

Norsk Vann

Rapport



293 | 2025

Håndtering av person- opplysninger i vannbransjen



Norsk Vann

Norsk Vann Rapport

Det utgis tre typer rapporter:

Rapportserie A

Dette er de opprinnelige hovedrapportene.

Dette kan være:

- Rapportering av prosjekter som er gjennomført innenfor organisasjonens eget prosjektsystem
- Rapportering av spleiselagsprosjekter hvor to eller flere andelseiere i Norsk Vann BA samarbeider for å løse felles utfordringer
- Rapportering av prosjekter som er gjennomført av andelseiere eller andre.
Rapporten vil i slike tilfeller kunne være en ren kopi av originalrapporten eller noe bearbeidet

Fortløpende nummer xx-årstall

Rapportserie B

Dette er en serie for «enklere» rapporter, for eksempel forprosjekter, som vil være grunnlag for videre prosjektvirksomhet mm.

Fortløpende nummer Bxx-årstall

Rapportserie C

Dette er rapporter delfinansiert av Norsk Vann, men som er utgitt av andre.

Fortløpende nummer Cxx-årstall



Norsk Vann BA, Vangsvegen 143, 2321 Hamar
Tlf: 62 55 30 30 E-post: post@norsk vann.no
www.norsk vann.no



Prosjekresultatene fra Norsk Vann Rapport (serie A og B) kan fritt benyttes internt i egen organisasjon. Når prosjekresultatene benyttes i skriftlig materiale, må kilde oppgis. Videre salg/ formidling av resultatene utover dette er kun tillatt etter skriftlig avtale med Norsk Vann BA.

Norsk Vanns rapporter utarbeides i samspill mellom rådgiver, styringsgruppe og referansegruppe for prosjektet og er ikke behandlet i Norsk Vanns styrende organer. Norsk Vann har ikke ansvar for feil eller ufullstendigheter som måtte forekomme i rapporten og kan ikke stilles økonomisk eller på annen måte til ansvar for problemer som måtte oppstå som følge av bruk av rapporten.

Norsk Vann Rapport

Ekstrakt

Økt bruk av digitale hjelpemidler og løsninger har gitt ansatte i kommuner og selskap i vannbransjen mulighet til å effektivisere saksbehandlingen. Samtidig medfører digitaliseringen at de behandler personopplysninger om abonnenter og andre de er i kontakt med i en rekke sakstyper og programvarer.

Denne rapporten gir en oversikt over typiske aktiviteter og programvarer vannbransjen benytter, som kan innebære behandling av personopplysninger. En av disse typiske behandlingsaktivitetene er bruk av digitale vannmålere. Rapporten tar for seg i hvilken utstrekning kommuner og selskap kan behandle personopplysninger gjennom digitale vannmålere etter dagens regelverk. Den viser typiske fallgruver og hva de ansatte bør være oppmerksomme på for å unngå disse.

Formålet med rapporten er å øke kompetansen om personvernregelverket. Den viser hvilke typiske behandlinger av personopplysninger som utføres, peker på særlige risikoområder og foreslår hvordan risikoen kan reduseres.

Norsk Vann BA

Adresse: Vangsvegen 143, 2321 Hamar

Telefon: 62 55 30 30

E-post: post@norsk vann.no

Internettadresse: norsk vann.no

Rapportens tittel

Håndtering av personopplysninger i vannbransjen

Forfatter(e):

Christine Ask Ottesen, Advokatfirmaet PwC

Henrik Gullaker, Advokatfirmaet PwC

Ine Møllegaard, Advokatfirmaet PwC

Rapportnummer: 293/2025

ISSN 1890-8802 (elektronisk utg.)

ISSN 1504-9884 (trykt utg.)

ISBN 978-82-414-0494-8

Emneord, norsk

Personvern, GDPR

Emneord, engelsk

Data protection, GDPR

Forord



Økt bruk av digitale hjelpemidler og løsninger har effektivisert saksbehandlingen. Digitaliseringen har imidlertid også medført at ansatte i vannbransjen behandler stadig flere personopplysninger.

Da personvernforordningen (GDPR) trådte i kraft i Norge i 2018, ble mange oppmerksomme på både eksisterende og nye krav til behandling av personopplysninger. Dette gjaldt også for ansatte i vannbransjen. Samtidig uttrykte flere at de savnet veiledning for behandlingen av personopplysninger i de spesifikke sakstypene de håndterer og programvarene de benytter.

Styret i Norsk Vann bevilget i 2021 midler fra prosjektsystemet til å utarbeide en oversikt over hvilke sakstyper og programvarer som kan inneholde personopplysninger, og vise hvilke problemstillinger både virksomhetene og de ansatte skal være oppmerksomme på.

Advokatfirmaet PWC, ved Christine Ask Ottesen, Henrik Gullaker og Ine Møllegaard, har utarbeidet denne rapporten, med gode innspill fra styringsgruppa, som har bestått av:

- Markus Horrigmo, fagansvarlig spredt avløp i Narvik Vann
- Kristine Edvartsen, juridisk rådgiver i Sandnes kommune (gikk ut av styringsgruppa pga. overgang til ny jobb høsten 2024)
- Ingvild Myrvold Solberg, Juridisk rådgiver i Vann- og avløpsetaten, Oslo kommune
- Stig Ove Haarberg, IKT rådgiver i Bergen Vann

Gjennom jevnlige møter diskuterte de involverte faglige spørsmål og problemstillinger, i tillegg til å gi skriftlige tilbakemeldinger på utkast til rapporten.

Høsten 2024 ga øvrige engasjerte personer i vannbransjen nyttige innspill under en digital workshop. En særlig takk for skriftlige innspill fra Anne Maria Pileberg i VAV Oslo kommune og Fred Ivar Aasand i Norsk Vann.

Underveis ble det stadig tydeligere at prosjektet måtte rette et betydelig fokus mot behandlingen av personopplysninger som innhentes via digitale vannmålere.

PWC kontaktet regulerende myndigheter, uten at dette ga noen avklaringer. Prosjektet gjennomførte deretter et veiledningsmøte med Datatilsynet, som problematiserte de personvernmessige sidene ved å hente inn data fra digitale vannmålerne til annen bruk enn å fakturere gebyr. At tilsynsmyndigheten uttrykte en såpass klar negativ holdning til

lovligheten, gjør det problematisk å benytte informasjon fra målerne til andre formål, som å avdekke lekkasjer, uten en egen klar hjemmel. Den manglende reguleringen står i kontrast til at nasjonale myndigheter har fastsatt et eget mål om å redusere andelen lekkasjer av drikkevann i sine Nasjonale mål for vann og helse. Som en oppfølging av prosjektet, vil Norsk Vann oppfordre lovgiver til å etablere dedikerte lovhjemler for lekkasjesøk og andre bruksområder for personopplysninger innhentet gjennom digitale vannmålere.

En varm takk til alle som har bidratt under utarbeidelsen av rapporten!

Hamar, 25.02 2025
Elin Riise
prosjektleder i Norsk Vann

Sammendrag

Ansatte som jobber med vann og avløp i kommuner og selskap behandler jevnlig personopplysninger. Denne rapporten gir en oversikt over typiske behandlingsaktiviteter og behandlingsformål, samt hva slags programvare de benytter. Rapporten gir også informasjon om særlige personvernutfordringer og typiske fallgruver. Målet er å øke kompetansen og bevisstheten rundt personvern.

Tjenesteleveransen består av flere ulike behandlingsaktiviteter, med et bredt spekter av personopplysninger. Det omfatter blant annet behandling av søknader om tilkobling til de kommunale vann- og avløpsledningene, utstedelse av ferdigmeldinger og fakturering av gebyr. Som forurensningsmyndighet fører kommunen tilsyn med utslipp fra avløpsanlegg og behandler søknader om utslipp av avløpsvann. Personene som får sine personopplysninger behandlet er typisk de som mottar en vanntjeneste fra kommunen eller som har et privat avløpsanlegg, men også privatpersoner eller kontaktpersoner i virksomheter, tiltakshavere og entreprenører.

De fleste behandlingsaktivitetene kan hjemles i personvernforordningens artikkel 6 (1) bokstav e, som tillater behandling som er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet. Kommuners tilbud om, og leveranse av, vann- og avløpstjenester er underlagt et omfattende regelverk, herunder forurensningsloven, forurensningsforskriften og drikkevannsforskriften. Dette regelverket danner i noen tilfeller et supplerende rettslig grunnlag for behandling av personopplysninger.

Rapporten identifiserer ni særlige personvernutfordringer, og gir anbefalinger om hvordan disse kan adresseres. Utfordringene er:

- 1) Organisatorisk avstand mellom vann- og avløpsavdelinger og den kommunale administrasjonen.
- 2) Varierende kunnskap og kompetanse om vannbransjen hos kommunal administrasjon
- 3) Sentraliserte og desentraliserte personvernroller.
- 4) Kompleks systemportefølje.
- 5) Mangel på fagsystemer og bruk av «skygge-IT».
- 6) Mangelfull internkontroll.
- 7) Mangelfull risikostyring.
- 8) Varierende personvernkompetanse hos ansatte i vann og avløp
- 9) Risiko for brudd på personopplysningssikkerheten.

Rapporten foreslår at kommuner og selskap etablerer regelmessige og hyppige kontaktpunkter med den kommunale administrasjonen, for å bedre kommunikasjonen og redusere konsekvensene av den organisatoriske avstanden. Den kommunale administrasjonen bør øke sin kunnskap og kompetanse om vannbransjen.

Ansatte som jobber med vann og avløp bør få mer og bedre opplæring om krav til personvern og hvordan dette skal ivaretas som en del av deres arbeidsoppgaver. I tillegg bør ansatte og kommunenes IT-avdelinger samarbeide tett om systemforvaltning for å sikre bedre og mer personvernvennlige løsninger og prosesser.

Rapporten understreker betydningen av å etablere retningslinjer og prosedyrer for personvern ute hos vann- og avløpsavdelingene/selskapene, samt effektiv internkontroll og risikostyring. Dette bidrar til å sikre etterlevelse av personvernregelverket. Det må generelt prioriteres opplæring og kompetanseheving om personvern.

Rapporten tar særskilt for seg i hvilken utstrekning kommuner og selskap kan behandle personopplysninger gjennom digitale vannmålere etter dagens regelverk. I dag har kommuner rettslig grunnlag for å samle inn personopplysninger knyttet til måling av vannforbruket for å kunne fakturere gebyr. Nasjonale krav, den teknologiske utviklingen og samfunnets forventninger til vanntjenestene har imidlertid ført til et behov for å kunne benytte personopplysninger som samles inn gjennom digitale vannmålere til nye formål. Dette er særlig aktuelt for å effektivisere søket etter lekkasjer.

Vår vurdering er at det er nødvendig med uttrykkelige lovhjemler for å kunne samle inn personopplysninger for disse formålene. Dette baserer vi primært på vurderingene fra Datatilsynet, som er tilsynsorgan for personopplysningsloven. Prosjektet anbefaler at Norsk Vann går i dialog med lovgiver, for å etablere dedikerte lovhjemler for å kunne innhente og bruke personopplysninger fra digitale vannmålere til lekkasjesøk og eventuelt også andre formål.

English summary

This report is published in Norwegian by Norwegian Water BA (Norsk Vann BA).

Address: Vangsvegen 143, NO-2321 Hamar, Norway
Phone: + 47 62 55 30 30
E-mail: post@norskvann.no
Website: www.norskvann.no

Report no: 293 – 2025
Report title:
Date of issue: February 2025

Author: Christine Ask Ottesen,
Henrik Gullaker and Ine Møllegaard.

Employees working with water and sewage in municipalities and companies regularly handle personal data. This report provides an overview of typical processing activities and purposes, as well as the types of software they use. The report also provides information on specific privacy challenges and common pitfalls. The goal is to increase competence and awareness around privacy.

The service delivery consists of various processing activities involving a wide range of personal data. This includes processing applications for connection to municipal water and sewage lines and billing fees. As a pollution authority, the municipality supervises discharges from sewage plants and processes applications for the discharge of wastewater. The individuals whose personal data are processed typically include those receiving a water service from the municipality or those with a private sewage system, but also individuals or contact persons in businesses, project owners, and contractors.

Most processing activities can be justified under Article 6(1)(e) of the General Data Protection Regulation (GDPR), which allows processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority. The provision and delivery of water and sewage services by municipalities are subject to regulation, including the Pollution and the drinkingwater regulation. This regulatory framework sometimes provides a supplementary legal basis for the processing of personal data.

The report identifies nine specific privacy challenges and provides recommendations on how to address them. The challenges are:

- 1) Organizational distance between water and sewage departments and municipal administration.

- 2) Varying knowledge and competence about the water industry within municipal administration.
- 3) Centralized and decentralized privacy roles.
- 4) Complex system portfolio.
- 5) Lack of specialized systems and the use of "shadow IT."
- 6) Inadequate internal control.
- 7) Inadequate risk management.
- 8) Varying privacy competence among water and sewage employees.
- 9) Risk of breaches in personal data security.

The report suggests that municipalities and companies establish regular and frequent contact points with municipal administration to improve communication and reduce the consequences of organizational distance. Municipal administration should increase its knowledge and competence about the water industry.

