Sorø Forsyning A/S

Politik for persondatasikkerhed.

Version 1

Gældende fra 25. maj 2018.

Indhold

Forord og læsevejledning

Denne politik for behandling af persondata imødekommer databeskyttelseslovens krav om, at vi skal beskytte fysiske personers oplysninger.
Politikken er formuleret og udformet, så den kan udleveres eller offentliggøres fx på Sorø Forsynings hjemmeside.
Ved offentliggørelse af politikken på hjemmesiden sikres gennemsigtighed for de registrerede kunder og ansatte.
Oplysninger, der ikke må offentliggøres, da en offentliggørelse kan true persondatasikkerheden, er samlet i bilag. Det drejer sig om detaljerede oplysninger om gennemført risikoanalyse samt gennemgang af den fysiske sikring af persondata.
Oplysninger om indgåede databehandleraftaler ajourføres i Sorø Forsynings dokumenthåndteringssystem, DokuNote og ajourføres ikke i nærværende politik.

Personoplysningerne er den enkelte persons ejendom, og vi låner disse oplysninger for at kunne overholde lovgivningen og for at kunne drive vores virksomhed.
Det giver god mening, at vi skal passe på de oplysninger vi låner, og at vi kun må bruge oplysningerne til det formål, vi har lånt dem til. Vi må naturligvis heller ikke videregive det, vi har lånt til andre uden at indhente tilladelse til det.
Når vi ikke længere har brug for oplysningerne, skal vi slette disse.
Den registrerede person kan kræve oplyst hvilke personoplysninger vi har og kræve disse fejlrettet eller slettet, og vi skal imødekomme dette krav, hvis ikke det strider mod anden lovgivning.
Endelig kan den registrerede kræve, at vi overfører de persondata vi har til en anden.
Det er nogle af de væsentlige forhold, der er fastlagt i databeskyttelsesloven og databeskyttelsesforordningen, men med mange flere ord.

Nærværende politik er opbygget med stærk inspiration fra ISO 9001, kvalitetsstandarden, og er inddelt i 9 kapitler.

Kapitel 1	Baggrund og anvendte betegnelser
Kapitel 2	Politik for behandling af personoplysninger i Sorø Forsyning
Kapitel 3	databeskyttelseslovens og databeskyttelsesforordningens mange ord er reduceret til konkrete krav
Kapitel 4	Organisation, ansvar og beføjelser
Kapitel 5	Beskrivelse af hvordan vi behandler persondata i Sorø Forsyning
Kapitel 6	Gennemgang af hvordan vi i Sorø Forsyning overholder krav som oplistet i kapitel 3
Kapitel 7	Risikoanalyse i forhold til personoplysninger
Kapitel 8	Input til udvikling af politikken. Rammevilkår kan ændres over tid, eller vi kan have overset forhold, der bør indarbejdes. Derfor er det forudsat, at politikken skal udvikles og forbedres løbende.
Kapitel 9	Ledelsens evaluering af politikken foretages hvert år, på baggrund af de input der er modtaget.

1.0 Baggrund for indførelse af politik for behandling af persondata.

Regler for behandling af personoplysninger er fastlagt i:

- Lov nr. xx af xx/xx/2018 ” Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven). Lovforslag vedtaget ved 3. behandling 17. maj 2018, afventer offentliggørelsen med lov nummer.

- Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, (Databeskyttelsesforordningen).
  Bilag 1 til databeskyttelsesloven.

1.1 Anvendte betegnelser.

Databeskyttelsesforordningens betegnelser er oplistet i uddrag herunder.

1.1.1 Personoplysninger.

Personoplysninger er enhver form for information om en identificeret eller identificerbar fysisk person (Den registrerede)

1.1.2 Behandling af personoplysninger.

Behandling af personoplysninger er enhver aktivitet eller række af aktiviteter, med eller uden brug af automatisk behandling, som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

1.1.3 Den dataansvarlige.

Den dataansvarlige er en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

1.1.4 Databehandler.

Databehandler er en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne.

1.1.5 Datamodtager.

Datamodtager er en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, hvortil personoplysninger videregives, uanset om det er en tredjemand eller ej.

1.1.6 Tredjemand.

Tredjemand er en anden fysisk eller juridisk person, offentlig myndighed eller institution eller ethvert andet organ end den registrerede, den dataansvarlige, databehandleren og de personer under den dataansvarliges eller databehandlerens direkte myndighed, der er beføjet til at behandle personoplysninger.

1.1.7 Samtykke.

Samtykke fra den registrerede er enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling.

2.0 Politik for behandling af persondata i Sorø Forsyning.

Sorø Forsyning koncernen opererer som forsyningsselskab, hvis kerneaktivitet er vandforsyning og spildevandsforsyning samt tømningsordning.
Nærværende "politik for persondatasikkerhed" er gældende for hele koncernen, der i det følgende betegnes Sorø Forsyning.

2.1 Forankring af Politik for persondatasikkerhed i Sorø Forsyning.

Forud for udarbejdelse af nærværende politik er især ansatte i administrationen orienteret om EU´s databeskyttelsesforordning.
Ved udarbejdelse af nærværende politik, er der afholdt workshops for det administrative personale

- Workshop 1, 11.10.2017, hvordan behandler vi persondata
- Workshop 2, 25.10.2017, gennemgang af krav til behandling af persondata
- Workshop 3, 25.10. og 14.11.2017, opfølgning på kravgennemgang.
- Workshop 4, 29.11.2017, Risikoanalyse.

Med baggrund i disse tilbagemeldinger blev der udarbejdet udkast til politik.

Efterfølgende er udvalgte administrative medarbejdere blevet interviewet i forhold til egen praksis og viden.
Resultatet af disse interviews er indarbejdet i den endelige politik.

Den høje grad af inddragelse har sikret, at politikken indledningsvist er kendt i organisationen.

Fremadrettet sikrer udvalget for informationssikkerhed at der gives orientering og at der sikres inddragelse ved revisioner af politikken.

3.0 Krav.

Databeskyttelsesloven og Databeskyttelsesforordningen er gennemgået og reduceret til konkrete krav relevante for Sorø Forsyning. Der er henvisning til Databeskyttelsesloven og Databeskyttelsesforordningen, hvor den fulde tekst kan læses.
Disse krav er oplistet i dette kapitel.

3.1 Krav til politik for behandling af persondata.

3.1.1 Krav om sikker håndtering af persondata.

Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med Databeskyttelsesforordningen. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.

Hvis det står i rimeligt forhold til behandlingsaktiviteter, skal den dataansvarlige implementere en passende databeskyttelsespolitik. (Databeskyttelsesforordningen artikel 24)

Den dataansvarlige gennemfører passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles (Databeskyttelse gennem design).

(Databeskyttelsesforordningen artikel 25)

3.1.2 Principper for behandling af personoplysninger.

1.Personoplysninger skal:

a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.

b) indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål.

c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

d) være korrekte og om nødvendigt ajourførte.

e) opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det er nødvendigt til formålet.

f) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse.

