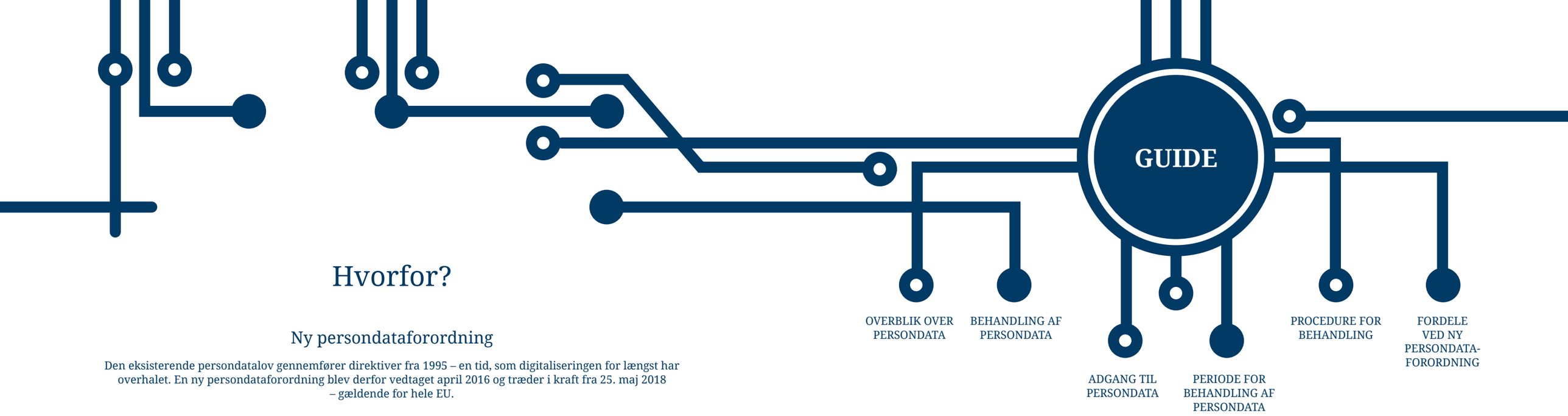

Mentor it
- med dig i fremtiden
Ny persondataforordning



Hvorfor?

Ny persondataforordning

Den eksisterende persondatalov gennemfører direktiver fra 1995 – en tid, som digitaliseringen for længst har overhalet. En ny persondataforordning blev derfor vedtaget april 2016 og træder i kraft fra 25. maj 2018 – gældende for hele EU.

Nye rammer for, hvorledes persondata behandles samt hvordan vi forholder os til retten til privatliv og egne data, er blandt andet en del heraf.

Og alle europæiske virksomheder, der behandler data, er omfattet af den nye persondataforordning.

Hvad kan du forvente fra 28.05.18

- Samme regler som nu med få tilføjelser og mere omfattende dokumentationskrav. Særligt i forhold til IT-processer
- Kontrolbesøg fra datatilsynet
- Mere ”afskrækkende” bøder, hvor bødeniveauet fremover vil være væsentligt højere end max. på kr. 25.000,- i dag

Fordele ved den nye persondataforordning

Mange beskuer den nye persondataforordning ud fra de udfordringer, den kan siges at medføre. Men den rummer også fordele, der er værd at tage med:

- Mere struktur og dokumentation på jeres IT
- Bedre overvågning af systemer
- Bedre forståelse for data og datatyper
- Større sikkerhed i forhold til kritiske aktiver
- Bedre overblik over data
- Fokus forebygger, så fejl undgås og mere tryghed opnås

Persondataforordningen kommer omkring tre parter:

Datasubjekt:
Den person, der registreres oplysninger om, og som beskyttes af loven

Dataansvarlig:
Den der afgør, til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger

Databehandler:
En der behandler data på vegne af og efter instruks fra den dataansvarlige

Datasubjektets rettigheder

1. Samtykke til brug af data
2. Letforståelig information om brugen af data
3. Indsigt i brugen af data
4. Indsigelse i forhold til brugen af data
5. Retten til at blive glemt
6. Ret til underretning om brud på datasikkerheden

Krav til den dataansvarlige

1. Dokumentation. Hvilke data ligger I inde med, hvordan opbevares de og til hvilket formål
2. Lovlig behandling. Sikre, at behandling af data er saglig, nødvendig og proportional
3. Hjemmel for behandling. Samtykke eller anden gyldig hjemmel for behandling
4. Procedure for behandling. Skriftlig politik om, hvordan persondata behandles og hvorfor
5. Sikkerhed. Er sikkerhedskravene opfyldt – både hos ansvarshavende og behandler?
6. Program for anmeldelse. Hvordan anmeldes brud senest 72 timer efter?
7. Fokus. Løbende overholdelse, kontrol og monitering
8. Databehandleraftale. Aftale med databehandler om, hvorledes data behandles

Valg af databehandler

Benytter du en databehandler, såsom: Research bureau, service provider, hosting, Cloud eller inkassobureau, bør du være opmærksom på, at:

1. Du skal have en databehandleraftale – denne udarbejder databehandleren typisk
2. Du skal være enig i aftalen – rammerne er meget standard, men du skal selvfølgelig føle dig tryg herved
3. Du skal have tillid til databehandleren – vælg en samarbejdspartner, hvis kvalifikationer er dokumenteret. For eksempel ved certificeringer

Hvad er lovlig behandling af data?

