Databeskyttelse og it-sikkerhed

En trin for trin-håndbog til persondatareglerne og generel it-sikkerhed.

Danske Vandværker

Databeskyttelse og it-sikkerhed (tidl. Persondataforordning og it-sikkerhed)
Af Danske Vandværker

2. udgave – 1. oplag
Juni 2020

Forsidefoto: Colourbox
Layout: Irene Blak Villadsen
Tryk: Sangill Grafisk

Danske Vandværker
Solrød Center 20C
2680 Solrød Strand
Tlf.: 56 14 42 42
Mail: info@danskevv.dk
Web: danskevv.dk

Indledning

EU's databeskyttelsesforordning trådte i kraft 25. maj 2018. Den erstattede det tidligere persondatadirektiv og indeholder en række nye og ændrede regler for, hvordan I skal behandle personoplysninger.

Tanken med den nye databeskyttelsesforordning er, at ensarte de forskellige persondatalove på tværs af EU medlemslandene samtidigt med en styrkelse af forbrugernes rettigheder og et stærkere beskyttelsesniveau af de personoplysninger, organisationer registrerer, indsamler og opbevarer. Den nye lovgivning er, med få undtagelser, ens på tværs af alle medlemslande i EU og erstatter de enkelte landenes egne lovgivninger. I Danmark betyder det ændringer i forhold til de nuværende regler, og det er derfor vigtigt, at I bliver klar til at varetage de nye regler på vandværket.

Hvad betyder databeskyttelsesforordningen for jer?

Langt hen ad vejen stiller databeskyttelsesforordningen de samme krav, som persondataloven gjorde tidligere. Men der er også kommet flere nye krav, som I skal leve op til, når I behandler personoplysninger.

Meget forsimplet skal I have bedre styr på jeres databehandling og it-sikkerhed. Konkret betyder det, at I skal sørge for:

- At oplyse de registrerede (ofte forbrugere og ansatte) om hvilke oplysninger, I behandler og til hvilke formål.
- At det kun er nødvendige oplysninger, I behandler.
- At oplysningerne er korrekte og opdaterede.
- At oplysningerne ikke bliver opbevaret længere tid end højst nødvendigt.
- At oplysningerne er godt nok sikret set i forhold til deres følsomhed.
- At I til hver en tid kan dokumentere, at I lever op til ovenstående.

Hvorfor skal I følge databeskyttelsesforordningen?

"Kan vi ikke bare arbejde videre og ignorere de nye regler, indtil der opstår noget problematisk?"

EU lægger op til at kunne slå hårdt ned på organisationer, der ikke lever op til databeskyttelsesforordningen. Også inden der opstår et eventuelt problem. På den måde sikres det, at I både overholder kravene til databeskyttelsesforordningen, og at I får styr på den generelle it-sikkerhed.

Indtil videre har den højeste danske bøde for at bryde persondatalovgivningen været på 25.000 kr.

Det ændres markant fra 25. maj 2018, hvor bøderne kan komme op på 20.000.000 euro eller 4% af virksomhedens globale omsætning – alt efter, hvad der er størst.

Hvordan gør I?

For at gøre arbejdet så nemt som muligt har Danske Vandværker i samarbejde med SOLID-IT udarbejdet denne håndbog. Når I læser den, vil I lære mere om databeskyttelsesforordningen, ligesom I vil få en trin for trin-vejledning i, hvordan I udfylder en række vigtige skabeloner.

Skabelonerne finder I på:
www.danskevv.dk > Viden om > Cybersikkerhed

Skabelonerne er blevet til på baggrund af interviews med vandværkerne i Lørslev, Strib og Birkerød, og det er Danske Vandværkers vurdering, at I vil kunne overholde databeskyttelsesforordningens vigtigste krav ved at benytte dem.

Selvom håndbogen og skabelonerne er lavet så de dækker de fleste vandværker, er det **meget** vigtigt, at I er opmærksomme på, om de matcher lige netop jeres vandværk.

Baggrundsinformation

Hvad er personoplysninger?

Personoplysninger er enhver form for information, der kan henføres til en identificerbar person. Oplysningerne er som udgangspunkt inddelt to primære kategorier, og skemaet nedenfor viser typer af personoplysninger i forhold til den tidligere persondatalov og EU databeskyttelsesforordningen.

Det er vigtigt, at I får et overblik over, hvilke personopysninger I behandler og i hvilke kategorier de hører hjemme.

OBS: Vær opmærksom på at almindelige personoplysninger kan være fortrolige og derfor skal beskyttes bedre. Det kan for eksempel være, at I videregiver oplysninger til kommunen om svage borgere i forbindelse med, at I overvejer at lukke for vandet, når regningen ikke er blevet betalt. Selvom behandlingen er lovlig, fordi det beskytter forbrugerens vitale interesser, er oplysningen om manglende betaling fortrolig og skal behandles fortroligt.

Kategori	Persondataloven	Databeskyttelsesforordningen
Almindelige oplysninger	• Navn • Adresse • Telefonnummer • Fødselsdato • Uddannelse • Beskæftigelse • Eksamensresultater • Bolig og bil • Løn og skat • Sygefraværsstatistik (uden helbredsoplysninger)	Omfatter herudover: • Væsentlige sociale problemer • Andre rent private forhold end følsomme oplysninger • CPR-nr. (Læs om Databeskyttelseslovens § 11 regler på næste side.) Særlig kategori • Oplysninger om strafbare forhold
Semifølsomme oplysninger	• CPR-nr • Oplysninger om strafbare forhold • Væsentlige sociale problemer • Andre rent private forhold end følsomme oplysninger	
Følsomme oplysninger	• Race • Etnisk oprindelse • Politisk religiøs eller filosofisk overbevisning • Fagforeningsmæssigt tilhørsforhold • Seksuelle forhold og seksuel orientering • Helbredsoplysninger	Omfatter herudover: Genetiske og biometriske oplysninger med det formål at identificere den enkelte