(Databeskyttelsesforordningen artikel 5)

3.1.3 Krav i forbindelse med ekstern databehandler.

Hvis en behandling skal foretages på vegne af en dataansvarlig, benytter den dataansvarlige udelukkende databehandlere, der kan stille de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandling opfylder kravene i denne forordning og sikrer beskyttelse af den registreredes rettigheder. (Databeskyttelsesforordningen artikel 28, 1)

En databehandlers behandling skal være reguleret af en kontrakt eller et andet retligt dokument i henhold til EU- retten eller medlemsstaternes nationale ret, der er bindende for databehandleren med hensyn til den dataansvarlige, der fastsætter genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder. (Databeskyttelsesforordningen artikel 28, 3)

Databehandleren og enhver, der udfører arbejde for den dataansvarlige eller databehandleren, og som har adgang til personoplysninger, behandler kun disse oplysninger efter instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-retten eller medlemsstaternes nationale ret. (Databeskyttelsesforordningen artikel 29)

3.1.4 Krav om medarbejderes autorisation til behandling af persondata.

Den dataansvarlige gennemfører passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles (Databeskyttelse gennem design).

(Databeskyttelsesforordningen artikel 25)

3.2 Krav for overholdelse af persondatasikkerhed.

3.2.1 Krav om samtykke til behandling at personoplysninger.

Hvis behandling er baseret på samtykke, skal den dataansvarlige kunne påvise, at den registrerede har givet samtykke til behandling af sine personoplysninger (Databeskyttelsesforordningen Artikel *7,* 1.).

Ved behandling af personoplysninger ud over hvad der er nødvendigt i et ansættelsesforhold eller et normalt kundeforhold, skal der forinden indhentes en skriftlig samtykkeerklæring.

3.2.2 Formålsbestemthed.

Indsamling af personlige oplysninger skal ske med udtrykkeligt angivne og legitime formål, (databeskyttelsesloven §5).

3.2.3 Proportionalitet.

Oplysningerne skal være relevante og tilstrækkelige, og må ikke omfatte mere end nødvendigt, (Databeskyttelsesforordningen Artikel 5 1.c.).

3.2.4 Datakvalitet

Der skal foretages fornøden ajourføring og kontrol, og urigtige/vildledende oplysninger skal slettes/rettes. (Databeskyttelsesforordningen Artikel 5 1.d.).

3.2.5 Opbevaring.

Personoplysninger skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles. (Databeskyttelsesforordningen *Artikel 5* 1. e).

3.2.6 Sletning

Den registrerede har ret til at få personoplysninger om sig selv slettet af den dataansvarlige uden unødig forsinkelse, og den dataansvarlige har pligt til at slette personoplysninger uden unødig forsinkelse, hvis et af følgende forhold gør sig gældende:

- Personoplysningerne er ikke længere nødvendige til at opfylde de formål, hvortil de blev indsamlet.
- Den registrerede trækker samtykke tilbage eller gør indsigelse mod behandlingen, og der foreligger ikke legitime grunde til behandlingen.
- Personoplysningerne er blevet behandlet ulovligt.

(Databeskyttelsesforordningen Artikel 17)

Hvis formålene med en dataansvarliges behandling af personoplysninger ikke kræver eller ikke længere kræver, at den registrerede kan identificeres af den dataansvarlige, er den dataansvarlige ikke forpligtet til at beholde, indhente eller behandle yderligere oplysninger for at kunne identificere den registrerede alene med det formål at overholde denne forordning.
(Databeskyttelsesforordningen Artikel 11, 1.)

3.2.7 Oplysningspligt.

Den dataansvarlige skal give den registrerede følgende oplysninger senest én måned efter personoplysningerne er indsamlet:

- Identitet på og kontaktoplysninger på den dataansvarlige
- Kontaktoplysninger på en eventuel databeskyttelsesrådgiver
- Formålene med den behandling, som personoplysningerne skal bruges til
- Retsgrundlaget for behandlingen
- De berørte kategorier af personoplysninger
- Eventuelle modtagere eller kategorier af modtagere af personoplysningerne
- Det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum
- Retten til at anmode den dataansvarlige om indsigt i og berigtigelse eller sletning af personoplysninger eller begrænsning af behandling vedrørende den registrerede og til at gøre indsigelse mod behandling samt retten til dataportabilitet.
- Retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af behandling, der er baseret på samtykke, inden tilbagetrækning heraf
- Retten til at indgive en klage til en tilsynsmyndighed
- Hvilken kilde personoplysningerne hidrører fra og eventuelt, hvorvidt de stammer fra offentligt tilgængelige kilder

(Databeskyttelsesforordningen Artikel 13 og 14)

3.2.8 Der registreredes indsigtsret

Enhver, også ikke-registrerede, har på anmodning ret til at få at vide, om der behandles oplysninger om vedkommende
På begæring skal den registrerede desuden have oplysning om:

- Formålene med behandlingen
- De berørte kategorier af personoplysninger
- De modtagere eller kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, navnlig modtagere i tredjelande eller internationale organisationer
- Muligt det påtænkte tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til fastlæggelse af dette tidsrum
- Retten til at anmode den dataansvarlige om berigtigelse eller sletning af personoplysninger eller begrænsning af behandling af personoplysninger vedrørende den registrerede eller til at gøre indsigelse mod en sådan behandling
- Retten til at indgive en klage til en tilsynsmyndighed
- Enhver tilgængelig information om, hvorfra personoplysningerne stammer, hvis de ikke indsamles hos den registrerede

(Databeskyttelsesforordningen Artikel 15)

Oplysninger skal gives uden unødig forsinkelse, og i alle tilfælde senest én måned efter anmodningen er modtaget.

Fremsendelse af disse oplysninger er som udgangspunkt gratis.
Hvis anmodningen er åbenbar grundløs eller overdreven, kan der opkræves gebyr, eller anmodning kan afvises.
(Databeskyttelsesforordningen Artikel 12, 5)

3.2.9 Indsigelse

Den registrerede har ret til at få urigtige personoplysninger om sig selv berigtiget af den dataansvarlige uden unødig forsinkelse. Den registrerede har under hensyntagen til formålene med behandlingen ret til at få fuldstændiggjort ufuldstændige personoplysninger, bl.a. ved at fremlægge en supplerende erklæring
(Databeskyttelsesforordningen Artikel 16).

3.2.10 Anmeldelsespligt

Der skal i visse tilfælde ske anmeldelse til Datatilsynet og indhentes tilladelse inden oplysninger behandles i følgende tilfælde:

- Med henblik på at advare andre mod forretningsforbindelser med eller ansættelsesforhold til en registreret (advarselsregister),
- Med henblik på erhvervsmæssig videregivelse af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed (kreditoplysningsbureau)
- Behandlinger af personoplysninger om
    - Race eller etnisk oprindelse
    - Politisk, religiøs eller filosofisk overbevisning
    - Fagforeningsmæssigt tilhørsforhold
    - Genetiske data, biometriske data
    - Helbredsoplysninger
    - Seksuelle forhold eller seksuelle orientering

(Datatilsynets nyhedsbrev af 09.04.18 samt databeskyttelsesforordningens artikel 9, stk. 1)

3.2.11 Anmeldelse af brud på persondatasikkerheden.

Ved brud på persondatasikkerheden anmelder den dataansvarlige uden unødig forsinkelse og om muligt senest 72 timer efter, at denne er blevet bekendt med det til Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
Foretages anmeldelsen til tilsynsmyndigheden ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen.
(Databeskyttelsesforordningen Artikel 33).

