Databeskyttelse

Kort resume af e-læringskurset om Databeskyttelsesforordningen (GDPR). Resuméet har samme formål som kurset: At øge bevidstheden om, hvordan man mest hensigtsmæssigt og forsvarligt behandler persondata.

Indhold

1) Hvad er personoplysninger

Personoplysninger er alle de informationer der kan henføre til en person - både direkte og indirekte.

Hvilke typer af personoplysninger er der?

Der findes 2 kategorier af personoplysninger

- **Almindelige personoplysninger**
  - Alle oplysninger som ikke er følsom
    (Navn, adresse, telefonnummer, e-mail, fødselsdato, nationalitet, civilstand eller køn)

- **Følsomme personoplysninger**
  - Er nævnt i databeskyttelsesforordningen
  - Race og etnisk oprindelse
  - Politisk, religiøs og filosofisk overbevisning
  - Fagforeningsmæssigt tilhørsforhold
  - Genetiske oplysninger
  - Biometriske oplysninger
  - Helbredsoplysninger
  - Seksuelle forhold og seksuel orientering

Ustrukturerede personoplysninger

Ustrukturerede personoplysninger opbevares ikke i systemer, der strukturerer dem. Som medarbejder påligger det eget ansvar at sikkerstille den sikre behandling af oplysningerne

Eksempel:

- To-do lister
- E-mails i mailboks
- Data på delte netværksdrev
- Filer med personoplysninger gemt på egen PC

For at undgår ustrukturerede personoplysninger skal der:

- Identificeres, organiseres, følges op og slettes
- Organiseres i mapper
- Beskyttes med adgangskode
- Begrænses adgang
- Rydes op

2) Hvad er behandling af personoplysninger?

Behandlingen kan være meget - set i bred forstand. Bruges data privat, er de ikke omfattet af databeskyttelsesforordningen. Der er tale om behandling når data:

- Indsamles
- Registreres
- Systematiseres
- Opbevares
- Tilpasses
- Ændres
- Selekteres
- Søges
- Videregives
- Formidles
- Overlades
- Sammenstilles
- Samkøres
- Blokeres
- Slettes
- Tilintetgøres

Hver gang man behandler data, skal det ske i overensstemmelse med databeskyttelsesforordningen.

3) Krav til god databehandlingsskik

Når personoplysninger behandles, skal det ske i overensstemmelse med god databehandlingsskik og de grundlæggende behandlingsprincipper - men hvad betyder det?

- Passe godt på persondata
- Opføre dig ordentlig med de informationer du har ansvar for
- Kun behandle dem hvis (retningslinjer):
    - Det har et udtrykkeligt og legitimt formål (det skal være rimelig præcis, hvad oplysningerne skal bruges til)
    - Ikke indsamle flere personoplysninger end hvad der er nødvendigt til formålet
    - Du må ikke anvende personoplysningerne til andre formål end hvad de oprindeligt er indsamlet til

Behandlingsprincipper

Følgende behandlingspricipper skal overholdes:

- Lovlighed, rimelighed og gennemsigtighed
- Formålsbegrænsning
- Dataminimering
- Rigtighed (oplysningerne skal være rigtige og ajourførte)
- Opbevaringsbegrænsning
- Integritet og fortrolighed (oplysningerne skal være beskyttet mod uautoriseret eller ulovlig behandling).

4) Hvornår må der behandles personoplysninger?

Personoplysninger må behandles, hvis der er et legitimt og udtrykkeligt formål med behandlingen.

Kan der svares med ja på efterfølgende spørgsmål må personoplysningerne behandles:

1. Er der tale om personoplysning?
2. Er der tale om en behandling?
3. Er der et retligt grundlag for behandlingen?
4. Er der et udtrykkeligt og legitimt formål med behandlingen?

Ofte skal der gives samtykke til behandling af personoplysninger. Husk at:

- Samtykke kan trækkes tilbage
- Samtykke skal være dokumenteret
- Der må ikke behandles personoplysninger, hvis samtykke er trukket tilbage
- For at et samtykke er gyldigt skal det være frivilligt, specifikt, informeret og utvetydigt samtykke

5) Den registreredes rettigheder

Oplysningspligt

Indsamles, registreres og behandles oplysninger, skal den registrerede oplyses herom. Formålet et, at den registrerede ved hvad oplysningerne bruges til. Dette gælder såvel, hvis man indsamler oplysningerne direkte fra den registrerede eller hos andre (fx arbejdsgiveren).

Der skal oplyses:

- Hvem er dataansvarlig
- Formålet med behandlingen samt retligt grundlag
- Hvilke kategorier af personoplysninger der indsamles
- Hvem modtager oplysningerne
- Overføres oplysningerne til modtagere uden for EU/EØS samt retligt grundlag
- Tidsperiode for opbevaringen
- Hvilke rettigheder den registrerede har
- At der er ret til at tilbagekalde samtykke - hvis indsamlingen baserer på samtykke
- Kilden til de indsamlede personoplysninger
- Klagemulighed til Datatilsynet
- Foretages automatiseret behandling af personoplysningerne (fx profilering)

Oplysningspligten gælder ikke:

- Hvis den registrerede allerede, har kendskab til behandlingen af data
    - Behandlingen sker ifølge samme formål
    - Den registrerede kender til oplysningerne

Retten til indsigt

Den registrerede har ret til indsigt i de oplysninger, der er registeret om vedkommende. Der skal hertil anmodes om indsigt (formløs).

