Oplæg om Persondataforordningen til SLRTV's årsmøde den 21-4-2018

Nye regler om datasikkerhed lige om hjørnet..

Den 25 maj 2018 træder EU's Persondataforordningen i kraft og så skal alle offentlige instanser, virksomheder, foreninger o.l. have sat sig ind i hvad det betyder for dem.
Virksomhedernes netværk og elektroniske systemer rummer på kolossale mængder af personlige oplysninger om både kunder og medarbejdere. Hvis ikke disse data opbevares og behandles efter forskrifterne kan det komme til at koste dyrt i form af bøder i millionklassen.

Dansk Erhverv er gennem en rundspørge i slutningen af 2017 blevet noget bekymret idet:
15% mente ikke det var relevant for dem
15% kendte ikke til reglerne
12% svarede "ved ikke" hvordan de skal forholde sig
og kun 4 ud af 10 virksomheder, der var i gang med arbejdet, mente at de kunne nå at være klar til at efterleve reglerne når de træder i kraft den 25 maj 2018

Reglerne gælder for alle, bare de har én kunde, ét medlem eller én ansat.

Samtidig indføres en omvendt bevisbyrde som betyder at man på datatilsynets forlangende øjeblikkeligt skal kunne dokumentere, at reglerne overholdes og kunne beskrive med hvem man har kontakt, hvilke type data man har liggende, hvilken type sikkerhed man har og hvilke type personoplysninger, der er særligt følsomme.
Kan man ikke dokumentere det vanker der en bøde af størrelsesordenen 4% af virksomhedens globale omsætning.

FAKTA
1. I forbindelse med de nye fælleseuropæiske sikkerhedsregler definerer EU persondata, som alle former for information der identificerer eller kan bruges til at identificere en person, herunder også kodede oplysninger.

2. Som almindelig persondata regner man almindeligvis oplysninger som navn, adresse, telefonnummer og e-mail.

3. Fortrolige persondata omfatter cpr-numre, økonomiske forhold og billeder.

4. Følsomme persondata vedrører bl.a. etnicitet, straffeattest, seksuel eller religiøs orientering og helbredsforhold.

5. Alle disse data skal sikres mod misbrug. Det har gennem flere år været lovbefalet men pr. 25 maj 2018 gælder nogle omfattende og skærpede fælleseuropæiske krav til, hvordan oplysninger om både ansatte og kunder opbevares og behandles.
Reglerne foreskriver udskrivelse af store bødeforlæg ved overtrædelse.

6. Både medarbejdere og kunder har til hver en tid krav på at få oplyst hvilke data, virksomheden har registreret, ligesom virksomhederne skal efterkomme alle krav om, at oplysningerne skal slettes.

Følgende bør som minimum afklares:

1. Dataanalyse

a. Der skal laves en skriftlig afdækning af hvilke former for persondata man er i besiddelse af og kontrol af om oplysningerne er korrekte. Afdækningen skal omfatte ansatte og ansatte hos samarbejdspartnere, bestyrelsesmedlemmer, medlemmer og frivillige.
Som minimum skal afdækkes:

Navne
Fysiske adresser
E-mail adresser
Telefonnumre
Medlemsnumre
IP adresser
Korrespondance (e-mails, sms, almindelige breve)
Andre persondata

Hvis man har ansatte, så har man også personfølsomme data som kræver at den ansatte skal give et skriftligt samtykke til at man behandler og opbevarer disse persondata.
Der stilles også højere krav til sikkerheden for behandling af personfølsomme data og det skal huskes beskrevet i denne dataanalyse.

b. Hvorfor vi har disse person data liggende.
Lav en forklaring der fortæller hvorfor vi har disse persondata liggende og hvad vi vil bruge dem til.

c. Udarbejd en skriftlig redegørelse for hvor foreningens persondata er placeret.
Redegørelsen skal af hensyn til udarbejdelsen af procedurer senere, indeholde en udtømmende beskrivelse af placeringen og skal som minimum indeholde:

- Hvilke personer (ansatte, bestyrelsesmedlemmer, frivillige) er i besiddelse af persondata og på hvilke platforme (pc'ere, Ipads, telefoner, usb-stik, skyen og fysisk opbevarede persondata), og kan disse data nemt findes og søges i.
  Er de i Word filer excel filer, e-mails m.v. eller står de i de papirer der laves interview ud fra eller står de på den video som er undertekstet.
  Vi skal også huske på at gæster der besøger os som f.eks. skal i studiet til et interview også er persondata som vi måske også opbevarer data på.