Anmeldelsen skal ske elektronisk via Virk.dk, og skal som minimum indeholde følgende oplysninger:

- Beskrive karakteren af bruddet på persondatasikkerheden mv.
- Angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
- Beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
- Beskrive de foranstaltninger, som du har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

(Datatilsynets vejledning, Brud på persondatasikkerheden)

3.2.12 Underretning om brud på persondatasikkerheden til den registrerede.

Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter den dataansvarlige uden unødig forsinkelse den registrerede om bruddet på persondatasikkerheden.
(Databeskyttelsesforordningen Artikel 34).

3.2.13 Dataportabilitet

Den registrerede har ret til i et struktureret, almindeligt anvendt og maskinlæsbart format at modtage personoplysninger om sig selv, som vedkommende har givet til en dataansvarlig og har ret til at transmittere disse oplysninger til en anden dataansvarlig.
(Databeskyttelsesforordningen Artikel 20)

3.2.14 Krav til uddannelse

Der er ikke formuleret krav til uddannelse, men det er en forudsætning, at ansatte, der behandler persondata har modtaget den fornødne instruktion og kender og følger nærværende politik.

3.3 Kundekrav for overholdelse af persondatasikkerheden.

Der er endnu ikke modtaget eller formuleret generelle eller specifikke kundekrav for overholdelse af persondatasikkerheden.

3.4 Ejerkrav for overholdelse af persondatasikkerheden.

Der er ikke formuleret supplerende krav fra Sorø kommune som ejer. Tvært imod har Sorø kommune i Ejerstrategien fastlagt at vand- og spildevandsforsyning drives på en effektiv måde, der er gennemsigtig for forbrugerne.

4.0 Organisation, ansvar og beføjelser.

4.1 Sorø Forsynings øverste ledelse.

Bestyrelsen i Sorø Forsyning A/S, samt bestyrelserne i Sorø Vand A/S, Sorø Spildevand A/S og Sorø Forsyningsservice A/S udgør den øverste ledelse, og har det overordnede ansvar for overholdelse af lovgivning, herunder Persondatabeskyttelsesforordningen. Bestyrelserne har gennem en direktørinstruks overladt den daglige ledelse til direktøren for selskaberne.

4.2 Den daglige ledelse.

Sorø Forsynings daglige ledelse varetages af selskabernes direktør.
Den daglige ledelse har det overordnede ansvar for IT-sikkerheden og har uddelegeret det daglige ansvar for IT-sikkerheden til udvalget for informationssikkerhed.

4.3 Data Protection Officer (DPO)

Sorø Forsyning har ikke udpeget en ekstern Data Protection Officer (DPO), da kerneaktiviteten ikke er behandling af persondata.

4.4 Udvalget for informationssikkerhed

Udvalget for IT-sikkerhed består af:

- Direktør
- Driftsleder
- Økonomichef
- Intern IT ansvarlig i Sorø Forsyningsservice

Funktionsadskillelse er det bærende kontrolprincip såvel på person- som på organisationsniveau.
Der er indført kompenserende kontroller, hvor dette ikke er praktisk eller økonomisk hensigtsmæssigt.

Udvalget for informationssikkerhed er normgivende og fastsætter, på grundlag af den vedtagne IT—sikkerhedspolitik, alle interne IT-retningslinjer.
Sorø Forsyning har outsourcet det daglige ansvar for IT-sikkerhed ved Hosted serverløsning hos Progressive A/S og med programmer fra Elbek & Vejrup A/S mfl.

Der er indgået Databehandleraftaler med Progressive A/S og Elbek & Vejrup A/S Klare roller og en præcis placering af ansvar fremgår heraf.

Udvalget for informationssikkerhed har ansvar for:

- At Politik for persondatasikkerhed og de regler, der er relevante i forhold til den enkeltes ansvarsområde, er kendte.
- At vurdere om politikken efterleves.
- At politikken gennemgås min. én gang årligt på P-med.
- At der ved installation af nye systemer gennemføres en forudgående sikkerheds- og risikovurdering.
- At sikre introduktion af nye medarbejdere

- At rolle-ID rettigheder løbende vurdering,
- At medarbejderes og andre aktørers rettigheder slettes ved fratrædelse eller ophør af aftale.
- At der af de dataansvarlige foretages opfølgning og rapportering af sikkerhedsbrud til udvalget for informationssikkerhed.
- At kritiske situationer vurderes straks de registreres.
- At foretage eventuelle anmeldelser til Datatilsynet, mfl.
- At samle og behandle input til udvikling af politikken, herunder ændret lovgrundlag.
- At ajourføre risikovurderingen.
- At der inden udgangen af 2018 udarbejdes en plan for sletning af persondata indsamlet før 25. maj 2018.

Herudover behandler udvalget alle sikkerhedsspørgsmål af principiel karakter, ligesom den kvartalsvis vurderer de hændelser, der er forekommet, og om der er behov for at tage yderligere forebyggende tiltag internt hos Sorø Forsyning.

4.5 Medarbejdere.

Den enkelte medarbejder har ansvar for:

1. At overholde Sorø Forsyning IT-politik som beskrevet i Personalehåndbogen.
2. At kende og overholde nærværende politik for persondatasikkerhed.
3. At slette eller makulere egne udskifter indeholdende persondata straks de ikke længere tjener et formål.
4. At sikre, at udskrifter med persondata ikke ligger fremme, så uvedkommende får lejlighed til at se dem i og udenfor arbejdstiden.
5. At rapportere om eventuelle sikkerhedsbrud eller mistanke herom til nærmeste chef og til udvalget for informationssikkerhed.
6. At persondata modtaget pr. mail arkiveres i DokuNote og slettes i outlook

Den enkelte medarbejder har beføjelse til:
At behandle persondata data i det omfang det er en forudsætning for varetagelse af den ansattes arbejdsopgaver.

Den enkelte medarbejder har ikke beføjelse til:
At indsamle persondata der ikke en forudsætning for varetagelse af den ansattes arbejdsopgaver.
At behandle indsamlede persondata til andet formål en det de er indsamlet til.

4.6 Databehandlere.

Den enkelte databehandlers ansvar og beføjelser er nærmere beskrevet i databehandleraftalen.
Databehandleraftaler arkiveres i DokuNote, hvorfra der kan dannes en ajourført liste over databehandleraftaler.
Databehandleraftalen kan udformes som et tillæg til aktuel aftale.

5.0 Beskrivelse af behandling af persondata i Sorø Forsyning.

For kunder der modtager drikkevand fra Sorø Vand A/S, som afleder spildevand til Sorø Spildevand A/S eller som er omfattet af tømningsordningen, behandler Sorø Forsyning persondata i det omfang det er en forudsætning for kundeforholdet.
Desuden behandler Sorø Forsyning persondata for borgere, hvor Sorø Forsyning på vegne af Sorø kommune opkræver drikkevandsafgift for vand fra egen brønd eller statsafgift for ejendomme med egen spildevandsløsning. I det følgende er disse borgere indeholdt i beskrivelsen for kunder, selvom der ikke er tale om et kundeforhold.

Sorø Forsyning behandler persondata for ansatte i det omfang det er en forudsætning for et ansættelsesforhold.

Behandlingen er nærmere beskrevet i nedenstående afsnit.

