Vejledning til GDPR

Vejledning til GDPR

1. Formål

Formålet med denne manual er at hjælpe små virksomheder, der selv ønsker at stå for arbejdet med at implementere EU persondataforordningen.

Anbefalingerne tager udgangspunkt i Justitsministeriets betænkning (analyse og tolkning af hvordan EU persondataforordningen kan integreres i den danske lovgivning), den nye fremsatte databeskyttelseslov, der forventes vedtaget i starten af 2018 samt vejledninger udarbejdet af Datatilsynet.

Hvis du som virksomhedsejer er i tvivl om retsgrundlaget, bør du opsøge juridisk bistand.

2. Generelle betragtninger

EU Persondataforordningen er lavet for at beskytte os som borgere i en digital verden mod, at vores personoplysninger opbevares usikkert og deles med andre uden vores viden eller tilladelse.

Som virksomhed er du dataansvarlig, når du behandler personoplysninger om både ansatte og private kunder. Personoplysninger opdeles i "almindelige" og "følsomme" oplysninger, og i Danmark har vi en særlig kategori, hvor CPR. nr. hører under.

Efter forordningen, skal man foretage "passende organisatoriske og tekniske sikkerhedsmæssige foranstaltninger", når man behandler personoplysninger digitalt. Som virksomhedsejer skal du antage en risikobaseret tilgang, når du skal tage stilling til, hvilke foranstaltninger du skal foretage for at sikre dine kunders (ikke firma kunder) og den ansattes data.

Det vil sige, at du, hver gang du behandler (indhenter, opbevarer eller videregiver) personoplysninger, skal overveje, om du har bemyndigelse til at gøre det, og alt efter typen af data skal du overveje risikoen for, at oplysningerne lækkes og konsekvenserne af et evt. læk i forhold til personen.

Hvis man har meget data, der er personfølsomt (herunder helbredsoplysninger, fagforeningsforhold, race og etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, biometrisk data med henblik på identifikation og seksuelle forhold) forventer myndighederne, at du er særlig omhyggelig i forhold til sikring af data.

Kategorier af personoplysninger		
Almindelige	**Personfølsomme**	**Særlig katagori**
Navn, køn, alder	Helbredsoplysninger herunder genetisk data	Cpr. nr.
Adresse, tlf	Fagforeningsforhold	Strafbare forhold
IP adresse	Race og etnisk oprindelse	
kreditkortoplysninger	Politisk, Religiøs eller filosofisk overbevisning	
	Biometrisk data med henblik på identifikation	
	Seksuelle forhold	

Vejledning til GDPR

3. Liste over punkter man skal igennem

Data-flow analyse (ikke et krav men et hjælpemiddel).

Fortegnelse over behandlingsaktiviteter (dette er et krav)

Informationssikkerhedspolitik / IT-sikkerhedspolitik

Implementering

3.1 Data-flow analyse

En data-flow analyse kan laves mere eller mindre omfattende. Formålet med data-flow analysen er at skabe et overblik over dine behandlinger af personoplysninger i virksomheden.

Det er ikke et specifikt krav i persondataforordningen, at der laves en data-flow analyse, men det er en stor hjælp i forhold til at kortlægge, hvilke arbejdsgange man har, hvor der behandles (indhentes, opbevares eller videregives) personoplysninger. En data-flow analyse gør det også nemmere at lave den interne "fortegnelse" over behandlingsaktiviteter, som ER et krav jf. forordningen.

Du kan hente en simpel *data-flow-analyse* på http://woller.biz

3.2 Fortegnelse over behandlingsaktiviteter

Det er et krav, at alle dataansvarlige og databehandlere fører interne fortegnelser over al behandling af personoplysninger, dvs. både almindelige personoplysninger og følsomme personoplysninger. Fortegnelsen skal kun sendes til Datatilsynet, hvis du bliver bedt om det. ***Du skal have både en elektronisk og en fysisk udgave af fortegnelsen.***

Fortegnelsen skal som minimum indeholde:

- Kontaktoplysninger for den dataansvarlige – og hvis relevant, fælles dataansvarlige, den dataansvarliges repræsentant og databeskyttelsesrådgiver.
- Formål med behandlingen af oplysningerne (f.eks. personaleadministration, journalføring).
- Kategorier af registrerede (f.eks. oplysninger om nuværende og tidligere medarbejdere eller kunder) og kategorier af personoplysninger (f.eks. identifikationsoplysninger, oplysninger om løn, arbejdstid, cpr.nr. m.v.).
- Kategorier af modtagere ved videregivelse (f.eks. SKAT, Danløn m.v.).
- Overførsler til tredjelande og internationale organisationer.
- Slettefrister/ forventede tidsfrister for sletning af de forskellige kategorier af oplysninger.
- Hvis muligt, en generel beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger (f.eks. individuelle brugernavne og passwords, procedurer og politikker for behandling og kommunikation af personoplysninger).

Du kan hente en simpel blanket til *fortegnelse over behandlingsaktiviteter* på http://woller.biz

Vejledning til GDPR

3.3 informationssikkerhedspolitik / IT-sikkerhedspolitik

Virksomhedens informationssikkerhedspolitik skal tage udgangspunkt i lovgivningen og virksomhedens risikovurdering.