Det lovlige grundlag for at behandle personoplysninger

Det er kun lovligt at behandle personoplysninger, hvis I opfylder mindst ét af følgende punkter:

a) *I har fået et frivilligt samtykke fra personen til et eller flere specifikke formål.*
OBS: *CPR-nr. kan jf. Databeskyttelseslovens § 11 kun behandles efter samtykke eller lovkrav i forbindelse med vandværkets almindelige drft. Følsomme personoplysninger kræver samtykke eller lovkrav.*

b) *Behandling er nødvendig aht. opfyldelse af en kontrakt, personen er part i, eller af hensyn til forberedelser der gennemføres på den registreredes anmodning forud herfor*

c) *Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige (fx. behandling af CPR-nr. når der indberettes løn eller honorar til Skattestyrelsen).*

d) *Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser.*

e) *Behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.*

f) *Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre personens rettigheder går forud herfor, navnlig hvis den registrerede er et barn.*

I langt de fleste tilfælde vil vandværker falde under kategorien c (retlig forpligtelse) og e (opgave i samfundets interesse).

For ansatte vil det iflg. Databeskyttelseslovens § 12 ofte være en kombination af b (kontrakt og/eller kollektiv overenskomst) og c (retlig forpligtelse) men det kan også ske af hensyn til vandværkets administration (legitim interesse).

Vær opmærksom på at følsomme personoplysninger, fx helbredsoplysninger om ansatte, som udgangspunkt kun må behandles efter skriftligt samtykke fra den ansatte - med mindre det følger af lovkrav, fx ifm. arbejdsskader.

Forbrugernes rettigheder i databeskyttelsesforordningen

I den nye databeskyttelsesforordning videreføres og udvides rettighederne fra persondataloven. Rettigheder er:

Detaljeret og klar information om behandlingen af personoplysninger
Forbrugerne har ret til at vide, hvilke data I gemmer om dem, samt hvordan disse data bliver behandlet.

Retten til sletning (retten til at blive glemt)
Forbrugerne har ret til få slettet alle data om sig selv, så længe det ikke påvirker jeres evne til at betjene dem som kunde. Hvis en forbruger ikke længere er kunde, har han/hun ret til at få slettet alle data om sig selv – så længe personoplysningerne ikke skal bruges i andre sammenhænge, eksempelvis bogføringslovens 5-årige dokumentationskrav.

TIP: Når en forbruger flytter fra sin bolig, bør der laves et ejerskifte i stedet for en ejernotering. Ved ejerskifte udarbejdes en flytteopgørelse og fraflyttende ejer bliver faktureret. Ved en ejernotering ændres navnet på forbrugeren.

Retten til dataportabilitet (retten til at få udleveret data)
Forbrugerne har ret til at få udleveret deres data i et

almindeligt maskinlæsbart filformat (fx Excel, CSV, XML), som for eksempel kan medbringes ved flytning til et andet forsyningsområde. Er der en anden metode til overførsel mellem vandværker der fungerer godt i praksis er de nye regler ingen hindring for at fortsætte dette - så længe det er let og sikkert for forbrugeren.

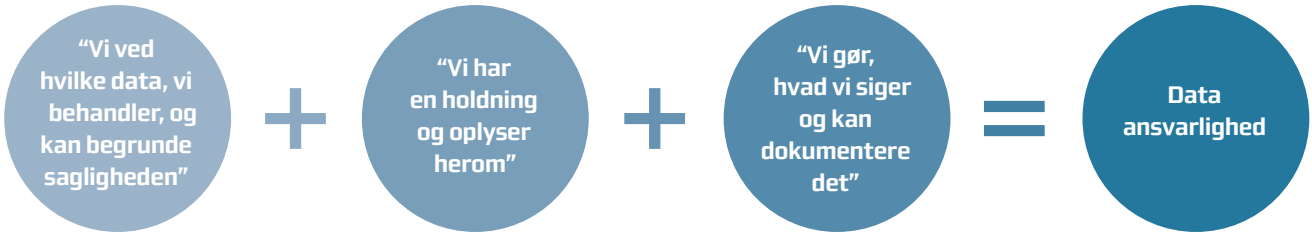
Hvem har ansvaret?

Ansvaret for at behandle personoplysninger er altid hos den enkelte juridiske enhed – det vil sige det enkelte vandværk. I praksis betyder det, at I skal udnævne en person, der i det daglige har ansvaret for persondata. Og som til hver en tid skal kunne påvise, at I overholder kravene.

I grafikken kan I se hvad dataansvarlighed indebærer.

Det er dog vigtigt at understrege, at selvom I udpeger en medarbejder til at være persondataansvarlig, så er det juridiske ansvar i sidste ende placeret hos vandværket.

For at håndtere dataansvarlighed i forhold til eksterne it-leverandører, der behandler personoplysninger for jer, skal I benytte en databehandleraftale. Det kan I læse mere om i kapitel 7.



Sådan bruger I håndbogen

Håndbogen er bygget op som en trin for trin-guide med tilhørende skabeloner, der skal udfyldes. Guiden giver jer et overblik over arbejdet med databeskyttelsesforordningen og it-sikkerhed, ligesom den fungerer som en tjekliste for de aktiviteter, I skal igennem.

Hvert kapitel i håndbogen indeholder en ny skabelon. Ved at følge de trin og opgaver, der er beskrevet i bogen, vil I få udfyldt skabelonerne og ende med færdige dokumenter.

Nogle steder i skabelonerne er markeret med gult. Det er der, hvor der oftest er forskel på, hvordan de enkelte vandværker behandler persondata, og som derfor kræver ekstra opmærksomhed fra jer. Det er også de punkter, der bliver gennemgået i de enkelte opgaver.