5.1 Persondata der behandles i Sorø Forsyning.

5.1.1 Persondata der behandles for personale.

- Ansøgning og CV (uddannelse, eksamensoplysninger, tidligere beskæftigelse)
- Identifikationsoplysninger (navn, adresse, e-mailadresse, tlf.nr)
- CPR-nummer.
- Kørekortoplysninger.
- Familieforhold
    - Navn og fødselsdato for hjemmeboende børn under 7 år, aht. afholdelse af barns første sygedag.
    - Kontaktoplysning om nærmeste pårørende, der kan kontaktes ved en eventuel arbejdsulykke (Frivilligt at oplyse)
- Fagforening
- Arbejdstider, fravær, sygedage
- Bankkontonummer
- Skatteoplysninger
- Oplysninger om helbredsforhold, men kun i det omfang det for den enkelte har betydning om ansættelsesvilkår fx skånejob og/eller lønrefusion fx § 56 refusion.

5.1.2 Persondata der behandles for kandidater som forbrugerrepræsentanter til bestyrelserne.

Ved bekræftelse af kandidatur til valg som forbrugerrepræsentanter til bestyrelserne i Sorø Vand A/S og Sorø Spildevand A/S skal kandidaten afgive følgende oplysninger på oplysningsblanket:

- Navn
- CPR-nummer
- Adresse.
- Telefonnumre
- E-mailadresse.

5.1.3 Persondata der behandles for kunder.

- Identifikationsoplysninger (navn, adresse, e-mailadresse, tlf.nr)
- Ejerskab til ejendomme.
- CPR-nummer.
- Bankkontonummer.

Sorø Forsyning modtager i konkrete tilfælde oplysning fra Sorø kommune om, at husejer er økonomisk trængt, og derfor er berettiget til at modtage tilbud på afdragsordning til kloaktilslutningsbidrag samt nødvendigt kloak arbejde på privat grund.

5.1.4 Persondata der ikke behandles i Sorø Forsyning.

Nedenstående persondata er følsomme oplysninger, der forudsætter udtrykkeligt samtykke forud for en behandling (Persondataforordningen §7).
Disse persondata behandles ikke i Sorø Forsyning.

- Racemæssig eller etnisk baggrund
- Politisk, religiøs eller filosofisk overbevisning
- Seksuelle forhold
- Væsentlige sociale problemer.
- Personlighedstest i forbindelse med ansættelser.
- Straffeattest.

5.1.5 Data der ikke betragtes som persondata i Sorø Forsyning.

Der kan være tvivl om afgrænsningen mellem persondata og andre data. Derfor er det valgt at opliste data, der ikke betragtes som persondata i Sorø Forsyning fordi oplysningerne ikke knytter sig til en identificeret eller identificerbar fysisk person, men til en ejendom eller til en husstand.

- Ejendomsnummer er en ejendomsoplysning, og er derfor ikke en persondata.
- Vandmålernummer er en ejendomsoplysning, og er derfor ikke en persondata.
- Installationsnummer er en ejendomsoplysning, og er derfor ikke en persondata.
- Vandforsyningsforhold er en ejendomsoplysning, og er derfor ikke en persondata.
- Spildevandsforhold er en ejendomsoplysning, og er derfor ikke en persondata.
- Vandmåleraflæsning er en ejendomsoplysning, og er derfor ikke en persondata.
- Vandforbrug /afledt spildevandsmængde er en oplysning, der omfatter hele husstanden, og er derfor ikke en persondata.
- Fotos taget af huse og haver forud for et gravearbejde som dokumentation af tilstanden før arbejdet, er en ejendomsoplysning, og er derfor ikke en persondata.

5.2 Indsamling og kvalitetssikring af persondata.

5.2.1 Indsamling og kvalitetssikring af persondata om ansatte.

- Skatteoplysninger downloades elektronisk fra SKAT og indlæses i lønsystemet, og kvalitetssikres derfor ikke yderligt.
- Kørekortsoplysninger indhentes ved ansættelse ved ansøgers forevisning af originalt kørekort. Fortsat besiddelse af kørekort kontrolleres én gang årligt.
- Arbejdstider, fravær og sygedage indtastes af ansatte i KLIK modulet i økonomisystemet. Korrekt timetal kontrolleres af teamleder eller udpeget administrativ medarbejder før registreringen bogføres i Navision og derefter overføres til lønsystemet.
- Eventuelle oplysninger om helbredsforhold, der har betydning for ansættelsesvilkår indhentes hos den ansattes bopælskommune og kvalitetssikres ikke.

Følgende oplysninger leveres af ansatte, og kvalitetssikres som udgangspunkt ikke.

- Ansøgning og CV (uddannelse, eksamensoplysninger, tidligere beskæftigelse) fremsendes af ansøger.
- Identifikationsoplysninger (navn, adresse, e-mailadresse, tlf.nr)
- CPR-nummer
- Navn og fødselsdato for hjemmeboende børn under 7 år.
- Kontaktoplysning om nærmeste pårørende.
- Fagforening.
- Bankkontonummer.
-

5.2.2 Indsamling og kvalitetssikring af persondata om kunder.

- Identifikationsoplysninger (navn, adresse, e-mailadresse, tlf.nr), kan indsamles på forskellig måde.
    - Oplysninger leveres af direkte af kunden og kontrolleres ikke.
    - Oplysninger om lejere med kundeforhold oplyses af udlejer og kontrolleres ikke.
- Oplysninger om ejerskab til ejendomme, kan indsamles på forskellig måde.
    - Oplysninger leveres af direkte af kunden kvalitetssikres ved opslag i tinglysning/OIS.
    - Oplysninger leveret af advokat eller ejendomsmægler kontrolleres ikke.
    - Oplysninger indhentes af databehandler, fx vandværk eller BlueIdea kvalitetssikres ikke.

- Oplysninger om kundes CPR-nummer, kan indsamles på forskellig måde.
    - CPR-nummer leveres skriftligt af kunden, kvalitetssikres via Modulus 11 i økonomisystemet.
    - CPR-nummer oplyst telefonisk af kunden, kvalitetssikres via Modulus 11 i økonomisystemet.
    - CPR-nummer indberettet af kunden via kundeportalen, kvalitetssikres via Modulus 11 i kundeportalen. Ukorrekt CPR-nummer kan ikke indberettes.
- Bankkontonummer leveres skriftligt af kunden og kvalitetssikres ikke.

5.3 Opbevaring af data

Alle personoplysninger opbevares elektronisk på Sorø Forsynings hostede server.

Følgende originale papirdokumenter indeholdende personoplysninger opbevares.

- Samtykkeerklæringer for behandling af personoplysninger, opbevares i Sorø Forsynings boks.
- Skadesløsbreve, i forbindelse med lån til kunder, opbevares i Sorø Forsynings boks.
- Gældsbrev, vedrørende lån til kunder, opbevares i Sorø Forsynings boks.
- Stamoplysninger for ansatte opbevares i aflåst skab.
-

Følgende personoplysninger synkroniseres desuden elektronisk med firmatelefoner og iPads udenfor hosted server.

- Outlooks kontaktoplysninger.
- E-mails der kan indeholde personoplysninger.

5.4 Behandling af persondata

5.4.1 Behandling af persondata for ansatte.

Indsamlede persondata om ansatte indtastes i økonomisystemets personalemodul hvor data systematiseres, og opbevares.
Ændringer i persondata tilrettes i økonomisystemets personalemodul.