Employees in water and sewage should receive more and better training on privacy requirements and how to incorporate these into their tasks. Additionally, employees and municipal IT departments should collaborate closely on system management to ensure better and more privacy-friendly solutions and processes.

The report emphasizes the importance of establishing guidelines and procedures for privacy within water and sewage departments/companies, as well as effective internal control and risk management. This helps ensure compliance with privacy regulations. Generally, training and competence development on privacy should be prioritized.

The report specifically addresses the extent to which municipalities and companies can process personal data through digital water meters under current regulations. Today, municipalities have a legal basis for collecting personal data related to water consumption measurement to bill fees. However, national requirements, technological developments, and societal expectations for water services have led to a need to use personal data collected through digital water meters for new purposes, particularly to streamline leak detection.

Our assessment is that explicit legal provisions are necessary to collect personal data for these purposes. This is primarily based on assessments from the Norwegian Data Protection Authority, which is the supervisory authority for the Norwegian Personal Data Act. The project recommends that Norsk Vann engage in dialogue with the legislator to establish dedicated legal provisions for collecting and using personal data from digital water meters for leak detection and possibly other purposes.

Innhold

1. Bakgrunn og mål	10	7.2. Innebygd personvern og personvern som standardinnstilling	27
2. Hva er en personopplysning?	12	7.3. Bruk av databehandlere og databehandleravtaler	27
3. Grunnleggende personvernprinsipper	13	7.4. Protokollføring	28
3.1. Lovlighet, rettferdighet og åpenhet	13	7.5. Risikovurderinger og personvernkonsekvensvurderinger (DPIA)	28
3.2. Formålsbegrensning	13	7.6. Brudd på personopplysningssikkerheten	29
3.3. Dataminimering	13	7.7. Lagringstid og arkivering	29
3.4. Riktighet	14	8. Særlige personvernutfordringer i vannbransjen	30
3.5. Lagringsbegrensning	14	8.1. Organisatorisk avstand	30
3.6. Integritet og konfidensialitet	14	8.2. Varierende kunnskap og kompetanse om vannbransjen hos kommunal administrasjon	31
3.7. Ansvarlighet	14	8.3. Sentraliserte og desentraliserte personvernroller	31
4. Behandlingsgrunnlag	15	8.4. Kompleks systemportefølje	32
5. Behandling av personopplysninger ved levering av vann- og avløpstjenester til abonnenter	17	8.5. Mangel på fagsystemer og bruk av «skygge-IT»	32
5.1. Organisering	17	8.6. Mangelfull internkontroll	33
5.2. Rettslige utgangspunkter	17	8.7. Mangelfull risikostyring	34
5.3. Behandlingsaktiviteter og personopplysninger	18	8.8. Varierende personvernkompetanse hos ansatte i vann og avløp	34
5.3.1. Søknad om tilkobling til vann- og avløpsledninger og dokumentasjon før ferdigmelding	18	8.9. Risiko for brudd på personopplysningssikkerheten	35
5.3.2. Vann- og avløpsgebyr	19	9. Digitale vannmålere	36
5.3.3. Varsling av abonnenter	20	9.1. Bruksområder og mulige gevinster	36
5.3.4. Kameraovervåking	20	9.2. Personopplysninger som behandles gjennom digitale vannmålere	37
5.3.5. Sosiale medier	20	9.3. Behandlingsgrunnlag for ulike formål	37
5.3.6. Behandling av ansattes personopplysninger	21	9.3.1. Måling og fakturering av vannforbruk	37
5.3.7. Behandling personopplysninger gjennom digitale vannmålere	21	9.3.2. Ytterligere bruksområder	39
6. Håndtering av personopplysninger ved behandling av søknader om utslippstillatelse og tilsyn med utslippene	22	9.4. Behovet for en klar hjemmel	39
6.1. Rettslige utgangspunkter	22	9.5. Prosjektets anbefaling	39
6.2. Behandlingsaktiviteter og personopplysninger	22	10. Referanser	41
6.2.1. Utslippstillatelser	22	11. Vedlegg	42
6.2.2. Tilsynsaktiviteter	23	Tidligere utgitte rapporter	46
7. Hvilke forpliktelser har den behandlingsansvarlige?	24		
7.1. Ivareta de registrertes rettigheter	24		
7.1.1. Retten til informasjon	24		
7.1.2. Retten til innsyn	24		
7.1.3. Retten til retting og sletting	25		
7.1.4. Retten til begrensning av behandling	25		
7.1.5. Retten til dataportabilitet	26		
7.1.6. Retten til å protestere	26		
7.1.7. Retten til å ikke være gjenstand for automatiserte individuelle avgjørelser, herunder profilering	26		
7.1.8. Unntak fra de registrertes rettigheter	26		

Forkortelser, begreper og definisjoner

Personvernforordningen: Forordning fra EU om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger. På norsk heter dette personvernforordningen. Inngår ved inkorporasjon i ny personopplysningslov.

Personopplysning: Enhver opplysning om en identifisert eller identifiserbar fysisk person.¹⁾

Den registrerte: En person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator, eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.²⁾

Behandling: Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.³⁾

Behandlingsansvarlig: En fysisk eller juridisk person som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.⁴⁾

Databehandler: En fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.⁵⁾

Ustrukturerte lagringsområder: Datalagringsområder hvor dataene ikke er organisert i en forhåndsdefinert eller lett identifiserbar struktur.

Kommuner og selskap: Kommuner med egne vann- og avløpsavdelinger, kommunale og interkommunale selskap og samvirkevannverk.

1) Personvernforordningen artikkel 4 (1).

2) Personvernforordningen artikkel 4 (1).

3) Personvernforordningen artikkel 4 (2).

4) Personvernforordningen artikkel 4 (7).

5) Personvernforordningen artikkel 4 (8)

1. Bakgrunn og mål

I takt med den teknologiske utviklingen har omfanget og bruken av personopplysninger økt. Det samles inn flere personopplysninger, og personopplysningene som samles inn er mer inngripende. Innsamlingen øker også i vannbransjen, da nye systemer, applikasjoner og verktøy tas i bruk for å modernisere og effektivisere tjenesteleveransen og myndighetsutøvelsen.

Økt bruk av digitale hjelpemidler og løsninger har effektivisert saksbehandlingen. Samtidig medfører disse løsningene at de ansatte behandler personopplysninger om abonnenter og andre de er i kontakt med i en rekke sakstyper og programvarer.

I 2018 trådte personvernforordningen i kraft i Norge, med strengere krav til hvordan virksomheter samler inn og håndterer personopplysninger, hvilke sikkerhetstiltak som må etableres, hvordan personopplysninger kan deles med tredjeparter, m.m. Dette førte til økt oppmerksomhet rundt håndteringen av personopplysninger, også i vannbransjen.

Norsk Vann har utarbeidet flere rapporter med personvernrelevant innhold.



Norsk Vann har erfart at mange opplever at de mangler kompetanse om rammene for lovlig innsamling og behandling av personopplysninger, og at de har for lite kunnskap om hvordan personopplysninger skal håndteres. Behandling av personopplysninger er helt nødvendig, både for å levere vann- og avløpstjenester og for å opptre som kommunal myndighet. Derfor er det viktig at de ansatte har en viss kjennskap til personvernregelverket og kravene som stilles.

Denne rapporten gir en oversikt over typiske behandlingsaktiviteter og hvilke sakstyper og programvarer de ansatte benytter for å behandle personopplysninger. Rapporten gir også informasjon om særlige personvernutfordringer og typiske fallgruver som kan oppstå, og hva de bør være oppmerksomme på for å unngå fallgruvne.

Formålet med rapporten er å bidra til økt kompetanse om personvernregelverket, vise i hvilke situasjoner ansatte typisk behandler personopplysninger, gi en oversikt over særlige risikoområder og vise hvordan den kan reduseres.

Prosjektet gjennomgikk flere tidligere rapporter utarbeidet av Norsk Vann og andre europeiske fag- og interesseorganisasjoner. Prosjektet innhentet også dokumentasjon fra kommuner og selskap. Dette omfattet blant annet abonnementsvilkår, protokoller og vurderinger. Både personvernlovgivning og annen relevant lovgivning ble gjennomgått og vurdert.

Funnene i denne rapporten er i hovedsak basert på intervjuer med ansatte i kommuner og IKS.

Det er gjennomført intervjuer med et utvalg ansatte fra et bredt spekter av roller og stillingsnivåer, herunder personvernansvarlig, personvernombud og sikkerhetsansvarlig i kommuner og selskap. De ansatte ble spurt om organisering, omfanget av behandlingsaktiviteter, bruken av digitale vannmålere, leverandørstyring og omfanget av styrings-systemet for personvern.

Ansatte i følgende kommuner og selskap ble intervjuet:

- Asker kommune
- Aukra kommune
- Bergen kommune
- Drammen kommune
- GIVAS IKS
- IVAR IKS
- Narvik Vann
- Oslo kommune
- Østre Toten kommune
- Sandnes kommune

2. Hva er en personopplysning?

Personopplysninger er «*enhver opplysning om en identifisert eller identifiserbar fysisk person*».⁶⁾ Hvis en opplysning kan knyttes til en enkeltperson, så vil det være en personopplysning. Klassiske eksempler på personopplysninger er navn, adresse, telefonnummer, fødselsnummer, bilde, fingeravtrykk og iris. Også mer avledede opplysninger vil være personopplysninger om de kan knyttes til en enkeltperson, som arbeidsgiver, bruksmønster og atferd.

Personvernforordningen skiller mellom ulike typer personopplysninger, basert på hvor sensitive de er. Noen kategorier av personopplysninger står i en særstilling i personvernforordningen.⁷⁾ Behandling av denne typen personopplysninger stiller strengere krav til virksomhetens behandlingsgrunnlag, risikovurderinger og sikkerhetstiltak.

Nr.	Særlige kategorier av personopplysninger:
1	Rase eller etnisk opprinnelse
2	Politisk oppfatning
3	Religion
4	Filosofisk overbevisning
5	Fagforeningsmedlemskap
6	Genetiske opplysninger
7	Biometriske opplysninger
8	Helseopplysninger
9	Seksuelle forhold
10	Seksuell legning

Personopplysninger som tilsynelatende ikke omhandler noen av de særlige kategoriene i tabellen over, kan likevel avsløre denne informasjonen dersom de kombineres og/eller analyseres.

En kommune samler inn forbruksdata fra en digital vannmåler. I utgangspunktet er dette ikke særlige kategorier av personopplysninger. Personopplysningene benyttes imidlertid også som en del av kommunens helse- og omsorgstjenester ved at hjemmetjenesten varsles og rykker ut ved unormalt forbruk. Forbruksdata kan da avsløre helseopplysninger.

Det er viktig å være oppmerksom på denne problemstillingen og håndtere personopplysninger med varsomhet, selv når de enkelte personopplysningene som samles inn i utgangspunktet ikke fremstår som sensitive.

6) Personvernforordningen artikkel 4 (1).

7) Personvernforordningen artikkel 9.

3. Grunnleggende personvernprinsipper

Personvernforordningen oppstiller noen grunnleggende personvernprinsipper⁸⁾ som gjelder for all behandling av personopplysninger. Virksomheter som behandler personopplysninger må tilpasse sine behandlingsaktiviteter og virksomhetsstyring slik at disse prinsippene ivaretas.

3.1. Lovlighet, rettferdighet og åpenhet

Prinsippet om lovlighet, rettferdighet og åpenhet innebærer at personopplysninger skal behandles i samsvar med personvernregelverket. Virksomheter må ha et lovlig behandlingsgrunnlag i samsvar med personvernforordningen artikkel 6 (og hvis det behandles særlige kategorier av personopplysninger; artikkel 9) for å kunne behandle personopplysninger.

Behandlingen skal være rettferdig overfor de registrerte. I dette ligger at behandlingen skal være nødvendig, forholdsmessig og forutsigbar. Virksomheter må vurdere hvordan deres behandlingsaktiviteter oppfattes av de registrerte.

Personopplysninger skal behandles på en åpen måte. I dette ligger at de registrerte blant annet skal få informasjon om behandlinger som virksomheten utfører, samt informasjon om hvordan de kan ivareta sine rettigheter.

3.2. Formålsbegrensning

Formålsbegrensning innebærer at personopplysninger bare skal behandles for spesifikke, eksplisitte og legitime formål. Videre behandling av allerede innsamlede personopplysninger må være forenlig med de opprinnelige formålene med innsamlingen av opplysningene.

3.3. Dataminimering

Virksomheter skal bare behandle personopplysninger som er nødvendige for å oppfylle formålene med behandlingen. Dette betyr at personopplysningene må være adekvate, relevante og begrenset til det som er nødvendig for formålene med behandlingen.

Eksempel:

Kommuner og selskap har bare lov til å innhente personopplysninger som er nødvendige for å kunne behandle søknader om å koble seg til hovedledningene. Personopplysninger som ikke er nødvendige i søknadsprosessen kan ikke samles inn.

8) Personvernforordningen artikkel 5.

3.4. Riktighet

Personopplysninger som samles inn og behandles skal være korrekte og holdes oppdatert. Virksomheten skal ta alle rimelige skritt for å sikre at personopplysninger som samles inn og deretter behandles er korrekte. Personopplysninger skal også periodisk vurderes, for å sikre at de er oppdaterte. Ukorrekte personopplysninger skal enten korrigeres eller slettes.