I finder alle skabelonerne på:
www.danskevv.dk > Viden om > Persondata og cybersikkerhed

Skabeloner I skal bruge

Kapitel 1: "Målrettet arbejde med databeskyttelsesforordningen"
Beskriver overordnet, hvordan I behandler personoplysninger. Når skabelonen er udfyldt, er den det centrale dokument, der skal bruges som dokumentation over for myndighederne: "fortegnelsen".

Kapitel 2: "Datastrømsanalyse, dokumentation for mindre vandværker"
Indeholder en liste over systemer, hvor der optræder persondata og fungerer desuden som supplement til ovenstående.

Kapitel 3: "Risikovurdering for mindre vandværker"
Indeholder en liste over potentielle trusler mod it-systemerne, som I skal forholde jer til i forhold til sandsynlighed og konsekvenser.

Kapitel 4: "Beredskabsplan for it-systemer"
Indeholder en liste over it-systemer hos vandværker og de beredskabsmuligheder, der findes for hvert system i tilfælde af længerevarende nedbrud.

Kapitel 5: "Persondatapolitik"
Beskriver jeres persondatapolitik. Når skabelonen er udfyldt, skal I sørge for indholdet bliver stillet til rådighed for jeres forbrugere, typisk sker dette ved publicering på jeres hjemmeside i kombination med en henvisning hertil i et velkomstbrev til nye forbrugere.

Kapitel 6: "It-sikkerhedspolitik"
Beskriver jeres generelle it-sikkerhed. For eksempel passwordpolitik, backup, logning.

Kapitel 7: "Databehandleraftale"
Denne skabelon er Datatilsynets eksempel på en databehandleraftale som vi har tilpasset med et eksempel på et vandværks it-leverandør, der behandler personoplysninger på vegne af vandværket.

Kapitel 8: "Retningslinjer for it-adfærd"
En PowerPoint-præsentation, der bruges til at informere medarbejdere på vandværket om it-sikkerhed og databeskyttelsesforordningen.

Kapitel 9: "Konsekvensanalyse for behandling af personoplysninger (DPIA)"
Denne skabelon skal alene benyttes ved højrisiko behandlinger af personoplysninger. Vi har pt. ikke fundet eksempler, hvor dette har været påkrævet i et vandværk.

Når I har gennemført trin for trin-guiden og fået udfyldt alle skabelonerne, har I et grundlag for arbejdet med persondata og it-sikkerhed, der kan bruges som dokumentation over for relevante myndigheder.

I bør få de færdige dokumenter godkendt af jeres bestyrelse og som minimum revidere dem én gang om året.

Skab overblik over vandværkets behandling af personoplysninger

ANVENDT SKABELON:
Målrettet arbejde med persondataforordningen.

I finder alle skabelonerne på:
www.danskevv.dk < Viden om > Cybersikkerhed

Introduktion

Skabelonen for målrettet arbejde med persondataforordningen er det mest centrale dokument. Ofte referes til dokumentet som en "fortegnelse". Det skal, sammen med datastrømsanalysen, dokumentere, hvordan I behandler personoplysninger, hvorfor I mener det er lovligt, hvor længe I forventer at opbevare oplysningerne og hvordan oplysningerne bliver beskyttet.

I skabelonen er der blandt andet eksempler på beskrivelser af, hvordan I behandler personoplysninger. Det drejer sig om helt almindelige personoplysninger med det formål at afregne vandforbrug samt almindelige HR-aktiviteter for vandværkets ansatte og i forbindelse med ansøgere til ledige stillinger på vandværket.

Skabelonen er blandt andet lavet på baggrund af Datatilsynets anbefalinger til, hvordan I behandler personoplysninger og de konkrete tekster stammer fra interviews med vandværker.

Det færdige dokument kan I bruge som en trin for trin-guide over de sikkerhedsforanstaltninger, I skal indføre på vandværket. Hvis I modtager en henvendelse fra Datatilsynet, hvor de beder om dokumentation for jeres persondatabehandling, skal det opdaterede dokument I har udfyldt kunne besvare langt de fleste spørgsmål.

De steder, der er markeret med gult, er de ting, I skal være ekstra opmærksom på. Det er også de steder, der bliver gennemgået i opgaverne.

Opgave 1.1

Udpeg en persondataansvarlig på vandværket.

1. Udpeg en persondataansvarlig. Det er den, der arbejder med persondata på vandværket.

TIP! Typisk vil den person, der i det daglige har ansvaret for persondata, i et mindre vandværk være kassereren og i et større, den daglige leder eller den regnskabsansvarlige.

2. Find skabelonen "Målrettet arbejde med persondataforordningen".

3. Find afsnittet "Kontaktoplysninger på persondataansvarlig" på side 4.

4. Noter for- og efternavn samt telefon og e-mail på den persondataansvarlige.

Opgave 1.2

Identificer aktiviteter hvor persondata indgår.

1. Dokumenter i hvilke aktiviteter, der indgår persondata. Det er oftest disse tre områder:

   • Forbrugsafregninger og relaterede aktiviteter.

   • Almindelige HR aktiviteter – jobansøgninger.

   • Almindelige HR aktiviteter – ansatte.

2. Find afsnittet "Fortegnelser over behandlingsaktiviteter" på side 5.

3. Bekræft, at informationerne, der allerede står på side 5-8, er korrekte – også underafsnittet om databehandlere (leverandører). Hvis ikke, så ret til, så informationerne passer.

4. Fjern eller tilføj databehandlere, der er relevante/ikke relevante for netop jeres aktivitet.

> **TIP!** Typiske databehandlere for mindre vandværker er Kamstrup og Rambøll.

5. Vurder, om der er yderligere aktiviteter, hvor I behandler persondata. Hvis det er tilfældet, skal I også notere det i dette afsnit.

Opgave 1.3

Generelle organisatoriske og tekniske foranstaltninger.

1. Gennemgå listen på side 8 i det afsnit, der hedder "Supplerende bemærkninger om generelle organisatoriske og tekniske foranstaltninger".

