Formål

Formålet med dette dokument er at dokumentere, at vandværket overholder kravene til behandling af personoplysninger.

Vandværket behandler i minimalt omfang personoplysninger og benytter primært branche it-løsninger til behandlingen. I det følgende dokumenteres persondatabehandlingen samt de tekniske og organisatoriske sikkerhedsforanstaltninger, der er etableret i forbindelse med behandlingen.

Databeskyttelsesrådgiver (DPO)

Behandling af persondata på vandværket udføres som støttefunktion til kerneaktiviteterne og udgør et minimalt omfang. Set i forhold til de risici der er forbundet med behandlingen, følsomheden, samt mængden af personoplysninger, der behandles, vurderer vi, at vandværket ikke skal have en databeskyttelsesrådgiver tilknyttet.

Kontaktoplysninger på persondataansvarlig

Jens Meldhede Mail: sekretaer@rydevand.dk, 26751605

Procedurer i forbindelse med henvendelser fra registrerede

I vandværket håndteres alle henvendelser af det administrative personale. I persondatapolitikken, som alle forbrugere og ansatte er bekendt med, har vi anført vores kontaktoplysninger for disse henvendelser.

De registreredes vigtigste rettigheder efter databeskyttelsesforordningen er:

- Retten til at modtage oplysning om behandling af deres personoplysninger (oplysningspligt).
- Retten til at få indsigt i deres personoplysninger.
- Retten til at få urigtige personoplysninger rettet.
- Retten til at få deres personoplysninger slettet.
- Retten til at gøre indsigelse mod at personoplysninger anvendes til direkte markedsføring.
- Retten til at gøre indsigelse mod automatiske individuelle afgørelser, herunder profilering.
- Retten til at flytte deres personoplysninger (dataportabilitet).

Alle ovenstående rettigheder håndteres manuelt ved henvendelse som anført i persondatapolitikken.

Fortegnelser over behandlingsaktiviteter

Forbrugsafregninger og relaterede aktiviteter

Almindelige personoplysninger med det formål at kunne gennemføre forbrugsafregninger og i øvrigt leve op til vandværkets kontraktlige forpligtelser samt forpligtelser i henhold til vandforsyningsloven og bogføringsloven.

Grundlag for behandlingen

Kontraktlig og retlig forpligtelse samt udførelse af en opgave i samfundets interesse.

Kategorier af registrerede

Forbrugere.

Kategorier af personoplysninger

- Navn, adresse, telefon, e-mail
- Målernumre, forbrugernummer (kundenummer)
- Forbrugsdata der kan henføres til en person

Kategorier af modtagere

Personoplysningerne videregives ikke til nogen udenfor organisationen ud over databehandlere.

Databehandlere

-

Tidsfrister for sletning / opbevaring

Ingen tidsfrister, dog minimum 5 år af hensyn til bogføringsloven.

Risikovurdering

- *Fortrolighed*: Det vurderes, at tab af fortrolighed vil have en minimal indflydelse på de registreredes rettigheder og frihedsrettigheder. Personoplysningerne, der behandles, vil ofte være offentligt tilgængelige – med undtagelse af de detaljerede forbrugsoplysninger fra måleraflæsningerne.
- *Integritet:* Det vurderes, at tab af integritet ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative processer omkring forbrugerafregning, hvorfor både it-systemer og administrative processer i forbindelse med databehandlingen skal beskytte mod tab af integritet.
- *Tilgængelighed:* Det vurderes, at tab af tilgængelighed ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative processer omkring forbrugerafregning, hvorfor både it-systemer, i særdeleshed backup, og administrative processer i forbindelse med databehandlingen skal beskytte mod længerevarende tab af tilgængelighed.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Se sektionen ”Supplerende bemærkninger om generelle organisatoriske og tekniske foranstaltninger”.

Kendte sårbarheder og planlagte forbedringer

Der er på nuværende tidspunkt ikke nogen specifikke, kendte sårbarheder eller planlagte forbedringer.

Almindelige HR aktiviteter - jobansøgninger

Almindelige personoplysninger med det formål at kunne vurdere kandidater til stillingsopslag.

Grundlag for behandlingen

Samtykke.

Kategorier af registrerede

Ansøgere.

Kategorier af personoplysninger

- Navn, adresse, telefon, e-mail
- CV
- Kan indeholde andre personoplysninger, der fremsendes af den registrerede.

Kategorier af modtagere

Personoplysningerne videregives ikke til nogen udenfor organisationen ud over databehandlere.

Databehandlere

- Ingen

Tidsfrister for sletning / opbevaring

Ingen specifikke tidsfrister. Oplysningerne opbevares dog ikke længere, end de er relevante. Slettes senest når stillingen er besat.

Risikovurdering

- *Fortrolighed*: Det vurderes, at tab af fortrolighed vil have en minimal indflydelse på de registreredes rettigheder og frihedsrettigheder. Personoplysningerne, der behandles, er i mange tilfælde offentligt tilgængelige – eksempelvis på ansøgerens LinkedIn profil.
- *Integritet:* Det vurderes, at tab af integritet ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative systemer, der benyttes til andre formål, hvorfor både it-systemer og administrative processer i forbindelse med databehandlingen skal beskytte mod tab af integritet.
- *Tilgængelighed:* Det vurderes, at tab af tilgængelighed ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative systemer, der benyttes til andre formål, hvorfor både it-systemer og administrative processer i forbindelse med databehandlingen skal beskytte mod længerevarende tab af tilgængelighed.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Se sektionen ”Supplerende bemærkninger om generelle organisatoriske og tekniske foranstaltninger”

Kendte sårbarheder og planlagte forbedringer

Der er på nuværende tidspunkt ikke nogen specifikke kendte sårbarheder eller planlagte forbedringer.

Almindelige HR aktiviteter – ansatte mv.

