# Målrettet arbejde med databeskyttelsesforordningen for Xyz Vandværk

***Sådan bruger du dokumentet***

*Afsnittet her, markeret med grønt, skal I slette, når I tager det i brug på vandværket.*

**Baggrund**: Dokumentets indhold er baseret på interviews med vandværkerne i Lørslev, Strib og Birkerød.

Intentionen med denne skabelon er, at udarbejde den nødvendige dokumentation, så I kan overholde de vigtigste krav i persondataforordningen. Med få justeringer bør de fleste mindre og mellemstore vandværker kunne opnå dette.

Nogle steder i skabelonen er markeret med gult. Det er de områder, der kræver størst fokus. Det er dog vigtigt, at I gennemlæser hele dokumentet kritisk og redigerer, så det, der står, afspejler jeres vandværks individuelle behandling af persondata.

Hvis I ikke allerede har gjort det, **skal I implementere** de organisatoriske og tekniske foranstaltninger, der er beskrevet i dokumentet. I modsat fald skal I opdatere dokumentet, så det afspejler den nuværende situation på vandværket, og områderne med ”kendte sårbarheder og planlagte forbedringer” skal opdateres med de tiltag, I tænker at indføre for at styrke sikkerheden.

Indholdsfortegnelse

[Formål 4](#_Toc477080807)

[Kontaktoplysninger på persondataansvarlig 4](#_Toc477080808)

[Procedurer i forbindelse med henvendelser fra registrerede 4](#_Toc477080809)

[Fortegnelser over behandlingsaktiviteter 5](#_Toc477080810)

[Forbrugsafregninger og relaterede aktiviteter 5](#_Toc477080811)

[Grundlag for behandlingen 5](#_Toc477080812)

[Kategorier af registrerede 5](#_Toc477080813)

[Kategorier af personoplysninger 5](#_Toc477080814)

[Kategorier af modtagere 5](#_Toc477080815)

[Databehandlere 5](#_Toc477080816)

[Tidsfrister for sletning / opbevaring 5](#_Toc477080817)

[Risikovurdering 5](#_Toc477080818)

[Tekniske og organisatoriske sikkerhedsforanstaltninger 5](#_Toc477080819)

[Kendte sårbarheder og planlagte forbedringer 5](#_Toc477080820)

[Almindelige HR aktiviteter 6](#_Toc477080821)

[Grundlag for behandlingen 6](#_Toc477080822)

[Kategorier af registrerede 7](#_Toc477080823)

[Kategorier af personoplysninger 7](#_Toc477080824)

[Kategorier af modtagere 7](#_Toc477080825)

[Databehandlere 7](#_Toc477080826)

[Tidsfrister for sletning / opbevaring 7](#_Toc477080827)

[Risikovurdering 7](#_Toc477080828)

[Tekniske og organisatoriske sikkerhedsforanstaltninger 7](#_Toc477080829)

[Kendte sårbarheder og planlagte forbedringer 8](#_Toc477080830)

[Supplerende bemærkninger om generelle organisatoriske og tekniske foranstaltninger 8](#_Toc477080831)

[Revisionshistorik 9](#_Toc477080832)

[Referencer 9](#_Toc477080833)

**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**

Fornavn, efternavn, telefon, e-mail

**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*

* GDPR Art.6(1)(b): Kontraktlig forpligtelse.
* GDPR Art.6(1)(c): Retlig forpligtelse.
* GDPR Art.6(1)(e): Udførelse af en opgave i samfundets interesse.

*Kategorier af registrerede*

* Forbrugere.

*Kategorier af personoplysninger*

* Navn, adresse og evt. opkrævningsadresse samt eventuelle kontaktoplysninger.
* Målernumre, Forbrugernummer (kundenummer.)
* Forbrugsdata der kan henføres til en person/husstand.

*Kategorier af modtagere og evt. tredjelande*

Vi videregiver ikke personlige oplysninger til eksterne virksomheder, organisationer og enkeltpersoner, undtagen i disse tilfælde:

1. Til afregning af vandafledningsafgift

Vi videregiver én gang om året, forbrugerens samlede forbrugsvolumen til det lokale forsyningsselskab der står for opkrævning af vandafledningsafgiften jfr. ”Miljøstyrelsens betænkning om principper for beregning af vandafledningsbidrag”, forbrugeren behøver derfor ikke indberette dette selv - med mindre der er korrektioner fra bimålere vedr. forbrug, der er undtaget fra vandafledningsafgift – dette skal forbrugeren selv indberette.

1. Med forbrugerens samtykke.

Vi videregiver personlige oplysninger til virksomheder, organisationer eller enkeltpersoner, hvis vi har forbrugerens samtykke og ønske herom. Vi kræver aktivt tilvalg af videregivelse af alle personoplysninger.

Dette kan eksempelvis være når forbrugeren tilmelder sig betaling via NETS/Betalingsservice eller når forbrugeren skal sælge din bolig og vi fra ejendomsmægler modtager en anmodning om oplysning af det historiske forbrug til brug for salgsopstillingen.