2. Tilføj eller fjern elementer, som er relevante/ikke relevante for jeres vandværk.

Opgave 1.4

Gennemgå dokumentet i sin helhed.

1. Gennemlæs hele dokumentet. Vurder undervejs, om I kan stå inde for indholdet. Ret til, så indholdet matcher jeres vandværk.

2. Slet introduktionsteksten, der er markeret med grønt på side 2. Nu har I en god beskrivelse af de aktiviteter, I behandler, grundlaget for at behandle dem, databehandlere, tidsfrister for sletning/opbevaring, en risikovurdering for behandlingerne og de tekniske og organisatoriske sikkerhedstiltag, der er lavet på baggrund af risikovurderingen.

Dokumenter i hvilke systemer, der findes persondata

ANVENDT SKABELON: Datastrømsanalyse

I finder alle skabelonerne på: www.danskevv.dk > Viden om > Persondata og Cybersikkerhed

Introduktion

Overblik er et af de centrale elementer for at kunne vise, at I har styr på, hvordan I behandler personoplysninger. Skabelonen til datastrømsanalyse hjælper med at dokumentere dette overblik.

Mange brancheløsninger går igen hos de fleste vandværker. Derfor indeholder skabelonen de mest brugte it-systemer. De fleste vandværker vil med meget få ændringer have et stærkt værktøj til at dokumentere deres it-systemer og hvilke aktiviteter i behandlingen, som systemerne understøtter.

TIP! Mindre vandværker: Skabelonen kan ofte benyttes uden større ændringer. Dog er det vigtigt, at I forholder jer til indholdet i dokumentet.

TIP! Større vandværker: Overvej om teksterne i dokumenterne kan genbruges. Det er vigtigt, at risikovurderingen afspejler jeres egen vurdering af de forskellige aktiviteter.

Opgave 2.1

Lav en liste over alle vandværkets it-systemer, der indeholder persondata.

1. Find skabelonen "Datastrømsanalyse, dokumentation for mindre vandværker".

2. Gennemgå hvert enkelt it-system på listen. Fjern it-systemer fra listen, som ikke er relevante for jeres vandværk, og tilføj it-systemer til listen, hvis de ikke findes i forvejen.

3. Gennemgå hvert it-system og notér kort oplysninger om formålet med behandlingen, personoplysninger, backup, kryptering, databehandler m.m.

Gennemfør en risikovurdering af vandværkets anvendelse af it

ANVENDT SKABELON:
Risikovurdering for mindre vandværker.

I finder alle skabelonerne på

www.danskevv.dk > Viden om > Persondata og Cybersikkerhed

Introduktion

Risikovurderingen skal finde og prioritere risici med udgangspunkt i jeres forretningsmæssige forhold. Resultatet skal være med til at fastlægge og prioritere de nødvendige handlinger for at undgå disse risici.

Skabelonen er på forhånd udfyldt med de mest almindelige trusler og forbedringsforslag. I skal dog være opmærksomme på, at det ikke er det fulde billede, da forholdene på de enkelte vandværker er meget forskellig.

Opgave 3.1

List og vurder potentielle og konkrete trusler mod vandværkets it-sikkerhed.

1. Find skabelonen "Risikovurdering for mindre vandværker".

2. Bekræft, at alle relevante trusler er med. Suppler eventuelt med yderligere trusler, hvis det er nødvendigt.

3. Vurder, sandsynligheden for, at hver enkelt trussel indtræffer efter følgende skala:

a. Høj
b. Mellem
c. Lav

4. Overvej og vurder konsekvenserne for hver enkelt trussel efter følgende skala:

d. Høj
e. Mellem
f. Lav

5. Vurder, det samlede risikobillede for truslen efter følgende skala:

a. Kritisk
b. Middel
c. Acceptabel

6. Angiv forslag til at undgå truslen.

7. Hvis der er trusler, I vurderer som kritiske, skal I reagere. Hvis der er trusler, I vurderer til at være middel, skal I beslutte, om truslen skal behandles som kritisk eller acceptabel.

Udarbejd en beredskabsplan for vandværkets it-systemer

ANVENDT SKABELON:
Beredskabsplan for it-systemer.

I finder alle skabelonerne på www.danskevv.dk > Viden om > Persondata og Cybersikkerhed

Introduktion

Det er vigtigt, at I formulerer arbejdsgange for, hvordan I håndterer enhver form for it-nedbrud, der kan forhindre den fortsatte drift af vandværket. Så ved alle præcis, hvad de skal gøre i en nødsituation.

En beredskabsplan er en drejebog for nødsituationer, og den bør ikke være kompliceret i sit indhold. Den kan dog kræve, at der bliver indsamlet en del informationer, mens den bliver lavet og efterfølgende under vedligeholdelsen.

I beredskabsplanen er der også et afsnit om "Handlingsplan for virus- eller hackerangreb". Det er i fagsprog også kendt som "Information Security Incident Management".

Det er vigtigt at understrege, at I kun skal benytte beredskabsplanen, når I ikke kan håndtere en hændelse eller et nedbrud indenfor rammerne af jeres normale processer og arbejdsgange.

Bemærk, hvis I allerede kender løsningen på et problem, skal I normalt ikke bruge beredskabsplanen.

De steder, der er markeret med gult, er de ting, I skal være ekstra opmærksom på. Det er også de steder, der bliver gennemgået i opgaverne.

Opgave 4.1

List og prioriter vandværkets it-systemer.

1. Find skabelonen "Beredskabsplan for it-systemer".

2. Udfyld afsnittet "Prioriteret systemliste" på side 1 med de it-systemer, som I benytter. Tilføj/fjern systemer fra listen, som er relevante/ikke relevante for jer.

3. Prioriter systemerne og noter hvor lang tid, der maksimalt må gå, før hvert it-system er reetableret.

4. Beskriv hvilke muligheder der er for, at en manuel arbejdsgang kan erstatte it-systemets funktion.

Opgave 4.2

Udfyld kontaktlister.