Retten til berigtigelse

Er der fejl i oplysningerne eller ufuldstændig, har den registrerede ret til ændring hvis det er vigtigt til formålet med behandlingen.

Retten til at blive glemt

Som udgangspunkt har den registrerede ret til at få slettet sine personoplysninger. Der skal dog være opfyldt nogle betingelser inden data kan blive slettet.

- Hvis oplysningerne ikke længere er nødvendigt til at opfylde formålet med behandlingen
- Hvis den registrerede tilbagekalder samtykke
- Hvis behandlingen er ulovligt
- Hvis sletningen er lovpligtigt

Oplysningerne skal slettes hurtigst muligt uden unødvendige forsinkelse. Er oplysningerne videregivet til andre, skal de også slettes der.

Man har ikke ret til at få oplysningerne slettet hvis:

- Hvis oplysningerne bruges til at kunne opfylde en aftale eller kontrakt
- Hvis oplysningerne skal gemmes ifølge loven

Retten til indsigelse

Den registrerede har ret til indsigelse mod behandlingen af oplysningerne.

- Behandlingen er i strid med dataforordningen

Retten til dataportabilitet

Den registrerede skal have kontrol over egne oplysninger. Borgeren har ret til at få oplyst de gemte personoplysninger og ret til at de elektroniske oplysningerne overføres til en anden kommune. Herved skal følgende krav være opfyldt:

- Oplysningerne har den registrerede selv givet til kommunen
- Oplysningerne behandles på baggrund af samtykke / kontrakt
- Behandlingen af personoplysningerne sker maskinelt

Retten til ikke at være genstand for en automatisk afgørelse

Det er almindeligt, at personoplysninger behandles automatiseret.

Hvis en automatisk afgørelse har retsvirkning for den registrerede, eller betydeligt påvirker den registrerede, har den registrerede ret til ikke at blive underlagt en sådan afgørelse. Så har den registrerede ret til at gøre indsigelse mod behandlingen. Efter indsigelsen skal den automatiske behandling (profilering) stoppes og den skal fortsættes manuelt.

Undtagelse:

- Hvis den automatiske behandling er nødvendig for at opfylde en kontrakt mellem kommunen og den registrerede
- Hvis der i loven står at kommunen må foretage en automatiserede behandling
- Hvis den automatiserede behandling baserer på samtykke fra den registrerede

6) Videregivelse af personoplysninger

Hvornår må der videregives personoplysninger?

Når man behandler personoplysninger, kan der opstå situationer, hvor man har brug for at videregive oplysningerne. En videregivelse er også en behandling af personoplysninger, og derfor skal man have det retlige grundlag for at gøre det.

Der er tale om videregivelse af personoplysninger når de gøres tilgængelige for andre - fx myndigheder eller virksomheder uden for kommunen.

Inden personoplysningerne videregives:

- Skal der være et retlig grundlag
- Grundlæggende behandlingspricipper skal være overholdt

Under videregivelsen skal der passes på at informationerne ikke falder i de forkerte hænder. E-mails med personfølsomme data skal altid sendes krypteret, eller sendes til e-boks.

Inden videregivelsen skal der foretages en vurdering

1. Er der samtykke eller andet retlig grundlag for videregivelsen af personoplysningerne?
2. Er de grundlæggende behandlingspricipper overholdt?

7) Dataansvarlig og databehandler

Når der behandles personoplysninger, er det vigtigt, at man kender til hvem der er dataansvarligt, og hvem der er databehandler. Til begge roller er der knyttet en række forpligtelser. Når en databehandler, skal behandle personoplysninger på vegne af en dataansvarlig, skal der udarbejdes en databehandleraftale.

Hvem er dataansvarlig og databehandler?

Dataansvarlig kan være:

- Enkeltpersoner
- Juridiske personer
- Virksomheder
- Offentlige myndigheder
- Andre organer

Den dataansvarlige har ansvar for:

- Hvordan personoplysningerne kan behandles
- Til hvilket formål
- Med hvilke hjælpemidler

Databehandler kan være:

- Enkeltpersoner
- Juridiske personer
- Virksomheder
- Offentlige myndigheder
- Andre organer

En databehandler indsamler og behandler data på vegne af en dataansvarlig. En databehandler **må ikke:**

- Bestemme hvad oplysningerne skal bruges til
- Bruge oplysningerne til egne formål

Eksempel:

1. Når en kommune bruger Microsofts cloudløsning og opbevarer oplysninger og dokumenter indeholdende personoplysninger i ”skyen”, er Microsoft databehandler for kommunen.

2. Når en kommune køber software og support hos en licensgiver, og supportmedarbejderne hos licensgiveren lejlighedsvis får adgang til kommunens IT-systemer for at kunne fejlfinde mv., vil licensgiveren være databehandlere for kommunen.

