Centex
it & netværksløsninger

Ny persondataforordning

www.centex.dk

Ny persondataforordning

Flere virksomheder betragter ikke deres persondata som et must. Det kan være at det ikke er set som et forretningskritisk område, og derfor er det ofte blevet forsømt. Den nuværende persondatalov gennemfører direktiver fra 1995, hvilket er en tid som digitaliseringen for længst har overhalet. Derfor blev en ny persondataforordning vedtaget i april 2016 som træder i kraft fra 25. maj 2018. I den forbindelse kommer nye krav, tiltag og ændringer som er gældende i hele EU.
Nye regler for håndtering af persondata kommer til at stille nye krav til virksomheder, offentlige myndigheder, forening og andre der berører personoplysninger, samt hvordan vi forholder os retten til privatliv og egne data.

Virksomheder har fået 2 år fra 2016 til at overgå til de nye krav, men da der er under 1 år tilbage, er det bestemt ikke for tidligt at påbegynde det forberedende arbejde.

Alle europæiske virksomheder som behandler data, er omfattet af den nye persondataforordning.

Hvad du kan forvente i den nye persondataforordning

- Konsekvensen for at overtræde persondata-lovgivningen bliver større og bøder kan være op til fire procent af årsomsætningen hvis reglerne overtrædes.

- Brugernes persondata har større beskyttelse og virksomheder skal have klare tilsagn fra brugerne i forhold til håndtering af persondata, i sær når det drejer sig om personfølsomme oplysninger.

- Hvis virksomheder har været udsat for hackerangreb eller anden uautoriseret adgang til persondata skal det indrapporteres til Datatilsynet indenfor 72 timer.

- De nye persondata regler bliver ens i hele EU, hvilket er en fordel hvis man som virksomhed gør forretning i andre EU lande. Man skal derfor som udgangspunkt ikke længere forholde sig til og opfylde mange forskellige persondata-lovgivninger.

- For virksomheder med over 250 ansatte skal dataansvarlige og databehandlere opbevare dokumentation for enhver behandling af personoplysninger.

Håndtering af data efter den nye persondataforordning

Oplysninger om ansatte

Nogle informationer og oplysninger er du nødt til at være i besiddelse af f.eks. i forbindelse med udbetaling af løn. Andre oplysninger, som i persondataforordningen kaldes følsomme oplysninger, kræver udtrykkeligt samtykke fra medarbejderen. F.eks. helbred, race, trosforhold, fagforening og politisk overbevisning. Enkelte følsomme oplysninger er du som virksomhed nødt til at indsamle, det kan f.eks. være registrering af fravær på grund af sygdom.

Oplysninger om tidligere ansatte

Den nye persondataforordning gør det klart, at du kun må holde personlige oplysninger om tidligere ansatte, hvis der er et klart og sagligt formål med det. Det kan f.eks. være nødvendigt at opbevare oplysninger om tidligere ansatte i forbindelse med aflønning og fritstilling.

Du kan allerede nu begynde at få styr på:

- Hvilke typer personoplysninger i indsamler
  Almindelige data, personfølsom data, CPR osv.
- Hvordan håndteres personoplysninger
  Fra de indsamles, bruges, gemmes og slettes
- Hvordan i undgår usikker omgang med data
  Filer på usikre tjenester, cd'er, usb nøgler o. lign.
- Hvem der har adgang til data og programmer
  Styring af adgang.
- Overvågning af, hvem der tilgår databaser og filer

Eksempler på persondata:

CPR-nr.	Køn	Fødselsdato	Religion
Navn	Race	Telefonnr.	Etnicitet
Adresse	Fagforening	MAC-adresse	IP-adresse
Nummerplade	Kreditoplysninger	Helbredsundersøgelses	Straffeattest
Filosofisk overbevisning	Økonomisk forhold	Politiske overbevisninger	Lønoplysninger
Nær familie	Sociale problemer	E-mailadresse	GPS-oplysninger
Personlighedstest	Seksualitet	Foto	Videoovervågning
Eksamenskarakter	Højde	Hårfarve	Tøjstørrelses
Genetik	Stilling	Medarbejder nr.	Interesser

Hvad er personfølsomme data?

Persondata er al information, der kan identificere en fysisk person. Her kan der være tale om navn, adresse, telefonnummer, cpr-nummer osv., som direkte identificerer en specifik fysisk person, men også indirekte information som f.eks. id-nummer, medlemsnummer, lokationsdata, ip adresse mm. hvor man ved sammenstilling af andre kilder kan identificere en fysisk personer. Sundhedsdata samt biometriske og genetiske data henregnes naturligvis også hertil og anses for yderst følsomme.