5.4.2 Behandling af persondata for kunder.

Indsamlede persondata om kunder indtastes i økonomisystemets opkrævningsmodul EV-ITA hvor data systematiseres, og opbevares.
Ændringer i persondata tilrettes i økonomisystemets opkrævningsmodul EV-ITA.

Som forberedelse af fjernaflæsninger af vandmålere dannes en standard fil fra økonomisystemets opkrævningsmodul EV-ITA.
Da filen efterfølgende skal gemmes på lokalt C drev, bliver alle navne slettet, før filen videresendes.

5.5 Anvendelse af persondata

5.5.1 Anvendelse af persondata for ansatte.

Persondata for ansatte samkøres med ansattes tidsregistrering i økonomisystemets KLIK modul til brug for beregning af løn og til anden løn- og personaleadministration, herunder ferieregnskab mv.
Persondata herunder lønoplysninger for ansatte benyttes desuden til følgende:

- Lovpligtige indberetninger
- Ved kontakt til ansattes fagforening.
- Ved kontakt til den ansattes hjemkommune.

Behandlingen er lovlig, da behandlingen er nødvendig for at overholde en retslig forpligtigelse, som påhviler Sorø Forsyning som arbejdsgiver.
(jf. Databeskyttelsesforordningen Artikel 6, c)

5.5.2 Anvendelse af persondata for kunder.

Persondata for kunder samkøres med oplysninger om bopælens afløbsforhold, vandforsyningsforhold, og registrerede vandmåleraflæsninger i økonomisystemets opkrævningsmodul EV-ITA, til beregning af opkrævninger.
Persondata for kunder benyttes desuden til følgende:

- Etablering af afdragsordning.
- Etablering af lån til kloaktilslutning.
- Tilbagebetalinger via nem konto.
- Kontakt til SKAT for inddrivelse af fordringer.

Behandlingen er lovlig, da behandlingen er nødvendig for at overholde en kontrakt indgået mellem kunder og Sorø Forsyning som forsyningsvirksomhed.
(jf. Databeskyttelsesforordningen Artikel 6, b)

5.6 Videregivelse af persondata

Persondata videregives som udgangspunkt kun som en del af Sorø Forsynings drift og administration, herunder overholdelse af gældende lovkrav.

Persondata videregives desuden kun i følgende oplistede tilfælde.

5.6.1 Videregivelse af persondata til visse private vandværker.

Der er indgået aftale med en del private vandværker om udveksling af vandmåleraflæsninger.
Som et element i disse aftaler, skal hver aftalepart videregive oplysninger om ejerskifte, i den kvalitet og i det omfang disse oplysninger kan samles til aftale partens eget formål.
Oplysninger om ejerskifte der videregives til private vandværker er:

- Ejendommens adresse
- Sælgers navn og nye adresse, hvis denne er kendt.
- Købers navn.
- Dato for købers overtagelse af ejendommen.
- Måleraflæsning for flytteafregning, hvis denne er modtaget.

5.6.2 Videregivelse af persondata i forbindelse med anmeldelser om lovbrud.

Ved anmeldelse af lovbrud til politi videregives persondata om den eller de anmeldte personer, samt eventuelle vidner, i det omfang disse oplysninger er tilgængelige.

5.6.3 Videregivelse af persondata på baggrund af krav om aktindsigt.

For ansatte gives der aktindsigt i følgende personoplysninger:

- Navn
- Stilling
- Uddannelse
- Arbejdsopgaver
- Lønmæssige forhold
- Tjenesterejser.

For chefer desuden:

- Oplysninger om disciplinære reaktioner indenfor de seneste 2 år.

For direktør desuden:

- Kontrakt.

Den ansatte skal orienteres om hvem, der har ønsket aktindsigt, og hvilke oplysninger der skal gives.
Der gives IKKE aktindsigt i private forhold, herunder CPR-nummer og privatadresse.

5.6.4 Videregivelse af persondata til tilknyttede rådgivere og konsulenter.

I forbindelse med tilknyttede rådgiveres og konsulenters opgaveløsning for Sorø Forsyning, kan det være en forudsætning for opgaveløsningen, at de modtager visse persondata.
Følgende oplysninger kan videregives til rådgivere og konsulenter, uden at der udarbejdes en særskilt databehandleraftale:

- Ejendommens adresse
- Beboers navn.
- Ejers navn og adresse, hvis denne er kendt.

5.6.5 Videregivelse af persondata til Sorø kommune.

I forbindelse men kontrol af ejendommes afløbsforhold udveksles lister med Sorø kommune for gensidig kvalitetssikring og opfølgning, hvor listerne kan indeholde følgende oplysninger:

- Ejendomsnummer.
- Matrikelnummer.
- Ejendommenes adresser
- Ejers navn
- Afløbsforhold.

5.7 Sletning af persondata.

5.7.1 Sletning af persondata indsamlet før 25. maj 2018.

Udvalget for informationssikkerhed skal inden udgangen af 2018 udarbejde en plan for sletning af persondata indsamlet før 25. maj 2018.
Planen skal omfatte:

- Metode til sortering/vurdering af hvilke data, der ikke har et formål og derfor skal slettes.
- Metoder til at slette disse data.

- Persondata på papir og i elektronisk form.
- Tids- og handleplan for sletningen.
- Kontrolforanstaltninger for at sikre, at sletningen er sket.

5.7.2 Sletning af persondata på papir.

Indhold fra vore papirkurve og affaldsposen i printerrummet bortskaffes som almindeligt affald. Derfor må papirkurve kun benyttes til papirer med ikke personfølsomme oplysninger fx reklamer, udregninger skitser mm.

Alle dokumenter på papir, der indeholder oplysninger, der kan identificere en person, skal makuleres af den, der har benyttet dokumenterne, når de ikke skal bruges længere.

Blanketter med personoplysninger på forbrugerkandidater til bestyrelsen, der ikke blev valgt makuleres ved ophør af klagefristen for det afholdte valg.

Blanketter med personoplysninger på forbrugerkandidater til bestyrelsen der blev valgt som suppleanter indscannes til DokuNote, og makuleres ved ophør af klagefristen for det afholdte valg.

Blanketter med personoplysninger for forbrugerkandidater der blev valgt til bestyrelsen makuleres, når oplysningerne er indtastet i lønadministrationsmodulet.

5.7.3 Sletning af persondata om ansatte i elektronisk form.

Der sker aktuelt ingen systematisk sletning af løndata i økonomisystemet vedrørende tidligere ansatte.
EV skal finde en løsning og sætte systemet op, fx med listeudtræk for manuel sletning eller med "bogføringskladder" der skal godkendes og "bogføres"

Senest ét år efter fratrædelse slettes elektroniske dokumenter i personalesagen i DokuNote, dog bevares oplysninger om

- Stillingsbetegnelse
- Ansættelsesperiode
- Eventuelle arbejdsskader.

5.7.4 Sletning af persondata om kunder på elektronisk form.

Der sker aktuelt ingen systematisk sletning af persondata vedrørende tidligere kunder.
EV skal finde en løsning og sætte systemet op, fx med listeudtræk for manuel sletning eller med "bogføringskladder" der skal godkendes og "bogføres"

Ved ophør af ejerskab for ejendomme med mere end én ejer, og hvor oplysningen fremgår af tingbogen slettes felt med ejer 2 i EV-ITA, såfremt der ikke er uindfriet gæld i ejendommen.