Almindelige og muligvis særlige (følsomme) personoplysninger behandles med det formål at kunne opfylde kontraktlige og lovpligtige ansættelsesretlige krav overfor ansatte og bestyrelsesmedlemmer. Herunder også forpligtelser i forhold til bogføringsloven.

Grundlag for behandlingen

Kontraktlig og retlig forpligtelse.

Kategorier af registrerede

Nuværende og tidligere ansatte samt bestyrelsesmedlemmer.

Kategorier af personoplysninger

- Billede (portræt og fra firmafester)
- Fulde navn og kontaktoplysninger (herunder privat e-mail og privat telefonnummer)
- Adresse
- CPR-nummer
- Bankkontooplysninger
- Lønsedler
- Historik på trækprocent og skattefradrag
- Pensionsoplysninger (*kan indeholde oplysning om fagforening og overenskomst*)
- Flextidsoplysninger
- Korrespondance udvekslet mellem medarbejderen/organisationschefen/cheferne vedrørende specifikke forhold omkring den pågældende medarbejder
- Referater fra MUS-samtaler igennem årene
- Disciplinærsager (advarsler m.v.)
- Refusionsopgørelser vedr. barsel og sygdom
- Straffeattest
- Sygehistorik (herunder sygemeldinger)
- Ansøgning og CV.

Kategorier af modtagere

Personoplysningerne videregives ikke til nogen udenfor organisationen ud over databehandlere.

Databehandlere

- *BlueGarden (lønkørsel)*

Tidsfrister for sletning / opbevaring

Ingen tidsfrister, dog minimum 5 år af hensyn til bogføringsloven.

Risikovurdering

- *Fortrolighed*: Det vurderes, at tab af fortrolighed potentielt kan have negativ indflydelse på de registreredes rettigheder og frihedsrettigheder. Der indføres derfor begrænset adgang samt underskrives tavshedserklæring, før der gives adgang.
- *Integritet:* Det vurderes, at tab af integritet ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative processer omkring lønkørsel mv., hvorfor både it-systemer og administrative processer i forbindelse med databehandlingen skal beskytte mod tab af integritet.
- *Tilgængelighed:* Det vurderes, at tab af tilgængelighed ikke vil have nogen nævneværdig indflydelse på de registreredes rettigheder og frihedsrettigheder. Det kan dog medføre udfordringer med de administrative processer omkring forbrugerafregning, hvorfor både it-systemer, i særdeleshed backup, og administrative processer i forbindelse med databehandlingen skal beskytte mod længerevarende tab af tilgængelighed.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Kun administrative medarbejdere har adgang til disse oplysninger. Det er således kun medarbejdere, hvor det er direkte relevant, der har adgang til personoplysninger om deres kolleger.
Afgrænsningen gælder som hovedregel alle. De grupper der i visse tilfælde har udvidet adgang er: HR-afdelingen, it, bogføring og ledelsen.

Nogle af oplysningerne opbevares desuden fysisk i aflåst skab.

Vandværket har vurderet, at det ikke er muligt at implementere falske/opdigtede navne (pseudonymer) i forbindelse med behandlingen af HR-aktiviteterne, når der skal tages hensyn til det aktuelle tekniske niveau og omkostningerne ved implementering

Se ydermere sektionen "Supplerende bemærkninger om generelle organisatoriske og tekniske foranstaltninger".

Kendte sårbarheder og planlagte forbedringer

Vandværket har et ønske om, senest med udgangen af 2018, at supplere de nuværende tekniske og organisatoriske sikkerhedsforanstaltninger med kryptering af HR-dokumenterne samt en mere detaljeret logning af adgangen til følsomme personoplysninger.

Supplerende bemærkninger om generelle organisatoriske og tekniske foranstaltninger

Vandværket har implementeret følgende organisatoriske og tekniske foranstaltninger generelt:

- Antivirus på alle it-systemer, der behandler personoplysninger.
- Backup af alle it-systemer, der behandler personoplysninger.
- Anvendelse af branchetypiske it-systemer til behandlingsaktiviteterne.
- Adgangsbegrænsning til personoplysninger, så der kun gives adgang, hvor det er nødvendigt.
- Databehandleraftaler med leverandører, der behandler personoplysninger på vandværkets vegne.
- Tavshedserklæringer med personale, der har behov for at behandle personoplysninger
- Vejledning i sikker behandling af personoplysninger og informationsaktiver for personale med adgang til informationssystemer
- Gennemførelse af ovenstående risikovurdering og dokumentation af alle systemer, der behandler personoplysninger. Det for at sikre et oplyst grundlag for sikkerhedsniveauet for persondatabehandlingen i vandværket

Revisionshistorik

Version	Note	Dato	Redigeret af
V1.00	Skabelon tilrettet Ryde Vandværk	03-09-2020	Jens Meldhede

