Referat, Temamøde om persondataforordning d. 22-11-2017

Sted: Kirke Såby Forsamlingshus
Deltagere: Repræsentanter fra følgende vandværker
Vandværker, medlem
Ejby Strand, Højby, Ny Tolstrup, Øm Bys, Hvalsø, Osted, Brusagergård, Sæby, Møllehøj, Skovholm, Gershøj Strand
Vandværker, ikke medlem
Vester Såby, Gevninge Overdrev, Sømod, Kornerup, Rorup
Referent: Søren G. Klingemann, Lejre Vandråd

22. november 2017

Deltagerne blev budt velkommen af Lejre Vandråds formand Søren Toft Nielsen der også kunne præsentere aftens indlægsholder, Teknisk rådgiver for Danske Vandværker Henrik Blomhøj

Persondataforordning og IT-sikkerhed

https://danskevv.dk/viden-om/persondata-og-cybersikkerhed/
Hent trin for trin-guide til persondata og IT sikkerhed
https://danskevv.dk/viden-om/persondata-og-cybersikkerhed/skabelonpakke-smaa-vandvaerker/
Persondataforordningen træder i kraft d. 25. maj 2018

PowerPoint præsentation er vedhæftet. Referatet er udformet som stikord med reference til nogle af PowerPoint siderne.
Dansks Vandværker har med det uddelte materiale, prøvet at gøre det nemt for vandværkerne. Selve lovgivningsmaterialet er på 1.600 sider og det udleverede materiale er et kommenteret sammendrag. Tekst og skabeloner kan findes på Danske Vandværkers hjemmeside på ovennævnte link.
De 9 skabeloner bliver trin for trin præsenteret og til sidst lidt om generel IT-sikkerhed, som er en forudsætning for at passe på vores elektroniske data.
DVV har lavet en række FAQ. (Ofte stillede spørgsmål med svar).

Ved køb af Bit-rater gennem DVV tilbydes 25% rabat. Programmet sikrer, at kun godkendte programmer kan starte på din PC. Aktiverer du, et medlem i bestyrelsen eller dine ansatte ved en fejl et ondsindet program, f.eks. ved at trykke på et link i en mail, vil Bit-rater forhindre, at programmet starter og dermed beskytte dit og vandværkets IT-system.

PP 4. EU's persondataforordning erstatter den nuværende Persondatalov. Der er meget genbrugt men også skærperede krav til dokumentation og overholdelse.

PP 7. I forbindelse med udbredelse og brug af de sociale medier, de digitale muligheder, er mængden af persondata eksploderet. Forbrugerbeskyttelsen gælder for alle virksomheder, foreninger etc. som indsamler, registrerer, opbevarer og videregiver personoplysninger.

Det gælder både Google, Facebook, det lille vandværk med 25 forbrugere, den lokale idrætsforening og alle der imellem.

PP 8-10. Vi skal være forsigtige med fjernaflæsninger. Fjernaflæsningen kan bruges til at følge forbrugerens adfærd. Vi må ikke videregive informationer uden skriftlig tilladelse.
Ved at kunne få indsigt i husstandens vandforbrug, kan en tyv planlægge besøget i huset med henblik på at stjæle værdier. Vandforbruget kan indikere hvor mange personer der bor i husstanden. Forbruget kan også afsløre, hvis en beboer ikke overnatter i ejendommen.
Økonomioplysninger kan være værdifulde med henblik på kreditvurdering og evnen til at kunne svare enhver sit.
Forbrug af vand pr. time kan fortælle noget om husstandens døgnrytme.

PP 13. Store bøder kan udskrives, fra 25.000 til flere millioner kr.

PP 14. Intelligente vandmålere må løbende aflæses. F.eks. har vi et problem ved årsopgørelse i forbindelse med ejerskifte. Tidligere forbruger må ikke vises. Vi må ikke fremsende materiale til ejendomsmægler uden forbrugerens skriftlige accept / fuldmagt.

PP 16-20. Vi skal udpege en Persondataansvarlig for vandværket. Vandværkets behandling af persondataoplysninger skal dokumenteres. Datatilsynet kan spørge ind til dette dokument.
For at håndtere dataansvarlighed i forhold til eksterne it-leverandører, der behandler persondataoplysninger for os, skal vi benytte en databehandleraftale. Mere herom i kapitel 7.
Ordbog findes bagest i Skabelonsamlingen
DPO Databeskyttelsesrådgiver er ikke nødvendig for et vandværk.

PP 22. Vi skal indskærpe overfor håndværkere, at de har tavspligt. Det må ikke fortælles nede i Brugsen, at nu er der lukket for vandforsyningen til xxx.
Når der er lavet en liste med vandværkets it-systemer, skal vi huske Microsoft Outlook, e-mail, Excel, Word og lign.