3.5. Lagringsbegrensning

Utgangspunktet er at virksomheter bare skal lagre personopplysninger så lenge det er nødvendig for å oppfylle formålene med behandlingen. Når personopplysninger ikke lenger er nødvendige for formålet med behandlingen, skal de slettes eller anonymiseres. Dette prinsippet skal sikre at personopplysninger ikke blir oppbevart på ubestemt tid, og oppfordrer til regelmessig gjennomgang og sletting av data som ikke lenger er nødvendige. I noen tilfeller kan det være nødvendig å lagre personopplysninger i lengre tid, f.eks. hvor det er en lovpålagt plikt til å lagre personopplysninger.

3.6. Integritet og konfidensialitet

Virksomheter skal sikre et tilstrekkelig beskyttelsesnivå for personopplysninger som behandles. Adekvate tekniske og organisatoriske tiltak skal implementeres. Tiltakene skal bygge på vurderinger av risikoen (varierende sannsynlighets- og alvorlighetsgrad) for fysiske personers rettigheter og friheter. Tiltakene skal sikre at uautoriserte personer ikke får tilgang til personopplysninger og at personopplysninger ikke endres, ødelegges eller mistes.

3.7. Ansvarlighet

Prinsippet om ansvarlighet understreker at den behandlingsansvarlige virksomheten både er ansvarlig for og skal kunne påvise at personvernprinsippene overholdes og at personvernforordningen etterleves.

Eksempel:

Ansatte som jobber med vann og avløp er ikke selv behandlingsansvarlige i juridisk forstand.

Det er kommunen eller selskapet som er behandlingsansvarlig og skal påse at de ansatte overholder kravene i personvernregelverket.

4. Behandlingsgrunnlag

Det grunnleggende personvernprinsippet om lovlighet, innebærer at det må foreligge et rettslig grunnlag for å kunne behandle personopplysninger. Virksomheter må derfor identifisere et lovlig behandlingsgrunnlag, før personopplysninger samles inn og behandles. De aktuelle behandlingsgrunnlagene står i personvernforordningen artikkel 6 og 9.

Typen personopplysninger som behandles har betydning for hvilke behandlingsgrunnlag som må etableres. For «ordinære» personopplysninger, er det nok å etablere et behandlingsgrunnlag i artikkel 6 i personvernforordningen. For sensitive personopplysninger, må virksomheten finne et behandlingsgrunnlag både i artikkel 6 og i artikkel 9.

Behandlingsgrunnlagene i artikkel 6 og 9 er likestilte. Samtykke er for eksempel ikke et foretrukket behandlingsgrunnlag fremfor avtale.

Behandlingsgrunnlag i personvernforordningen artikkel 6:

- a) den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål
- b) behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse
- c) behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige
- d) behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser
- e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt
- f) behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn

Behandlingsgrunnlag i personvernforordningen artikkel 9:

- a) den registrerte har gitt uttrykkelig samtykke til behandling av slike personopplysninger for ett eller flere spesifikke formål
- b) Behandlingen er nødvendig for at den behandlingsansvarlige eller den registrerte skal kunne oppfylle sine forpliktelser og utøve sine særlige rettigheter på området arbeidsrett, trygderett og sosialrett i den grad dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett, eller en tariffavtale i henhold til medlemsstatenes nasjonale rett som gir nødvendige garantier for den registrertes grunnleggende rettigheter og interesser
- c) Behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser dersom den registrerte fysisk eller juridisk ikke er i stand til å gi samtykke
- d) Behandlingen utføres av en stiftelse, sammenslutning eller et annet ideelt organ hvis mål er av politisk, religiøs eller fagforeningsmessig art, som ledd i organets berettigede aktiviteter og med nødvendige garantier, forutsatt at behandlingen bare gjelder organets medlemmer eller tidligere medlemmer eller personer som på grunn av organets mål har regelmessig kontakt med det, og at personopplysningene ikke utleveres til andre enn nevnte organ uten de registrertes samtykke
- e) Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har offentliggjort
- f) Behandlingen er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav eller når domstolene handler innenfor rammen av sin domsmyndighet
- g) Behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser
- h) Behandlingen er nødvendig i forbindelse med forebyggende medisin eller arbeidsmedisin for å vurdere en arbeidstakers arbeidskapasitet, i forbindelse med medisinsk diagnostikk, yting av helse- eller sosialtjenester, behandling eller forvaltning av helse- eller sosialtjenester og -systemer på grunnlag av unionsretten eller medlemsstatenes nasjonale rett eller i henhold til en avtale med helsepersonell og med forbehold for vilkårene og garantiene nevnt i nr. 3
- i) Behandlingen er nødvendig av allmenne folkehelsehensyn, f.eks. vern mot alvorlige grenseoverskridende helsetrusler eller for å sikre høye kvalitets- og sikkerhetsstandarder for helsetjenester og legemidler eller medisinsk utstyr, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett der det fastsettes egnede og særlige tiltak for å verne den registrertes rettigheter og friheter, særlig taushetsplikt

- j) Behandlingen er nødvendig for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1 på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser

Enkelte behandlingsgrunnlag krever i tillegg at det finnes et supplerende rettsgrunnlag. Et eksempel på dette er hvor behandlingen er *nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige*.⁹⁾ En virksomhet som planlegger å benytte dette behandlingsgrunnlaget må identifisere en bestemmelse i en norsk lov eller forskrift som krever at virksomheten behandler personopplysninger for å oppfylle forpliktelsen.

Eksempel:

For å fakturere abonnenter for deres vannforbruk benytter kommunene informasjon fra vannmålere. Det rettslige grunnlaget for å behandle informasjonen er gitt i forurensingsforskriften § 16-4. Dette rettslige grunnlaget blir da et supplerende rettsgrunnlag for kommunen som gebyrmyndighet.

Eksempel:

En kommune ønsker å bruke samtykke som grunnlag for å behandle personopplysninger om ansatte i vann- og avløpsavdelingen. Et samtykke skal være frivillig, spesifikt, informert, utvetydig, avgitt gjennom en aktiv handling, dokumenterbart og mulig å trekke tilbake like lett som det ble gitt. Alle disse vilkårene må være oppfylt for at samtykket skal være gyldig.

En kommune bør være forsiktig med å bruke samtykke som grunnlag for å behandle personopplysninger om ansatte i vann- og avløpsavdelingen. Dette er fordi maktforholdet mellom arbeidsgiver og ansatte er ujevnt, noe som kan gjøre at samtykket ikke regnes som frivillig.

9) Personvernforordningen artikkel 6 (1) bokstav c.

5. Behandling av personopplysninger ved levering av vann- og avløpstjenester til abonnenter

5.1. Organisering

Rundt 85% av Norges befolkning mottar vann- og avløpstjenester fra kommuner og kommunalt eide selskap. Tjenestene leveres som oftest av en egen vann- og avløpsavdeling, som sorterer under tekniske tjenester i kommunene. Mange ansatte ivaretar flere roller enn å levere vann- og avløpstjenester, eksempelvis at de også har fått delegert kommunal vegmyndighet og myndighet etter forurensningsforskriften.

Noen kommuner har organisert hele eller deler av tjenesten i interkommunale selskap (IKS). Vanligvis leverer disse selskapene tjenester til sine eierkommuner som har kontakten med abonnentene, men ett selskap (Givas IKS) leverer vann- og avløpstjenesten direkte til abonnentene.

Det finnes også private samvirker som leverer vanntjenester direkte til abonnentene.

5.2. Rettslige utgangspunkter

Leveransen av vann- og avløpstjenester er underlagt ulike regelverk, de mest sentrale er:

- Lov om kommunale vass- og avløpsanlegg
- Forskrift om begrensning av forurensning (forurensningsforskriften) kap. 16
- Lov om vern mot forurensninger og om avfall (forurensningsloven)
- Forskrift om begrensning av forurensning (forurensningsforskriften) del 4
- Lov om matproduksjon og mattrygghet mv. (matloven)
- Forskrift om vannforsyning og drikkevann (drikkevannsforskriften)
- Lov om planlegging og byggesaksbehandling (plan- og bygningsloven)

Ansatte med ansvar for å levere vann- og avløpstjenester kan i tillegg ha fått delegert myndighet etter forurensningsforskriften og plan- og bygningsloven.

De som ønsker å motta vann- og avløpstjenester må søke om dette. Kommuner og selskap benytter standardiserte avtalevilkår, både for utførelsen av selve tilkoblingen (tekniske bestemmelser) og for den løpende leveransen (administrative bestemmelser). Eierrådigheten over den offentlige hovedledningen er grunnlaget for at kommunen kan bestemme hvordan de private stikkledningene skal utføres. Når de private stikkledningene er etablert og koblet på hovedledningen, avsluttes det som regel med en ferdigmelding.

Som vannverkseier skal kommuner og selskap levere nok og rent vann til abonnentene i samsvar med drikkevannsforskriften. Når de som eier av avløpsanlegg slipper renset vann tilbake til vannkretsløpet må de overholde kravene i forurensningsforskriften og vilkår i utslippstillatelsene.

Som et generelt utgangspunkt vil behandlingen av personopplysninger som er nødvendig for å kunne yte vann- og avløpstjenester kunne hjemles i artikkel 6 (1) bokstav e:

«behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt»

Å utøve offentlig myndighet eller utføre en oppgave i allmennhetens interesse, krever et supplerende rettsgrunnlag i det ovennevnte regelverket.

Et sentralt spørsmål er om personopplysningene er **nødvendige** for å yte vann- og avløpstjenester. Nødvendighetskravet er nært knyttet til dataminimeringsprinsippet.¹⁰⁾ Kommunen eller selskapet skal bare samle inn og behandle personopplysninger som er adekvate, relevante og nødvendig for å oppfylle formålet med behandlingen, som er å levere vann- og avløpstjenester. De må derfor foreta en streng vurdering av om personopplysningene som behandles er nødvendige for å kunne yte tjenestene.

Hvis personopplysningene ikke er nødvendige, så kan bokstav e ikke benyttes som rettslig grunnlag. I en slik situasjon må kommunen eller selskapet vurdere om det finnes et annet behandlingsgrunnlag i personvernforordningen artikkel 6 og 9 (forutsatt særlige kategorier av personopplysninger)¹¹⁾, for å kunne behandle personopplysningene.

5.3. Behandlingsaktiviteter og personopplysninger

Å levere vann- og avløpstjenester kan innebære flere ulike behandlingsaktiviteter som omfatter et bredt spekter av personopplysninger. I det videre redegjøres det for de ulike behandlingsaktivitetene som en kommune eller selskap typisk vil gjennomføre for å kunne levere vann- og avløpstjenester til abonnentene.

5.3.1. Søknad om tilkobling til vann- og avløpsledninger og dokumentasjon før ferdigmelding

Kommuner og selskap behandler personopplysninger i søknader fra utbyggere (i praksis entreprenører) som ønsker å legge stikkledninger fra sine bygninger og koble disse til hovedledningene. Slike søknader sendes i forkant av søknader om byggetillatelser. Noen har elektroniske søknadsskjemaer, mens andre krever at utfylt søknadsskjema sendes til postmottaket. Typen personopplysninger som innhentes og hvem de registrerte er kan variere.

Kommuner og selskap mottar og behandler også personopplysninger når utbyggere orienterer kommunen om at stikkledningene er etablert (ofte kalt en ferdigmelding) før bygningsmyndigheten utsteder ferdigattester.

Typen registrerte:

Utferdigelse av søknad om å koble stikkledningene til hovedledningene gjøres ofte av ansvarlig entreprenør. Det vil derfor behandles personopplysninger om kontaktperson hos ansvarlig entreprenør ifbm. søknad om tilkobling. Videre kreves det også underskrift fra hjemmelshaver eller tiltakshaver, samt rørlegger og ansvarlig søker.

I noen tilfeller vil det også fremkomme opplysninger om naboer eller andre tredjeparter som berøres av vann- og avløpsledningene.

Typen personopplysninger:

Søknadsskjemaer for tilkobling til hovedledninger og ferdigmeldinger inneholder typisk:

- Adresse, gårdsnr., bruksnr., festenr. og seksjonsnr., som er opplysninger som kan knyttes til hjemmelshaver eller tiltakshaver.
- Tekniske spesifikasjoner ved eiendom eller tiltak som kan knyttes til hjemmelshaver eller tiltakshaver, herunder avledning av overvann, sprinkleranlegg, reduksjonsventil, ledningsstrekke, m.m.
- Tinglyste erklæringer/avtaler med naboer eller andre tredjeparter som berøres av vann- og avløpsledningene.
- Fødselsnummer, adresse og kontaktinformasjon til hjemmelshaver/tiltakshaver/fakturamottaker.
- Underskrift og arbeidsgiver for ansvarlig entreprenør og rørlegger.
- Underskrift for ansvarlig søker og hjemmels-/tiltakshaver.

10) Se rapportens pkt. 3.3.

11) Se rapportens pkt. 4.

Systemer/applikasjoner som benyttes:

Mange kommuner og selskap har dedikerte systemer for å motta og håndtere søknader om tilkobling til hovedledningene, samt ferdigmeldinger. Flere av kommunene som ble intervjuet i forbindelse med denne rapporten hadde tatt i bruk én eller flere av følgende løsninger:

- Gemini privat
- Gemini Entreprenørportal
- KOMTEK VA

Disse løsningene muliggjør blant annet saksbehandling, innsendelse av dokumentasjon og arkivering.