Databehandleraftale

Når en dataansvarlig anmoder en, databehandler om at behandle data, skal der udarbejdes en skriftlig databehandleraftale inden data behandles.

Indgår kommunen en aftale med en leverandør, der skal behandle data, skal der indgås en databehandleraftale.

8) Overførsel af personoplysninger til tredjelande

Hvad er overførelse til tredjelande?

Reglerne for behandling af personoplysninger er ens indenfor EU, og derfor er der samme ret til at overføre personoplysninger imellem EU-landene, som inden for Danmark. Men der gælder særlige regler, hvis oplysningerne skal overføres til et tredjeland.

Hvad er et tredjeland?

Et tredjeland er et land uden for EU. Lande inden for EU er ikke tredjelande.

Sikre tredjelande har et tilstrækkeligt beskyttelsesniveau (fx New Zealand)

- Kræver ikke særlig tilladelse / godkendelse
- Kræver en databehandleraftale

Usikre tredjelande har ikke et tilstrækkeligt beskyttelsesniveau (fx Indien)

- Kræver særlig tilladelse / godkendelse

9) Databeskyttelse gennem design og standardindstillinger

Hvad er beskyttelse gennem design og standardindstillinger?

Databeskyttelse gennem design og standardindstillinger kan aktivt medvirke til, at databeskyttelse bliver en del af arbejdspladen og noget, der tænkes ind i alle handlinger, processer og IT-systemer.

Privacy by Design and Default

To principper der overlapper hinanden

Databeskyttelse gennem design skal medvirke til at alle fremtidige processer, der behandler personoplysninger, tager højde for persondatabeskyttelse gennem design.

Nye IT-systemer skal leve op til dette princip. Systemer der allerede er i brug, skal ikke redesignes.

Databeskyttelse gennem standardindstillinger henviser til, at de indstillinger der bedst sikrer den registrerede skal være indstillet som standard i systemer og være hovedregler i processer medmindre den registrerede aktiv fravælger denne beskyttelse.

Standardindstillingerne sikrer, at der kun indsamles, behandles og gemmes personoplysninger som er nødvendigt for det specifikke formål.

Der er ikke et krav, at standardindstillingerne ændres i eksisterende systemer, hvor de ikke kan ændres. Men de skal ændres, hvis det er muligt

10) Sikkerhed

Behandling af personoplysninger skal ske med sikkerhedsmæssigt fuld forsvarlighed. Borgere og medarbejdere skal have tillid til at deres oplysninger ikke kommer i de forkerte hænder og at de ikke misbruges.

Hvilke krav stilles der til sikkerhed?

Databeskyttelsesforordningen indeholder ikke nogen specifikke krav til, hvordan sikkerheden skal være i forbindelse med behandling af personoplysninger. Dels fordi det ikke er muligt, dels fordi sikkerhedsteknologien hele tiden udvikles.

Derfor er kravet til sikkerhed ret bredt: At både den dataansvarlige og databehandleren skal sikre, at der **træffes de fornødne fysiske, tekniske og organisatoriske sikkerhedsforanstaltninger**, så det sikres, at oplysningerne ikke ved uheld eller ulovligt tilintetgøres, fortabes eller videregives.

Om sikkerhedsniveauet er passende eller ej, kræver en **konkret vurdering** ud fra følsomheden af de personoplysninger, der behandles og den konkrete risiko for den registrerede. Risiko forstås som sandsynligheden for, at der sker et brud på persondatasikkerheden og konsekvensen for den registrerede, hvis det sker.

Fysisk, organisatorisk og teknisk sikkerhed

- Fysiske sikkerhed sikrer personoplysninger fysisk (fx brandsikre skabe)
- Organisatorisk sikkerhed betyder, at organisationen behandler personoplysninger i overensstemmelse med databeskyttelsesforordningen og egen informationssikkerhedspolitik. (fx undervisning)
- Tekniske sikkerhed betyder, at IT-systemer og processer skal sikres (fx antivirus program)

Brud på persondatasikkerheden

Der er tale om et brud i persondatasikkerheden hvis bruddet fører til en:

- Hændelig eller ulovlig tilintetgørelse
- Tab
- Ændring
- Ubeføjet videregivelse
- Adgang til personoplysninger
    - Der sendes (fysisk eller elektronisk)
    - På anden måde behandles (fysisk eller elektronisk)

I tilfælde af et brud på persondatasikkerheden

Hvis der opstår et brud på persondatasikkerheden, har den dataansvarlige som udgangspunkt pligt til at melde det til Datatilsynet. Sikkerhedsbruddet skal anmeldes hurtigst muligt og senest 72 timer efter, at sikkerhedsbruddet er blevet opdaget. Derudover skal de berørte personer underrettes.

Ved anmeldelse af et brud på persondatasikkerheden, skal den dataansvarlige **som minimum:**

- beskrive karakteren af bruddet på persondatasikkerheden
- angive navn og kontaktoplysninger på databeskyttelsesrådgiveren
- beskrive de sandsynlige konsekvenser, som bruddet medfører
- beskrive de foranstaltninger, som den dataansvarlige vil implementere for at håndtere sikkerhedsbruddet.