1. Udfyld kontaktlisterne i afsnittet "Kontaktlister" på side 2.

2. Tilføj eller fjern informationer fra listen, som er relevante/ikke relevante for jeres vandværk.

Opgave 4.3

Opdater handlingsplaner.

1. Udfyld handlingsplanerne under afsnittet "Handlingsplaner" på side 3-4. Bemærk, at der er to typer af handlingsplaner – én for interne servere og systemer, og én for eksterne services.

2. Gennemgå handlingsplanerne, så I sikrer, at alt er korrekt.

3. Udfyld afsnittet "Denne handlingsplan er gældende for følgende systemer" for begge handlingsplaner (interne servere og systemer + eksterne services) side 3-4.

Opgave 4.4

Gennemgå handlingsplan for virus- eller hackerangreb.

1. Gennemgå afsnittet "Handlingsplan for virus- eller hackerangreb" på side 5.

2. Sæt jer godt ind i indholdet, så I ved, hvad I skal gøre, hvis der sker et virus- eller hackerangreb. Der er ikke noget i handlingsplanen, der umiddelbart skal udfyldes, men den bør gennemlæses og tilrettes det enkelte vandværk, hvis det er nødvendigt.

Udarbejd en persondatapolitik for vandværket

ANVENDT SKABELON:
Persondatapolitik.

I finder alle skabelonerne på:
www.danskevv.dk > Viden om > Persondata og Cybersikkerhed

Introduktion

Databeskyttelsesforordningen stiller skrappere krav til de informationer, som forbrugere og ansatte gives i forbindelse med behandlingen af deres personoplysninger. Med en god persondatapolitik bliver disse oplysninger overskuelige og lettere at forstå for forbrugerne, ligesom de får indsigt i deres rettigheder samt databeskyttelsesforordningens formelle krav.

De steder, der er markeret med gult, er de ting, I skal være ekstra opmærksom på. Det er også de steder, der bliver gennemgået i opgaverne.

Opgave 5.1

Udfyld kontaktoplysningerne for den persondataansvarlige på vandværket.

1. Find skabelonen "Persondatapolitik".

2. Find afsnittet "Kontaktoplysninger på persondataansvarlig" (den person, der i det daglige har ansvaret for persondata) på side 2.

3. Noter kontaktoplysninger samt telefon og e-mail på den persondataansvarlige (samme person som blev noteret i opgave 1.1). Hvis I ønsker det, kan I efter aftale med den persondataansvarlige oplyse for- og efternavn for at gøre kontakten mere personlig, men det er ikke et krav.

Opgave 5.2

Udfyld oplysninger på den dataansvarlige juridiske enhed.

1. Find afsnittet "Dataansvarlig" på side 2.

2. Udfyld oplysningerne på den dataansvarlige juridiske enhed. Det er vandværkets juridiske informationer, der skal stå her.

Opgave 5.3

Generelle organisatoriske og tekniske foranstaltninger.

1. Find afsnittet "Informationssikkerhed" på side 4.

2. Gennemgå listen. Tilføj eller fjern elementer, som er relevante/ikke relevante for jeres vandværk.

Opgave 5.4

Gennemgå dokumentet i sin helhed.

1. Gennemlæs hele dokumentet. Vurder undervejs, om I kan stå inde for indholdet. Hvis ikke så ret til, så indholdet matcher jeres vandværk.

2. Slet introduktionsteksten, der er markeret med grønt på side 2. I har nu en persondatapolitik, der indeholder kravene til oplysningspligt om hvilke personoplysninger, I behandler, og forbrugerens rettigheder i den forbindelse.

3. Offentliggør det færdige dokument, hvor I normalt offentliggør information til forbrugerne (ofte er det på jeres hjemmeside). Link også til persondatapolitikken fra jeres leveringsbetingelser og velkomstbrev.

Udarbejd en it-sikkerhedspolitik for vandværket

ANVENDT SKABELON: It-sikkerhedspolitik.

I finder alle skabelonerne på: www.danskevv.dk > Viden om > Persondata og Cybersikkerhed

Introduktion

Databeskyttelsesforordningen stiller krav om at man opretholder et sikkerhedsniveau, både organisatorisk og teknisk, som imødekommer de risici, der er forbundet med de personoplysninger der behandles. Niveauet af sikkerhed man som vandværk skal opnå skal måles ift. ressourcerne det enkelte vandværk har samt følsomheden og mængden af personoplysninger der behandles. Med andre ord, skal ledelsen træffe beslutning om hvor mange af vandværkets ressourcer, de vil investere i sikkerheden for at sikre personoplysningerne ikke kommer i forkerte hænder, mistes helt eller forvanskes.

Det er vigtigt, at alle på vandværket forstår arbejdet med it-sikkerhed, og hvad det kan betyde, når det en dag går galt. Derfor skal ledelsen udforme en it-sikkerhedspolitik med retningslinjer alle skal følge.

På den måde kan I styrke både it-sikkerheden om personoplysninger samt den tekniske sikkerhed omkring vandværkets drift, så risikoen for, at uvedkommende trænger ind i systemerne og manipulerer dem med et driftsstop som konsekvens, reduceres.

En it-sikkerhedspolitik skal ses som det første skridt i retningen af et samarbejde om it-sikkerhed på tværs af samfundet. Et direktiv fra EU opfordrer nemlig til at styrke samarbejdet om *"Sikkerhed i net- og informationssystemer"* samt til *"Udvikling af principper for et europæisk cyberkrise samarbejde"*.

It-sikkerhed eller cybersikkerhed

Begrebet it-sikkerhed er ved at blive afløst af et nyere begreb – cybersikkerhed. Men der er ikke den store forskel. Cybersikkerhed er dog lidt mere omfattende, fordi den også inkluderer digitalt styrede produktionssystemer og ikke kun informationssystemer.

