Vandforsyningens håndtering af den kommende persondataforordning

Danske Vandværker

Praktiske spørgsmål vi modtog

- Hvem har ansvaret for beskyttelse af forbrugernes persondata?
- Er medlemslister i ringbindsmapper også persondata som skal beskyttes?
- Hvilke persondata må vandforsyningen være i besiddelse af?
- Hvordan skal de beskyttes?
- Hvordan kan persondata og overholdelse af den kommende lovgivning bedst håndteres af vandforsyningens personale, og eksterne samarbejdspartnere?

Spørgsmål 1

- Hvem har ansvaret for beskyttelse af forbrugernes persondata?

Dataansvarlig

- *»dataansvarlig«: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre* ***afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger****; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret.*

Spørgsmål 2

- Er medlemslister i ringbindsmapper også persondata som skal beskyttes?

Hvad er en personoplysning?

- *»personoplysninger«: **enhver form for information om** en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar fysisk person forstås **en fysisk person**, **der direkte eller indirekte kan identificeres**, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.*

Hvornår er en personoplysning følsom?

- Race eller etnisk oprindelse
- Politisk, religiøs eller filosofisk overbevisning
- Fagforeningsmæssigt tilhørsforhold
- Genetiske eller biometriske data med det formål entydigt at identificere en fysisk person
- Helbredsoplysninger
- Seksuelle forhold eller seksuelle orientering
- *(Samt straffedomme og lovovertrædelser, der kun må behandles under kontrol af en offentlig myndighed / hjemlet ved lov)*
- Særregler for CPR nummer (vedtages ved national lovgivning jfr. artikel 87)

Hvad betyder persondataforordningen for mig? (privatperson)

Langt strammere håndhævelse af rettighederne og nye rettigheder

- Oplysningspligt (”hvad gør I med mine data og hvorfor?”)
- Ret til berigtigelse (”det der står er forkert”)
- Ret til at blive glemt (”slet mig” – også fra backup!)
- Ret til begrænsning af behandling (”stop!”)
- Ret til dataportabilitet (”jeg flytter, hjælp mig”)
- Ret til indsigelse (”det er ikke ok, det I gør”)

Inden spørgsmål 3

De grundlæggende krav

Grundlæggende krav til lovlig behandling

Krav om dokumentation for at man lever op til forordningens krav.

- Lovlig, rimelig og gennemsigtig behandling af personoplysninger
- Udtrykkelige formål for behandlingen
- Dataminimering ift. nødvendighed
- Ajourførte data (”ethvert rimeligt skridt”) ift. behandlingens formål
- Anonymiseres / slettes når data ikke længere er nødvendige
- Sikres tilstrækkeligt (både mod lækage, sletning og beskadigelse)
  Både teknisk og organisatorisk.
- Ansvarlighed – påvise at ovenstående overholdes

Spørgsmål 3

- Hvilke persondata må vandforsyningen være i besiddelse af?

Hjemmel for behandlingen

Hvornår må man behandle **almindelige** personoplysninger?

- **Samtykke** – skal kunne trækkes tilbage, så let som det gives!
- **Nødvendig pga. aftale** med den registrerede (eller af hensyn til samme)
- **Retlig forpligtelse** (*lovgivning*)
- Beskyttelse af vitale interesser
- **Nødvendig for samfundets interesse** (*lovgivning*)
- **Forfølgelse af en legitim interesse** – med mindre den registreredes interesser/rettigheder går forud herfor

Hjemmel for behandlingen

Hvornår må man behandle **særlige (”følsomme”)** personoplysninger?

- **Udtrykkeligt samtykke** til et eller flere specifikke formål – skal kunne trækkes tilbage, så let som det gives!
- Arbejds-, sundheds- og socialretlige forpligtelser og specifikke rettigheder (*lovgivning*)
- Beskyttelse af vitale interesser i tilfælde, hvor den registrerede fysisk eller juridisk ikke er i stand til at give samtykke
- Behandling foretages af en stiftelse, en sammenslutning eller et andet organ, som ikke arbejder med gevinst for øje, og hvis sigte er af politisk, filosofisk, religiøs eller fagforeningsmæssig art, som led i organets legitime aktiviteter og med de fornødne garantier, og på betingelse af at behandlingen alene vedrører organets medlemmer, tidligere medlemmer eller personer, der på grund af organets formål er i regelmæssig kontakt hermed, og at personoplysningerne ikke videregives uden for organet uden den registreredes samtykke.
- Personoplysninger, som tydeligvis er offentliggjort af den registrerede.
- Nødvendig, for at retskrav kan fastlægges, gøres gældende eller forsvares.
- **Nødvendig for væsentlige samfundsinteresser (*lovgivning*)**
- Nødvendig i forbindelse med medicinsk diagnose, behandling eller sundhedsomsorg (*lovgivning*)
- Nødvendig for samfundsinteresser på folkesundhedsområdet (*lovgivning*)
- Nødvendig til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1 (*lovgivning*)

Spørgsmål 4

- Hvordan skal de beskyttes?