5.3.2. Vann- og avløpsgebyr

Kommuner og selskap behandler personopplysninger i forbindelse med at de sender faktura for gebyrene til abonnentene. Dette er gjerne den mest omfattende behandlingsaktiviteten de gjennomfører som tjenesteleverandør, hvor de blant annet innhenter eiendomsinformasjon fra Matrikkelen til Kartverket. De mottar også henvendelser fra abonnenter som ikke kan betale gebyret eller bestrider fakturaen. Slike henvendelser kommer både via e-post og telefon. Flere av kommunene som ble intervjuet ga uttrykk for at de ofte mottar mer personopplysninger enn de har behov for når abonnentene henvender seg til dem. Denne typen overskuddsinformasjon kan inneholde særlige kategorier av personopplysninger.

Typen registrerte:

Abonentene får sine personopplysninger behandlet ved innkreving av vann- og avløpsgebyr. Abonnentene kan være innbyggere, hytteeiere eller virksomheter. I det sistnevnte tilfellet vil den registrerte typisk være en kontaktperson i virksomheten.

Typen personopplysninger:

Saksbehandlingen ved innkreving av vann- og avløpsgebyr vil typisk omfatte:

- Navn og kontaktinformasjon til abonnent.
- Navn og kontaktinformasjon til kontaktperson i virksomhet.
- adresse, gårdsnr., bruksnr., festnr., seksjonsnr., som kan knyttes til abonnent.
- Fødselsnummer.
- Kundenummer.
- Avtalenummer.
- Konto- og bankinformasjon.
- Vannforbruk.
- Purregebyrer.
- Henvendelser/klager på vann- og avløpsgebyr.

Systemer/applikasjoner som benyttes:

Kommuner og selskap benytter flere systemer/applikasjoner for å kreve inn gebyret. Disse systemene sammenstiller i mange tilfeller data fra Kartverket og andre kilder for å kunne gi informasjon om tinglyst eier, gårdsnr., bruksnr., festnr., seksjonsnr., m.m. Flere som ble intervjuet i forbindelse med denne rapporten hadde tatt i bruk følgende systemer:

- Gemini privat
- KOMTEK
- GISLINE

Flere av disse systemene har integrasjoner mot kommunens eget sak- og arkivsystem.

5.3.3. Varsling av abonnenter

I noen situasjoner kan kommuner og selskap ha behov for å varsle abonnenter om hendelser som får betydning for vann- og avløpstjenesten. Eksempler på dette er kokevarsel ved mistanke om at drikkevannet er forurensset og varsel om avstenging ved rehabilitering av ledninger. Flere metoder benyttes for å varsle abonnentene, som SMS og e-post. Noen benytter dedikerte systemer for å sende ut varslene. Slike systemer gjør det mulig å bruke såkalt geofencing, som innebærer at det kan opprettes en virtuell grense i et geografisk område, slik at det bare sendes ut varsler til abonnenter innenfor dette området.

Typen registrerte:

Abonentene kan være innbyggere og hytteeiere i kommunen, samt virksomheter. I det sistnevnte tilfellet vil de registrerte typisk være en kontaktperson i virksomheten.

Typen personopplysninger:

Varsling av abonnenter vil typisk innebære behandling av:

- E-post.
- Telefonnummer.
- Dersom geofencing eller lignende teknologi benyttes, vil også lokasjonsdata bli behandlet.

Typen systemer som benyttes:

Varsling av abonnenter skjer vanligvis per SMS eller e-post.

5.3.4. Kameraovervåking

Eiere av vann- og avløpsanlegg behandler personopplysninger i forbindelse med kameraovervåking av anlegg, bygninger og driftskontrollsystemer. Formålene med denne overvåkingen faller i hovedsak innenfor to kategorier:

- 1) Driftsovervåking for å sikre effektiv drift og håndtering av avvik.
- 2) Overvåking av sikkerhetsmessige hensyn.

De som har blitt intervjuet har gitt uttrykk for at omfanget av kameraovervåkingen er begrenset, både når det gjelder driftsovervåking og overvåking av sikkerhetsmessige hensyn. Et typisk tilfelle er at det settes opp kameraer på inngjerdet område rundt anlegg som har vært gjenstand for gjentatt hærverk.

Typen registrerte:

Omfanget av de registrerte som kan bli fanget opp gjennom kameraovervåking, avhenger av hvilket formål overvåkingen har. For driftsovervåking vil det nesten utelukkende være ansatte som blir fanget opp av kameraet. Overvåking av sikkerhetsmessige årsaker vil i større grad gjøres på områder hvor det er større sannsynlighet for at andre blir fanget opp av kameraene. Dette kan være forbipasserende eller personer som ulovlig oppholder seg på eiendommen.

Typen personopplysninger:

Kameraovervåking innebærer behandling av video og bilder av de registrerte.

Typen systemer som benyttes:

Det benyttes et bredt spekter av ulike kameraovervåkingsløsninger.

5.3.5. Sosiale medier

Noen kommuner og selskap har etablert egne sider på sosiale medier (SoMe). Disse kanalene benyttes blant annet til å informere om aktiviteter og hendelser. Abonnenter og andre kan kommunisere direkte med kommunen eller selskapet på disse sosiale mediene. I tillegg er det mulig å kommentere og dele innlegg som legges ut.

Typen registrerte:

De registrerte vil være brukere som interagerer med SoMe-profilene.

Typers personopplysninger:

Kommuner og selskap behandler typisk følgende personopplysninger i forbindelse med SoMe:

- Navn og profilopplysninger.
- Delinger, likes, kommentarer og andre reaksjoner som den registrerte har på innlegg.
- Henvendelser på direktemeldinger/chat. Disse henvendelsene kan inneholde et stort antall personopplysninger, men som regel vil det være enkle spørsmål eller tilbakemeldinger fra abonnenter.

Systemer/applikasjoner som benyttes:

Det er mange tilbydere av SoMe-plattformer, og det kommer nye tilbydere til fortløpende. De intervjuede kommunene og selskapene benytter i hovedsak Facebook og X (tidligere Twitter) og har etablert offisielle profiler for sine virksomheter.

5.3.6. Behandling av ansattes personopplysninger

En del kommuner og selskap behandler personopplysninger om et stort antall ansatte, mens andre bare har en enkelt ansatt med ansvar for vann- og avløpstjenestene og som i tillegg kan ha andre roller, som å være kommunal forurensningsmyndighet. Organiseringen av HR-funksjonen varierer. Noen har dedikerte ressurser, mens andre benytter HR-avdelingen i den kommunale administrasjonen. IKSene som ble intervjuet hadde en egen dedikert HR-funksjon.

Personopplysningene til ansatte samles inn og behandles gjennom hele arbeidsforholdet, herunder ved oppstart, lønnskjøring, utviklingssamtaler og avslutning av arbeidsforhold.

Typers registrerte:

De registrerte vil være ansatte, konsulenter og innleide.

Typers personopplysninger:

Arbeidsgivere behandler typisk følgende personopplysninger:

- Navn, kjønn, kontaktinformasjon og adresse.
- Søknadsopplysninger, som CV, utdanning, resultater fra evne- og personlighetstester, personlige egenskaper, språkkunnskaper, m.m.
- Fødselsnummer.
- Ansattnummer.
- Stillingsnivå og organisasjonstilhørighet.
- Opplysninger i personalmappe, som pårørende, utviklingssamtaler, advarsler m.m.
- Timeføring.
- Fravær og sykemeldinger.
- Lønns- og kontoinformasjon.
- Skatt og andre lønnstrekk.
- Fagforeningsmedlemskap.
- Ombudsroller.
- Utlegg.
- Tilganger til systemer/applikasjoner.

Systemer/applikasjoner som benyttes:

De fleste har dedikerte HR-systemer hvor ansattopplysninger lagres og behandles. Disse systemene kan enten være en del av systemporteføljen¹²⁾ til den kommunale administrasjonen eller være anskaffet spesifikt for vann- og avløpsavdelingene i kommunene.

5.3.7. Behandling personopplysninger gjennom digitale vannmålere

Se rapportens kapittel 9.

12) Samling av alle IT-systemer og applikasjoner som en organisasjon bruker.

6. Håndtering av personopplysninger ved behandling av søknader om utslipps-tillatelse og tilsyn med utslippene

6.1. Rettslige utgangspunkter

Kommunen har i medhold av forurensningsloven og forurensningsforskriften myndighet til å behandle søknader om tillatelse til utslipp av avløpsvann i mellomstore og små tettbebyggelser og utslipp fra de minste avløpsanleggene. Forurensningsloven pålegger også kommunen å føre tilsyn med utslippene. Som et generelt utgangspunkt vil behandlingen av personopplysninger som er nødvendig for å kunne behandle utslippstillatelser og føre tilsyn med utslippene kunne hjemles i artikkel 6 (1) bokstav e.

6.2. Behandlingsaktiviteter og personopplysninger

Behandling av søknader om utslippstillatelse og tilsynsaktiviteter kan innebære flere ulike behandlingsaktiviteter som omfatter et bredt spekter av personopplysninger. I det videre redegjøres det for de ulike behandlingsaktivitetene som en kommune eller et selskap typisk vil gjennomføre for å kunne behandle søknader om utslippstillatelse og føre tilsyn med utslippene.

6.2.1. Utslippstillatelser

Den som vil slippe ut avløpsvann fra bolighus, hytter, turistbedrifter, virksomheter, ol. plikter å søke den kommunale forurensningsmyndigheten om utslippstillatelse.

Personopplysninger som behandles i forbindelse med utslippstillatelser innhentes som regel gjennom søknadsskjemaer.

Typen registrerte:

De registrerte er typisk:

- Bygningseiere
- Kontaktpersoner hos foretak.

Typen personopplysninger:

Søknadsskjemaer for utslippstillatelser inneholder typisk følgende personopplysninger:

- Navn og kontaktinformasjon.
- Adresse, gårdsnr., bruksnr., festnr. og seksjonsnr., som er opplysninger som kan knyttes til hjemmelshaver eller tiltakshaver.
- Tekniske spesifikasjoner ved eiendom eller tiltak som kan knyttes til hjemmelshaver eller tiltakshaver
- Beskrivelse av utslippskilden og miljøpåvirkning.

Systemer/applikasjoner som benyttes:

Kommuner og selskap benytter typisk:

- KOMTEK.
- Gemini privat.
- Kommunale sak- og arkivsystemer som ACOS WebSak.

6.2.2. Tilsynsaktiviteter

Omfanget av kommunenes tilsynsaktiviteter varierer basert på blant annet ressurser, kompetanse og organisering.¹³⁾ Noen kommuner er proaktive i sin tilnærming med planer for regelmessig tilsyn. Andre har en mer ad-hoc-basert tilnærming, hvor tilsyn gjennomføres etter konkrete hendelser, henvendelser og/eller klager.

Hvordan tilsyn gjennomføres, vil blant annet avhenge av hva slags anlegg som kontrolleres, lokal praksis og om det har skjedd et utslipp. Flere av de som er intervjuet har beskrevet en utstrakt bruk av bilder og film for å dokumentere eventuelle funn og andre forhold på eiendommer det gjennomføres tilsyn på. Det innhentes videre personopplysninger per telefon før, under, og etter et tilsyn.

Typer registrerte:

Kommunene gjennomfører tilsyn hos både virksomheter og privatpersoner. De registrerte vil derfor i hovedsak omfatte eiere av avløpsanlegg og kontaktpersoner i virksomheter. I noen tilfeller mottar kommunene varsler eller klager fra naboer eller andre tredjeparter, som dermed også får sine personopplysninger behandlet.

Typer personopplysninger:

Kommuner behandler typisk følgende personopplysninger i forbindelse med tilsynsaktiviteter:

- Navn, adresse og kontaktinformasjon til hjemmelshavere.
- Navn og kontaktinformasjon til kontaktpersoner i virksomheter.
- Tekniske spesifikasjoner ved eiendom eller tiltak som kan knyttes til hjemmelshaver.
- Gårdsnr., bruksnr., festnr. og seksjonsnr. som kan knyttes til hjemmelshaver.
- Pålegg om utbedring.
- Forelegg og dagmulkt.
- Film og bilde.

Systemer/applikasjoner som benyttes:

Kommunene benytter ulike systemer for saksbehandlingen forbundet med tilsyn. Mange benytter kommunale saksbehandlingssystemer som ACOS WebSak og Public 360°. Andre har dedikerte saksbehandlingssystemer for vann og avløp, som Gemini-systemene.

¹³⁾ Se Norsk Vann Rapport 184/2011 Tilsyn med utslipp fra avløpsanlegg innen kommunens myndighetsområde, kap. 4.

7. Hvilke forpliktelser har den behandlingsansvarlige?

Personvernregelverket pålegger behandlingsansvarlige et stort antall plikter. De mest aktuelle vil omtales i det følgende.

7.1. Ivareta de registrertes rettigheter

Personvernforordningen definerer en rekke rettigheter som de registrerte har overfor den behandlingsansvarlige. Rettighetene gir de registrerte større kontroll over hvordan personopplysningene deres behandles, og sikrer åpenhet rundt behandlingsaktivitetene som kommuner og selskaper gjennomfører.