Ikke sikkerhed for enhver pris

Der er ingen forventninger om perfektion, men Datatilsynet forventer at alle gennemfører en risikovurdering (se kapitel 3) og træffer beslutning om hvad et rimeligt sikkerhedsniveau er for jeres vandværk og derefter implementerer dette i praksis. Altså: ikke sikkerhed for enhver pris – I skal finde et fornuftigt niveau, så I passer tilstrækkeligt på personoplysningerne i forhold til jeres vandværks ressourcer hertil.

Vi har på de følgende sider angivet de ting, der bliver betragtet som almindeligt forventeligt af alle.

De steder, der er markeret med gult, er de ting, I skal være ekstra opmærksom på. Det er også de steder, der bliver gennemgået i opgaverne.

Opgave 6.1

Gennemgang og tilretning af den indledende del af politikken.

1. Find skabelonen "It-sikkerhedspolitik".
2. Læs afsnittene "Introduktion", "Formål" og "Ledelsens udmelding om de overordnede mål og principper" på side 2-3.
3. Tag stilling til, om de tre punkter dækker jeres ønsker, og om I måske skal prioritere dem ved at give dem en nummeret rækkefølge.
4. De tre afsnit "Introduktion", "Formål" og "Ledelsens udmelding om de overordnede mål og principper" på side 2-3 skal udtrykke ledelsens holdninger, så de kan blive meldt ud til medarbejdere og omverdenen. Ret dem til, så det passer på jeres vandværk.

Opgave 6.2

Gennemgang og tilretning af "Vigtige grundprincipper for sikkerhedsarbejdet".

1. Find afsnittet "Funktionsadskillelse" på side 3 og læs det godt igennem.

Hvad betyder funktionsadskillelse?

Funktionsadskillelse betyder, at den person, der beslutter ændringer på it-sikkerhedsområdet ikke må være den samme person, som også gennemfører ændringerne. I nogle vandværker kan funktionsadskillelse være en udfordring, da der er begrænsede it-ressourcer til rådighed. I kan derfor vælge at benytte en ekstern it-konsulent til det formål.

Husk, at it-konsulenten skal underskrive en fortrolighedserklæring. Hvis it-konsulenten ikke er tilgængelig i en akut situation, bør den daglige leder have rettigheder som administrator, som han får udleveret i en "nødkuvert". Efterfølgende har den daglige leder pligt til at dokumentere hændelsesforløbet.

Alternativt kan reglen også være, at bestyrelsen eller et bestyrelsesmedlem skal orienteres om og godkende nye tiltag, **inden** de bliver gennemført.

2. Tag stilling til hvilken model, I ønsker. Notér den i afsnittet "Funktionsadskillelse" og fjern overflødig tekst.

3. Find afsnittet "Sikkerhedsforanstaltninger" på side 4 og læs det godt igennem.

God it-sikkerhedspraksis

I afsnittet om sikkerhedsforanstaltninger bliver der taget principiel stilling til, at privat it-udstyr ikke må bruges til at udføre arbejde for vandværket. Privat udstyr må heller ikke bruges til fjernopkobling til vandværkets systemer. Det vil sige, at it-udstyret skal stilles til rådighed af vandværket og kun bruges arbejdsmæssigt. Vælger I i stedet den anden løsning, hvor privat it-udstyr gerne må bruges, skal I gennemføre nogle særlige sikkerhedsforanstaltninger. Der vil blandt andet være behov for, at I udarbejder særlige instrukser for, hvordan I skal forholde jer sikkerhedsmæssigt.

Bemærk, at forbud mod brug af privat it-udstyr er "god it-sikkerhedspraksis". Dog kan det medføre en ekstra udgift for vandværket.

4. Tag stilling til hvilken model for brug af privat it-udstyr, I ønsker at benytte. Notér den i afsnittet "Sikkerhedsforanstaltninger".

5. De resterende punkter på side 4 i skabelonen nævner en række tiltag om blandt andet risikovurdering og databehandleraftaler. Skabelonen for risikovurdering har I udfyldt i kapitel 3, og skabelonen for databehandleraftale kommer I til at udfylde i kapitel 7.
I skal således ikke gøre mere lige nu.

Opgave 6.3

Gennemgang og tilretning af "Hovedpunkterne i regelsættet/retningslinjerne".

1. Find afsnittet "Hovedpunkterne i regelsættet/retningslinjerne er:" på side 5, og læs det godt igennem (side 5-12).

Retningslinjer for it-sikkerhedspolitik

Afsnittet handler om de retningslinjer, der fremgår af it-sikkerhedspolitikken. En række skabeloner i skabelonpakken har til formål at understøtte de retningslinjer, der bliver nævnt. Det handler om skabelonerne:

- "Risikovurdering for vandværker".
- "Retningslinjer for it-adfærd".
- "Datastrømsanalyse, dokumentation for vandværker".
- "Databehandleraftale".
- "Konsekvensanalyse for behandling af personoplysninger (DPIA)".
- "Beredskabsplan".

2. Ret afsnittet på alle de områder, det er relevante for jer.

Opgave 6.4

Gennemgå dokumentet i sin helhed.

1. Gennemlæs skabelonen fra start til slut. Vurdér teksten undervejs for at se, om der er beskrivelser, der skal rettes, så de passer til jeres vandværk.
2. Skriv jeres vandværks navn, alle de steder, hvor der står **<Xyz Vandværk>**
3. Slet introduktionsteksten, der er markeret med grønt på side 2.
4. Få godkendt it-sikkerhedspolitikken af jeres bestyrelse.

Opgave 6.5

Straks-tiltag

1. Mens I arbejder på at gøre it-sikkerhedspolitikken færdig og realisere den, bør I straks indføre følgende sikkerhedsforanstaltninger. Bemærk, de er forskellige for henholdsvis medarbejdere og ledelse samt it-administrator:

Huskeregler for alle medarbejdere

1. Undlad at koble privat it-udstyr op til vandværkets it-systemer. Brug kun it-udstyr, der er godkendt og udleveret fra vandværket.