d. Udarbejd en skriftlig redegørelse for hvorledes persondata på nuværende tidspunkt er beskyttet på de enkelte platforme og underplatforme, herunder:

- Tilstrækkelige passwords til elektroniske platforme.
- Opbevares fysiske dokumenter forsvarligt i aflåste arkiver m.v.
- Tilgængelighed for uvedkommende, kollegaer, børn ægtefæller o.l. har de adgang til PC'er der anvendes i virksomheden, eller ligger der fysiske dokumenter, usb stiks o.l. frit fremme på hjemmekontoret.
- Er systemerne tilstrækkelig beskyttet af virusprogrammer, firewalls o.l.
- Bliver der fortaget de nødvendige backups og er disse backups forsvarligt opbevaret.

e. Hvis der ved gennemgang af c. og d. konstateres at der er behov for at stramme op på sikkerhedsniveauet, således at persondata ikke havner i uvedkommendes hænder, skal I her beskrive – og selvfølgelig gennemføre – de foranstaltninger, der er nødvendige for en sådan opstramning. (password låst inde o.l.)

2. Dataminimering (oprydning)

a. Er man i besiddelse af persondata som man ikke længere har brug for (udmeldelser, samarbejds ophør o.l.) skal de som udgangspunkt slettes straks.
Hvis der er en begrundet mistanke om at der senere kan opstå en tvist omkring vedkommende kan data blive liggende i op til 3 år.
Er en persons data en del af bogføringen kan de ligge i op til 5 år (bogføringsloven).

b. Nogle af disse persondata bliver måske aldrig slettet da det mange gange er dokumentarlignende ting der går i mediearkiverne alle mulige steder som f.eks. Statsbiblioteket i Århus, lokalhistoriske arkiver, you-tube o.l. steder.
Derfor skal det overvejes om der skal laves en samtykke erklæring inden en person skal interview'es så vedkommende person ved sit samtykke er klar over at det aldrig vil blive slettet.

3. Udarbejd en procedure for indsigtsbegæring

En indsigtsbegæring vil typisk komme fra nuværende eller tidligere personer der har været knyttet til virksomheden. Eftersom en indsigtsbegæring skal efterkommes senest 1 måned efter fremsættelsen, er det vigtigt at have været igennem de øvelser der er beskrevet under punkt 1 og 2 inden denne procedure nedfældes. Proceduren skal minimum indeholde beskrivelser af følgende:

a. Uanset hvem der modtager indsigtsbegæringen, så skal I have udpege én person, der håndterer begæringen.

b. Den udpegede ansvarlige besvarer straks anmodningen om indsigtsbegæring.

c. Den udpegede ansvarlige underretter alle de medarbejdere og eksterne databehandlere der er i besiddelse af persondata på den indsigtsbegærende og fremsende dem til den udpegede ansvarlige inden 8 dage.

d. Proceduren bør indeholde en huskeliste over de platforme, hvor persondata behandles, og som derfor skal tilgås for indsigt. Herved minimeres risikoen for, at nogle persondata overses eller glemmes i indsigtsproceduren. Da der under pkt. 1.c.- burde være udfærdiget en udtømmende oplistning af platforme, burde denne oplistning kunne bruges som huskeliste.

e. Senest én måned efter modtagelsen af begæringen skal den udpegede ansvarlige sende kopi af alle de oplysninger vi har om den indsigtsbegærende til vedkommende.

f. Kan denne måneds frist ikke overholdes skal den udpegede ansvarlige snarest muligt kontakte den indsigtsbegærende og oplyse om forsinkelsen og grunden hertil. Samtidig underrettes datatilsynet om anmodningen, - om at besvarelsen er forsinket og om årsagen hertil.