Nogle gode råd er:

Opdater IT-systemerne
Sårbarheder i styresystemer som feks. Windows XP og andre programmer som f.eks. Adobe Reader, Adobe Flash, Java og QuickTime m.v. udnyttes ofte af de kriminelle. Sørg derfor for, at styresystemet og andre programmer bliver opdateret, så sårbarhederne kan minimeres eller fjernes.

Programoprydning
For at minimere risikoen for cyberangreb anbefales det at antallet af benyttede programmer som virksomheden benytter holdes nede, så antallet af programmer som skal holdes opdateret nedbringes. Brug kun de programmer der er behov for.

Fil delings tjenester
Brug ikke OneDrive, Dropbox eller Google Drive så man ikke kommer til at gemme personfølsomme data (i skyen uden for EU)

Firewall
Installere firewall på arbejdsstationerne, firewall gør det svært for cyber-kriminelle at komme i kontakt med virksomhedens IT-udstyr/systemer.

Antivirusprogram
Installere et antivirusprogram på arbejdsstationerne, antivirusprogrammer undersøger, om der ligger skadelige virus og/eller koder i virksomhedens IT-udstyr.

Spamfilter
Installere et spamfilter på arbejdsstationerne, spamfilter forhindrer virksomheden i at modtage spammails.

Browser sikkerhed
Sørg for at indstille sikkerhedsniveauet for arbejdsstationens browser, så bliver brugeren/medarbejderen spurgt, inden filer, programmer m.v. overføres til computeren.

Kryptering af netværk
Sørg for at slå krypteringen TIL på virksomhedens trådløse netværk. Krypteringen beskytter virksomheden mod, at andre uønskede personer får adgang til netværket.

Back-up
Sørg for at tage sikkerhedskopier/back-up af virksomhedens vigtigste informationer. Opsæt eventuelt en struktur og process internt i virksomheden, så det bliver gjort regelmæssigt, inden uheldet er ude.

VPN
Få en krypteret VPN-forbindelse skabes der en sikker forbindelse over bl.a. et offentligt trådløse netværk samt personlige netværk, som er ukrypteret eller svagt krypteret. VPN kan med fordel benyttes til virksomheder der benytter hjemmearbejdspladser eller hvor medarbejderne skal have adgang til virksomhedens server, filer, mapper, intranet m.v. udenfor virksomheden.

Passwords
Brug lange passwords til beskyttelse på arbejdsstationerne og steder hvor virksomheden gemmer persondata. Udskift jævnligt jeres password.

Log af pc
Husk at logge af sin PC når man forlader den
lav en strømstyringsplan på din PC, så den slukker skærmen og kræver password efter f.eks. 2 min. uden berøring.

Kryptering af drev/ PC
Du bør kryptere din PC hvis du opbevarer personfølsomme data på din pc og har den med på farten.
der er indbygget et program i de fleste udgaver af Windows : BitLocker

3.4 Implementering

Du skal sikre dig at der ikke er uvedkommende der får adgang til dine data:

For data i fysisk form:
Lås det inde når det ikke benyttes. I et sikret skab, i aflåst rum, hvis du har det med på farten, opbevar i aflåst handskerum eller i en dokumentmappe med lås.

For data i digital form:
Følg din IT sikkerheds politik.
Udarbejd et skema hvor du noterer, hvilke forholds regler du har foretaget.

4. Databehandleraftaler

Efter persondataforordningen er der krav om, at der skal indgås en skriftlig databehandleraftale mellem dataansvarlige og databehandler, hvori det er beskrevet hvem, der kan tilgå data, evt. erklæring om tavshedspligt, og hvordan data skal behandles/opbevares/slettes.

Du vil som virksomhedsejer være dataansvarlig i forhold til en lang række personoplysninger, f.eks. om dine ansatte og dine kunder. Som dataansvarlig skal du blandt andet sikre dig:

- At du har lov til at behandle de oplysninger, som du og dine databehandlere er i besiddelse af.
- At du er i stand til at efterleve den registrerede persons rettigheder (f.eks. opfylde din oplysningspligt i forhold til, hvilke oplysninger du har om den pågældende)
- At du får indberettet eventuelle brud på persondatasikkerheden til Datatilsynet inden for 72 timer.

En databehandler er en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne, dvs. at databehandleren f.eks. indsamler, registrerer, opbevarer, videregiver eller sletter personoplysninger efter instruks fra dig som virksomhedsejer (dataansvarlig). Et eksempel på en databehandler kan være din Lønleverandør til de ansattes løn.

Databehandleraftalen skal sikre, at databehandleren kun behandler personoplysningerne på den måde, der er aftalt med og godkendt af dig, og det er dit ansvar at føre tilsyn med databehandleren.

Databehandleren har dog også et selvstændigt ansvar, derved at "han" ikke må lave behandling af personoplysninger, der er ulovlige jf. forordningen, selvom det sker efter instruks fra den dataansvarlige.

5. Oplysning

Den nemmeste måde at gøre dine kunder opmærksom på hvordan du behandler deres data på er:
Hvis du har en hjemmeside tilføj en side der kort forklarer det. Og skriv i din E-mail signatur at folk kan læse det på din hjemmeside.
Hvis du ikke har en hjemmeside så bare lav en kort forklaring på din E-mail signatur.

6. Dokumentation

- Print en kopi af alle de bilag du har udarbejdet ud.
- Kom det hele i mappe så det er samlet og lige til at tage frem.
- Gem desuden digitale kopier af det hele i en mappe på et sikkert sted