Hvilke sikkerhedskrav vil man forventeligt have til et vandværks behandling af personoplysninger?

- *”sikrer tilstrækkelig sikkerhed”* mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

- Risikovurdering (overvej brug af konsekvensanalyse/DPIA)

- I praksis betyder ovenstående at man skal vurdere hver behandlingsaktivitet og sikre den til det niveau man mener er tilstrækkeligt – og dokumentere hvorfor og hvordan man gør det.

Normal forventelig sikkerhed

- Uddannelse af personale
- Styr på adgangsrettigheder (både mennesker og IT systemer)
  Så få personer som muligt må have adgang til personoplysninger
- I papirform er styring af adgangsrettigheder = lås
- Logning af forgæves adgangsforsøg og blokering af adgang ved flere forsøg
- Kryptér persondata når det er muligt (både ved overførsel og lagring)
- Backup
- Opdater software
- Firewall og antivirus/antimalware
- Procedure for sletning/makulering

Spørgsmål 5

- Hvordan kan persondata og overholdelse af den kommende lovgivning bedst håndteres af vandforsyningens personale, og eksterne samarbejdspartnere?

Brug af databehandlere

Hvornår er en underleverandør databehandler?

- »databehandler«: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der **behandler personoplysninger på den dataansvarliges vegne.**

Når man vælger underleverandører

Den dataansvarlige har pligt til at:

- *udelukkende at benytte databehandlere, der [...] gennemføre de passende tekniske og organisatoriske foranstaltninger […] opfylder kravene […] beskyttelse af den registreredes rettigheder.*
- *Databehandleren må ikke gøre brug af en anden databehandler uden forudgående […] godkendelse fra den dataansvarlige*
- *Kontrakt […] genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder*

Hvad SKAL databehandleren

Som databehandler har man pligt til at

- ***kun** må **behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige** […] medmindre det kræves i henhold til […] ret, som databehandleren er underlagt.*
- ***sikrer**, at de personer, der er autoriseret til at behandle personoplysninger, har […] **tavshedspligt***
- *iværksætter alle foranstaltninger, som kræves i henhold til artikel 32 (*behandlingssikkerhed*)*
- ***bistår den dataansvarlige […] med opfyldelse af den dataansvarliges forpligtelse […] de registreredes rettigheder***
- *bistår den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af artikel 32-36 (*hele pakken fra behandlingssikkerhed, anmeldelse til datatilsyn, underretning af brud på sikkerhed, konsekvensanalyser og evt. forudgående høring af datatilsynet)
- *efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger til den dataansvarlige*
- *stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i denne artikel, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige*

Erfaringer

Forudsætninger for compliance med persondataforordningen

- Overblik over behandlingsaktiviteter der indeholder personoplysninger
- Formkrav til oplysning til de registrerede
- Procedurer for håndtering af rettigheder (indsigtsanmodninger, sletning, etc.)
- Hjemmel for behandlingen – hvis samtykke, er det gyldigt? (formkrav)
- Særlige krav vedr. børns personoplysninger
- Procedurer for anmeldelse af brud på persondatasikkerheden (72 timer)
- Risikovurdering (konsekvensanalyse/DPIA)
- Indtænke databeskyttelse i processer og IT systemer (ingen krav til ændring af eksisterende IT systemer – dog skal indstillinger justeres, hvis man kan)
- Styr på databehandlere
- Skal I have en DPO? (Ønsker I en DPO, hvis nu det ikke er et krav?)
- Internationale overførsler – koncernstruktur – databehandlere udenfor EU

Learnings

- Fokuser i starten på at få overblik over behandlingsaktiviteterne (artikel 30)
- Identificer hurtigst muligt de behandlingsaktiviteter, hvor hjemlen er samtykke, disse tekster skal sandsynligvis opdateres – og samtykke derfor genindhentes fra alle!
- Vælg et solidt framework til at støtte jeres governance arbejde – vi valgte ISO 27001 for at komme ”hele vejen rundt” – inkl. undervisning af medarbejdere.
- Sørg for de rette kompetencer er med i projekt teamet.
- Lav procedurer og overvej hvor understøttelse med IT skaber værdi. Hvordan sletter man en persons oplysninger? (backup?)
- Hvordan sikres ajourføring af personoplysninger? (evt. integration med offentlige datakilder)

”Det var noget af en mundfuld!”

Håndbøger og skabelonerne indeholder vores
erfaringer og struktur fra alle projekterne!

-husk: man spiser elefanter én bid ad gangen…