Risikovurdering for vandværker

#	Trussel	Sandsynlighed	Konsekvens	Samlet risikobillede	Forslag til yderligere sikkerhedstiltag for at imødegå de konstaterede trusler
1	Uautoriseret adgang til it-systemer	LAV	LAV	LAV	Undgå at bruge faste passwords. Indfør personlige passwords samt krav til sværhedsgrad og ændring af passwords
2	At en ansat får uretmæssig adgang til fortrolige data	LAV	LAV	ACCEPTABEL	Lav løbende kontrol af, at brugerrettigheder er korrekte. Opsæt logning på adgang til filer med persondata, gennemse log.
3	Fyrede/fratrådte medarbejdere får ikke frataget adgangsrettigheder	LAV	LAV	LAV	Implementer procedurer for nedlukning af tidligere medarbejderes it-adgange
4	Vandværket rammes af et ransomware eller virusangreb	LAV	LAV	LAV	Implementer software, der blokerer trusler proaktivt (før der sker angreb)
5	Samme login og password bruges af flere	LAV	LAV	LAV	Hvis det ikke kan undgås, må logning gøres mere effektiv
6	Datamedier, diske eller dokumenter med fortrolige data bliver stjålet/tabt/glemt, f.eks. under transport	LAV	LAV	LAV	Indfør værktøjer til at slette data på computeren, hvis den mistes. Efterlad aldrig fortroligt materiale i bil, når den forlades
7	Misbrug af anden brugers adgang da der ikke logges ud efter brug af systemet	LAV	LAV	LAV	Indfør automatisk logoff, når computeren har været inaktiv i 5 minutter (pauseskærm)
8	Brugere skifter ikke adgangskode løbende	LAV	LAV	MIDDEL	Indfør passwordpolitik, med jævnlig ændring af passwords. Kontroller at den følges
9	Der er fejl på backup, så data ikke kan genskabes ved datatab eller nedbrud	LAV	LAV	LAV	Test jævnligt om backup virker ved at udføre tests af genoprettelse
10	En medarbejder modtager og aktiverer virus eller trojansk hest via e-mail, browser eller usb-nøgle	LAV	LAV	LAV	Indfør sikkerhedsværktøjer, virusscanning af e-mail osv.
11	Brug af privat computer eller brug af firmacomputer til private formål åbner for misbrug eller hacker/virusangreb	LAV	LAV	LAV	Undlad at gøre brug af privat computer. Brug computer kun til firmaformål
12	En ansat lokkes til at udlevere fortrolig/kritisk information til uvedkommende (social engineering)	LAV	LAV	LAV	Informer medarbejdere, om hvad man skal passe på. Lad fortrolighedserklæringer indgå i ansættelsesaftaler/-kontrakter
13	*Indsæt flere relevante trusler her*				

Intern kontaktliste for vandværket

Kontaktlister

Rolle	Primær/substitut	Navn	Adresse	E-mail	Tlf.
Daglig leder på vandværket	Primær	Karsten Hansen		Pedel@rydevand.dk	23445908
	Substitur	Mads Nielsen		formand@rydevand.dk	24275205
Administrativ medarbejder på vandværket	*Primær*	*Jens Meldhede*		*sekretaer@rydevand.dk*	*26751605*
	Substitut				
Teknisk medarbejder på vandværket	*Primær*	Karsten Hansen		Pedel@rydevand.dk	23445908
Bestyrelsesformand	Primær	Mads Nielsen		formand@rydevand.dk	24275205
Bestyrelsesmedlem	Primær	Torben			

Borbjerg Sparekasse
Bukdalvej 5
Borbjerg 7500 Holstebro
Tlf. 97 46 14 22

RTM A/S
Greve Centervej 90
2670 Greve
Telefon: (+45) 43 53 14 44
Mail: mail@rtm.dk

Nets Denmark
Klausdalsbrovej 601
2750 Ballerup
44 68 44 68

Danske Lønsystemer
Engholm Parkvej 8
3450 Allerød
70 80 60 58

Revisionskontoret Vest Holstebro
Lægårdvej 91C
7500 Holstebro
70 26 66 00

Winko Software
Østrøjel 5
2670 Greve
43 90 28 12

Hjerm Byg
Øster Hjermvej 19
7560 Hjerm
97464511

Haderup-Djeld Smede & VVS
Sevelskovbyvej 2
7830 Vinderup
97 44 80 73

Højvang Laboratorier A/S
Industri Vest 8
4293 Dianalund
Telefon: 58 24 24 58

Poul Thomsen
Nr Bjertvej 1
7830 Vinderup
97 44 10 45

Aura Energi
Skanderborgvej 180
8260 Viby J
87 92 55 55

Vinderup Entreprenørforretning
Toften 24
7830 Vinderup
97 44 12 05

Norlys Energi
Over Bækken 6
9000 Aalborg
70 15 16 70

Salling Kloakservice

Viumvej 20-22
7870 Roslev
97 57 90 04

Tanderups Entreprenørfirma
Øster Hjermvej 23
7830 Vinderup
20 68 60 15

Hvis vandværket ønsker at anvende SOLID-IT som it-driftsleverandør, kan SOLID-IT kontaktes på 7025 6005 med henblik på at lave en aftale om leverance og beredskab. Se evt. mere på http://solidit.dk

Handlingsplaner

Handlingsplan for interne servere og systemer på vandværket

Denne handlingsplan er baseret på interne servere og systemer. Det vil sige systemer, som står på vandværkets adresse, og som vandværket har det fulde driftsansvar for.

Introduktion

For at kunne levere vandforsyning er der vigtige personoplysninger, vi har behov for at behandle. Vores persondatapolitik er ment som en hjælp til at forstå, hvilke data vi indsamler, hvorfor vi indsamler dem, og hvad vi anvender dem til. Dette er vigtige oplysninger, så vi håber, at du vil tage dig tid til at læse dem.

Skulle du have spørgsmål, eller ønsker du yderligere information, er du velkommen til at henvende dig til vores persondataansvarlige:

Kontaktoplysninger på persondataansvarlig

Jens Meldhede sekretaer@rydevand.dk 26751605

Dataansvarlig

Rydevand A.M.B.A , Vester Trabjergvej 17, 7830 Vinderup CVR-nummer 34743622)

Vores behandling af dine personoplysninger

Vi behandler personoplysninger, som du eller en anden part, eksempelvis ejendomsmægler eller udlejer, har udleveret til os i forbindelse med din tilflytning til vandværkets forsyningsområde. Endvidere behandler vi løbende oplysninger om dit forbrug af vand.

Disse personoplysninger behandler vi for at kunne leve op til vores kontraktlige forpligtelser overfor dig i forbindelse med afregning af forbrug samt vores forpligtelser i forbindelse med vandforsyningsloven.

Uden disse oplysninger vil vi ikke kunne forsyne dig med vand.