4. Udarbejd en procedure for sletning af persondata uden begæring

Se også ovenfor i pkt 2 Dataminimering om sletning af unødvendige data. Det er de samme principper der er gældende her. Følgende bør iagttages:

a. Udpeg en koordinator som skal iværksætte at sletning skal udføres.
b. Proceduren skal indeholde en beskrivelse af hvorledes koordinatoren skal underrette de forskellige interne og eksterne databehandlere om at en sletning skal iværksættes.
c. Proceduren bør indeholde en huskeliste over de platforme, hvor persondata behandles, og som derfor skal tilgås for sletning. Herved minimeres risikoen for, at nogle persondata overses eller glemmes i indsigtsproceduren. Da der under pkt. 1.c.- burde være udfærdiget en udtømmende oplistning af platforme, burde denne oplistning kunne bruges som huskeliste.
d. Proceduren bør udformes så det sikres at der med jævne mellemrum kontrolleres at man ikke er i besiddelse af overflødige persondata.
   Kontrollen bør som minimum gennemføres hvert kvartal.
e. Proceduren skal endvidere indeholde en beskrivelse af hvordan koordinatoren sikrer at sletning af samtlige overflødige persondata har fundet sted og suppleres med en beskrivelse af hvorledes eksterne databehandlere melder tilbage om udført sletning

5. Udarbejd en procedure for sletning af persondata efter begæring

I store træk vil en sådan procedure kunne bygges op efter de principper der er gennemgået under pkt 3 om indsigtsbegæringer – dog med enkelte ændringer..

a. Uanset hvem der modtager sletningsbegæringen, bør I udpege en person, der håndterer begæringen. Formuleringen i proceduren kunne være: ”[navn på den udpegede person] er ansvarlig for håndtering af sletningsbegæringer. Sletningsbegæringer modtaget af andre videregives omgående til [navn på den udpegede person].

b. Den udpegede ansvarlige besvarer uden unødigt ophold anmodningen om sletning, - eksempelvis med følgende formulering:

   ”Vi har modtaget din sletningsbegæring, og jeg har anmodet alle medarbejdere og samarbejds-partnere om at slette samtlige persondata, vi er i besiddelse af om dig. Jeg vender tilbage, så snart jeg har modtaget bekræftelse på sletningen og inden en måned fra begæringens fremsættelse.”

c. Den udpegede ansvarlige underretter samtlige interne som eksterne databehandlere og andre, der måtte være i besiddelse af persondata på den sletningsbegærende, og anmoder disse om – inden 8 dage – at slette alle oplysninger om pågældende.

d. Proceduren bør indeholde en ”huskeliste” over de platforme, hvor persondata behandles, og som derfor skal tilgås for sletning. Herved minimeres risikoen for, at nogle persondata overses eller glemmes i sletningsproceduren. Da der under pkt. 1.c.- burde være udfærdiget en udtømmende oplistning af platforme, burde denne oplistning kunne bruges som huskeliste.

e. Proceduren skal endvidere indeholde en beskrivelse af, hvorledes den udpegede ansvarlige skal sikre, at sletning af samtlige persondata har fundet sted. Dette punkt kan suppleres med en beskrivelse af, hvorledes de øvrige interessenter skal melde tilbage til den udpegede ansvarlige.

f. Hvis den udpegede ansvarlige konstaterer, at det ikke er muligt at overholde fristen på én måned, skal den udpegede ansvarlige snarest muligt kontakte sletningsbegæreren og oplyse om forsinkelsen og grunden til denne. Samtidig skal den udpegede ansvarlige underrette Datatilsynet om anmodningen, - om at sletningen er forsinket og om årsagen hertil.

g. Hvis den udpegede ansvarlige konstaterer, at sletningsbegæringen helt eller delvist ikke kan imødekommes af hensyn til anden lovgivning, eller som følge af, at virksomhedenss fortsatte behandling skønnes nødvendig for at virksomheden kan forfølge en berettiget interesse, der skønnes at overstige den registreredes fundamentale rettigheder og friheder, skal den ansvarlige meddele dette til sletningsbegæreren hurtigst muligt med oplysning om, at denne beslutning kan indbringes for Datatilsynet.

6. Udarbejd en procedure for sikkerhedsbrud og hændeligt tab af data

Man skal ikke undervurdere betydningen af denne procedure, da faldgruberne er virkeligt mange, og da forebyggelsen og reaktionen på sikkerhedsbrud, er en af de bærende søjler i Persondataforordningen.

Eksempler på sikkerhedsbrud er:

a. Uautoriseret tilgang til persondata på internettet,
b. Tyveri, indbrud, røveri, ”hacking” med tab af persondatabærende platform(e) til følge,
c. Hændeligt tab, f.eks. en glemt mobiltelefon eller anden persondatabærende platform.

