SikkerhedsBranchen

Processen med opfyldelse af persondataforordningen

Version 8 05022018
KSM

Her følger SikkerhedsBranchens oplæg til hvordan implementeringen af Persondataforordningen gribes an.

Hvad er behandling af personoplysninger (persondatabehandling)?

Persondatabehandling er ifølge artikel 4 aktiviteter, hvor personoplysninger indsamles, registreres, organiseres, systematiseres, opbevares, tilpasses eller ændres, genfindes, søges, bruges, videregives, transmitteres, overlades, sammenstilles eller sammenkøres, begrænses, slettes eller tilintetgøres. Kort sagt alt hvad man kan gøre med personoplysninger.

Personoplysninger er enhver form for information om en identificeret eller identificerbar fysisk person. Det kan være navn, cpr-nummer, lokaliseringsdata, onlineidentifikation, eller personens fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet. Kort sagt alt hvad der gør os i stand til at identificere en person.

Dokumentation er et meget vigtigt element i GDPR. Alt skal dokumenteres. De vigtigste dokumentationskrav er nævnt i processerne herunder.

Grundprincipper (artikel 5)
Lovlighed, rimelighed og gennemsigtighed
Formålsbegrænsning
Dataminimering
Rigtighed
Opbevaringsbegrænsning
Integritet og fortrolighed
Ansvarlighed

Ansvar (artikel 24)
Under hensyntagen til den pågældende behandlings: karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandlingen er i overensstemmelse med denne forordning.

Kortlægning af omfanget af persondatabehandling

1. Kortlægning af persondata
   1.1. Hvilke typer persondata behandler du? Kundedata, medarbejdere, TVO etc.
   1.2. Artikel 30 fortegnelser:
   Den dataansvarlige skal føre fortegnelser over alle persondatabehandlingsaktiviteter – altså typer af aktiviteter medmindre behandlingen er lejlighedsvis.
   1.3. Fortegnelserne skal indeholde: Kontaktoplysninger på den dataansvarlige, formål med behandlingen, kategorier af registrerede, Kategorier af personoplysninger, hvem der modtager oplysningerne, eventuelle slettefrister m.v.
   1.4. Databehandlere skal føre lignende lister se artikel 30 stk. 2

2. Hvilken rolle har du i persondatabehandlingen?
   2.1. Er du dataansvarlig, databehandler, eller ingen af delene i forhold til de enkelte behandlinger og persondatatyper?

3. Anvendte it-løsninger
   3.1. Hvilke it-systemer bruger du ved behandlingen af persondata?
   3.2. Er der indbygget privacy by default eller design?
   3.3. Sikrer systemet, at personoplysninger ikke mistes, ikke er forkerte og ikke kommer til uvedkommendes kendskab?
   3.4. Det skal dokumenteres, at behandlingssikkerheden er i orden. Kravene er beskrevet i artikel 32
   3.5. Konsekvensanalyse vedrørende databeskyttelse skal dokumenteres. Hvis en behandling indebærer brug af nye teknologier eller i kraft af sin karakter, sit omfang, sammenhæng og formål indebærer en høj risiko for personers rettigheder, skal der udføres en analyse af behandlingens konsekvenser for beskyttelsen af personoplysninger. Det drejer sig først og fremmest om:
      3.5.1. Automatisk foretaget omfattende, systematisk vurdering af personlige forhold (f.eks. profilering, kreditvurderinger m.v.)
      3.5.2. Behandling af store mængder oplysninger vedrørende lovovertrædelser og domme
   3.6. Systematisk overvågning af offentligt tilgængeligt område i stort omfang. Det vurderes at de sidste to punkter, særligt det sidste, har betydning for sikkerhedsbranchen, særligt TVO (se dog nedenfor om databehandlere).

Organisation

4. Databeskyttelsespolitik
   4.1. Beskriv jeres overordnede databeskyttelsespolitik,
   4.2. at det er vigtigt for jer at beskytte de registreredes rettigheder,
   4.3. Hvordan arbejdet er organiseret og forankret, hvem der er ansvarlige for hvad
   4.4. Hvad medarbejderne må gøre i forbindelse med behandling af personoplysninger og hvem der skal henvises til i tvivlstilfælde (overordnede/ressourcepersoner m.v.)

4.5. Medarbejdere der behandler personoplysninger skal instrueres om hvordan vedkommende skal forholde sig til alle ovennævnte punkter. En lang række af dem vil medarbejderen ikke skulle tage stilling til, men henvende sig til den eller de ressourcepersoner/DPO (artikel 37 – 39) virksomheden har udpeget. Hele den ansvarsfordeling skal være beskrevet i virksomhedens databeskyttelsespolitik
4.6. Medarbejderne, der behandler personoplysninger, skal underskrive en tavshedserklæring
4.7. Der bør gennemføres jævnlige opdateringer af disse medarbejdere og såkaldte awareness aktiviteter, der sikrer at medarbejderne har fokus på persondatasikkerheden.