Typisk drejer det sig om disse personoplysninger:

- Navn, adresse, telefon, e-mail
- Målernumre, forbrugernummer (kundenummer)
- Forbrugsdata der kan henføres til en person

Tidsfrister for sletning/opbevaring

Vi stræber efter at slette (eller anonymisere) personoplysninger, så snart de ikke har nogen relevans. Dog opbevarer vi dem altid i minimum 5 år af hensyn til bogføringsloven. Ofte opbevarer vi forbrugsoplysninger længere af hensyn til statistiske formål, eksempelvis i forbindelse med ejerskifte.

Dine rettigheder efter persondataforordningen

I forbindelse med vores behandling af dine personoplysninger har du adskillige rettigheder:

- Retten til at modtage oplysning om hvordan vi behandler dine personoplysninger (oplysningspligt).
- Retten til at få indsigt i dine personoplysninger.
- Retten til at få urigtige personoplysninger rettet.
- Retten til at få dine personoplysninger slettet.
- Retten til at gøre indsigelse mod at dine personoplysninger anvendes til direkte markedsføring.
- Retten til at gøre indsigelse mod automatiske, individuelle afgørelser, herunder profilering.
- Retten til at flytte dine personoplysninger (dataportabilitet).

Alle ovenstående rettigheder håndteres manuelt ved henvendelse til vores persondataansvarlige.

Vi kan afvise anmodninger, der er urimeligt gentagende, kræver uforholdsmæssig meget teknisk indgriben (f.eks. at udvikle et nyt system eller ændre en eksisterende praksis væsentligt), påvirker beskyttelsen af andres personlige oplysninger, eller noget som vil være ekstremt upraktisk (f.eks. anmodninger om oplysninger der findes som sikkerhedskopier).

Hvis vi kan rette oplysninger, gør vi naturligvis dette gratis, med mindre det kræver en uforholdsmæssig stor indsats. Vi bestræber os på at vedligeholde vores tjenester på en måde, der beskytter oplysninger fra fejlagtig eller skadelig ødelæggelse. Når vi sletter dine personoplysninger fra vores tjenester, er det derfor muligt, at vi ikke altid kan slette tilhørende kopier fra vores arkivservere med det samme, og det er ikke sikkert, at oplysningerne fjernes fra vores sikkerhedskopisystemer.

Du har til hver en tid retten til at klage til Datatilsynet (https://www.datatilsynet.dk/borger/klage-til-datatilsynet/

Oplysninger, som vi videregiver

Vi videregiver ikke personlige oplysninger til virksomheder, organisationer og enkeltpersoner uden for vandværket. Undtagelsen er i disse tilfælde:

- Med dit samtykke
  Vi videregiver personlige oplysninger til virksomheder, organisationer eller enkeltpersoner uden for vandværket, hvis vi har dit samtykke. Vi kræver aktivt tilvalg af videregivelse af alle personoplysninger.

- Til ekstern databehandling
  Vi videregiver personlige oplysninger til vores samarbejdspartnere eller andre betroede virksomheder eller personer, der behandler dem for os. Deres behandling er baseret på vores instrukser og i overensstemmelse med vores privatlivspolitik og andre gældende tiltag til fortrolighed og sikkerhed, eksempelvis vores databehandleraftale.

- Af juridiske årsager
  Vi videregiver personlige oplysninger til virksomheder, organisationer eller enkeltpersoner uden for vandværket, hvis vi i god tro mener, at adgang, brug, bevarelse eller offentliggørelse af oplysningerne er nødvendig for at:

    - Overholde gældende love, bestemmelser, sagsanlæg eller retsgyldige anmodninger fra offentlige myndigheder.
    - Håndhæve gældende servicevilkår, herunder undersøgelse af potentielle overtrædelser.

- Registrere, forhindre eller på anden måde beskytte mod problemer med bedrageri, sikkerhed eller tekniske problemer.
- Holde vandværket fri fra skade, vores medlemmer eller offentlighedens rettigheder, ejendom eller sikkerhed, sådan som det kræves eller tillades i henhold til lovgivningen.

Vi kan dele oplysninger, der ikke identificerer personer, med offentligheden og vores partnere. Vi kan f.eks. dele oplysninger med offentligheden for at vise generelle tendenser om, hvordan vores forbrugeres forbrug fordeler sig.

Informationssikkerhed

Vi arbejder hårdt for at beskytte vandværket og vores forbrugere mod uautoriseret adgang, ændring, offentliggørelse eller ødelæggelse af personoplysninger, som vi lagrer.

Vi har implementeret følgende organisatoriske og tekniske foranstaltninger generelt på vandværket:

- Antivirus på alle it-systemer, der behandler personoplysninger.
- Backup af alle it-systemer, der behandler personoplysninger.
- Anvendelse af branchetypiske it-systemer til behandlingsaktiviteterne.
- Adgangsbegrænsning til personoplysninger, så der kun gives adgang, hvor det er nødvendigt.
- Databehandleraftaler med leverandører, der behandler personoplysninger på vandværkets vegne.
- Tavshedserklæringer med personale, der har behov for at behandle personoplysninger.
- Vejledning i sikker behandling af personoplysninger og informationsaktiver for personale med adgang til informationssystemer.
- Gennemførelse af ovenstående risikovurdering og dokumentation af alle systemer der behandler personoplysninger for at sikre et oplyst grundlag for sikkerhedsniveauet for persondatabehandlingen i vandværket.

Overholdelse og samarbejde med tilsynsmyndigheder

Vi gennemgår regelmæssigt, at vi overholder vores egen persondatapolitik. Vi overholder også adskillige selvregulerende sikkerhedspolitikker. Når vi modtager formelle skriftlige klager, kontakter vi afsenderen for at følge op på klagen. Vi samarbejder med de relevante lovgivende myndigheder, f.eks. Datatilsynet, om at løse klager om overførsel af personlige data, som vi ikke kan løse direkte med vores brugere.