Lovlig behandling af data hører blandt andet ind under, hvad der er god databehandlingsskik. Herunder at behandling af persondata er saglig og formålsbestemt. At kun mest nødvendige data behandles *(dataminimering)*, at disse data er ajour *(korrekte data)* samt at lagringstiden er begrænset, og at der er høj integritet og fortrolighed forbundet hermed *(sikkerhed)*.

- Og det er den dataansvarliges ansvar at kunne påvise, at dette overholdes!

467949

Persondata er oplysninger, der kan være med til at identificere en given person

Eksempler på persondata:

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

Hav styr på dit hjemmelsgrundlag

Helt principlet kræver behandling af data en hjemmel, således man sikrer, at datasubjektet er bekendt med de betingelser, der er forbundet med behandling af persondata. Om end det er almindelige eller følsomme data, der er tale om.

Almindelige data er for eksempel:
Navn, e-mail, adresse, køn, alder, A-kasse medlemskab, bankkonto og lønoplysninger.

Følsomme data er for eksempel:
Race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforening, helbredsmæssige og seksuelle forhold samt genetisk og biometrisk data.

- CPR nr. er særskilt regulering.

Hvilke data du behandler er afgørende for, hvilken hjemmel du behøver.

Almindelige data kan behandles ved samtykke, lovkrav, nødvendighed ved retskrav, for at indgå eller opfylde aftale med datasubjekt eller interesseafvejningsreglen.

Følsomme data kan behandles ved samtykke, lovkrav eller nødvendighed ved retskrav.

173 SYS. mmHg
86 DIA. mmHg
51 PUL. /min.

Behandling af data inden og udenfor EU

Der er særskilte regler for, hvorledes data skal behandles i forhold til om det er inden- eller udenfor EU's grænser. Helt overordnet kræver det en hjemmel at overfører data til et tredjeland.

Dette kan for eksempel være:

1. Sikre lande eller brancher, f.eks. Island, Israel, Norge, Schweiz
2. Koncernregler (Binding Corporate Rules)
3. EU's standard dataoverførselsaftaler
4. Overførsel til certificerede virksomheder i USA
5. Datasubjektets samtykke
6. Nødvendigt for at rejse juridisk krav
7. Nødvendigt for at opfylde en aftale
8. Overførsel efter "interesse-afvejning" og anmeldelse til
9. Datatilsyn, men reglen er begrænset og omfatter ikke jævnlig eller større overførsler

Hovedregel:

Det er den dataansvarlige, der er bødeansvarlig!

Som dataansvarlig er du ansvarlig og hæfter for databehandlingen, hvorfor du skal have foranstaltninger, der sikrer, at du er i stand til at overholde forordningen.

Allerede nu kan du begynde at få styr på:

- Identifikation af, hvilke data i har (Fra de indsamles, bruges, gemmes og slettes)
- Hvordan I undgår usikker omgang med data (Filer på diske og brug af USB-stik)
- Hvem der har adgang til programmer og data (Adgangsstyring)
- Hvorledes I sikrer data i databaser
- Overvågning af, hvem der tilgår databaser og filer

Dataansvarlighed

Hvad gør vi – som databehandler?

Mentor IT er hosting leverandør og vi behandler derfor store mængder data for flere kunder. Dette karakteriserer os som databehandler, og vi skal derfor leve op til de forpligtelser, der findes herfor.

For os er gældende, at vi skal have en databehandleraftale, der skitserer, hvorledes vi behandler data på vegne af vores kunder. Hvilket vi allerede har. Og som alle vor kunder er indbefattet af. Nye såvel som eksisterende.

- Fordi vi ved, at den nye persondataforordning fylder meget, tilbyder vi vor kunder, at vi sammen med en ekspert kan komme forbi og fortælle mere herom. Blot for at sikre et højt informationsniveau.

Kontakt os gerne og hør mere herom.

Persondata og cybersikkerhed

Behandling af data og sikkerheden herved vedrører i høj grad jeres IT-sikkerhed. Hvor let eller besværligt det er for IT-kriminelle at komme i nærheden af jeres personfølsomme oplysninger, samt hvilke sikkerheds-foranstaltninger I har – eller måske bør have?

Hos Mentor IT tilbyder vi kursus i brugersikkerhed samt et gratis sikker-hedstjek af jeres IT-løsning.

Kontakt os på 70 122 124 og hør mere.

Kilder:
Materialet er udarbejdet af Mentor IT med inspiration fra Ernst & Young, Deloitte og Delacour.