Helt principielt kræver behandling af data en hjemmel, så man sikrer at datasubjektet (den registrerede) er bekendt med de betingelser, der er forbundet med behandling af persondata. Hvilke data du behandler er afgørende for, hvilken hjemmel du behøver. Persondata deles op efter om det er almindelige data eller følsomme.

Almindelige data er for eksempel:
Personnavn, adresse, telefonnr, email, køn, løn, arbejdstider, kontonummer

Følsomme oplysninger er for eksempel:
Helbredsforhold, fagforening, straffeattest, racemæssig eller etnisk baggrund, personlighedstest, væsentlige sociale problemer og genetisk og biometrisk data.

Virksomheder må kun behandle en medarbejders CPR-Nummer, hvis det er et lovkrav som f.eks. indberetning til SKAT, eller hvis der er givet udtrykkeligt samtykke.

Det kan være en god idé at påbegynde analyse af hvilke personfølsomme data du opbevarer. Gennemgå systemet og lav en analyse af, hvilke data der opbevares om kunder, relationer og ansatte og få dem klassificeret i forhold til kritikalitet.

Den nye persondataforordning kommer omkring 3 parter

Datasubjekt er en identificeret eller identificerbar fysisk person som der registreres oplysninger om og som beskyttes af loven.

Dataansvarlig er den der afgør, til hvilket formål og hvilke hjælpemidler der må foretages behandling af personoplysninger.

F.eks. arbejdsgiver der behandler personoplysninger.

Databehandler er en der behandler data og oplysninger på den dataansvarliges vegne efter deres instrukser.

F.eks. en hosting udbyder.

Datasubjektet

Krav om samtykke

- Det skal være lige så let at trække et samtykke tilbage som at afgive det.
- Samtykke som behandlingsgrundlag.
    - Almindelige oplysninger: samtykke.
    - Følsomme oplysninger: udtrykkeligt samtykke.

- Indsigt i brugen af data.
- Retten til at blive glemt.
- Ret til underretning om brud på datasikkerheden.

Dataansvarlige

Krav om den dataansvarlige

- Der skal kunne dokumenteres hvilke data i ligger inde med, hvordan de opbevares og til hvilke formål.
- Skriftlig politik og procedure for hvordan persondata handles og hvorfor.
- Lovlig behandling af data og sikre at behandling af data er saglig, nødvendig og proportional.
- Er sikkerhedskravene opfyldt – både hos ansvarshavende og behandler?
- Program for anmeldelser hvis der har været hackerangreb eller anden uautoriseret adgang til persondata, hvilket skal indrapporteres til Datatilsynet indenfor 72 timer.
- Løbende kontrol og monitering.
- Aftale med databehandler om hvorledes data behandles.

Databehandler

Benytter du en databehandler som f.eks.: server- eller cloudhosting, service provider, research bureau eller lign. bør du være opmærksom på:

- Du skal have en databehandleraftale. Typisk udarbejdes denne af databehandleren.
- Du skal være enig i den aftale du laver. Rammerne er meget standarde, men du skal føle dig tryg herved.
- Det er vigtigt at du har tillid til databehandleren. Vælg derfor en samarbejder hvis kvalifikationer er dokumenteret.

Lovlig behandling af data

Oplysninger og data skal behandles lovligt, rimeligt og på en gennemsigtig måde for datasubjektet (den registrerede). Overordnet handler det om hvad der er god databehandlingsskik.

Behandling af persondata skal være formålsbestemt og kun det mest nødvendige data behandles. Lagringstiden af data skal være begrænset og relevant i perioden.

Forordningen fastslår at behandling af persondata kun er lovlig, hvis og i det omfang mindst ét af følgende forhold gør sig gældende.

- Den registrerede skal give sammentykke til behandling af data.
- Behandlingen af data er nødvendig –
  - for at opfylde en kontrakt som den registrerede er part i.
    Det kan f.eks. være en ansættelseskontrakt
  - for at overholde en retlig forpligtelse, der påhviler den dataansvarlige.
  - for at beskytte den registreredes eller en anden fysisk persons vitale interesser
  - af hensyn til udførelse af en opgave i samfundets interesse
  - for at den dataansvarlige eller tredjemand kan forfølge en legitim interesse og hensynet til den registrerede ikke overstiger denne interesse.