Ændringer

Vores privatlivspolitik kan ændres fra tid til anden. Vi begrænser ikke dine rettigheder i henhold til denne privatlivspolitik uden dit udtrykkelige samtykke. Eventuelle ændringer af denne privatlivspolitik angives på denne side, og hvis der sker væsentlige ændringer, vil vi gøre opmærksom på dem på en mere iøjnefaldende måde (for visse tjenester oplyser vi bl.a. om ændringer via e-mail).

Revisionshistorik

Version	Note	Dato	Redigeret af
V0.9	Første udkast til skabelon	13. marts 2017	Tor Valstrøm
V1.00	Tilrettet Ryde vandværk AMBA	04-10-2020	Jens Meldhede

Introduktion

Denne it-sikkerhedspolitik, som er besluttet af bestyrelsen, udgør den overordnede ramme for at opretholde it-sikkerheden hos Ryde vandværk AMBA. Hermed ønsker vandværket at demonstrere sin seriøse holdning til at skabe sikkerhed for persondata, systemer og andre it-aktiver

Hensigten er at lægge et fundament, så kritiske og fortrolige informationer og systemer kan bevare deres fortrolighed, integritet og tilgængelighed.

Der bliver fokuseret på de vigtigste krav i EU's generelle persondataforordning samt på relevante krav i de internationale it-sikkerhedsstandarder ISO 27001 og 27002.

Formål

Idet brugen af it anses for at være en meget vigtig forudsætning for vandværkets eksistens, vil det være nødvendigt at sikre vandværkets it-ressourcer (data, software, hardware og kommunikationsforbindelser).

Derfor vil vi etablere og vedligeholde en afbalanceret it-sikkerhed, som i denne sammenhæng omfatter alle nødvendige organisatoriske, fysiske og tekniske sikkerhedsforanstaltninger.

It-ressourcerne skal med andre ord beskyttes mod misbrug, manipulation, ødelæggelse og tab, samt mod at blive fejlbehæftede. Beskyttelsen skal virke mod alle former for trusler, interne eller eksterne, hændelige eller bevidste.

Databehandleraftale

Mellem

Ryde vandværk AMBA Vester Trabjergvej 17

7830 Vinderup

CVR-nr. 34743622

Herefter kaldet: Dataansvarlig

Og

<databehandlers navn, adresse og CVR nr> (vi skal have kigget på hvem der er data behandler)

Herefter kaldet: Databehandler

er der d.d. indgået følgende databehandleraftale.

§ 1: Baggrund, formål og definitioner

1.1 Denne databehandleraftale (herefter kaldet "Aftalen") vedrører <system eller projekt>.

1.2 Formålet med indgåelsen af Aftalen er at sikre, at Dataansvarlig og Databehandler lever op til de krav, der er til it-sikkerhed og behandling af persondata i gældende lovgivning.

1.3 I denne aftale skal anvendes samme definitioner som beskrevet i Artikel 4 i EU's forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger 2016/679 (i det følgende kaldet Persondataforordningen), eksempelvis:

- "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,

Konsekvensanalyse – DPIA

Introduktion til gennemførsel af DPIA

Nedenfor er der 27 spørgsmål, som du skal besvare kort og præcist. Når du besvarer et spørgsmål, skal du vurdere, om dit svar giver anledning til, at du bør ændre den måde, du udfører databehandling på.

Det overordnede spørgsmål for alle de 27 spørgsmål er:

Kan du gøre databehandlingen mere sikker for de personer, der indgår i din databehandling? (forbrugere, ansatte og bestyrelsen)

Projekt	
Dato	
Godkendt af	
Udfyldt af	

Oplysninger om oplysninger

1. Hvilke oplysninger er det, som du indsamler eller behandler?

   Helt konkret hvilke oplysninger er der tale om? Eksempelvis navne, varenumre, adresser, kunder nummer, koordinater, e-mail adresser, cvr-numre, priser, osv.

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

2. Er disse oplysninger om fysiske personer?

   Relaterer oplysningerne sig på nogen måde til fysiske enkeltpersoner? Eksempelvis navne, e-mail adresser, telefonnumre, kundenumre og cpr-numre. Hvis oplysningerne ikke omhandler fysiske personer, så skal der **ikke** laves en konsekvensanalyse. Dvs. oplysninger om ting, steder, hændelser, osv. (spørgsmålet gælder også for enkeltmandsfirmaer)

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

3. Kan enkeltpersoner blive identificeret ud fra oplysningerne? Hvis ja, hvordan?

   Kan personer blive genkendt ud fra oplysningerne, du behandler? Dette gælder også, selvom oplysningerne ikke direkte afslører, hvilke personer oplysningerne omhandler? Eksempelvis et

navn, foto, et identifikationsnummer, GPS-information eller oplysninger, der er særlige for denne fysiske person, og som derved kan afsløre personens identitet?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

4. Er disse oplysninger af følsom karakter?

Handler de personoplysninger, som du behandler om personernes race, etnicitet, politisk/religiøs/filosofisk overbevisning, fagforeningsmæssige forhold, helbredsforhold, seksuelle forhold, strafbare forhold eller om genetiske data?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

Formålet

5. Hvordan vil du behandle personoplysningerne?

Hvad skal der ske med personoplysningerne? Vil der eksempelvis ske en indsamling, registrering, redigering, beregning, sammenstilling, videregivelse, læsning, opbevaring, sletning, osv.?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

6. Hvad er formålet med at behandle personoplysningerne?

Hvorfor skal personoplysningerne behandles? Et eksempel kan være, at man opbevarer kundeoplysninger, så man kan fakturere sine kunder.

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

7. Er personoplysningerne nødvendige for at opnå formålet, eller kan man undlade at behandle personoplysningerne og stadig opnå formålet?