2. Brug kun VPN-forbindelser (eller andre krypterede forbindelser), når I kobler jer op til vandværkets it-systemer.

3. Klik aldrig på vedhæftede filer eller links i e-mails fra afsendere, I ikke kender.

4. Download aldrig ikke-arbejdsrelaterede datafiler - heller ikke fra USB-nøgler.

5. Indsæt ikke ukendte USB-nøgler i en arbejdscomputer.

6. Upload aldrig arbejdsrelaterede filer til web-baserede services med mindre de er godkendt af vandværket.

7. Brug altid kryptering, når mails indeholder fortroligt materiale. Hvis I er i tvivl, så benyt kryptering.

8. Passwords er personlige og fortrolige og må ikke overdrages til andre.

9. Hvis I har mistanke om, at computeren er inficeret med malware, skal I øjeblikkeligt afbryde forbindelsen til netværket.

10. Tag regelmæssigt sikkerhedskopi af data og opbevar dem sikkert.

11. Hvis I finder en sikkerhedsbrist, skal I rapportere til nærmeste leder.

12. Installer sikkerhedsopdateringer, når de er tilgængelige. Det gælder både Microsoft Windows opdateringer og opdateringer til andre programmer som for eksempel JAVA, Adobe Reader, Flash, Skype, Firefox m.fl.

Huskeregler for ledelsen og it-administratoren

[Hvis I ikke har en it-administrator, kan I lade et eksternt it-firma udføre funktionen].

1. Stil it-udstyr ejet af vandværket til rådighed for medarbejderne til arbejdsbrug. Henstil til, at medarbejdernes private udstyr ikke bliver anvendt.

2. Benyt lange kodeord (gerne en sætning) og slå altid multi-faktor login til når du kan (fx engangskode via app eller SMS).

3. Sørg for, at medarbejdernes computere har installeret fungerende antivirus/anti-malware, der løbende bliver opdateret automatisk.

4. Sørg for, at medarbejdernes computere automatisk er sat op til at installere sikkerhedsopdateringer til operativsystem og andre programmer som for eksempel JAVA, Adobe Reader, Flash, Skype, Firefox.

5. Forlang at pauseskærm bliver aktiveret efter 10 minutters inaktivitet, hvorefter password skal bruges igen.

6. Ledelsen beslutter hvornår og hvem, der skal have adgang til hvilke systemer og data. It-administratoren gennemfører beslutningerne i praksis.

7. Hvis I bruger hjemmearbejdspladser, skal sikkerhedsniveauet være på højde med vandværkets kontorarbejdsplads. Det vil sige, at fortrolige print skal opbevares i et aflåst skab, trådløs kommunikation skal sikres, andres adgang til brug af computeren skal være begrænset, lokal lagring af fortrolige data skal beskyttes af kryptering, og ledelsen skal i passende omfang kontrollere, at reglerne bliver overholdt.

8. Medarbejderne skal tilbydes undervisning eller information om betydningen af it-sikkerhed på vandværket. Der skal følges op på, om regler og retningslinjer bliver fulgt (dels ved hjælp af sikkerhedssoftware, dels på basis af logs og overvågning). Benyt gerne PowerPoint-præsentationen i skabelonpakken "Retningslinjer for it-adfærd" til undervisningen.

9. Sørg for, at medarbejdernes computere og mobiltelefoner kan fjern-slettes, hvis de bliver tabt eller stjålet. Af samme årsag er det vigtigt de er krypteret (krypter fx computere med Microsoft Bitlocker som er integreret i Windows 10).

10. Sørg for at følgende regler bliver anvendt på it-systemer, der indeholder personoplysninger (for eksempel på en filserver):

    a. Begræns adgangen til så få brugere som muligt.

    b. Krypter backup af systemet samt harddisken.

    c. Gennemfør logning af hvem, der tilgår hvilke data og hvornår.

    d. Hvis data bliver kopieret ud på brugernes arbejdsenheder (laptop, mobiltelefon, tablet m.m.) skal data (eller enheden) krypteres.

11. Mindst én gang om året skal it-sikkerheden gennemgås med efterfølgende opdatering af it-sikkerhedspolitikken og de andre skabeloner i skabelonpakken (risikovurdering, beredskabsplan, datastrømsanalyse, leverandørforhold, osv.). Dette punkt kan eventuelt gennemføres ved hjælp af en konsulent.

Ovenstående regler for medarbejdere, ledelse og it-administrator er i overensstemmelse med it-sikkerhedsdokumentet.

Indgå databehandleraftaler med relevante leverandører

ANVENDT SKABELON: Databehandleraftale.

I finder alle skabelonerne på: www.danskevv.dk > Viden om > Persondata og Cybersikkerhed

Introduktion

Det er et krav, at I ikke giver personoplysninger videre til andre virksomheder og organisationer, uden at I har styr på de formelle krav til, hvordan data bliver behandlet. Databehandleraftalen er et eksempel på, hvordan I kan regulere disse forhold, når personoplysninger skal behandles af en underleverandør.

Det er relevant, når I eksempelvis har data på en hostet it-løsning hos jeres it-leverandør, eller hvis I benytter en ekstern service, hvor der behandles personoplysninger på vandværkets vegne – eksempelvis fjernaflæsninger af målere.

Det er ikke nødvendigt at indgå en databehandleraftale med en leverandør, der bare sælger en licens eller et abonnement, der alene er installeret lokalt hos vandværket (for eksempel Office-pakken), hvis ikke de behandler personoplysninger for jer. Men hvis personoplysningerne overlades til en leverandør, for eksempel fjernbackup, skal I indgå en databehandleraftale.