Henvendelser fra registrerte som påberoper seg en rettighet, skal i utgangspunktet besvares så fort som mulig og senest innen én måned.

7.1.1. Retten til informasjon

Kommuner og selskap må informere abonnenter, de som søker om utslippstillatelse eller som kommunen fører tilsyn med, ansatte og andre registrerte om hvordan personopplysningene deres behandles. Kravene til informasjon avhenger av om personopplysningene innhentes fra de registrerte selv eller fra andre kilder.

Vanligvis gis informasjon gjennom en egen personvernerklæring, for eksempel på kommunens hjemmeside. Det er imidlertid ikke alltid at personvernerklæringen gir tilstrekkelig informasjon om behandlingsaktivitetene. Det vil da være nødvendig å supplere informasjonen i personvernerklæringen med ytterligere informasjon.

Informasjonen som må gis avhenger av hvor kommunen eller selskapet har hentet personopplysningene til den registrerte fra.¹⁴⁾

Eksempel:

En kommune velger å inkludere informasjon om hvordan de behandler personopplysninger de får fra digitale vannmålere i sine abonnementsvilkår som finnes på hjemmesiden til kommunen.

For ansattes personopplysninger vil det typisk være en intern personvernerklæring tilgjengelig på kommunens eller selskapets intranett.

7.1.2. Retten til innsyn

De registrerte har rett til å be om innsyn i sine egne personopplysninger som behandles av kommunen eller selskapet. I tillegg til å få innsyn personopplysningene, skal de registrerte også få følgende informasjon:

- Formålene med behandlingen.
- Hvilke kategorier av personopplysninger som behandles.
- Mottakere/kategorier av mottakere av personopplysninger, herunder mottakere som befinner seg i land utenfor EU/EØS.
- Lagringstiden til personopplysningene.
- De registrertes rettigheter.
- Retten til å klage til en tilsynsmyndighet.
- (Dersom personopplysningene ikke ble samlet inn fra den registrerte selv) Hvor personopplysningene stammer fra.
- (Dersom relevant) Forekomsten av automatiserte avgjørelser, herunder profilering.
- (Dersom personopplysninger overføres til land utenfor EU/EØS eller internasjonal org.) Informasjon om nødvendige garantier¹⁵⁾ iht. Personvernforordningen artikkel 46.

¹⁴⁾ Se vedlegg 1.

¹⁵⁾ Nødvendige garantier kan bl.a. sikres gjennom standard contractual clauses (SCC) eller bindende virksomhetsregler (BCR).

De registrerte skal bare få en kopi av sine egne personopplysninger. Kommuner og selskap må derfor påse at andre personers personopplysninger sladdes.

Når det gjelder innsynsbegjæringer, er det viktig å merke seg at det finnes flere regelverk som kan gi grunnlag for slike forespørsler. I tillegg til personvernforordningen, som gir enkeltpersoner rett til innsyn i sine egne personopplysninger, kan offentlighetsloven og forvaltningsloven også gi rett til innsyn i dokumenter og informasjon som forvaltes av kommunen. Dette kan skape en kompleks situasjon for de ansatte, som må navigere mellom ulike regelverk for å sikre at de oppfyller sine lovpålagte forpliktelser.

For å unngå misforståelser og sikre korrekt behandling, bør kommuner og selskap avklare med den registrerte hvilket regelverk innsynsbegjæringen gjelder. Dette kan innebære å informere om forskjellene mellom de ulike regelverkene og hvilke rettigheter og begrensninger som gjelder for hver av dem.

En annen utfordring er at ulike regelverk kan ha forskjellige krav til hvordan innsyn skal gis og hvilke opplysninger som kan unntas. For eksempel kan personopplysninger måtte sladdes før dokumenter utleveres etter offentlighetsloven. Dette krever nøye vurdering og ofte en betydelig administrativ innsats, for å sikre at alle relevante lover og forskrifter overholdes. Kommuner og selskap må derfor ha gode rutiner og kompetanse på plass for å håndtere innsynsbegjæringer på en korrekt og effektiv måte.

Det finnes også lovgivning som pålegger kommuner og selskap å utlevere opplysninger, som kan inneholde personopplysninger, til tredjeparter. Et eksempel på dette er ledningsregistreringsforskriften.¹⁶⁾ I slike tilfeller vil kommunen eller selskapet være rettslig forpliktet til å utlevere personopplysninger, men det er likevel ikke slik at enhver personopplysning kan utleveres. I tråd med dataminimeringsprinsippet¹⁷⁾, skal det bare utleveres personopplysninger som er adekvate, relevante og nødvendig for å oppfylle formålet med utleveringen. Kommuner og selskap må derfor være varsomme med å utlevere personopplysninger, selv om utleveringen i seg selv er påkrevd i medhold av lov eller forskrift.

7.1.3. Retten til retting og sletting

De registrerte kan be om at kommuner og selskap retter uriktige personopplysninger eller supplerer mangelfulle personopplysninger.

De registrerte kan også kreve at kommuner og selskap sletter deres personopplysninger i følgende situasjoner:

- Personopplysningene er ikke lenger nødvendige for formålet de ble samlet inn for.
- Den registrerte trekker tilbake samtykket som ligger til grunn for behandlingen.
- Den registrerte protesterer mot behandlingen.
- Personopplysningene er blitt behandlet ulovlig (f.eks. uten et behandlingsgrunnlag).
- En rettslig forpliktelse pålegger kommunen eller selskapet å slette personopplysningene.

Det er flere unntak fra retten til sletting, herunder hvor fortsatt behandling er nødvendig for å anlegge eller forsvare seg mot rettslige krav.

7.1.4. Retten til begrensning av behandling

De registrerte kan kreve at behandlingen begrenses i flere situasjoner. Når den registrerte krever begrensning av behandlingen, skal den, med unntak av lagring, opphøre. Andre former for behandling kan bare skje hvor den registrerte samtykker eller hvor det er nødvendig for å anlegge eller forsvare seg mot rettslige krav.

16) Forskrift om innmåling, dokumentasjon og utlevering av geografisk informasjon om ledninger og annen infrastruktur i grunnen, sjø og vassdrag § 5.

17) Se rapportens pkt. 3.3.

Retten kan gjøres gjeldende hvor:

- Den registrerte mener personopplysningene er uriktige og kommunen eller selskapet trenger tid til å kontrollere opplysningene.
- Behandlingen er ulovlig, men den registrerte motsetter seg sletting og i stedet ber om begrensning av behandlingen.
- Den registrerte har behov for opplysningene, for å anlegge eller forsvare seg mot rettslige krav.
- Den registrerte protesterer mot behandlingen, i påvente av kontrollen av om kommunens eller selskapets berettigede interesser veier tyngre enn sine egne.

Den registrerte skal informeres før behandlingen eventuelt gjenopptas.

7.1.5. Retten til dataportabilitet

De registrerte har i visse situasjoner rett til å få utlevert personopplysninger som de har gitt til kommunen eller selskapet. Opplysningen skal utleveres i et strukturert, vanlig brukt og maskinlesbart format¹⁸⁾. De registrerte kan også be om at dataene overføres til en annen behandlingsansvarlig. Dette kalles retten til dataportabilitet og kan påberopes når behandlingen er basert på samtykke eller en avtale med den registrerte, eksempelvis der hvor abonnenter mottar vann- og avløpstjenester basert på disse rettslige grunnlagene. Det samme gjelder hvor behandlingen utføres automatisk.

7.1.6. Retten til å protestere

Hvis kommuner og selskap behandler personopplysninger basert på en berettiget interesse, eksempelvis behandling av personopplysninger gjennom bruk av kameraovervåking (personvernforordningen artikkel 6 (1) bokstav f), så kan de registrerte protestere mot behandlingen. De som mottar slike henvendelser, må da vurdere om behandlingen likevel kan fortsette, basert på tvingende berettigede grunner som veier tyngre enn interessene til den registrerte.

De registrerte kan alltid protestere mot behandlinger med formål om å gjennomføre direkte markedsføring, noe som nok uansett er lite relevant i vannbransjen.

7.1.7. Retten til å ikke være gjenstand for automatiserte individuelle avgjørelser, herunder profilering

De registrerte har rett til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering, som har rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker vedkommende. Det er flere unntak fra denne retten, herunder hvor avgjørelsen er nødvendig for å inngå/oppfylle en avtale mellom den registrerte og kommunen eller selskapet eller hvor den registrerte har gitt uttrykkelig samtykke.

7.1.8. Unntak fra de registrertes rettigheter

Det finnes flere unntak fra de registrertes rettigheter i kapittel 4 i personopplysningsloven. Personopplysningsloven § 16 gjør det blant annet mulig å holde helt eller delvis tilbake opplysninger i forbindelse med retten til informasjon og innsyn dersom:

- Det må anses utilrådelig at den registrerte får kjennskap til av hensyn til vedkommendes helse eller forholdet til personer som står vedkommende nær
- Opplysningene i lov eller med hjemmel i lov er underlagt taushetsplikt
- Det utelukkende finnes i tekst som er utarbeidet for intern saksforberedelse, og som heller ikke er utlevert til andre, så langt det er nødvendig å nekte innsyn for å sikre forsvarlige interne avgjørelsesprosesser

Kommuner og selskap som ønsker å holde tilbake personopplysninger i medhold av denne bestemmelsen, må gjøre en grundig vurdering av om vilkårene for å holde tilbake opplysninger er oppfylt. Det kan være at bare deler av opplysningene kan holdes tilbake. Vurderingen må dokumenteres.

18) Det er viktig å merke seg at retten til dataportabilitet ikke gjelder for all behandling av personopplysninger. For eksempel gjelder den ikke for behandling som er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet. Videre gjelder den heller ikke for behandling som er basert på andre rettslige grunnlag enn samtykke eller avtale.

7.2. Innebygd personvern og personvern som standardinnstilling

Innebygd personvern og personvern som standardinnstilling, stiller krav til at en kommune eller selskap tar hensyn til personvern i alle faser av en behandlingsaktivitet.¹⁹⁾ Det skal etableres tekniske og organisatoriske tiltak for å sikre en effektiv implementering av personvernprinsippene og at de registrertes rettigheter og friheter ivaretas gjennom hele behandlingsprosessen. De mest personvernvennlige løsningene skal som utgangspunkt benyttes i enhver behandlingsaktivitet.

Eksempel:

Et vann- og avløpsselskap har anskaffet et nytt kameraovervåkingssystem for å overvåke sine anlegg. Kameraene vil potensielt fange opp bilder av ansatte, besøkende og andre personer som befinner seg på området. For å sikre at personvernet ivaretas i henhold til kravene om innebygd personvern og personvern som standardinnstilling, har selskapet etablert følgende tiltak:

- Systemet settes opp med personvernvennlige standardinnstillinger. Dette inkluderer tilgangsstyring til opptakene, kryptering av lagrede data, og automatisk sletting av opptak etter en viss periode.
- Kameraovervåkingssystemet konfigureres, slik at det kun gjøres opptak på relevante områder på anlegget. Ansikter og områder hvor ansatte jobber, sladdes når det gjøres opptak.
- Ansatte, besøkende og andre berørte parter informeres om kameraovervåkingen, formålet med overvåkingen, og deres rettigheter i henhold til personvernregelverket.

7.3. Bruk av databehandlere og databehandleravtaler

Hvis en kommune eller selskap benytter en tredjepart til å behandle personopplysninger på vegne av seg, så har de engasjert en «databehandler». Personvernforordningen pålegger kommuner og selskap å bare benytte databehandlere som gir tilstrekkelige garantier for at de behandler personopplysninger i samsvar gjeldende regelverk og etablerer tekniske og organisatoriske tiltak for å verne de registrertes rettigheter.²⁰⁾

Behandling som utføres av en databehandler skal være underlagt en avtale. Det er vanlig å inngå en egen databehandleravtale som et vedlegg til hovedavtalen med databehandleren. Personvernforordningen stiller flere krav til hva en slik avtale skal inneholde.²¹⁾

Eksempel:

Et vann- og avløpsselskap flytter et driftskontrollsystem over i en skyløsning. Driftskontrollsystemet inneholder personopplysninger om ansatte, noe som fører til at leverandøren av skyløsningen blir en databehandler. Selskapet inngår en databehandleravtale med skyleverandøren som uttrykkelig regulerer hvordan personopplysninger skal behandles og beskyttes.

Databehandlere har ofte egne maler for databehandleravtaler som inkluderes i kontraktspakken som sendes til behandlingsansvarlig. Disse databehandleravtalene kan være utformet på en måte som stiller databehandler i en fordelaktig stilling, dersom det skulle oppstå uenigheter, brudd på avtalen, brudd på personopplysningssikkerheten, osv. i løpet av avtaleforholdet. Kommuner og selskap bør, hvor mulig, forsøke å benytte en egen mal for databehandleravtaler.

19) Personvernforordningen artikkel 25.

20) Personvernforordningen artikkel 28 (1).

21) Personvernforordningen artikkel 28. (3).