Proceduren ved sikkerhedsbrud bør som minimum indeholde følgende:

a. Der udpeges en ansvarlig (den sikkerhedsansvarlige), der koordinerer indsatsen.
b. Alle medarbejdere, der udsættes for sikkerhedsbrud, kontakter omgående den sikkerheds-ansvarlige efter konstateringen af sikkerhedsbruddet.
c. Den sikkerhedsansvarlige kontakter Datatilsynet omgående og inden 72 timer efter konstatering af sikkerhedsbruddet med oplysning om bruddets karakter og omfanget og karakteren af de muligt berørte persondata.
d. Den sikkerhedsansvarlige kontakter alle de muligt berørte hurtigst muligt efter konstatering af sikkerhedsbruddet med oplysning om, hvilke persondata, der kan være omfattet.
e. Den sikkerhedsansvarlige skal i videst muligt omfang sikre, at begrænse de skadelige følger af sikkerhedsbruddet samt dertil inddæmme omfanget heraf.

7. Databehandleraftaler

Hvis der er andre foretagender som håndterer virksomhedens persondata skal der laves en databehandleraftale med dette foretagende. Denne aftale skal beskrive hvordan de håndterer vores persondata. Databehandleraftalen skal ikke nødvendigvis udarbejdes af jer selv men det er jer selv der har ansvaret for at den indgås.

Følgende databehandleraftaler er indgået:

Følgende databehandleraftaler mangler:

8. Udarbejd herefter jeres politik for persondatabehandling samt indberetning af overordnet persondataansvarlig til Datatilsynet:

Når alle de foregående punkter 1 til 7 er gennemført, vil virksomheden kunne nedskrive den egentlige politik for den nuværende og fremtidige overholdelse af persondataforordningens regler.

Et forslag til formulering kunne være:

[Navnet på virksomheden] har i tilknytning til EU's Persondataforordning, gennemført de nødvendige analyser af persondata, indgået de fornødne databehandleraftaler samt udarbejdet nødvendige procedurer for virksomhedens behandling af persondata.

Virksomhedens nuværende medarbejdere har modtaget den oplæring og instruktion, der skønnes nødvendig for, at virksomheden kan leve op til sine forpligtelser under Persondataforordningen.

Virksomheden har i forbindelse med den nævnte analyse foretaget en vurdering af sikkerheds-niveauet og foretaget de ændringer, som virksomheden har skønnet nødvendige for at leve op til Persondataforordningens standarder herfor.

Virksomheden vil til enhver tid efterleve Persondataforordningens regler, og herunder foretage nødvendig opdatering og revision af gældende procedurer i det omfang eksterne eller interne omstændigheder tilsiger dette.

Interne omstændigheder vil eksempelvis kunne opstå ved udskiftning eller ændringer i ledelsens sammensætning, med deraf følgende ændringer af ansvarlige for de særskilte procedurer, ved fremtidig indgåelse af databehandleraftaler, eller ved ny-ansættelser.

Eksterne omstændigheder vil særligt kunne opstå ved lovændringer eller ved etablering af andre former for databehandling end kendte på nuværende tidspunkt, eller ved behandling af persondata på andre platforme end de anvendte på tidspunktet for den oprindelige dataanalyse.

Såfremt interne eller eksterne omstændigheder indebærer behov for oplæring eller træning vil dette finde sted i det fornødne omfang.

Opdatering og revision finder derudover sted én gang om året, og der føres en særskilt protokol om alle ændringer og/eller tilpasninger.

Foreningen har udpeget [Navnet på den ansvarlige] som overordnet ansvarlig for foreningens behandling af persondata, og har oplyst Datatilsynet herom.

Det anbefales at samle samtlige dokumenter, der udfærdiges efter denne vejledning, og opbevare denne dokumentsamling - og senere ændringer - i flere eksemplarer således, at den på forlangende kan udleveres til Datatilsynet.

De nævnte procedurer kan blive en hjælp, den dag, hvor indsigtsbegæringen, sletningsbegæringen eller sikkerhedsbruddet rammer jer.

Det er betydeligt nemmere at træffe sine forholdsregler nu – og fra den 25. maj 2018 er det lovpligtigt, at forholdsreglerne skal være på plads.

Gunnar Thomsen
SLRTV

Tips:
Det vil være ret smart at slette alle mails når de er læst også fremadrettet.
Man kan jo overføre de mail oplysninger der skal gemmes til andre arkiver der er nemmere at håndtere og søge i.
Er alle personoplysninger i ét arkiv og på én computer med én backup er det ret nemt at håndtere persondataforordningen efterfølgende især dokumentationsmæssigt.