NYE REGLER FOR HÅNDTERING AF PERSONDATA

Overblik, indblik og compliance!

En vejledning udarbejdet til Dansk Lives og Danske Koncert- og Kulturhuses medlemmer juli 2017.

Nye krav og regler fra 2018!

Den 25. maj 2018 træder EU's nye persondataforordning i kraft i Danmark. Med de nye regler introduceres en række udvidede rettigheder for borgerne samt en række skærpede forpligtelser for virksomheder og organisationer, som de skal være opmærksomme på og leve op til i forbindelse med indsamling og behandling af personoplysninger.

Med lovændringerne lægges der samtidig op til markant skærpede bøder for overtrædelse af de persondataretlige regler, og det kan derfor i fremtiden få stor økonomisk betydning, hvis man ikke overholder reglerne.

Da området er både stort og komplekst, har Dansk Live og Danske Koncert- og Kulturhuse fundet det hensigtsmæssig at udvikle denne korte vejledning, der forhåbentlig kan bidrage til større indsigt i persondataområdet og hjælpe medlemmer til at komme i gang med compliancearbejdet, så det er på plads, inden de nye regler træder i kraft.

> Frem mod 2018 udgives en række officielle vejledninger til området (link)

SE DET SOM EN MULIGHED — IKKE KUN ET KRAV!
Nogle vil påstå, at persondataloven og færdselsloven er de love, der overtrædes oftest. Og ligesom man i forhold til reklame og promotion kender til god markedsføringsskik, bør man tilsvarende arbejde for bedre databehandlingsskik, der ikke kun følger loven, men også behandler personoplysninger, som man selv ønsker det.

God, sikker og effektiv datahåndtering hører sig nemlig til i den digitale tidsalder, og mange mener, at compliance (dokumenteret overholdelse af reglerne) og god dataetik fremover vil blive et markant konkurrenceparameter i forhold til at sikre tilliden hos kunder, samarbejdspartnere, investorer, medarbejdere osv.

En kortlægning af data og gennemgange af datastrømme er samtidig en mulighed for at finde nye måder til at optimere og forenkle processer. Det kan også medvirke til en øget bevidsthed blandt ansatte om risikoen forbundet med behandling af persondata. Vi håber derfor, at I også vil kunne se fordele og muligheder i de nye persondataregler.

OM VEJLEDNINGEN
Med vejledningen ønsker vi at give et hurtigt ***overblik*** over persondataloven (s. 3), et mere udførligt ***indblik*** i relevante emner og tematikker (s. 4-5) samt en ***guide*** (s. 6-7) til at komme i gang med en god proces om compliance og nå i mål inden maj 2018.

Det er en god idé at begynde arbejdet allerede nu, for compliance tager ofte længere tid, end man måske lige tror, og kan kræve allokering af ressourcer mv.

Og lyder det hele allerede alt for tungt? Så prøv at starte bagfra. På sidste side har vi nemlig gengivet ***datatilsynets 12 spørgsmål om databeskyttelse***, som virksomheder og organisationer bør forholde sig til fremadrettet. Det kan måske give videre inspiration.

De bedste hilsner
Dansk Live og Danske Koncert- og Kulturhuse

Overblik

EU vedtog i april 2016 en ny databeskyttelsesforordning – den såkaldte *GDPR, General Data Protection Regulation.* Forud var gået fire års forhandlinger, og efterfølgende har Danmark sammen med de øvrige EU-lande fået to år til at implementere forordningen i den nationale lovgivning. Det skal være på plads senest d. 25. maj 2018.

De nye regler skal erstatte de eksisterende på området, og der pågår i øjeblikket en større proces i bl.a. Justitsministeriet for at få implementeret forordningen i den danske lovgivning. Dette kan man læse mere om på Justitsministeriets hjemmeside (link).