Hvis databehandleren motsetter seg dette, bør kommunen eller selskapet gjennomgå avtalen nøye og identifisere eventuelle ufordelaktige eller uakseptable bestemmelser.²²⁾

7.4. Protokollføring

Personvernregelverket pålegger virksomheter å føre en protokoll over hvilke behandlingsaktiviteter som gjennomføres.²³⁾ Protokollen skal blant annet inneholde en beskrivelse av formålene med de ulike behandlingene, hvem de registrerte er, og en generell beskrivelse av hvilke tekniske og organisatoriske sikkerhetstiltak som er etablert for å beskytte personopplysningene.²⁴⁾

7.5. Risikovurderinger og personvernkonsekvensvurderinger (DPIA)

Kommuner og selskap må gjennomføre risikovurderinger for å kunne identifisere og etablere tilstrekkelige tekniske og organisatoriske sikkerhetstiltak ved behandling av personopplysninger.²⁵⁾ Hendelser som kan få betydning for personvernet og rettighetene og frihetene til personer må identifiseres. Eksempler på slike hendelser er hacking, ansattes snoking i personopplysninger og at personopplysninger lagres lengre enn tiltenkt. Sannsynligheten for at slike hendelser inntreffer og konsekvensene for personvernet og rettighetene og frihetene til fysiske personer må vurderes. Basert på disse risikovurderingene må kommuner og selskap etablere egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er tilpasset risikoen. Eksempler på slike sikkerhetstiltak er kryptering, tilgangsstyring og rutiner for sletting av personopplysninger.

Personvernkonsekvensvurderinger (DPIA) er en egen, særlig regulert, form for risikovurdering som må gjennomføres når behandlingen medfører høy risiko for de registrertes rettigheter og friheter.²⁶⁾ Behandlinger som typisk innebærer høy risiko er hvor det behandles særlige kategorier av personopplysninger i stort omfang, bruk av ny teknologi og systematisk overvåking i stor skala av et offentlig tilgjengelig område. En kommune bør f.eks. vurdere om kame-raovervåking bør underlegges en DPIA-vurdering.

Eksempel:

En kommune ønsker å ta i bruk digitale vannmålere for å måle forbruk og fakturere abonnenter. Bruk av ny teknologi og løsninger som dette må risikovurderes for å avdekke om tilstrekkelige tekniske og organisatoriske sikkerhetstiltak for å beskytte personopplysningene er etablert. Hvis kommunen ønsker å benytte personopplysninger som avslører helseopplysninger fra vannmåleren for velferdsteknologiske formål, så kan dette innebære at behandlingen representerer en høy risiko for abonnentene, og det blir dermed nødvendig å gjennomføre en DPIA i tillegg.

22) Se også Norsk Vann Rapport 238/2018 Informasjonssikkerhet i skybaserte tjenester for vannbransjen, s. 58.

23) [Datatilsynet har laget maler for protokoller som kan lastes ned.](#)

24) Personvernforordningen artikkel 30.

25) Personvernforordningen artikkel 32.

26) Personvernforordningen artikkel 35.

7.6. Brudd på personopplysningssikkerheten

Et brudd på personopplysningssikkerheten er brudd på sikkerheten som fører til at personopplysninger på en eller annen måte kommer på avveie. Dette kan være utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.²⁷⁾

Hvis et brudd på personopplysningssikkerheten oppstår, kan kommunen eller selskapet bli nødt til å rapportere bruddet til Datatilsynet. Utgangspunktet er at brudd skal meldes, med mindre det er sannsynlig at bruddet ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Den behandlingsansvarlige må vurdere konkret hva slags risikoer et brudd representerer for personer som er omfattet av bruddet. Hvis den behandlingsansvarlige konkluderer med at et brudd må rapporteres til Datatilsynet, skal dette skje uten ugrunnet opphold, og senest innen 72 timer.²⁸⁾

Hvis et brudd på personopplysningssikkerheten er så alvorlig at det representerer en høy risiko for rettighetene og frihetene til personer som er omfattet, vil kommunen eller selskapet i tillegg være nødt til å underrette de registrerte om bruddet.²⁹⁾

Eksempel:

En ansatt i kommunen oppdager at det har vært en alvorlig feil i deres IT-system som har ført til at tilgangsstyringen har sviktet. Dette har resultert i at personopplysninger, inkludert helseopplysninger, personnummer og adresser, har vært tilgjengelige for alle ansatte i kommunen over en lengre periode. Bruddet involverer sensitive personopplysninger, og konsekvensene for de berørte personene er vurdert som alvorlige, da det kan føre til bl.a. identitetstyveri og diskriminering.

I dette tilfellet er det nødvendig å rapportere bruddet til Datatilsynet. Kommunen beslutter at de berørte ansatte også må informeres om bruddet og hvilke tiltak som er iverksatt for å begrense skadevirkningene. Internt må bruddet rapporteres i kommunens kvalitetssystem, og det må gjennomføres en grundig gjennomgang av tilgangsstyringen for å identifisere og rette opp svakheter. Videre må det implementeres strengere sikkerhetstiltak og opplæring for ansatte, for å forhindre at lignende hendelser skjer i fremtiden.

7.7. Lagringstid og arkivering

I tråd med lagringsbegrensningsprinsippet,³⁰⁾ skal personopplysninger bare lagres så lenge de er nødvendige for å oppfylle formålet med behandlingen. Det finnes imidlertid situasjoner hvor en kommune eller selskap er lovpålagt å lagre personopplysninger i lengre tid enn det som i utgangspunktet er nødvendig for formålet med behandlingen.

Arkivloven³¹⁾ med tilhørende forskrifter pålegger kommuner å ha et arkiv og lagre opplysninger som er omfattet av arkivplikten. Dette omfatter også personopplysninger. Dersom personopplysninger er arkivpliktige, skal de oppbevares i tråd med denne plikten. Kommunen må vurdere konkret om personopplysningene er omfattet av arkivplikten.

27) Personvernforordningen artikkel 4 (12).

28) Personvernforordningen artikkel 33.

29) Personvernforordningen artikkel 34.

30) Se rapportens pkt. 3.5.

31) Arkivlova § 6.

8. Særlige personvernutfordringer i vannbransjen

Kommuner og selskap møter på flere personvernproblemstillinger og fallgruver i sitt daglige virke. Mange av disse utfordringene skyldes særegenheter ved vannbransjen, som organisatorisk plassering, bruk av teknologi, kompetanse og personvernkultur. I dette kapitlet redegjøres det for disse personvernutfordringene og fallgruvene. Det vil videre bli redegjort for hvilke organisatoriske og tekniske tiltak som bør etableres, for å håndtere disse personvernproblemstillingene.

8.1. Organisatorisk avstand

Majoriteten av de som jobber med å levere vann- og avløpstjenester er ansatt i kommuner. Det varierer fra kommune til kommune hvor de ansatte organisatorisk er plassert, men mange steder er tjenesten plassert i egne vann- og avløpsavdelinger, eventuelt sammen med andre tekniske tjenester, eller i et kommunalt eid selskap. Dette innebærer at det ofte er betydelig organisatorisk avstand mellom disse ansatte og ansatte som ivaretar personvernfunksjonene i den kommunale administrasjonen.

Ansatte som jobber som forurensningsmyndighet kan være plassert i en vann- og avløpsavdeling, men også i en byggesaksavdeling eller i en vertskommune. Avstanden til kommuneadministrasjonen vil derfor variere.

Personvernrelevante funksjoner som ofte er knyttet til den kommunale administrasjonen er:

- Personvernombudet
- Personvernansvarlig
- Sikkerhetsleder/-ansvarlig
- CISO(32)
- Kommuneadvokat
- Juridisk avdeling
- IT

I tillegg til den organisatoriske avstanden, er det ofte også geografisk avstand mellom den kommunale administrasjonen og de som jobber med vann og avløp. I mange tilfeller opererer de ut fra egne lokaler. Denne avstanden bidrar i mange tilfeller til å gjøre kommunikasjonen med de som ivaretar personvernfunksjonene i kommunen vanskelig.

Flere av de intervjuede hadde lite eller ingen jevnlig kommunikasjon med personvernfunksjonene i kommunen. Noen ga også uttrykk for at det kan være utfordrende å få bistand til å ivareta sine forpliktelser etter personvernregelverket.

Personvernombudet har både en rådgivende og en kontrollerende rolle.³³⁾ Ansatte skal kunne henvende seg til ombudet med alle personvernspørsmål. Noen ansatte påpekte at det er lite kontakt med kommunens personvernombud, og at ivaretagelse av forpliktelsene i personvernregelverket må gjøres uten bistand fra personvernombudet og andre personvernfunksjoner i kommunen.

Den organisatoriske avstanden og begrensede kommunikasjonen fører også til at det blir vanskeligere for kommunen å ivareta sine forpliktelser etter personvernregelverket. Flere av de intervjuede ga uttrykk for at protokollen³⁴⁾, som ivaretas av kommunens administrasjon, ikke gir et korrekt bilde av deres behandlingsaktiviteter. God kommunikasjon og samarbeid vil også være viktig hvor registrerte påberoper seg sine rettigheter, som for eksempel innsyn.³⁵⁾

For å bedre kommunikasjonen og redusere konsekvensene av den organisatoriske avstanden, bør det etableres faste og jevnlig kontaktpunkter mellom kommunens personvernfunksjoner og de som jobber med vann og avløp. Eksem-

32) Chief Information Security Officer/informasjonssikkerhetsleder.

33) Personvernforordningen artikkel 39.

34) Se rapportens pkt. 6.3.

35) Se rapportens pkt. 6.1.2.

pelvis kan det etableres et personvernforum, hvor personvernombudet og relevant personell som jobber med vann og avløp møtes regelmessig for å diskutere problemstillinger, utveksle erfaringer og oppdatere hverandre på status i arbeidet med personvern.

8.2. Varierende kunnskap og kompetanse om vannbransjen hos kommunal administrasjon

De som jobber med vann og avløp må forholde seg til et stort antall lover og forskrifter. Samtidig oppstår det flere personvernmessige problemstillinger i tilknytning til deres særegne oppgaver, prosesser og bruk av teknologi. Håndtering av disse problemstillingene krever at man har kompetanse og kunnskap om hvordan bransjen fungerer og opererer.

Flere ansatte innenfor vann og avløp har påpekt at kommunens personvernfunksjoner som skal støtte virksomheten, ikke har nødvendig kunnskap og kompetanse om vannbransjen. Dette fører potensielt til at kommunikasjonen blir dårligere og bistanden mindre tilpasset deres behov. Utfordringene forbundet med manglende kunnskap og kompetanse forsterkes ytterligere av den organisatoriske avstanden til kommunenes personvernfunksjoner.³⁶⁾

Behandlingsaktivitetene³⁷⁾ representerer en ikke ubetydelig risiko for personvernet til abonnenter, ansatte og andre. Det er derfor viktig at sentrale personvernfunksjoner i kommunene gis opplæring og jobber aktivt med å øke sin kompetanse om hvordan vannbransjen opererer. På denne måten kan disse funksjonene gi mer effektivt støtte og bidra til å redusere risikoen for å komme i konflikt med personvernet.

8.3. Sentraliserte og desentraliserte personvernroller

Organiseringen av personvernarbeidet varierer. Noen kommuner og selskap har egne personvernressurser som jobber i organisasjonen (desentralisert), mens andre er mer avhengig av bistand fra ressurser i kommunens administrasjon (sentralisert). Egne personvernressurser bidrar i mange tilfeller til en mer moden organisasjon på personvern. Kommuner og selskap benytter ulike titler på disse personvernressursene, herunder personvernkoordinator, personvernansvarlig og personvernrådgiver.

Prosjektet observerte at en desentralisert organisering førte til økt etterlevelse av krav og forpliktelser, sammenlignet med en sentralisert organisering. De med egne personvernressurser gjennomførte i større grad egne internkontrollaktiviteter for å sikre etterlevelse av personvernregelverket. Personvernressursene fører ofte også en egen protokoll over behandlingsaktivitetene, noe som kan bidra til å sikre en kvalitativt bedre protokoll. Disse kunne også i større grad vise til dokumenterte rutiner, prosedyrer og retningslinjer for ivaretagelse av personvern i virksomheten.

Det er flere fordeler med egne dedikerte personvernressurser, men ikke alle kommuner og selskap har budsjetter og personell til å ha dette. Prosjektet observerte at den desentraliserte organiseringen var vanligere i større kommuner med relativt sterk økonomi.

For de som opererer med sentraliserte personvernressurser, er det desto viktigere at konsekvensene av den organisatoriske avstanden³⁸⁾ reduseres. Personvernressursene i kommunens administrasjon bør følge opp de som jobber med vann og avløp tettere i slike situasjoner. Samtidig bør de som jobber med vann og avløp etablere rutiner og prosedyrer som sikrer at kommunens personvernressurser involveres i relevante personvernprosesser og -problemstillinger.

36) Se rapportens pkt. 71.

37) Se rapportens pkt. 5.3.

38) Se rapporten pkt. 71.

8.4. Kompleks systemportefølje

Ansatte som jobber med vann og avløp benytter et bredt spekter av ulike systemer og applikasjoner i sin daglige drift. Dette kan være driftskontrollsystemer (DKS), saksbehandlingssystemer og overvåkingssystemer. De har både behov for særskilte systemer/applikasjoner innenfor vann- og avløpshåndtering, samt mer generelle systemer for saksbehandling og IT-drift. Dette resulterer i at mange har en systemportefølje bestående av løsninger anskaffet særskilt for vann og avløp, i tillegg til løsninger fra kommunen.