1. Til ekstern databehandling.

Vi videregiver (”overlader”) personlige oplysninger til vores samarbejdspartnere eller andre betroede virksomheder eller personer, der behandler dem for os baseret på vores instrukser og i overensstemmelse med vores persondatapolitik og andre gældende tiltag til fortrolighed og sikkerhed, fx vores databehandleraftale.

1. Af juridiske årsager, fx til vores advokat, revisor eller myndigheder vi pålægges at udlevere oplysningerne til.

*Personoplysningerne overføres ikke til tredjelande.*

*IT systemer til understøttelse af behandlingsformål*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Fagsystem** | **Personoplysninger** | **Dataejer** | **Placering** | **Backup** | **Databehandler** |
| Rambøll FAS | Navn, Adresse, Telefon, Email, Målernumre, Forbrugernummer (kundenummer), Forbrugsdata historisk | Regnskabsansvarlig | På lokal server | Backup tages månedligt og opbevares krypteret hos Rambøll | Rambøll |
| NETS betalingsservice | Navn, Adresse, Telefon, Email, Målernumre, Forbrugernummer (kundenummer), Forbrugsvolumen | Regnskabsansvarlig | Hos NETS som er selvstændigt dataansvarlig | Stamdata er i Rambøll FAS og NETS tager selv backup af deres | Ingen |
| Kamstrup READy | Forbrugsdata og målernumre | Driftschef | Hos Kamstrup | Tages af Kamstrup og overføres til Rambøll FAS | Kamstrup |
| ebutler.dk | Forbrugsdata og målernumre samt adresse | Driftschef | Hos Kamstrup | Tages af Kamstrup og overføres til Rambøll FAS | Kamstrup |

*Databehandlere*

* Rambøll (fjernbackup af Rambøll FAS)
* Kamstrup (”READy” og ebutler.dk måleraflæsning)

*Tidsfrister for sletning / opbevaring*

Vi sletter / anonymiserer oplysningerne X måneder/år efter fraflytning, dog opbevares oplysninger der medfører økonomiske transaktioner altid 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, som kun i ganske særlige tilfælde vil kunne gøre skade på forbrugeren.
* *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*

* GDPR Art.6(1)(a): 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 og evt. tredjelande*

Personoplysningerne videregives ikke til nogen udenfor organisationen ud over databehandlere.

*Personoplysningerne overføres ikke til tredjelande.*

*IT systemer til understøttelse af behandlingsformål*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Fagsystem** | **Personoplysninger** | **Dataejer** | **Placering** | **Backup** | **Databehandler** |
| Email | Som nævnt ovenfor | Driftschef | Hosted hos Rambøll | Backup tages af Rambøll | Rambøll |

*Databehandlere*

* Rambøll (email hosting)

*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 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*

* GDPR Art.6(1)(b): Kontraktlig forpligtelse (ansættelseskontrakt samt evt. kollektive overenskomster).
* GDPR Art.6(1)(c): Retlig forpligtelse.
* Databeskyttelseslovens § 12.

*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 og evt. tredjelande*

Personoplysningerne videregives ikke til nogen udenfor organisationen ud over databehandlere samt som pålagt ved lov (fx indberetning til Skattestyrelsen) og til de organisationer der er indgået aftaler med på vegne af medarbejderne (fx pensionsselskab) eller af administrative årsager (fx NETS Overførselsservice.

*Personoplysningerne overføres ikke til tredjelande.*

*IT systemer til understøttelse af behandlingsformål*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Fagsystem** | **Personoplysninger** | **Dataejer** | **Placering** | **Backup** | **Databehandler** |
| Email | Som nævnt ovenfor | Driftschef | Hosted hos Rambøll | Backup tages af Rambøll | Rambøll |
| Aflåst arkivskab til udskrevne dokumenter | Som nævnt ovenfor | Driftschef | På kontoret hos driftschefen | Der tages ikke backup af de udskrevne dokumenter, men de opbevares i et aflåst brandsikkert skab. | Ingen |
| Bluegarden | Som nævnt ovenfor | Regnskabsansvarlig | Hos Bluegarden | Tages af Bluegarden | Bluegarden |

*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

V0.9 Første udkast til skabelon 13. marts 2017 Tor Valstrøm

V0.91 Revideret skabelon 21. maj 2019 Tor Valstrøm

V1.00 Skabelon tilrettet Xyz Vandværk xx-xx-xxxx x x

**Referencer**

Dokumentet indeholder elementer og inspiration fra følgende:

1. Datatilsynets “12 spørgsmål som dataansvarlige allerede nu med fordel kan forholde sig til”.
2. EU forordning 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger (”Persondataforordningen”).
3. Focus Advokaters ”Sådan bliver din virksomhed klar til at håndtere persondata efter de nye regler”.
4. Bird & Bird ”Guide til den nye Persondataforordning”.
5. DI’s skabelon for Privacy Impact Assessment.
6. ISO/IEC 27002:2013 Information Technology — Security Techniques — Code of practice for Information Security Management <http://www.iso.org>
7. Information Security Forum (ISF) – Standard of Good Practice for Information Security (SOGP) 2011 <https://www.securityforum.org/>