I det omfang, der er oprettet sager i DokuNote, med baggrund i henvendelse fra kunder, bevares disse sager, også efter ophør af kundeforholdet.

6.0 Overholdelse af krav for overholdelse af persondatasikkerhed

I dette afsnit beskrives hvordan Sorø Forsyning sikrer overholdelse af krav som oplistet i kapitel 3.

6.1 Sikker håndtering af persondata.

Sorø Forsyning har formuleret en politik for overholdelse af persondataloven, der beskriver, hvordan vi sikrer håndtering af persondata.

Politikken fastlægger selskabets og ansattes adfærdskodeks for sikker håndtering af persondata.

6.2 Interne sikkerhedsforanstaltninger og tilsyn med disse.

Der er nedsat et udvalg for informationssikkerhed, der forestår og fører tilsyn med de interne sikkerhedsforanstaltninger. Jf. kapitel 4.4.

6.3 Skriftlig aftale med ekstern databehandler.

Der er indgået skriftlige aftaler med databehandlere.

Oversigt over indgåede data behandleraftaler kan udtrækkes fra DokuNote.

6.4 Medarbejderes autorisation til behandling af persondata.

Adgang til persondata er fastlagt ved tildeling af roller i økonomisystemet.

6.5 Revisors og systemteknikkeres autorisation til behandling af persondata.

Revisor autorisation og adgang til behandling af persondata er dækket via revisionsaftale.

Systemteknikere/hosting autorisation og adgang til behandling af persondata er dækket via databehandleraftale.

6.6 Sikring mod uautoriseret adgang til persondata.

Autoriseret adgang til elektroniske data gives ved opsætning af brugerprofil til relevante programmer for hver enkelt medarbejder, hvor opsætningen foretages af databehandler efter instruks fra Sorø Forsyning.

Sikring mod uautoriseret adgang sker ved krav om password til system, computere, tablets og mobiltelefoner.

Fysiske data er sikret ved aflåsning.

6.7 Registrering af afviste adgangsforsøg til persondata.

Registrering af alle afviste adgangsforsøg logges maskinelt af data behandlere, som fastlagt i databehandleraftalerne med disse.

6.8 Logning af anvendelse af persondata.

Maskinel logning af anvendelse af persondata foretages af data behandlere, som fastlagt i databehandleraftalerne med disse.

6.9 Behandling af persondata på hjemmearbejdsplads mv.

Adgang til Sorø Forsynings persondata fra PC udenfor Sorø Forsynings lokaler må kun ske via Citrix forbindelse. Fx må persondata ikke lagres og overføres via bærbar diskette/USB-nøgle eller lignende.
Persondata må ikke lagres lokalt på PC udenfor Sorø Forsynings lokaler.
Persondata må ikke udskrives på printer udenfor Sorø Forsynings lokaler.

6.10 Fysisk sikring af steder, hvor der behandles persondata.

Fysisk sikring af steder, hvor der behandles persondata, er nærmere beskrevet i bilag til nærværende politik. Dette bilag offentliggøres ikke.

6.11 Skrotning af IT-udstyr m.m.

Persondata må ikke gemmes lokalt på pc. Ved udskiftning vil der dermed ikke ligge data på det skrottede udstyr. Sorø Forsynings It-udstyr sælges ikke videre, men kasseres og bortskaffes som elektronikaffald.

I forbindelse med reparation og service af dataudstyr, indeholder disse ikke personoplysning og udgør ikke en risiko.

6.12 Sikring af eksterne kommunikationsforbindelser

Eksterne kommunikationsforbindelser er gennem TDC´s ledninger.

Vi har den 14. november 2017 pr. mail spurgt TDC, om deres system understøtter, at uvedkommende ikke kan få adgang til personoplysninger i telefonlinjer og disses endepunkter.

TDC har pr. mail d. 16. november 2017 bekræftet dette.

6.13 Indhentning af samtykkeerklæring

6.13.1 Indhentning af samtykkeerklæringer fra personale.

Ansøgere til stillinger i Sorø forsyning har ved fremsendelse af sin ansøgning underforstået givet samtykke til behandling at de fremsendte personoplysninger.

Ansatte i Sorø Forsyning, herunder bestyrelsesmedlemmer, har ved sin accept af ansættelsen underforstået givet samtykke til behandling at de personoplysninger, der er nødvendig i forbindelse med en ansættelse, herunder en eventuel afskedigelse.

Ansatte i Sorø Forsyning, der på grund af personlige eller familiemæssige årsager ønsker særlige vilkår, har med sit ønske underforstået givet samtykke til behandling at de supplerende personoplysninger, der er nødvendig i forbindelse med disse særlige vilkår.

For supplerende personoplysninger om ansatte, der frivilligt leveres af den ansatte til et konkret formål, forudsættes disse givet med et underforstået samtykke til denne anvendelse.
Disse oplysninger kan fx være:

- Kontaktoplysninger om nærmeste pårørende.
- Navn og CPR nr. på hjemmeboende børn under 7 år.

Der indsamles ikke personoplysninger for personale, der fordrer en samtykkeerklæring.

6.13.2 Indhentning af samtykkeerklæringer fra kunder.

Kunder i Sorø Forsyning har i kraft af kundeforholdet underforstået givet samtykke til behandling at de personoplysninger, der er nødvendige i forbindelse med administration af et normalt kundeforhold, der er en konsekvens af den lovgivningsmæssige forsyningspligt.

For personoplysninger, der frivilligt leveres af kunden til et konkret formål, forudsættes disse givet med et underforstået samtykke til denne anvendelse.
Disse oplysninger kan fx være:

- Bankoplysninger til brug for Sorø Forsynings udbetaling til kundens bankkonto.
- Adresse for fremsendelse af opkrævninger og anden korrespondance.
- E-mail adresse.
- Telefonnummer.

Der skal indhentes samtykkeerklæring fra kunder i følgende situationer:

- I forbindelse med etablering af afdragsordning for kloaktilslutning.

6.14 Der indsamles alene persondata med et sagligt formål.

I kapital 5.1.3 er noteret, hvilke persondata, der ikke behandles og ikke må indsamles hos Sorø Forsyning.

6.15 Udlevering eller overførsel af data ved henvendelse fra den registrerede.

Oplysning om ejendommens forbrug udleveres ved henvendelse fra ejer på telefon eller e-mail.
Personoplysninger udleveres eller overføres kun med baggrund i skriftlig fuldmagt fra den registrerede.

6.16 Ajourføring og kvalitetssikring af persondata.

Vi opdaterer løbende persondata og ved mistanke om fejl, undersøges det nærmere, og eventuelle fejl rettes.

6.16.1 Ajourføring og kvalitetssikring af persondata for personale.

Skatteoplysninger downloades elektronisk forud for hver enkelt lønkørsel.
Øvrige persondata/stamdata kontrolleres én gang årligt.

6.16.1 Ajourføring og kvalitetssikring af persondata for kunder.

Oplysninger om kunder, herunder om ejerskifte kan ajourføres på baggrund af oplysninger fra forskellige kilder:

- Oplysninger offentliggjort i Statstidende modtages via BlueIdea.
- Oplysninger modtages skriftligt i form af udfyldt og underskrevet ejerskifteskema.
- Oplysninger modtages fra private vandværker.
- Oplysninger modtaget skriftligt fra kunden.