En kompleks systemportefølje gjør det vanskeligere å vurdere personvernrisikoer forbundet med bruk av systemene, flyten av personopplysninger mellom ulike systemer, behovet for ulike rutiner og prosedyrer for bruk av systemene, m.m. Noen av de intervjuede ga uttrykk for at noen systemer/applikasjoner som kommer fra kommunen er lite egnet for behovene og bruken til organisasjonen.

Kommunens IT-avdeling kan på sin side oppleve utfordringer rundt at ulike systemer for vann og avløp blir anskaffet og skal ivaretas i kommunens egen IT-infrastruktur. Ansatte som jobber med vann og avløp og kommunenes IT-avdelinger bør søke å etablere et tettere samarbeid om forvaltning av systemporteføljen for å sikre at personopplysninger i systemene/applikasjonene behandles i tråd med personvernregelverket og eventuelle interne prosedyrer og retningslinjer. Det bør også etableres rutiner for å involvere IT-avdelingen i eventuelle anskaffelsesprosesser av systemer for vann- og avløpshåndtering.

8.5. Mangel på fagsystemer og bruk av «skygge-IT»

Kommuner og selskaps komplekse systemportefølje dekker ikke alle behovene til ansatte i vannbransjen i deres daglige drift. Prosjektet intervjuet flere som ga uttrykk for at de var tillagt oppgaver/funksjoner som ikke var understøttet av noe fagsystem. Et eksempel var dokumentasjon av tilsyn med utslipp av avløpsvann. Flere bruker bilder og video i forbindelse med slike tilsyn, uten å ha fagsystemer eller formaliserte prosesser for å håndtere dette. Bilder og videoer ble i stedet lagret på ustrukturerte lagringsområder, som lokalt på ansattes PCer eller i SharePoint.

Bruk av ustrukturerte lagringsområder til personopplysninger gjør det vanskeligere å holde oversikt over arten og omfanget av personopplysninger som behandles, samt øker risikoen for at de ikke slettes i tråd med interne slettefrister og dermed strider mot lagringsbegrensningsprinsippet.³⁹⁾

Mangel på fagsystemer øker risikoen for at ansatte tar i bruk såkalt «skygge-IT». Skygge-IT er systemer og løsninger som brukes, uten eksplisitt organisatorisk godkjenning. Dette kan være bruk av ikke-godkjente programvareapplikasjoner, verktøy, systemer og enheter. Bruk av skygge-IT kan føre til at kommuner og selskap mister kontrollen over personopplysninger og øker risikoen for brudd på informasjons- og personopplysningssikkerheten. I mange tilfeller vil leverandører av skygge-IT også fungere som databehandlere, uten at kommunen eller selskapet har inngått databehandleravtaler med disse.⁴⁰⁾

Kommuner og selskap bør med jevne mellomrom kartlegge hvilke oppgaver og funksjoner de utfører og sammenligne disse med sin systemportefølje. Oppgaver og funksjoner som krever at det behandles personopplysninger, bør ha et fagsystem tilknyttet seg. Det bør videre utarbeides konkrete prosedyrer og retningslinjer som beskriver hvordan de ansatte skal behandle personopplysninger som en del av deres oppgaver, herunder hvordan personopplysninger skal innhentes, hvor de skal lagres og hvilke fagsystemer som skal benyttes.

Ansatte bør jevnlig minnes på at bare autoriserte systemer og applikasjoner skal benyttes ved utførelsen av oppgaver og funksjoner. All bruk av nye eller uautoriserte systemer og applikasjoner må først avklares med ledelsen.

39) Se rapporten pkt. 3.5.

40) Se rapportens pkt. 6.2.

8.6. Mangelfull internkontroll

Personvernforordningen krever at behandlingsansvarlige etablerer en egnet internkontroll for personvern.⁴¹⁾ Gjennom policyer og prosedyrer skal behandlingsansvarlig beskrive hvordan virksomheten sikrer etterlevelse av personvernregelverket og hvordan ansatte skal utføre sine oppgaver i overensstemmelse med kravene i regelverket. Omfanget av dokumentasjon som må etableres, vil blant annet avhenge av kompleksiteten i behandlingsaktivitetene og risikoeksponeringen til den behandlingsansvarlige.

De intervjuede har i varierende grad etablert policyer og prosedyrer for personvern. Noen har bare en overordnet personvernpolicy, mens andre har etablert mer omfattende dokumentasjon, bestående av prosedyrer og retningslinjer som stiller konkrete krav til ansattes håndtering av personopplysninger.

Omfanget av dokumentasjon avhenger også av organiseringen av personvernarbeidet.⁴²⁾ Prosjektet observerte at de med sentraliserte personvernroller og -funksjoner i mindre grad hadde egne policyer og prosedyrer, og i stedet benyttet kommunens rammeverk for personvern. De med desentraliserte personvernroller og -funksjoner hadde i større utstrekning egne policyer og prosedyrer som var tilpasset virksomheten og oppgavene til de ansatte.

Flere ga uttrykk for at det generelt var lite kjennskap til policyer og prosedyrer for personvern i organisasjonen. Noen var også usikre på hvilke krav disse styringsdokumentene stilte til organisasjonens håndtering av personopplysninger. Flere trakk også frem at dokumentasjonen som var utarbeidet var overordnet og lite tilpasset vann- og avløpsvirksomheten.

For å sikre at den enkelte ansatte og virksomheten som helhet etterlever personvernregelverket, bør kommuner og selskap vurdere om de eksisterende styringsdokumentene for personvern er tilstrekkelig dekkende og konkrete i lys av behandlingsaktivitetene og risikoeksponeringen til virksomheten. Jo mer omfattende og inngripende en behandlingsaktivitet er, jo større grunn er det til å etablere dedikerte prosedyrer og retningslinjer for hvordan ansatte skal håndtere personopplysningene i denne aktiviteten.

Eksempel:

Et vannverk har satt opp kameraer på sine høydebasseng for å forebygge at uvedkommende begår skadeverk. Vannverket bør da etablere rutiner og retningslinjer som beskriver hvem som skal ha tilgang til opptakene, i hvilke situasjoner opptakene kan benyttes, når opptakene skal slettes, osv.

Den behandlingsansvarlige skal kunne påvise at behandlingsaktivitetene skjer i samsvar med personvernregelverket. Det er derfor nødvendig å gjennomføre jevnlig kontroll av virksomhetens etterlevelse av personvernregelverket og interne policyer og prosedyrer.

Flere av de intervjuede ga uttrykk for at det ikke ble gjennomført jevnlig kontroll av organisasjonens etterlevelse av personvernregelverket eller interne policyer og prosedyrer. Dette var særlig tilfellet for de med sentraliserte personvernroller og -funksjoner. Disse hadde bare unntaksvis vært gjenstand for kontroller av personvernombudet eller andre kontrollerende funksjoner. Den organisatoriske avstanden til den kommunale administrasjonen,⁴³⁾ fører her til dårligere oppfølging og kontroll med etterlevelsen av personvernregelverket.

Personvernombudets og andre kommunale personvernfunksjoners oppfølging og kontroll av etterlevelsen av personvernregelverket bør styrkes. Dette er spesielt viktig der organiseringen av personvernroller og -funksjoner er sentralisert. Tettere og jevnligere kontroller av personvernetterlevelsen vil bidra til kontinuerlig forbedring av personvernprosessene.

41) Personvernforordningen artikkel 24.

42) Se rapportens pkt. 7.2.

43) Se rapportens pkt. 7.1.

8.7. Mangelfull risikostyring

Personvernregelverket krever at virksomheter etablerer egnede tekniske og organisatoriske tiltak for å oppnå et tilstrekkelig sikkerhetsnivå.⁴⁴⁾ Den behandlingsansvarlige må gjennomføre risikovurderinger på personvern for å kunne identifisere hvilke tiltak som det er nødvendig å implementere. I tilfeller hvor risikoen for de registrertes rettigheter og friheter er høy, kan det være nødvendig å gjennomføre en DPIA.

Flere av de intervjuede hadde ikke blitt involvert i, eller selv gjennomført, risikovurderinger av sikkerheten rundt behandlingsaktivitetene i virksomheten. Mange kunne vise til risikovurderinger på andre områder, men det var få som hadde gjennomført risikovurderinger spesifikt på personvern eller DPIA.

De som jobber med vann og avløp bør i større grad bli involvert i eller selv gjennomføre risikovurderinger på behandlingsaktivitetene som gjennomføres i virksomheten. De besitter selv dybdekunnskap om virksomheten og særskilte risikoer forbundet med behandlingsaktivitetene som gjennomføres. De med en sentralisert personvernorganisering bør følgelig få uttrykke sine synspunkter rundt risikoscenarioer, sannsynlighet for og konsekvenser av uønsket hendelser, samt eventuelle tekniske og organisatoriske tiltak for å redusere risiko.

8.8. Varierende personvernkompetanse hos ansatte i vann og avløp

Flere av de intervjuede ga uttrykk for at personvernkompetansen blant de ansatte ikke er god nok, og at det er et generelt ønske om å øke kompetansen i organisasjonen. Frekvensen og omfanget av opplæringsaktivitetene på personvernområdet varierte, men det var en tendens til at de med en desentralisert organisering hadde jevnligere opplæringsaktiviteter.

Ansatte er avhengige av å få opplæring i å håndtere personopplysninger og hvordan personvernet til abonnenter og andre skal ivaretas. Jevnlig opplæring bidrar til å sikre en god personvernkultur i organisasjonen og reduserer risikoen for brudd på personopplysningssikkerheten.

De med en sentralisert organisering av personvernarbeidet gjennomførte i mindre grad jevnlig opplæring. Disse er i større grad avhengig av at personvernombudet, personvernansvarlig m.fl. i den kommunale administrasjonen gjennomfører opplæringsaktiviteter for deres ansatte. Den organisatoriske avstanden til personvernfunksjoner fører også her til at oppfølgingen blir dårligere.

Uavhengig av organisering, bør de som jobber med vann og avløp etablere en årlig plan⁴⁵⁾ for opplæring, ut fra virksomhetens størrelse og behov på personvernområdet. Opplæringsplanen bør blant annet inneholde tematikken det skal gis opplæring i og hvem (hvilken rolle) som skal gjennomføre de ulike aktivitetene. Opplæringen bør fokusere på områder som utgjør en særlig risiko for etterlevelsen av personvernregelverket. Slike risikoområder kan blant annet identifiseres gjennom internkontrollaktivitetene i kommunene og selskapene.

Personvernombudet, personvernansvarlig og andre relevante personvernroller bør bistå med både planlegging, forberedelser og gjennomføring av opplæringsaktivitetene. På denne måten sikres kvaliteten på opplæringen, samt at den organisatoriske avstanden reduseres.

44) Se rapportens pkt. 6.5.

45) Dette kan eksempelvis være et årshjul som beskriver hvilke opplæringsaktiviteter som skal gjennomføres i hvert kvartal.

8.9. Risiko for brudd på personopplysningssikkerheten

Forurensning av drikkevann, bortfall av vann og manglende rensing av avløpsvann medfører risiko for liv og helse, og kan få store konsekvenser for samfunnet. Vann- og avløpstjenestene er kritiske samfunnsfunksjoner som skal fungere uten avbrudd og forstyrrelser. Kommuner og selskap som skal bidra til dette, vil i økende grad kunne bli utsatt for cyberangrep fra ondsinnede aktører, herunder også fremmede stater. I tiden fremover må de håndtere et endret trusselbilde, med økt IKT-sårbarhet i overvåkings- og styringssystemer.⁴⁶⁾

Angrep mot IKT-systemer og applikasjoner vil i de fleste tilfeller også innebære et brudd på personopplysningssikkerheten⁴⁷⁾ ved at angriper eksempelvis får tilgang til og sprer personopplysninger. De personvernutfordringene som er identifisert i denne rapporten, herunder mangelfull risikostyring, internkontroll og personvernkompetanse, indikerer at tjenestene vil være sårbare for angrep som rammer IKT-systemer og applikasjoner. Hvis slike sårbarheter utnyttes, kan dette få alvorlige konsekvenser for personvernet til personer som får sine personopplysninger behandlet.

Både norske myndigheter og EU har igangsatt lovgivningsinitiativ som stiller krav til at tilbydere av samfunnsviktige tjenester etablerer grunnleggende tekniske og organisatoriske sikkerhetstiltak. Lov om digital sikkerhet⁴⁸⁾ er vedtatt, men har ikke trådt i kraft, på tidspunktet for denne rapporten. Denne loven implementerer EUs NIS1-direktiv⁴⁹⁾ i norsk rett og vil få anvendelse på vannbransjen. EU har vedtatt et ytterligere NIS2-direktiv, som oppstiller konkrete minimumskrav til hvilke sikkerhetstiltak som må etableres. NIS2-direktivet er vurdert som både EØS-relevant og akseptabelt for Norge, men er foreløpig ikke implementert i norsk rett.

Det såkalte CER-direktivet (Critical Entities Resilience Directive) vil også få relevans for vannbransjen. Direktivet tar sikte på å forbedre beskyttelsen av kritiske infrastrukturer i EU. Vann- og avløpstjenester anses som en kritisk infrastruktur. Direktivet er foreløpig ikke gjennomført i norsk rett, men er vurdert som både EØS-relevant og akseptabelt for Norge.