Ændringerne har helt overordnet til hensigt at:

- Harmonisere reglerne på tværs af EU-landene og sikre et bedre samarbejde mellem myndighederne
- Sikre borgerne bedre rettigheder ift. registrering og behandling af persondata
- Stille nye og skærpede forpligtelser for virksomhederne ift. persondatahåndtering

ÆNDRINGER IFT. EKSISTERENDE LOVGIVNING

De væsentligste nye regler, der har betydning for virksomheden, er:

Nye rettigheder til den registrerede: Ved indsamling af personoplysninger skal der oplyses om, hvilket hjemmelsgrundlag der anvendes. Den registrerede får desuden ret til at blive glemt igen.

Risikoanalyse: Før virksomheden behandler personoplysninger, skal der foretages en analyse af konsekvensen af de påtænkte behandlinger.

Dokumentation af compliance: Virksomheder skal kunne dokumentere, hvordan de overholder de persondataretlige regler og løbende føre en fortegnelse over de kategorier af persondatabehandling, som foretages.

Rapportering af databrud: Virksomheder skal underrette myndigheder og kunder om sikkerhedsbrud mv., hvis kunders personoplysninger er blevet kompromitterede.

Indarbejde persondatabeskyttelse: Hvis virksomheder udvikler nye produkter, ydelser eller forretningsgange, skal de tage persondatabeskyttelse med i deres overvejelser og sikre, at kunder altid som udgangspunkt beskyttes bedst muligt.

Databeskyttelsesofficer: Nogle virksomheder skal udpege en databeskyttelsesofficer, der er ansvarlig for virksomhedens behandling af personoplysninger. Dog primært virksomheder, der monitorerer personer i stort omfang, eller som behandler mange følsomme personoplysninger.

NYE STORE BØDEMULIGHEDER

Med forordningen følger også en skærpet bødepraksis, der arbejder med en bøderamme på op til 2 og 4 pct. af omsætningen (afhængig af karakteren af forseelserne), hvis reglerne ikke overholdes. Dette står i kontrast til, at der indtil videre i dansk kontekst kun er givet bøder på op til 25.000 kr. ved brud på gældende persondataregler.

Indblik

For at komme et spadestik dybere vil vi på de følgende sider gennemgå en række emner og tematikker, der giver et grundlæggende indblik i persondataområdet.

GENERELT OM PERSONDATA OG FØLSOMHEDSKATEGORIER
Persondata er lagrede oplysninger om en person, og personoplysninger er enhver form for information om en identificeret eller identificerbar fysisk person. For personoplysninger gælder det, at man kan inddele dem i flere typer af følsomhedskategorier.

Almindelige personoplysninger: Oplysninger, som ikke har følsom karakter. Det er blandt andet navn, adresse, telefonnummer, e-mailadresse eller oplysninger om køb af varer eller ydelser – dvs. købshistorik. Oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold kategoriseres i dag som **semifølsomme oplysninger,** men flyttes med forordningen i udgangspunktet til de almindelige oplysninger, og kategorien bortfalder.

Følsomme personoplysninger: En række personoplysninger betragtes som følsomme oplysninger. Det drejer sig om race, etnicitet, politisk eller fagforeningsmæssigt tilhørsforhold, religiøs eller filosofisk overbevisning. Det gælder også oplysninger, der angiver eller indikerer, at en person har en sygdom (eksempelvis oplysninger om køb af medicin eller hjælpemidler) eller en persons religiøse overbevisning (fx ønsker til bestemt mad, beklædning mv.).

CPR-oplysninger: Endeligt er brugen af CPR-numre særligt reguleret i persondataloven, men det gælder alene, hvis det fulde CPR-nummer registreres. Hvis det alene er de fire første cifre i kundens CPR-nummer, der registreres, er der tale om almindelige personoplysninger.

OM BEHANDLING AF PERSONDATAOPLYSNINGER
Data og oplysninger får ofte først sin relle værdi, når de behandles eller indgår i processer. En behandling af personoplysninger skal forstås bredt og dækker over enhver operation, som personoplysningerne gøres til genstand for. Det er fx indsamling, registrering, organisering, systematisering, opbevaring, læsning, redigering, tilpasning, ændring, beregning, sammenstilling, samkøring, genfinding, søgning, videregivelse, formidling, overladelse, begrænsning, sletning eller tilintetgørelse af personoplysninger.