6.17 Opbevaring af persondata

6.17.1 Opbevaring af persondata på papirform.

Persondata på papirform, der skal bevares, opbevares i aflåst skab eller i Sorø Forsynings boks.

6.17.2 Opbevaring af persondata på elektronisk form.

Persondata i elektronisk form opbevares på Sorø Forsynings hostede server, der er beskyttet med personlige passwords til serveren.
Persondata opbevares i en række programmer, der kan være yderligt beskyttet.

- Medarbejderes Outlook konti kan kun tilgås, af den pågældende medarbejder. Ved fratrædelse eller ved begrundet mistanke om misbrug kan ledelsen dog skaffes adgang.
- Adgang til persondata i DokuNote beskyttes af adgangsrettigheder til de arkivskabe eller mapper, hvor persondata opbevares,
- Adgang til persondata i økonomisystem beskyttes ved tildeling af rettigheder gennem rolleprofil.

For mails der kan indeholde personoplysninger, og hvor der sker synkronisering med bærbare enheder fx smartphone eller tablet, beskyttes disse oplysninger af password til den bærbare enhed.

6.18 Sletning af persondata

6.18.1 Sletning af persondata for kunder.

Fysiske papirer med persondata makuleres efter 5 fulde regnskabsår.
For dokumenter med persondata vedrørende lån makuleres disse 5 fulde regnskabsår, efter lånet er afviklet.
Persondata slettes i bogføringssystem efter 5 fulde regnskabsår efter kundeforholdet er afsluttet.
Ved afsluttes menes fraflyttet fra forsyningsområdet og alle økonomiske mellemværender er udlignet.

Bemærk at data om ejendommens vandforsyningsforhold og spildevandsforsyningsforhold, herunder måleraflæsninger ikke slettes, men bevares.

6.18.2 Sletning af persondata for ansatte.

Ansattes navn, CPR-nr., oplysning om arbejdsfunktion og ansættelsesperiode slettes ikke.
Oplysninger gemmes af hensyn til mulige fremtidige arbejdsmiljøsager.
E-mail konto slettes 12 mdr. efter fratrædelse.
Lønoplysninger slettes efter 5 fulde regnskabsår efter fratrædelsen.
Påtaler og advarsler slettes 2 år efter de påtalte forhold er bragt i orden.

6.19 Overholdelse af oplysningspligt ved henvendelse fra den registrerede.

Anmodninger fra personer om ret til at få at vide, om der behandles oplysninger om vedkommende, behandles kun, hvis der er vished for, at personen der henvender sig, er den person som vedkommende udgiver sig for.
I tvivlstilfælde kan fremmødte personers identitet fx dokumenteres ved forevisning af billedlegitimation og sundhedskort.

Skriftlige anmodninger fremsendt pr. brev med underskrift behandles.

Anmodning om at få oplyst om, der behandles oplysninger om vedkommende, og i givet fald hvilke, besvares kun pr. brev sendt til pågældendes bopælsadresse.

Besvarelsen skal indeholde oplysning om:

- Hvilke oplysninger, der behandles om vedkommende,
- Formålet med behandlingen
- Kategorierne af eventuelle modtagere af oplysningerne
- Hvor oplysningerne stammer fra (så vidt det er muligt)

Svar skal som hovedregel gives inden 4 uger, ellers skal forsinkelsen begrundes.

Henvendelser med ønske om generel oplysning om hvilke typer af personoplysninger vi behandler og med hvilket formål, kan besvares pr. mail eller telefon, og der er ikke krav om, at den der ønsker disse generelle oplysninger dokumenterer sin identitet. Besvarelsen må naturligvis kun inde holde generelle oplysninger, og ikke oplysninger om navngivne personer.
Der kan henvises til nærværende politik, der er offentlig tilgængelig på selskabets hjemmeside.

6.20 Håndtering af indsigelse fra den registrerede

Nødvendige data for kundeforholdet slettes ikke.
Vi behandler kun indsigelser om registrering og videregivelse af oplysninger ved brev med underskrift fra den registrerede.
Indsigelser vedrørende berigtigelse af oplysninger kan behandles telefonisk, hvis vi registrerer, at der er fejl.

6.21 Overholdelse af anmeldelsespligt til Datatilsynet

Vi behandler som udgangspunkt ikke data, der skal anmeldes til Datatilsynet.

6.21.1 Data der ikke indhentes og derfor ikke skal indberettes.

- Racemæssig eller etnisk baggrund
- Politisk, religiøs eller filosofisk overbevisning
- Seksuelle forhold
- Væsentlige sociale problemer
- Straffeattest for ansatte.
- Personlighedstest for ansatte

6.21.2 Data der skal indberettes hvis de indhentes i særlige tilfælde.

Indhentning af nedenstående data skal i hvert enkelt tilfælde forhåndsgodkendes af Udvalget for informationssikkerhed, der har ansvar for indberetning til Datatilsynet.

- Oplysninger om strafbare forhold, fx tyveri fra virksomheden, indhentelse af ren straffeattest eller lign.
- Oplysninger om at en medarbejder er bortvist fra jobbet pga. en grov væsentlig misligholdelse af ansættelsesforholdet
- Oplysninger om væsentlige sociale problemer
- Oplysninger om tidligere, nuværende eller fremtidige helbredsforhold herunder vedkommendes fysiske eller psykiske tilstand samt misbrug af alkohol, nydelsesmidler mv., med mindre behandlingen heraf er nødvendig for at opfylde relevante bestemmelser i lov eller forskrifter fastsat i relevante love.
- Resultater af en personlighedstest, fx i forbindelse med en ansættelsesproces (det er underordnet, om personlighedstesten efterfølgende kasseres)

6.21.3 Data der ikke skal indberettes.

- Navn
- Adresse
- Installationsnummer
- Løbende oplysninger om kunders restancer vedr. løbende forbrug og tilslutningsbidrag
- Oplysninger om ansattes medlemskab af en fagforening

6.22 Udlevering eller overførsel af persondata ved henvendelse fra den registrerede

Anmodninger fra personer om udlevering eller overførsel af egne persondata behandles kun, hvis der er vished for, at personen der henvender sig, er den person som vedkommende udgiver sig for.
I tvivlstilfælde kan fremmødte personers identitet fx dokumenteres ved forevisning af billedlegitimation og sundhedskort.
Skriftlige anmodninger fremsendt pr. brev med underskrift behandles.
Ved anmodningen skal personen skriftligt og udtrykkeligt angive hvordan og hvortil oplysninger persondata skal udleveres eller overføres.
Udlevering eller overførsel af persondata forudsætter, at data ikke er en forudsætning for fortsat ansættelse, fortsat kundeforhold eller overholdelse af lovgivning.

Persondata på papir udleveres i originalformat. Eventuelle fotokopier makuleres.
Persondata der opbevares elektronisk udtrækkes og leveres som ønsket, i det elektroniske format det er muligt. Efterfølgende skal data på elektronisk form slettes.

6.23 Uddannelse og instruktion.

Ved udarbejdelse af nærværende politik var administrative medarbejdere involveret i arbejdet.
Ved ikrafttræden af nærværende politik gives en overordnet orientering på personalemøde for alle ansatte.