I skal indgå en databehandleraftale med hver virksomhed, der behandler personoplysninger på jeres vegne. I skal forvente at indgå i dialog med de leverandører, som skal underskrive en databehandleraftale, da de skal forpligte sig til indholdet. I kan med fordel benytte datastrømsanalysen fra kapitel 2 til at danne jer et overblik over hvilke leverandører, I skal indgå en databehandleraftale med.

TIP! Selvom ordlyden i databehandleraftalen er til forhandling med databehandlerne, er der formkrav i forordningen, som I skal kende. Se ordlyden i Databeskyttelsesforordningens artikel 28, inden I retter i teksten.

EKSEMPEL

Når I benytter cloud services, fx Dropbox eller Microsoft Office 365, bliver der i langt de fleste tilfælde automatisk udstedt en databehandleraftale som I ikke har indflydelse på indholdet af. Her er det vandværkets beslutning og ansvar at indholdet og niveaet er godt nok til vandværket og lovens krav.

Overvej derfor om I vil:
- Fortsætte med at benytte cloud servicen eller finde en anden leverandør.
- Opbevare personoplysninger i andre systemer end cloud servicen.

Hvis I vælger at opbevare personoplysninger på en lokal filserver, hvor der ikke er nogen ekstern it-leverandør involveret, bør I:
- **Begrænse adgang** så kun relevante medarbejdere har adgang.
- **Kryptere både backup og lagermedier**.
- **Kryptere de computere**, hvor filerne ligger.
- **Logge**, hvem som har set og hentet hvilke data og hvornår.
- **Begrænse og instruere** medarbejderne via politik i at HR oplysninger kun må ligge på filserveren.

Opgave 7.1

Tilpas skabelonen til vandværk og relevant leverandør.

1. Find skabelonen "Databehandleraftale".
2. Gennemgå skabelonen fra start til slut. Ret undervejs beskrivelserne, så de passer til jer.
3. Indsæt de korrekte oplysninger om leverandøren, som aftalen skal indgås med.
4. Slet introduktionsteksten, der er markeret med grønt på side 1.
5. Skabelonen er nu klar til at blive forhandlet med leverandøren.

Informer medarbejdere i vandværket om de nye tiltag

ANVENDT SKABELON:
Retningslinjer for it-adfærd.

I finder alle skabelonerne på:
www.danskevv.dk > Viden om > Persondata og Cybersikkerhed

Introduktion

De ansatte på vandværket skal have kendskab til databeskyttelsesforordningen og it-sikkerhed. Det sker blandt andet gennem uddannelse og vejledning, og I kan med fordel benytte skabelonen "Retningslinjer for it-adfærd". Det er en PowerPoint-præsentation, som nemt kan tilpasses jeres eget materiale til medarbejdere, der har behov for at benytte de administrative it-systemer. Den indeholder blandt andet tips til, hvordan I laver et godt password, og hvordan I anvender mobile enheder, e-mail, internet, osv.

Præsentationen kan med fordel indgå i introduktionen til nye medarbejdere.

TIP! Mindre vandværker har typisk få eller slet ingen ansatte. Derfor kan det være vanskeligt at gennemføre decideret undervisning. I bør i stedet for fokusere på at gennemføre opgaverne i håndbogens kapitel 1-7 for at sikre dokumentation af forordningens krav.

Opgave 8.1

Gennemgå præsentationen og informer medarbejderne.

1. Find skabelonen "Retningslinjer for it-adfærd".
2. Gennemgå præsentationen. Ret den til undervejs, så den passer på netop jeres vandværk.
3. Præsentér materialet for medarbejderne.

Brug af DPIA – konsekvensanalyse for behandlinger af personoplysninger, der sandsynligvis medfører en høj risiko for personerne

ANVENDT SKABELON:
Konsekvensanalyse for behandling af personoplysninger (DPIA).

I finder alle skabelonerne på:
www.danskevv.dk > Viden om > Persondata og Cybersikkerhed

Introduktion

Efter 25. maj 2018 er det et krav, at der udarbejdes en konsekvensanalyse (DPIA), inden I sætter nye behandlinger i gang, hvis den kan indebære en høj risiko for personers rettigheder. Det kan for eksempel være, hvis I behandler store mængder følsomme og fortrolige personoplysninger.

TIP! Til mindre vandværker vil det være meget usandsynligt, at der vil opstå behov for konsekvensanalyser.

TIP! Til større vandværker: Det er vigtigt at dokumentere, at I eventuelt fravælger at gennemføre en konsekvensanalyse i forbindelse med en risikovurdering af nye og større it-systemer.

Et eksempel kan være et nyt it-system, der automatisk håndterer klagesager for forbrugere (og dermed får retsvirkning for personen). Eller et nyt it-system, der behandler data om de ansattes helbredsoplysninger.

Er I i tvivl om jeres nye system kan medføre en høj risiko, anbefaler vi at I altid udfylde en DPIA, inden I sætter behandlingen i gang. DPIA kan bruges som dokumentation af risikovurderingen, som I har foretaget i forbindelse med planlægningen af persondatabehandlingen.

Skabelonen skal bruges som inspiration for jeres risikovurderinger med persondatabehandlingen.

EUs datatilsyn har udarbejdet lister med eksempler, hvor DPIA specifikt er påkrævet og vi har ikke fundet eksempler, der generelt er relevante for vandværkerne.

Opgave 9.1

Gennemgå DPIA'en for systemer, der igangsættes efter 25.5.2018 og som sandsynligvis vil medføre en høj risiko for personerne der er registreret.

1. Find skabelonen "Konsekvensanalyse for behandling af personoplysninger (DPIA)".

2. Svar på spørgsmålene i skabelonen.

3. Følg instruktionerne til sidst i skabelonen.

Danske Vandværker

Solrød Center 20 C
2680 Solrød Strand

www.danskevv.dk
info@danskevv.dk

Sekretariatets åbningstid
Mandag-torsdag kl. 09-15.00
Fredag kl. 9.00-14.00