Principperne i persondataforordningen inkluderer generelt, at personoplysninger:
- skal behandles ***lovligt, fair og transparent***
- skal være ***korrekte og opdaterede***
- kun må behandles til et ***specifikt, eksplicit og legitimt formål***
- ikke må ***lagres*** længere end nødvendigt
- skal ***beskyttes*** via sikkerhedsforanstaltninger iværksat efter en risikovurdering

Principperne inkluderer desuden, at der ikke må behandles flere personoplysninger end nødvendigt.

DOKUMENTATIONSKRAV
Med den nye forordning skal der gives langt flere oplysninger til den registrerede om behandlingen, end virksomhederne er vant til i dag. De oplysninger, der skal gives, indeholder bl.a. den dataansvarliges kontaktinformation, formålet med behandlingen, lovligheden af behandlingen (hjemmelgrundlag), perioden for behandlingen (inkl. lagring), evt. overførsel til tredjeparter, retten til at gøre indsigelse og begrænse behandlingen, muligheden for at trække samtykke tilbage samt muligheden for at klage til Datatilsynet, og om behandlingen indgår i en profilering.

UTVETYDIGT SAMTYKKE
For at en behandling af personoplysninger kan være lovlig, skal der indhentes samtykke til behandlingen fra de registrerede. Det er der ikke noget nyt i. Når det drejer sig om behandling af almindelige personoplysninger, skal samtykket være ***frit, specifikt og informeret***. Det nye er, at samtykket skal være ***utvetydigt!***

Samtykket er utvetydigt, når den registrerede foretager en bekræftende handling, som tilkendegiver, at han eller hun accepterer den konkrete behandling af personoplysningerne til det konkrete formål. Fx hvis de klikker i en boks, vælger indstillinger, afgiver en erklæring eller på anden måde udviser en adfærd, der tilkendegiver samtykket.

**NYE RETTIGHEDER: FX RET TIL AT BLIVE GLEMT,
IKKE AT BLIVE PROFILERET OG DATAPORTABILITET**
Ud over retten til at blive informeret om behandlingen af personoplysninger får de registrerede med ændringerne en ret til at blive glemt. De får også ret til at få deres oplysninger udleveret, så de kan bæres videre til en anden tjenesteudbyder (dataportabilitet), og desuden har de i udgangspunktet ret til ikke at blive profileret.

NYE PLIGTER: FX KRAV TIL BESKYTTELSE OG RISIKOVURDERING
Som virksomhed eller organisation har man pligt til at beskytte personoplysninger tilstrækkeligt og herunder i et vist omfang designe beskyttelse af personoplysninger ind i de anvendte it-systemer. Disse tiltag skal baseres på en risikoanalyse eller en konsekvensanalyse. Er virksomheden selv eller antallet af behandlinger store nok, skal der udpeges en egentlig databeskyttelsesansvarlig (Data Protection Officer), som har en særlig rolle i forhold til at dokumentere persondatabehandlinger og sikkerhedstiltag samt reagere på sikkerhedshændelser og melde disse til myndigheder og eventuelle berørte registrerede. Yderligere skal de have kontrol med databehandleren. Endelig skal man være opmærksom på reglerne for overførsel af personoplysninger til lande uden for EU.

ANDRE FORHOLD: FX TV-OVERVÅGNING, ADVARSELSLISTER, SAMTALER, BØRN MV.
I relation til persondatareglerne gælder der en række særlige forhold ift. fx TV-overvågning, cookies, advarselslister (fx ikke ønskede gæster), registrering af personoplysninger om børn, man som virksomhed eller organisation skal være opmærksom på.
I tilfælde, hvor man samarbejder med eksterne partnere, fx billetudbydere, om udveksling af personoplysninger, er det desuden vigtigt at gøre sig klart, om man er dataansvarlig, databehandler eller måske begge dele.