PP 24. Ligesom ved risikovurdering ifm. kvalitetssikring, vurderes det samlede risikobillede ud fra sandsynlighed og konsekvens.

PP 25-26. 3. Risiko vurdering. Skabelonen er på forhånd udfyldt med de mest kendte trusler og forbedringsforslag. Det anbefales at skifte password med jævne mellemrum.

PP 27. Persondataforordningen stiller skrappere krav til de informationer, som forbrugere og ansatte giver i forbindelse med behandling af deres personoplysninger. Med en persondatapolitik bliver disse krav overskuelige og lettere at forstå for forbrugerne.
De steder der er markeret med gult, er de ting vi skal være ekstra opmærksomme på.

PP28. IT-sikkerhed. Brug kun en PC med virusbeskyttelse – betalt løsning med daglig opdatering. Undersøg sikkerheden på din router. Er den beskyttet med et langt password? Mange routere kan åbnes og konfigureres med brugernavnet: admin og password: password.

PP30. Det er et krav, at vi ikke giver personoplysninger videre til andre virksomheder og organisationer, uden at vi har styr på de formelle krav til, hvordan data bliver behandlet. Databehandleraftalen er et eksempel på, hvordan vi kan regulere disse forhold, når personoplysninger skal behandles af en underleverandør.
Det er relevant, når vi eksempelvis har data og en server liggende på en hostet it-løsning hos vores it-leverandør, eller hvis vi benytter en ekstern service, hvor vi sender personoplysninger – eksempelvis Nets.

Det er ikke nødvendigt at indgå en databehandleraftale med en leverandør, der bare sælger en licens eller et abonnement, der er installeret lokalt på vandværket (for eksempel Office-pakken), hvis ikke de får adgang til personoplysninger. Men hvis der er den mindste chance for, at en leverandør får adgang til personoplysninger, for eksempel gennem fjernsupport, skal vi indgå en databehandleraftale.
Vi skal indgå en databehandleraftale med hver virksomhed, der behandler personoplysninger på vores vegne.
Vi skal forvente at indgå i dialog med de leverandører, som skal underskrive en databehandleraftale, da de skal forpligte sig til indholdet. Vi kan med fordel benytte datastrømsanalysen fra kapitel 2 til at danne et overblik over hvilke leverandører, vi skal indgå en databehandleraftale med.

PP36. 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
I løbet af 2017 forventes det, at Datatilsynet kommer med en liste over eksempler, hvor DPIA specifikt er krævet samt en opdateret skabelon til formålet.
I skemaet skal du i forbindelse med igangsættelse af det ny it-system besvare 27 spørgsmål. Kan du svare nej til alle disse spørgsmål, behøver du ikke at ændre i din databehandling.

PP38. Computere kan stjæles fra vandværket, fra privaten, fra bilen, under rejse. Nogle gange må politiet kigge langt efter det stjålne – meget langt (og måske findes de aldrig).

HB: Når PC-udstyr med adgang til vandværkets drift eller administration bortkommer, er det som at miste en systemnøgle til virksomheden. Måske sker der slet ikke noget, men alligevel vælger den ansvarlige virksomhedsejer at omstille låsen.

PP 42. **Sådan undgår du phishing**
Phishing er en form for svindel, hvor bagmændene prøver at narre dig til at give dem fortrolige oplysninger. De vil for eksempel gerne have fat i dit navn, adresse, kreditkortnummer, cpr-nummer eller brugernavn og password til Facebook, Gmail og andre populære tjenester.

Du kan undgå phishing ved at bruge din sunde fornuft og lære nogle få ting.
Den typiske phishing-svindel foregår i to faser: E-mail og webside. Først modtager du for eksempel en e-mail. Den ser ud til at komme fra nogen, du har tillid til, for eksempel Skat, din bank eller din uddannelsesinstitution. I mailen får du måske besked om, at der har været misbrug af din konto, og at du er nødt til at bekræfte dine brugeroplysninger. Mailen foreslår, at du gør det på en webside, der er angivet et link til.
Hvis du klikker på linket, kommer du til en forfalsket webside. Den er udformet, så den til forveksling ligner en side fra eksempelvis Skat, banken eller uddannelsesinstitutionen. Siden har en række felter, som du bliver bedt om at udfylde. Når du klikker på OK-knappen, sendes de data du har indtastet til svindlerne, som herefter kan misbruge dem.

For at undgå at blive offer for phishing kan du følge disse råd:

1. Forhold dig skeptisk til e-mails og websteder, der beder om følsomme oplysninger om dig

Du kan i en e-mail blive bedt om at bekræfte dine brugeroplysninger ved at indtaste dem – enten i en vedhæftet fil eller på en webside, som der linkes til. Det er yderst sjældent at legitime afsendere vil bede dig om dette. Din bank, en producent eller en offentlig myndighed vil aldrig vil bede dig om dette.
Selv hvis afsenderen i mailen bruger dit navn eller andre personlige oplysninger om dig, kan der være tale om svindel. For eksempel kan du være udsat for et målrettet angreb, hvor svindlerne har fundet frem til data om dig selv, din organisation og dem, du ofte kommunikerer med og forsøger udnytter den tillid du har til disse personer eller organisationer.