   Er der nogen anden mulighed, hvorpå du kan løse opgaven uden at behandle personoplysningerne?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

8. Vil personoplysningerne kun blive brugt til det formål, de er indsamlet til?

   Er det kun det formål, som personoplysningerne er indsamlet til, som de vil blive brugt til? Eller vil personoplysningerne også blive brugt til noget andet som eksempelvis reklame via e-mail?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

9. Er der en risiko for, at personoplysningerne kan eller vil blive brugt til noget andet end det formål, de er indsamlet til?

   Er der en risiko for, at oplysningerne på et eller andet tidspunkt vil blive brugt til noget andet end det, de var tiltænkt? Eksempelvis at sende reklamer ud til kunder.

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

Adgangen til oplysningerne

10. Hvem er den dataansvarlige?

    Hvem er den fysiske person eller organisation, som har ansvaret for behandlingen af personoplysningerne, og som afgør til hvilket formål og på hvilke måde, der må foretages behandling af oplysningerne?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

11. Hvem har mulighed for at se, redigere, fjerne, osv. personoplysningerne?
Hvem har adgang til personoplysningerne?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

12. Er der en risiko for, at personoplysningerne kan falde i uvedkommendes hænder?

Er der en risiko for, at uvedkommende kan få fat i oplysningerne? Bliver persondata eksempelvis sendt med e-mail, uden at de er krypteret?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

Selve behandlingen

13. Hvad skal der ske med personoplysningerne, efter de er blevet indsamlet, og indtil behandlingen af oplysningerne er afsluttet?

Hvad skal der helt konkret ske med personoplysningerne fra start til slut? Med start menes fra det tidspunkt, de er blevet registreret, og med slut menes, til behandlingen er færdig, og til at der ikke længere er brug for personoplysningerne.

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

Opbevaringen

14. Hvordan bliver personoplysningerne opbevaret?

Bliver personoplysningerne opbevaret fysisk i et arkiv, på et kontor, i en computer, i skyen (cloud computing) eller andet?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

15. Er teknologien, der anvendes til at opbevare personoplysninger, designet til at håndtere personoplysninger?

Er teknologien specielt fremstillet til at kunne opbevare personoplysninger? Eksempelvis er e-boks fremstillet til at kunne håndtere personoplysninger, hvorimod Microsoft Office ikke er designet til at håndtere personoplysninger.

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

16. Er den teknologi, der anvendes til at behandle personoplysningerne, sikkerhedstestet?

Er teknologien (eksempelvis programmet eller computeren), som behandler personoplysningerne, testet mod eksempelvis hacking og fejl?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

17. Bliver den teknologi, som anvendes, jævnligt sikkerhedsopdateret?

Igangsættes der ofte enten manuelle eller automatiske opdateringer af systemerne, så systemerne altid er sikret bedst muligt? Eksempelvis udsender Microsoft automatiske sikkerhedsopdateringer hver måned.

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

Sikkerheden

18. Hvis personoplysningerne kommer til uvedkommendes kendskab, vil det så kunne skade de berørte personer?

Hvis personoplysningerne skulle blive spredt til uvedkommende, ville der så kunne ske en økonomisk, fysisk, renommemæssig eller lignende skade for de berørte personer?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

19. Kan der ske utiltænkte ændringer eller tilintetgørelse af personoplysningerne?

Kan der eksempelvis ved et uheld/fejl blive slettet oplysninger, eller kan der utilsigtet blive ændret i oplysningerne?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

20. Er der et sikkerhedsteam/organisation eller lignende, som skal sørge for, at personoplysningerne er sikret korrekt?

Er der en bestemt gruppe personer som tjekker, at personoplysningerne bliver opbevaret og behandlet sikkert?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

21. Er der en procedure, som sikrer, at der periodisk bliver foretaget sikkerhedsrisikoanalyser i hele virksomheden/organisationen?

Har virksomheden, organisationen eller lignende en bestemt procedure, som sikrer, at sikkerheden for personoplysningerne bliver vurderet i hele virksomheden?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

Den registreredes muligheder

22. Kan personen, hvis personoplysninger bliver behandlet, få indsigt i behandlingen af sine oplysninger?

Har den person, hvis personoplysninger bliver behandlet, mulighed for selv at se en oversigt over hvilke informationer, der er registreret, og hvad de bliver brugt til?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

23. Blev personen, hvis oplysninger bliver behandlet, orienteret om behandlingen af personoplysningerne, før oplysningerne blev indsamlet?

Fik personen fortalt, inden oplysningerne blev indsamlet, at de ville blive registreret og behandlet?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

24. Har personen mulighed for at give sit samtykke til, at dennes personoplysninger bliver behandlet?

Har personen, hvis personoplysninger bliver behandlet, mulighed for at godkende, at deres oplysninger bliver behandlet? Enten skriftligt eller mundtligt.

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

25. Har personen mulighed for at afvise, at dennes personoplysninger bliver behandlet?

Har personen, hvis oplysninger bliver behandlet, mulighed for at frabede sig at dennes personoplysninger bliver behandlet?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

26. Er der en fast procedure for, at personen, hvis oplysninger bliver behandlet, kan trække sit samtykke for behandling af personoplysninger tilbage?

Har virksomheden, organisationen eller lignende en bestemt procedure for at imødekomme en persons ønske om at trække sit samtykke til behandling af oplysninger tilbage?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

Efter behandlingen

27. Hvad sker der med personoplysningerne efter behandlingen af disse?

Hvad skal der ske med oplysningerne, efter formålet med indsamlingen af dem er opnået og efter den færdige behandling? Skal de eksempelvis slettes eller anonymiseres, eller bliver de stående i et register eller lignende?

Begrund:
Giver dit svar anledning til, at du bør ændre din databehandling? Ja ☐ Nej ☐

Resultat

Nu har du udfyldt din konsekvensanalyse DPIA. Hvis du har svaret "ja" til ét eller flere spørgsmål, bør du lave en handlingsplan, som er med til at sikre, at I får behandlet punktet på en god måde.