> Læs mere om de nuværende regler, pligter og særlige forhold på Datatilsynets erhvervsside (link)

Compliance

Med de nye regler skal man som virksomhed eller organisation kunne dokumentere, at man overholder og efterlever regler og retningslinjer ift. persondataloven – en såkaldt compliance.

Vi giver derfor på de følgende sider en kort guide til, hvordan man kommer i gang med og styrker sin compliance ift. de gældende og kommende persondataregler. Guiden er blot en overordnet anbefaling som inspiration til videre arbejde.

ROLLER OG VIDEN

1. DEFINÉR ROLLER: HVEM SKAL GØRE HVAD, OG HVEM ER DATAANSVARLIG

Indledningsvis kan man med fordel udpege en overordnet ansvarlig for processen og få beskrevet opgaven i hovedtræk.

Man bør også undersøge, hvem der er og bør være den dataansvarlige. I små organisationer vil det typisk være den administrerende direktør. I lidt større organisationer er der måske en administrativ medarbejder, som kan håndtere disse forhold – men det kræver viden. I store virksomheder kan der udpeges en databeskyttelsesansvarlig og/eller flere ejere af systemerne.

2. KOMPETENCER: ER DER TILSTRÆKKELIG VIDEN?

Undersøg, om I føler jer klædt godt nok på ift. at igangsætte processen. Man behøver ikke vide alt, men omvendt er det en god idé at kende til de grundlæggende præmisser. Der er stor bevågenhed på området, så tilmeld jer et relevant kursus eller læs evt. selv op, fx på Datatilsynets erhvervsside (se link på s. 5).

KORTLÆGNING OG OPRYDNING

3. SKAB ET OVERBLIK OVER JERES PERSONDATA

Gå i gang med kortlægningen af jeres eksisterende data. Undersøg, hvilke personoplysninger I har indsamlet gennem tiden, og hvor de er placeret. Tænk på oplysninger om **kunder, medarbejdere og samarbejdspartnere** – både nuværende, tidligere og kommende.

Persondataregistreringer finder man typisk i it-systemer (fx HR-, CRM- og regnskabssystemer mv.), men også i e-mailprogrammer, på netværksdrev og hos onlinetjenester eller samarbejdspartnere. Undersøg følgende ifm. kortlægningen:

- Hvor er personoplysningerne lagret?
- Hvor stammer personoplysningerne fra?
- Hvilket formål (nødvendighed), hjemmel og følsomhed har personoplysningerne?
- Er personoplysningerne korrekte og ajourført?
- Er der fastsat udløbsdato for personoplysningerne?
- Hvem har adgang til oplysningerne, og hvem videregives de eventuelt til?

Sørg for at få dokumenteret kortlægningen undervejs, så I kan genfinde data og dokumenter hurtigt igen.

4. FÅ STYR PÅ, HVORDAN I BEHANDLER DATA
Undersøg og kortlæg herefter, hvordan I behandler jeres persondata, herunder om eller hvordan I forholder jer til de nuværende og kommende følsomhedskategorier. Målet er at få en generel fortegnelse over jeres behandlingsaktiviteter.

Behandlingen kan som tidligere angivet antage mange former, men forhåbentlig vil man kunne udlede en del af behandlingerne ud fra kortlægningen af data. Fremadrettet bør der desuden sættes ord på, hvilke behandlinger I ønsker at foretage – og hvordan. Og igen – husk at dokumentere undervejs.

5. FÅ STYR PÅ SAMTYKKEERKLÆRINGEN OG OPLYSNINGSPLIGTEN
Få derefter styr på, hvornår der skal indhentes samtykke og undersøg i forlængelse af de to kortlægninger, hvordan I får samtykke i dag, når I indhenter personoplysninger, og om de registrerede er oplyst om jeres registrering af oplysningerne?

Samtykket skal fremadrettet være utvetydigt. Sørg derfor for, at I kan dokumentere samtykket efter reglerne. Udarbejd/opdater evt. jeres samtykkeerklæring, så den matcher de nye krav og sæt gerne indhentningen af samtykke i system. Bemærk i øvrigt, at der kommer en officiel vejledning til samtykke til oktober 2017 fra justitsministeriet.