Formål og lovlighed

5. Formål og lovlighed (artikel 5 og 6)
   5.1. Du skal beskrive hvordan du sikrer, at personoplysninger kun bruges til udtrykkeligt angivne lovlige formål,
   5.2. at de er tilstrækkelige og relevante, korrekte og ajourførte,
   5.3. at de er begrænset til det nødvendige,
   5.4. at personoplysninger ikke opbevares længere end nødvendigt - sletterutiner skal være på plads
   5.5. at behandlingen af personoplysninger skal være proportional

Samtykke

6. Samtykke
   6.1. Behandling af en lang række personoplysninger kan kun ske efter samtykke. Det samtykke skal du som dataansvarlig kunne dokumentere i hvert tilfælde
   6.2. Samtykket skal gives frivilligt, specifikt og informeret i et letforståeligt sprog
   6.3. Hvis samtykket er en del af en (ansættelses)kontrakt eller andet større dokument skal samtykket til behandling af personoplysninger klart kunne skelnes fra de andre forhold i dokumentet
   6.4. Samtykker (se ovenfor) skal kunne dokumenteres

Registreredes rettigheder

7. Registreredes rettigheder
   7.1. Det skal dokumenteres at du overholder alle den registreredes rettigheder eller hvordan du har tænkt dig at gøre det. Det drejer sig først og fremmest om:
      7.1.1. Oplysningspligt overfor den registrerede (artikel 13 og 14)
      7.1.2. Indsigtsret. Den registrerede har ret til information om og adgang til de personoplysninger du har om vedkommende (artikel 15)
   7.2. Den registrerede har ret til berigtigelse af personoplysninger (artikel 16)
   7.3. Den registrerede har ret til at få personoplysningerne slettet (artikel 17)
   7.4. Den registrerede har ret til at få begrænset behandlingen af personoplysningerne (artikel 18)

7.5. Medmindre det er uforholdsmæssigt vanskeligt, skal alle modtagere som oplysningerne er videregivet til have underretning, når der ændres i data som nævnt ovenfor i artikel 16 – 18. (artikel 19)
7.6. Dataportabilitet. Den registrerede har ret til at få udleveret personoplysninger om sig selv (artikel 20)
7.7. Indsigelse. Den registrerede kan altid gøre indsigelse mod behandling af vedkommendes personoplysninger jf. artikel 12 – 22
7.8. Profilering. Den registrerede har ret til at modsætte sig at være genstand for automatiske individuelle afgørelser, herunder profilering.

Brud på datasikkerheden

8. Brud på datasikkerheden
   8.1. Man skal have dokumenterede procedurer for håndtering af brud på persondatasikkerheden, der indebærer en risiko for personers (friheds)rettigheder. Man skal:
      8.1.1. Underrette Datatilsynet indenfor 72 timer (artikel 33)
      8.1.2. Underrette den eller de registrerede, hvis der er en høj risiko for disses (friheds)rettigheder (artikel 34

Databehandlere

1. Hvis man benytter sig af en underleverandør til behandling af personoplysninger skal man:
   1.1. Have en skriftlig aftale med databehandleren (se eksempel på en databehandleraftale udarbejdet af SikkerhedsBranchen)
   1.2. Sikre sig at vedkommende kan stille garantier for tekniske og organisatoriske rammer der sikrer beskyttelsen af den registreredes rettigheder
   1.3. Skrive en instruks (skal også stå overordnet i aftalen) til databehandleren, der beskriver genstanden for behandling, behandlingens karakter, varighed, formål, typen af personoplysninger, kategorierne af registrerede (se eksempel på instruks i databehandleraftalen udarbejdet af SikkerhedsBranchen)
2. Hvis man er databehandler skal man:
   2.1. Hjælpe kunden med at overholde kravene til databehandleraftale og instruks jf. artikel 28
   2.2. Udelukkende behandle personoplysninger i overensstemmelse med databehandleraftalen og instruksen.
   2.3. Hjælpe den dataansvarlige med at opfylde sine forpligtelser overfor den registrerede og overfor Datatilsynet, politiet og andre myndigheder.
   2.4. Hvis man som databehandler benytter underleverandører til behandling af personoplysninger, må det kun ske efter skriftlig godkendelse fra den dataansvarlige
   2.5. Fortegnelse efter artikel 30 stk. 2. Databehandleren skal føre en fortegnelse over behandling af personoplysninger, der foretages for den dataansvarlige.

3. Hvornår er man databehandler?
   3.1. Det er man som udgangspunkt, når man har en aftale med den dataansvarlige om at behandle personoplysninger.
   3.2. Hvis aftalen går ud på noget andet, f.eks. en ydelse som reparation, service og vedligeholdelse på AIA-, ADK- eller TVO-anlæg, hvor man nok kan komme til at se og dermed behandle personoplysninger, men det slet ikke er det aftalen går ud på, er man ikke databehandler (og ej heller dataansvarlig). Kunden (den dataansvarlige) skal således ikke have en databehandleraftale, men kan nøjes med en passus i aftalen om, at medarbejdere hos den udførende virksomhed har tavshedspligt. Dette følger af Datatilsynets og justitsministeriets vejledning om dataansvarlige og databehandlere punkt 3.
   3.3. For så vidt angår de banale personoplysninger man kommer til at behandle som installatør eller KC, f.eks. om kontaktpersoner hos kunden, er det ikke nok til at man bliver databehandler. På samme måde er behandling af alarmsignaler o.l. ikke omfattet af reglerne.