Husk, at ajourføre handlingsplaner og konsekvensanalysen ved ændringer.

En handlingsplan bør som minimum indeholde følgende:

Navn på plan:

- Ansvarlig:
- Dato for udførelse:
- Dato for forventet afslutning:
- Ressourcer:
- Godkendt af:
- Tiltag:
- Modforanstaltning:
- Løsning:

Kilde: http://www.risikoanalyser.dk/konsekvensanalyse-dpia.html

Ordbog og eksempler

Ordbog

Backup
Dublering af data som gemmes på et eksternt medie, eller via nettet på en ekstern server.

Databehandler
Er en ekstern leverandør, som på vandværkets vegne anvender data, der tilhører vandværket.

Dataejer
Typisk vandværket selv, som har indsamlet forbruger-, drifts- og ledningsdata.

Dataportabilitet
Overførelse af data fra ét vandværk til et andet. Hvis forbrugeren flytter, kan forbrugeren kræve sine data overført til det nye vandværk.

Dataansvarlig
Den person på vandværket, som er ansvarlig for vandværkets indsamling, håndtering og opbevaring af data.
Ser også under "Funktionsadskillelse".

Dekryptering
En metode, som gør en e-mail eller lign. læsbar for den modtager, der har den rigtige software og den rigtige kode.

DPIA
Data Protection Impact Assessment = konsekvensanalyse. Hvilken betydning vil en given hændelse have for dit vandværk, og fordrer det, at foranstaltninger, som forstærket it-sikkerhed, ekstra uddannelse eller ekstern automatisk backup, skal iværksættes.

DPO
Data Protection Officer eller Databeskyttelsesrådgiver. Offentlige myndigheder og enkelte private virksomheder skal udpege en person, som skal understøtte, at den dataansvarlige overholder reglerne i forordningen. Vandforsyninger skal normalt ikke have en DPO.

Funktionsadskillelse
En bestyrelsesformand må ikke både kunne beslutte, bestille, betale, godkende og bogføre et eventuelt køb. Funktionerne skal adskilles således at mistanke om misbrug og interessekonflikter kan udgås. I forbindelse med funktionsadskillelse, gives herunder et bud på, hvem der kan have hvilke roller i vandværket/vandforsyningen.

Rolle	Lille vandværk	Mellem vandværk	Stort Vandværk	Meget stort vandværk
Antal ansatte	Ingen	1 – 2	3 – 10	>10
Ledelse	Bestyrelsen	Bestyrelsen	Bestyrelsen	Direktionen
Daglig leder	Formand	Formand	Driftsbestyrer	Direktør
It-ansvarlig	Kasserer / It-konsulent	Driftsbestyrer / It-konsulent	Administrativ medarbejde	Administrativ / It- medarbejde

Hardware
Fysiske komponenter som f.eks. computer, skærm, tastatur, mus tablet, og bærbar pc.

Hosted it-løsning
Betyder at programmer og data, der anvendes til f.eks. forbrugeradministration, ikke befinder sig på vandværkets adresse, men i stedet tilgås via internettet. Hvis it-udstyret på vandværket lider fysisk overlast eller bliver stjålet, vil vandværkets data fortsat være tilgængelige.

HR-aktivitet
Human Resource er udtryk for virksomhedens eller organisationens personale.

Integritet
Hæderlighed, ærlighed, uafhængighed. Sammenhængen imellem det, I på vandværket siger, at I gør, og det, som I rent faktisk gør.

It-ressourcer
Data, software, hardware og kommunikationsforbindelser.

Konfiguration
Kan i it-sammenhæng oversættes til "Opsætning". At indstille et program eller en computer til en bestemt type opgave, for eksempel at komme på internettet eller sende/modtage mail.

Kryptering
En metode som gør for eksempel en e-mail ulæselig for andre end den modtager, der har den rigtige software og den rigtige kode.

Malware
En sammentrækning af de engelske ord malicious software, som svarer til et ondsindet program. Programmet kan, når/hvis det aktiveres, skade andre programmer og hardware.

Mindre vandværker
Betegnelsen mindre vandværker anvendes typisk, når der faktureres < 200.000 m3/år eller om vandværker uden fast ansat personale.

Nøgleadministration
Håndtering og opbevaring af krypteringsnøglen, som er en kode, der anvendes ved kryptering og dekryptering af data.

Personoplysninger
Enhver form for informationer, der direkte eller indirekte kan identificere en fysiske nulevende eller afdød person.

Pseudonymisering
Pseudonymisering er ikke det samme som anonymisering. Ved pseudonymisering kan en ejer eller en forbrugsadresse erstattes af en kode, så sammenkobling med en afregningsmåler kan ske, uden at identiteten på personen afsløres.

Ransomware
Ondsindet program, som typisk låser tilgangen til vandværkets datafiler. Kun ved at betale en løsesum (Ransom = løsesum), kan datafilerne blive frigivet.

Restore
Genskabelse (af data). Det modsatte af backup. Er en filmappe blevet slettet, kan denne med en restore-funktion genskabes med et minimum at datatab til følge. Restore kan også ske ved indlæsning af en backup fra et usb-stik, en cd eller fra en ekstern server.

Risikovurdering
En vurdering, der sammenholder risikoen for, at en hændelse indtræffer, og den konsekvens, hændelsen i så fald måtte få for vandværket.

Selvregulerende sikkerhedspolitikker
Skabelonen ”it-sikkerhedspolitik for Xyz Vandværk” er et eksempel på en selvregulerende sikkerhedspolitik. Vandværket udarbejder, udvikler og efterprøver selv sikkerhedspolitikken.