Kan I ikke dokumentere samtykket i jeres nuværende setup, så sørg for at indhente en ny godkendelse.

6. RYD OP!
Endelig kan man med fordel benytte gennemgangen af data, databehandling og samtykkeerklæringer som en anledning til at få ryddet op.

ETABLERING AF EN EGENTLIG PERSONDATAPOLITIK

Efter den indledende kortlægning og oprydning i de eksisterende persondata og -behandlinger bør man gå videre til de mere avancerede dele af persondatareglerne. Det handler typisk om virksomhedens procedurer og retningslinjer, hvor målet er at sikre, at de fornødne tekniske og organisatoriske foranstaltninger truffet.

Her bør man undersøge behovet for at udpege en egentlig dataansvarlig, udarbejde en række 'hvad-nu-hvis'-tests, blive klædt på til at indgå bedre databehandlingsaftaler og medtænke persondatabeskyttelse ifm. forretningsudvikling og udvikling af nye produkter, design og serviceydelser.

Et par spørgsmål til udviklingen af en egentlig persondatapolitik kunne være: Er der procedurer for dialog med Datatilsynet? Er der procedurer, som sikrer, at den registreredes rettigheder kan håndteres? Er der procedurer, som beskriver de nødvendige tiltag ved brud på persondatasikkerheden? Foreligger der gyldige databehandleraftaler? Dækker dokumentationen efterlevelse af persondataforordningen i hele virksomheden?

Konkret bør man forholde sig til en række scenarier og udarbejde en række relevante ***'hvad-nu-hvis-tests',*** så man fx kan håndtere datanedbrud, uretsmæssig indtrængen, eller hvis den registrerede ønsker at få oplysninger, få flyttet sine data eller helt at blive glemt.

Dansk Live sætter fokus på de nye persondataregler

EU-landene har besluttet, at persondatabeskyttelsen skal styrkes, og derfor indføres der nye regler om persondatabeskyttelse fra 2018. Reglerne betyder, at der kommer en række markante ændringer i den eksisterende persondatalovgivning i Danmark.

Da ændringerne får betydning for alle virksomheder og organisationer, vil Dansk Live og Danske Koncert- og Kulturhuse gerne bidrage til, at kendskabet til de nye regler udbredes mest muligt, så vores medlemmer også fremadrettet kan leve op til reglerne og 'god persondataskik'.

Derfor har vi udviklet denne vejledning, der giver overblik, indblik og en guide til at komme i gang med arbejdet.

12 SPØRGSMÅL TIL VIRKSOMHEDEN OM PERSONDATA

Vi har til inspiration medtaget datatilsynets 12 spørgsmål, som er udgivet i forbindelse med implementeringsarbejdet.

1. Har jeres virksomhed eller organisation tilstrækkeligt kendskab til den nye databeskyttelsesforordning?
2. Har I overblik over, hvilke personoplysninger I behandler?
3. Hvilken information giver I de registrerede?
4. Hvordan opfylder I de registreredes rettigheder?
5. Hvilke kategorier af personoplysninger behandler I, og på hvilket retsligt grundlag gør I det?
6. Hvordan indhenter, opbevarer og dokumenterer I samtykke?
7. Behandler I personoplysninger om børn?
8. Hvad gør I, hvis der sker brud på persondatasikkerheden?
9. Er jeres behandlinger af persondata forbundet med særlige risici?
10. Har I indtænkt databeskyttelse i jeres it-systemer?
11. Hvor i jeres organisation ligger ansvaret for databeskyttelsesspørgsmål?
12. Diver I virksomhed i flere lande?

Hvis I ikke mener, at I kan svare fyldestgørende på disse spørgmål, så vil der forhåbentlig være inspiration og hjælp at hente i vejledningen.

For opdateringer og yderligere information kan man desuden følge med på Dansk Lives hjemmeside www.dansklive.dk