Den dataansvarlige har ansvaret for at kunne påvise at dette overholdes samt at kunne dokumentere at grundprincipperne også er overholdt.

Behandling af data inden- og udenfor EU

Overførsel indenfor EU: Som udgangspunkt tilladt
Overførsel udenfor EU (Tredjelande): Som udgangspunkt forbudt

Hvis der er tale om behandling og overførsel af data udenfor EU's grænser er der særskilte regler for hvordan dette behandles. Dataoverførsel kan ske til tredjeland, hvis modtager landet har et tilstrækkeligt sikkerhedsniveau overfor de overførte oplysninger og data. Overordnet kræver det en hjemmel at overføre data til et tredjeland.

Dette kan f.eks. være

- EU's standard dataoverførselsaftaler
- Binding Corporate Rules - skal godkendes af Datatilsynet og evt. andet EU tilsyn.
- Samtykke eller en af de andre undtagelser, f.eks. kontrakt- eller lovgrundlag.
- Sikre lande, såsom Israel, Argentina, Canada og Schweiz
  - Her er det ikke et krav om tilladelse fra Datatilsynet for overførsel af almindelige oplysninger, men tillades kræves ift. følsomme oplysninger.
- Nødvendigheder for at rejse juridiske krav.
- Nødvendigt for at opfylde aftaler.

Den dataansvarlige er også bødeansvarlig!

Som dataansvarlig er du ansvarlig og hæfter for databehandling. Derfor skal du have foranstaltninger, der sikrer at du er i stand til at overholde forordningen, da en af de større tiltag i den nye persondataforordning er den massive stigning i størrelsen på bødestraffen, hvis du overtræder forordningens bestemmelser.

Når de nye regler træder i kraft, vil der kunne udstedes administrative bøder på op til € 20 mio. eller 4% af virksomhedens/koncernens globale opsætning. Stigningen er meget stor i forhold til hvad der i dag gælder i Danmark hvor bøderne typisk ligger mellem Kr. 5-10.000,-.

Det er nok de færreste virksomheder der får så store bødestraffer, men det giver en indikation af, at det generelle bødeniveau vil stige markant.

Som databehandler

Centex IT & Netværksløsninger behandler store mængder data for vores mange kunder og derfor er vi karakteriseret som databehandler, derfor skal vi leve op til de forpligtelser der findes herfor. Efter den nye forordning skal vi have en databehandler aftale som skitserer hvordan vi behandler data på vegne af vores kunder, som vi har og vores nuværende såvel som nye kunder er indbefattet af.

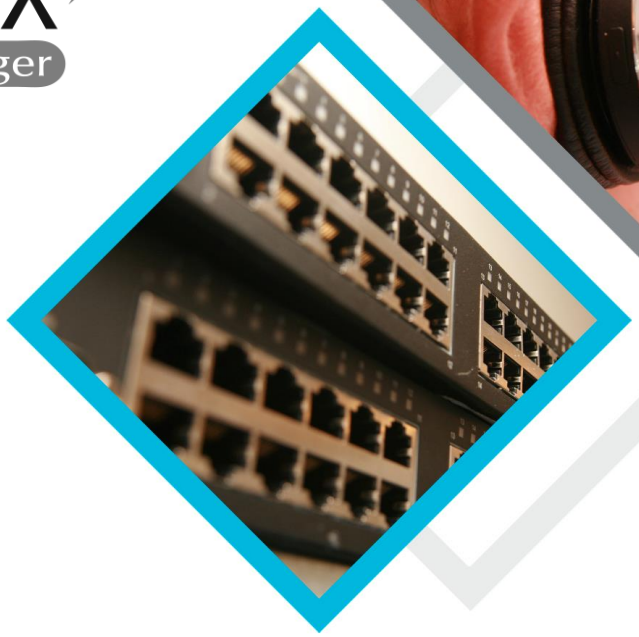
Vi er ISEA 3402 certificeret og kan derfor dokumentere ordentlige it-forhold og lever op til lovkrav herom. Vi har derfor allerede erfaring med specifikke it-forhold og lovkrav som vi udvider med den nye persondataforordning og kan rådgive jer inden for området.

Kontakt os gerne for at høre nærmere omkring den nye persondataforordning.
Vi kigger gerne forbi og tager en snak.

Vi er ISAE 3402 certificeret

Som it og hosting udbyder lever vi op til de forpligtelser der hører med til den nye persondataforordning

Vi handler ud fra lov og regler og kan dokumentere det



Centex

it & netværksløsninger