Ved ikrafttræden af nærværende politik gives en målrettet orientering til administrativt personale.
Udvalget for informationssikkerhed sikrer, at nyansatte får en passende og rettidig gennemgang af nærværende politik.

Udvalget for informationssikkerhed sikrer, at der med passende mellemrum gives en opfølgende orientering om nærværende politik, mindst én gang årligt på personalemøde for alle ansatte.

Det vurderes ikke relevant, at ansatte skal have supplerende uddannelse som følge af ikrafttræden af nærværende politik.

I databehandleraftaler fremgår det, at der skal kunne stilles tilstrækkelig ekspertise til rådighed, hvilket betyder, at der også kræves en tilstrækkelig kompetence.

6.24 Overholdelse af generelle og specifikke krav fra kunder

Der er endnu ikke modtaget eller formuleret generelle eller specifikke kundekrav for overholdelse af persondatasikkerheden.

6.25 Overholdelse af ejers krav for overholdelse af persondatasikkerheden

Der er endnu ikke modtaget eller formuleret generelle eller specifikke ejerkrav for overholdelse af persondatasikkerheden.

7.0 Risikoanalyse

Der vurderes kun på risiko i forhold til at persondata mistes eller kommer uvedkommende i hænde. Risikovurderingen er foretaget ud fra det aktuelle nationale risikoniveau. Ved et skærpet nationalt risikoniveau skal risikovurderingen ajourføres.

Risiko kan forstås som sandsynligheden for en uønsket hændelse kombineret med konsekvensen af at den indtræffer.

Populært kan man sige:

Risiko = Sandsynlighed gange Konsekvens

7.1 Sandsynlighed for at en hændelse forekommer.

Sandsynlighed betegner i denne forbindelse hvor hyppigt en hændelse vil forekomme.
Sorø forsyning har besluttet, at anvende nedenstående kategorier for hyppighed.

Sandsynlighed	
Kategori	**Hyppighed, pr. år**
Meget hyppigt	1 gang pr. år
Forekommer	1 gang på 10 år
Uhyre sjældent	Under 1 gang pr. 10 år.

Sorø Forsyning har ikke kendskab til, at persondata er kommet uvedkommende hænde i siden stiftelsen. Derfor er de angivne hyppigheder fastsat på et løst grundlag, men hvor der taget udgangspunkt i de ca. 10 år Sorø Forsyning har eksisteret.

7.2 Konsekvens af at en hændelse forekommer.

Konsekvens betegner i denne forbindelse, hvilken betydning en hændelse vil have for den eller de personer, der måtte blive berørt af, om persondata kommer uvedkommende i hænde, og om mange eller få er berørt.
Sorø Forsyning har besluttet at anvende nedenstående kategorier for konsekvens at en given hændelse.

Konsekvens	
Kategori	**Beskrivelse**
Kritisk	Kritisk for mange personer
Væsentlig	Kritisk for en enkelt person
Marginalt	Begrænset betydning

7.3 Screeningsmatrice til risikovurdering.

Sorø Forsyning har opstillet nedenstående screeningsmatrice, der er et skema hvor sandsynlighed og konsekvens kombineres for en uønsket hændelse.
Screeningsmatricen benyttes til vurdering en given risiko.
Der er i screeningsmatricen anvendt følgende forkortelser:

- TUA = En totalt uacceptabel risiko.
- UA = En uacceptabel risiko.
- UØ = En uønsket risiko

Screeningsmatrice. Til vurdering af hændelser		**Sandsynlighed**		
		Meget hyppigt	Forekomme	Uhyre sjældent
Konsekvens	Kritisk	TUA	TUA	TUA
	Væsentlig	TUA	UA	UA
	Marginal	UA	UA	UØ

7.4 Handlingsmatrice for risikohåndtering.

Sorø Forsyning har opstillet nedenstående handlingsmatrice, der fastlægger hvordan en risiko for en uønsket hændelse skal håndteres.

Handlingsmatrice		**Håndtering af risiko for hændelsen**
TUA	Totalt uacceptabelt	Må ikke forekomme, risiko skal straks håndteres og minimeres.
UA	Uacceptabelt	Må ikke forekomme, risiko skal håndteres og minimeres i forbindelse med den årlige evaluering.
UØ	Uønsket	Risikoen skal vurderes i forbindelse med den årlige evaluering, hvor risikoen skal nedbringes, hvis det kan ske uden større investeringer i tid eller penge.

7.5 Den gennemførte risikoanalyse.

Sorø Forsyning har besluttet at gennemføre risikoanalysen på en workshop for det administrative personale.
Resultatet af gennemgangen er et udarbejdet risikoskema for hver vurderet hændelse.

Da omfanget af risikovurderingen er begrænset af fantasi og kendskab til mulige uønskede hændelser forudsættes risikovurderingen fremadrettet at kunne omfatte flere vurderede uønskede hændelser.

8.0 Input til udvikling af politik for overholdelse af politik for persondatasikkerhed

Det er forudsat at nærværende politik skal udvikles og forbedres løbende. Denne udvikling sikres gennem input til udvikling, som beskrevet herunder.

8.1 Gennemgang af krav

Som forberedelse til ledelsens evaluering gennemgås ny relevant lovgivning for at afdække, om der måtte fremkomme supplerende eller ændrede krav.
Mindst én gang årligt gennemgås gældende lovgivning og datasikkerhedsforordningen af udvalget for informationssikkerhed for at afdække, om der er ændring i krav.

8.2 Korrigerende handlinger

Der skal løbende i værkssættets risikovurdering for alle forekommende uønskede hændelser, der kan true datasikkerheden, og som ikke er behandlet i nærværende politik.
Der skal foretages en fornyet risikovurdering hvis risikobilledet ændres for forudsete hændelser.
Risikovurderingen kan udløse omgående korrigerende handlinger efterfulgt af en fornyet risikovurdering.

Disse supplerede eller reviderede risikovurderinger indgår i ledelsens evaluering.

8.3 Forebyggende handlinger

Det skal til stadighed vurderes, om datasikkerheden kan forbedres med forebyggende handlinger eller ændrede arbejdsprocesser.

8.4 Løbende forbedringer

Ved indførelse af nærværende politik blev den udarbejdet under hensyn til Sorø Forsynings aktuelle situation og handlemuligheder. Det skal løbende vurderes, om datasikkerheden kan forbedres med ny teknik, nye data behandlere eller nye arbejdsgange.

8.5 Anbefalinger om forbedringer

Det forventes, at der fremadrettet kommer vejledninger med anbefalinger om generelle forbedringer i forhold til datasikkerheden.

Det forventes, at der fremadrettet kommer konkrete anbefalinger til forbedring af nærværende politik fx fra ejer, revisor eller ansatte.

8.6 Innovation.

Muligheden for anvendelse af nye teknikker eller nye arbejdsgange skal indgå i ledelsens evaluering.

9.0 Ledelsens evaluering.

Ledelsen foretager en årlig vurdering af politikken for behandling af persondata med baggrund i de input, der er kommet til udvikling af politikken.
Ledelsen vurderer løbende det generelle trusselsniveau, og om der er behov for en fornyet risikovurdering.

10.0 Bilag der IKKE offentliggøres.

- Risikoanalyse.
- Gennemgang af den fysiske sikkerhed
- Udtræk fra DokuNote med databehandleraftaler.