle orientering.

Denne DPO skal have et særligt kendskab til forordningens krav til persondatabeskyttelse og har ansvaret for at sikre, at forordningens nye regler overholdes i forbindelse med virksomhedens daglige drift. For virksomheder, der bliver omfattet af dette krav, er det derfor en god idé at begynde at gøre sig nogle tanker om, hvem af virksomhedens medarbejdere der eventuelt har kompetencerne til at kunne løse denne opgave, eller om man alternativt skal have iværksat en rekrutteringsproces for at få de rette kompetencer ind i virksomheden.

Sørg for, at den mest restriktive privatlivsbeskyttende indstilling automatisk gælder i produkterne

En af nyskabelserne ved persondataforordningen er indførelse af principperne om "privacy by design" og "privacy by default" (databeskyttelse gennem design og gennem standardindstillinger).

Dette betyder kort fortalt, at virksomheder for fremtiden skal tænke persondatabeskyttelse i hele deres værdikæde, helt fra produktudviklingsfasen og til produktet havner hos slutkunden, samt at virksomhedens interne forretningsprocesser skal indrettes på en sådan måde, at de fremmer persondatabeskyttelse.

Principperne indebærer blandt andet et krav om, at de mest restriktive privatlivsbeskyttende indstillinger automatisk skal gælde, når en kunde køber et nyt produkt eller en service, hvor de afgiver personhenførbare oplysninger; fx opretter sig som bruger på sociale medier eller downloader apps.

Få kortlagt, hvilke personoplysninger virksomheden behandler

Selv om den kommende persondataforordning som omtalt ovenfor medfører en række nyskabelser, er det vigtigt at have for øje, at de grundlæggende principper for behandling af persondata stort set forbliver uforandrede.

Det betyder med andre ord, at hvis man har styr på reglerne i persondataloven og har sikret, at virksomheden opererer efter dem, så vil det for mange virksomheder være en relativt overkommelig opgave at foretage den opgradering af de allerede implementerede processer, som efterlevelse af persondataforordningen vil kræve.

For at få det nødvendige overblik over virksomhedens reelle niveau af regelefterlevelse af den nuværende persondatalov er det vigtigt, at virksomhederne afsætter tid og ressourcer til at få kortlagt, hvilke personoplysninger virksomheden behandler.

Dette kan afhængigt af virksomhedens størrelse og kompleksitet være en meget tidskrævende proces, da dette vil kræve, at der stilles de rigtige spørgsmål til mange forskellige personer på tværs af hele virksomheden, ligesom man gennem hele processen skal have for øje, at der er overensstemmelse mellem de svar, man får.

Kortlægningen skal give et detaljeret billede af, hvilke typer af personoplysninger der indsamles, hvorfra oplysningerne indsamles, hvordan oplysningerne indsamles, om oplysningerne videregives og til hvem, hvor og hvordan oplysningerne er gemt og sikret, hvordan oplysningerne bruges (herunder potentielle fremtidige formål), samt hvornår og hvordan oplysningerne vil blive slettet.

Da denne kortlægning danner grundlaget for at kunne iværksætte de korrekte foranstaltninger til overholdelse af både den nuværende persondatalovs og den kommende persondataforordnings regler, er det vigtigt, at kortlægningen bliver fuldstændig og korrekt. Det betyder, at der bør afsættes tilstrækkelig tid og tilstrækkelige ressourcer til gennemførelsen af denne proces.

Prioritér indsatsområderne

Den kommende persondataforordning indeholder mange regler og krav, hvilket selvsagt vil påvirke danske virksomheder i vidt forskelligt omfang alt efter karakteren af deres forretning. Det er derfor vigtigt for virksomhederne ret hurtigt at få identificeret, hvilke dele af persondataforordningen der har størst indflydelse på deres forretning, så virksomheden målrettet kan fokusere på at få sikret de områder, som har størst forretningsmæssig betydning og/eller medfører den største risikoeksponering.

Vær opmærksom på virksomhedens brug af databehandlere

Et af de områder, hvor virksomheder erfaringsmæssigt ikke er opmærksom på overholdelse af reglerne er ved brug af eksterne databehandlere. Den kommende persondataforordning stiller skærpede krav til brugen af eksterne databehandlere.

Derfor er det vigtigt, at virksomhederne i forlængelse af den ovenfor beskrevne kortlægningsproces ligeledes foretager en minutiøs gennemgang af, hvilke eksterne leverandører der er indgået aftaler med, og hvor der sker behandling af personoplysninger. Det kan for eksempel være aftaler med cloudleverandører,

outsourcingaftaler eller leverandører af internetbaserede personaleadministrationsværktøjer og meget, meget mere.

Når der er opnået et overblik over virksomhedens brug af databehandlere, bør der herefter tages skridt til en egentlig gennemgang af kontrakterne med disse med henblik på at identificere, om de pågældende kontrakter lever op til de skærpede krav i forordningen. Når dette er afklaret, kan det være nødvendigt at igangsætte en egentlig genforhandlingsproces med visse leverandører, så det sikres, at kontrakten for fremtiden tager højde for de nye krav, som persondataforordningen indebærer, hvilket vil bidrage til, at man mindsker virksomhedens risikoeksponering i forbindelse med brugen af databehandlere væsentligt.

Start processen nu

Persondataforordningen skal anvendes fra den 25. maj 2018. Det giver virksomhederne tid til at indrette sig på de nye regler forud for deres ikrafttræden, men det kan tage 18-24 måneder at komme igennem processen, bl.a. fordi der skal tilvejebringes et budget til aktiviteterne, og medarbejdere skal have frigjort tid til projektet eller der skal indhentes ressourcer udefra.

Udarbejdet af LETT Advokatpartnerselskab i samarbejde med DANSK IT maj 2016.

For yderligere information kontakt Susanne Mark, medlem af DANSK IT's fagråd for it og jura og til daglig Advokat (H), LETT, telefon 33 34 02 36, mobil +45 20 64 60 38, mail: sma@lett.dk