Sikkerhedsbrud
Indtrængning i vandværkets it-systemer eller tyveri af data. Hvis der sker brud på sikkerheden, skal vandværket indberette det til Datatilsynet.

Software
Elektroniske programfiler, der anvendes til styring af alle it-programmer.

Systemejer
Ejeren af f.eks. et styrings- eller forbrugeradministrationssystem, som vandværket har købt en licens til at anvende.

Tredjemand
Juridisk udtryk for den, der står uden for et aftaleforhold.

Vandværkets juridiske informationer
Vandværkets navn, adresse, postnummer, by og CVR-nummer.

VPN-forbindelse
En krypteret og sikker forbindelse imellem den enkelte pc og en pc på en anden lokation. Forbindelsen skabes via et softwareprogram og kan kun anvendes ved brug af korrekt adgangskode.

Eksempler

Ledelsens udmelding om de overordnede mål og principper

Eksempel 1

En accepteret størrelse kan for eksempel være en tidskrævende genetablering af data i form af indkøring af backup og tab af få og på anden måde tilgængelige data. Det er normalt aldrig acceptabelt, hvis vandværket mister store datamængder uden mulighed for umiddelbart at kunne reetablere dem.

Det er også uacceptabelt, hvis forbrugere, medarbejdere eller samarbejdspartneres fortrolige data kan kompromitteres.

Vigtige grundprincipper for sikkerhedsarbejdet

Funktionsadskillelse

Eksempel 1

Programmer og dokumenter er i denne sammenhæng vandværkers ressourcer. Kun driftspersonale og enkelte nøglepersoner skal normalt have adgang til vandværkets SRO-system og programmer til ledningsregistrering. Det er også kun regnskabsføreren og/eller kassereren, der skal have adgang til forbrugerafregning, indkomne mails fra forbrugerne samt løn og ansættelsesforhold.

Eksempel 2

Adgang til mapper og programmer tildeles eller begrænses til hver enkelt medarbejder eller bestyrelsesmedlem. Det er en forudsætning, at hver enkelt bruger har sit eget login. En it-konsulent kan eventuelt hjælpe med denne opsætning, men planen for systemadgang skal fastlægges af driftslederen eller bestyrelsen.

Styring af sikkerhedshændelser

Eksempel 3

Vurdering sker ved at følge meddelelser og opdateringer fra systemleverandøren f.eks. Microsoft, Rambøll eller lignende. Sikkerheden kan trues, hvis en hacker har fundet et ”hul” i adgangen til leverandørens system, så han/hun kan tilgå data og foretage ændringer, steder hvor f.eks. regnskabsføreren kun har adgang via sin adgangskode.

Eksempel 4

Risikobilledet udtrykker den generelle bekymring for, om en uautoriseret adgang til vandværkets it-system kan finde sted. En ændring i vandværkets skema til risikovurdering kan være konsekvensen af et midlertidigt eller permanent ændret risikobillede.

Dokumentation

Eksempel 5

En væsentlig sikkerhedsaktivitet er at skifte adgangskoder jævnligt. Opdatering og opgradering af it-programmer som eksempelvis Windows eller Rambøll Fas er også en væsentlig sikkerhedsaktivitet. I

beskrivelsen af proceduren nævnes de enkelte aktiviteter, tidsplan for udførelsen, og hvem, der er ansvarlig for opgaven. Tidsplan for revidering af proceduren beskrives også.

Sikkerhed i forbindelse med outsourcing.

Eksempel 6

Brug Danske Vandværkers skabelon til en databehandleraftale.

Hovedpunkterne i regelsættet/retningslinjerne er:

Punkt 4: Styring af aktiver

Eksempel 7

For at undgå at data falder i de forkerte hænder, kan det være nødvendigt at ødelægge it-udstyr eller dele af dette. Eksempelvis harddisken inden den bortskaffes. USB-nøgler og CD'er skal også ødelægges inden de bortskaffes. Hvis I blot sletter indholdet på en harddisk eller en USB-nøgle, kan det reetableres.

Punkt 5: Adgangsstyring

Eksempel 8

System- og dataejer er programleverandøren (f.eks. Rambøll) og vandværket.

Punkt 8: Driftssikkerhed

Eksempel 9

En sikkerhedsforanstaltning kan eksempelvis være installation af et whitelist-program, der sikrer, at pirat-programmer ikke kan gøre skade. Kombineres dette med et antivirusprogram, eksempelvis fra Microsoft, kan farlige programmer også slettes. Hvis programmerne indstilles til automatisk opdatering, vil ovenstående foregå uden, at it-brugeren bemærker det i dagligdagen.

Eksempel 10

En teknisk sårbarhed kan eksempelvis være anvendelse af trådløst netværk på vandværket, fjernkommunikation med en privat medarbejder pc, eller fjernstyring af drift og administration i forbindelse med support. De sårbare punkter og forholdsreglerne, der træffes, skal beskrives og med jævne mellemrum revideres.

Punkt 11: Leverandørforhold

Eksempel 11

Ved fjernbetjening anvender medarbejderen hos leverandøren en pc, der kan udgøre en sikkerhedsrisiko, hvis den ikke som minimum overholder vandværkets egne regler for it-sikkerhedspolitik.

Punkt 12: Styring af brud på informationssikkerhed

Eksempel 12

Kommunikation om sikkerhedstruende hændelser og svagheder indebærer eksempelvis, at medarbejdere giver besked til ledelsen, hvis de modtager potentielt farlige e-mails, også selvom det ikke har medført et sikkerhedsbrud. Der skal også kommunikeres til ledelsen, hvis uvedkommende har uhindret adgang til software på vandværket.

Punkt 13: Beredskabsstyring m.m.

Eksempel 13

Hvordan kan eksempelvis forbrugerdata, som blandt andet indeholder oplysninger om måleraflæsning til brug for årsafregning, genskabes eller tilvejebringes inden udsendelse af årsopgørelse