2. Brug forskellige og stærke passwords til hvert websted

Brug ikke det samme password flere steder. Hvis du gør det, skal svindlerne kun have fat i dit password til et enkelt websted for at få adgang til alle de øvrige steder, hvor du også har brugt det.
Brug stærke passwords, det vil sige minimum 8 karakter med både tal, tegn, og store og små bogstaver og specialtegn.
Hvis f.eks. dit webhotel bliver hacket, og hackerne får fat i dit brugernavn og password, vil de straks teste, om samme brugernavn og password også giver adgang til Facebook, Gmail, Hotmail, Dropbox, PayPal, Steam og andre populære tjenester. Benytter du arbejdsrelaterede tjenester, vil hackerne sandsynligvis også prøve at teste dit brugernavn og password dér. Hvis det er svært at huske dine password, findes der password manager løsninger, som kan hjælpe dig med at huske dem (de kan findes via søgemaskine).

3. Hvis du er i tvivl om ægtheden af en mail eller webside, så kontakt afsenderen

Hvis du er i tvivl om en mail er ægte, så ring eller mail til afsenderen. Brug ikke svar-funktionen eller telefonnummer i den mail, du har modtaget – for så ryger dit svar tilbage til svindlerne. Find i stedet selv mailadressen eller telefonnummer via en søgemaskine.

4. Tjek at links til sider med fortrolig information begynder med https

Forbindelser med https er som regel markeret med en hængelås i adressefeltet. Når et link begynder med https, betyder det, at forbindelsen til webstedet er krypteret. Det har to fordele: Dels kan andre ikke umiddelbart aflytte kommunikationen, dels garanterer det, at du kommunikerer med den rette server. Hver server der anvender https, er nemlig udstyret med et digitalt certifikat. Klik på hængelåsikonet i adressefeltet, hvis du vil se certifikatet.

5. Undgå at klikke på links i e-mails. Indtast i stedet selv web-adressen
Links i phishing-mails har til formål at narre dig hen på et forfalsket websted. Ofte er de forklædt, så de ser ud til at føre til det rigtige websted.
Som regel kan du se, hvor et link faktisk fører hen ved at føre musen hen over det uden at klikke på det. Så viser mail-programmets eller browserens statuslinje i bunden af vinduet den web-adresse, linket fører til (bemærk at denne metode ikke virker på tablets og smartphones).
Det mest sikre er slet ikke at klikke på links i e-mails eller på websider, du ikke umiddelbart har tillid til. Indtast i stedet selv web-adressen i browserens adressefelt.
6. Slå to-faktor-autentifikation til
To-faktor-autentifikation giver ekstra beskyttelse af adgangen til dine data. Det består i en yderligere sikring som supplement til dit password. Når et websted bruger to-faktor autentifikation, skal du foruden brugernavn og password indtaste en engangskode. Den kan stå på et nøglekort (for eksempel NemID), blive sendt via sms eller dannes af en særlig app på din mobiltelefon. Fordelen er, at en hacker ikke kan bruge dit brugernavn og password til noget, fordi adgang til dine data også kræver at man har nøglekortet eller din mobiltelefon. Ofte kan du vælge kun at slå to-faktor-autentifikation til, første gang du bruger en bestemt computer. På den måde slipper du for at indtaste den ekstra kode, hver gang du logger ind. En lang række web-tjenester tilbyder to-faktor-autentifikation, for eksempel Gmail, Dropbox, Facebook og Apples og Microsofts webtjenester.

PP49. Solid IT tilbyder at lave dokumentationen for 15.000 kr. til vandværker under 200.000 m3

PP 50. Henrik Blomhøj sluttede med en pep-talk.
Kære vandværker.
Med jeres ni skabeloner og trin for trin guiden, er I nu i stand til at leve op til alle dokumentationskrav vedrørende EU-forordningen, over for myndigheder og jeres forbrugere.
Når I efterfølgende også efterlever alle forholdsregler og anbefalinger som fremgår i skabelonerne, vil i kunne sikre alle vandværkets personhenførbare oplysninger imod spredning og misbrug.
I vil også kunne beskytte vandværkets IT-systemer imod indbrud, hærværk og tab af data.
Kære datatilsyn. Bare kom an. Vi ser frem til jeres besøg.

Sidst men ikke mindst, alle vandværker, små som store, skal registreres på VIRK.DK

Tak til Henrik Blomhøj for et spændende indlæg.

Det blev så tid til at sludre og fornøje sig med gløgg og æbleskiver.

Formanden takkede af for i aften