I påvente av at dette EU-regelverket gjennomføres i Norge, bør kommuner og selskap forberede sin organisasjon og systemportefølje på strengere krav til IKT-sikkerhet og hendelseshåndtering.

46) [Nasjonale mål for vann og helse med gjennomføringsplan - regjeringen.no](#), s. 10.

47) Se rapporten pkt. 6.5.

48) [Lov om digital sikkerhet](#).

49) Network and information security directive.

9. Digitale vannmålere

Både kommunen og den som mottar vann- og avløpstjenesten kan kreve at det årlige gebyret fastsettes ut fra målt forbruk, dvs. ved bruk av vannmåler.⁵⁰⁾ «Digitale», «automatiske», «fjernavleste» eller «smarte» vannmålere (heretter kaller vi det «digitale vannmålere») skiller seg fra tradisjonelle analoge vannmålere ved at de inneholder sensorer og elektroniske komponenter som gjør det mulig å nøyaktig måle og overvåke vannforbruk, samt overføre forbruksdata direkte til kommunene og selskapene, uten at abonnenten behøver å lese dette av manuelt. Flere kommuner og selskap har tatt i bruk slike målere, men det er knyttet usikkerhet til hvilke formål målerne kan benyttes til og hvilke data som kan samles inn.



9.1. Bruksområder og mulige gevinster

Digitale vannmålere plasseres, i likhet med analoge vannmålere, på den innvendige vanninstallasjonen. I Norge er det vanlig praksis at kommunene eller selskapene eier vannmåleren og abonnenten betaler for leien.

Bruksområdene for digitale vannmålere er mange. De fleste benytter dem til å måle vannforbruket, på lik linje med analoge målere. Data samlet inn gjennom målerne bidrar til en mer effektiv faktureringsprosess for både saksbehandlere og abonnentene selv.

Data som samles inn gjennom digitale vannmålere, herunder gjennom måling av forbruk eller akustisk sensor, kan også benyttes til å avdekke lekkasjer fra vannledninger, både inne i huset og på stikkledningene. Det er flere mulige gevinster ved en slik innsamling av data:

- **Redusert vannsvinn:** Digitale vannmålere kan raskt identifisere lekkasjer på vannledninger, noe som bidrar til å redusere vannsvinn. Dette er spesielt viktig i kommuner med begrensede vannressurser.
- **Kostnadsbesparelser:** Dersom lekkasjer kan oppdages tidligere, kan de repareres før de utvikler seg til å bli større og fører til skader som er mer kostbare å utbedre. Dette vil også redusere behovet for at kommuner og selskap gjennomfører manuelle lekkasjesøk på ledningsnett.
- **Miljøfordeler:** Redusert vannsvinn fører til mindre belastning på vannkildene og kan dermed bidra til å bevare naturlige vannmiljøer. Redusert vannsvinn kan dessuten redusere energiforbruket knyttet til vannbehandling og distribusjon.
- **Bedre tjenester:** Rask identifisering og reparasjon av lekkasjer sikrer en mer pålitelig vannforsyning og reduserer risikoen for innsug av forurenset vann.

Det finnes også andre områder hvor data samlet inn gjennom digitale vannmålere kan tenkes brukt. Data om vannforbruk kan eksempelvis brukes for å avdekke informasjon om abonnentenes bruksmønster, herunder om det vannes i strid med vanningsforbud, om det «sløses» med vann og om en abonnent overholder boplikten. Å avdekke uønskede eller avtalestridige bruksmønstre, kan bidra til å redusere svinn og beskytte hardt pressede vannressurser i sårbare perioder.

Data samlet inn gjennom digitale vannmålere kan også spille en rolle i velferdsteknologisk sammenheng. Data om vannforbruk kan bl.a. avdekke om en abonnent har behov for bistand av hjemmesykepleien. Kommunale helse- og omsorgstjenester vil kunne effektiviseres og utsatte og pleietrengende innbyggere vil kunne få tettere oppfølging.

⁵⁰⁾ Forurensningsforskriften § 16-4 annet ledd.

9.2. Personopplysninger som behandles gjennom digitale vannmålere

Data som samles inn gjennom digitale vannmålere vil kunne knyttes til enkeltpersoner. Dette skyldes at vannmåleren, som plasseres på vannledningen til abonnenten, gjør det mulig å identifisere huseier og husstanden.⁵¹⁾ Disse dataene blir da å regne som personopplysninger.⁵²⁾

Dette vil rett nok ikke være tilfelle i alle situasjoner hvor vannmålere benyttes. Eksempelvis kan flere boenheter være knyttet til samme vannmåler, som i et borettslag, eller husstander med et større antall beboere. I slike tilfeller kan opplysningene være anonyme, fordi det ikke er mulig å identifisere enkeltindivider. All den tid alle kommuner vil ha vannmålere som det er knyttet færre beboere til, er det likevel riktig å ta utgangspunkt i at å benytte digitale vannmålere vil innebære en behandling av personopplysninger.

Omfanget av personopplysninger som samles inn, vil avhenge av funksjonaliteten til vannmåleren. I utgangspunktet er det forbruksdata som innhentes gjennom digitale vannmålere. Isolert sett er dette lite inngripende personopplysninger, men løpende forbruksdata er også egnet til å avsløre andre opplysninger om abonnenten, som når vedkommende er på jobb eller ferie, om det er lekkasje på abonnentens stikkledning eller avtalestridig vannforbruk. I visse situasjoner kan det også tenkes at forbruksdata vil kunne avsløre helseopplysninger om abonnenten.

Hvilken funksjonalitet kommunen velger å benytte, vil være avgjørende for hvilke personopplysninger som behandles og for hvilke formål. Hvor ofte personopplysninger innhentes fra måleren, vil være et moment av betydning i denne sammenheng. Innsamling av forbruksdata for faktureringsformål vil som regel innebære månedlig, kvartalsvis eller årlig innsamling. For andre formål, som lekkasjesøk, er det nødvendig å samle inn opplysninger om vannforbruk mer regelmessig. Jo hyppigere data samles inn, desto flere personopplysninger kan utledes om abonnenten.

Digitale vannmålere med akustisk sensor kan avsløre om det er en lekkasje på stikkledningen. Denne funksjonaliteten sier ingenting om abonnentens forbruk, men vil likevel innebære en behandling av personopplysninger, fordi den avslører om abonnenten har en lekkasje på stikkledningen.

9.3. Behandlingsgrunnlag for ulike formål

Innsamling og behandling av personopplysninger gjennom digitale vannmålere krever at kommuner og selskaper har et lovlig behandlingsgrunnlag.⁵³⁾

9.3.1. Måling og fakturering av vannforbruk

Kommuner har behandlingsgrunnlag til å behandle personopplysninger innsamlet fra digitale vannmålere for faktureringsformål i forurensningsforskriften § 16-4. Bestemmelsen er begrenset til å omhandle bruk av vannmålere for faktureringsformål, og gir dermed ikke rettslig grunnlag for annen bruk av opplysninger om vannforbruk.

Datatilsynet har på sine hjemmesider uttalt at kommuner i utgangspunktet bare har rettslig grunnlag til å innhente avlesninger fra automatiske vannmålere i henhold til faktureringsfrekvens, på samme måte som for analoge vannmålere. Dette er som regel en til fire ganger årlig. Bruk av måleravlesning for andre formål enn fakturering, forutsetter som hovedregel en høyere sendingshyppighet. Denne behandlingen har ikke sammenheng med faktureringsformålet som avlesningene opprinnelig innhentes for.⁵⁴⁾

51) Det kan diskuteres hvorvidt vannmålere på stikkledninger til større boligkomplekser eller næringseiendommer gjør det mulig å identifisere enkeltindivider. Det er antakelig mer hensiktsmessig for kommuner og selskaper å behandle all data som samles inn gjennom digitale vannmålere som personopplysninger.

52) Se rapportens pkt. 2.

53) Se rapportens pkt. 4.

54) <https://www.datatilsynet.no/personvern-pa-ulike-omrader/overvaking-og-sporing/strommaling/>

9.3.2. Lekkasjesøk

Effektivt lekkasjesøk krever, hyppigere innsamling av data enn for måling og fakturering av vannforbruk. For kommuner og selskap som allerede har tatt i bruk digitale vannmålere for måling og fakturering, mener Data-tilsynet at bare samtykke eller hjemmel i lov kan gi grunnlag for andre former for behandling, som lekkasjesøk.⁵⁵⁾ Dette skyldes at det er strengere krav for å behandle personopplysninger for andre formål enn det de opprinnelig ble samlet inn for.⁵⁶⁾

Personvernforordningen stiller strenge krav til et gyldig samtykke i. En abonnents samtykke skal være frivillig, spesifikt, informert, utvetydig, gitt gjennom en aktiv handling, dokumenterbart og mulig å trekke tilbake like lett som det ble gitt.⁵⁷⁾

Bruk av samtykke som behandlingsgrunnlag vil være lite hensiktsmessig. For det første vil det kunne være både utfordrende og tidkrevende å innhente samtykker fra samtlige samtykkekompetente beboere i hver enkel boenhet, og deretter å holde dette oppdatert ved utskiftninger av beboere. Videre vil det kunne være utfordrende å sikre et reelt frivillig samtykke, da styrkeforholdet mellom en abonnent og kommunene er skjevt. Ettersom samtykker kan trekkes tilbake når som helst, vil innsamlingen av data kunne bli fragmentert og lite effektiv. Samtykkebasert behandling vil også risikere at kommuner og selskap ikke vil kunne realisere gevinstene, som redusert vannsvinn og miljøgevinster.

Hjemmel i lov vil kunne være et bedre egnet behandlingsgrunnlag enn samtykke for lekkasjesøk. En klar hjemmel vil kunne gi en stabil og forutsigbar ramme for lekkasjesøk og redusere administrative byrder forbundet med innhenting av samtykke, samt resultere i en mer konsekvent gevinstrealisering.

På nåværende tidspunkt finnes det ikke klar lovhjemmel som gir kommunene et behandlingsgrunnlag for lekkasjesøk, herunder bruk av vannmålere med akustiske sensorer.

Dansk Vand- og Spildevandsforening (DANVA) henviser i sin veiledning om personopplysninger for vannselskaper at Energistyrelsen tidligere har lagt til grunn at:

«hyppig dataindsamling via fjernaflæsningsmålere kunne basere sig på en samfundsmæssig interesse og/eller en legitim interesse hos forsyningen, der vejer tungere end kundernes/den registreredes interesse»⁵⁸⁾

Berettiget interesse er et behandlingsgrunnlag som i utgangspunktet ikke kan benyttes av offentlige myndigheter på behandlinger som ledd i utførelsen av deres oppgaver.⁵⁹⁾ Lekkasjesøk har en nær sammenheng med kommuner og selskaps vannleveranse, men det er i dag ikke en del av deres uttrykkelige lovpålagte oppgaver.

Norsk Vann engasjerte i 2022 Advokatfirmaet Guttorm Jakobsen AS for å gjennomføre en utredning av adgangen til fjernavlesning av vannmålere i henhold til personopplysningsloven. I utredningen konkluderes det blant annet med at det sannsynligvis finnes et behandlingsgrunnlag i utførelsen av en oppgave i allmennhetens interesse eller berettiget interesse.⁶⁰⁾

Prosjektet fremla denne argumentasjonen i et veiledningsmøte med Datatilsynet. Tilsynet var av den oppfatning at bruk av personopplysninger fra vannmålere til lekkasjesøk vil kreve hjemmel i lov.

55) Ibid.

56) Se personvernforordningen art. 6 (4).

57) Se rapportens pkt. 4.

58) [Veiledning om persondata for vandselskaber](#), s. 26 og [Dansk afklaring fra Energistyrelsen](#)

59) Se personvernforordningen art. 6 (1).

60) Se personvernforordningen art. 6 (1) bokstav e og f.

9.3.3. Ytterligere bruksområder

Ytterligere bruksområder for digitale vannmålere, herunder avdekking av bruksmønster som er strid med vanningsforbud eller boplikten, vil på lik linje med lekkasjesøk være avhengig av hyppigere innsamling av data enn forbruksmåling og fakturering. Samtykke vil ikke være praktisk for denne typen behandling. Også her vil en klar lovhjemmel være det beste alternativet for å sikre et lovlig behandlingsgrunnlag for kommunene og selskapene.

For bruk av personopplysninger i forbindelse med velferdsteknologi, vil det være risiko for at det samles inn og behandles personopplysninger som avslører helseopplysninger. I slike tilfeller må kommuner og selskap sikre at det også foreligger et lovlig behandlingsgrunnlag for å behandle særlige kategorier av personopplysninger.⁶¹⁾

9.4. Behovet for en klar hjemmel

Prosjektet har vært i dialog med flere offentlige aktører, herunder Datatilsynet, Digitaliserings- og forvaltningsdepartementet og Miljødirektoratet, for å identifisere mulige lovhjemler eller andre behandlingsgrunnlag for lekkasjesøk og andre bruksområder. Datatilsynet mener lekkasjesøk og andre bruksområder vil kreve en egen lovhjemmel. På nåværende tidspunkt finnes det ikke en klar og dekkende lovhjemmel for disse behandlingsaktivitetene.

Det er et presserende behov for å få på plass en lovhjemmel som gir kommuner og selskap mulighet til å bruke data fra digitale vannmålere til å gjennomføre lekkasjesøk. I tillegg til at bransjen selv ser behovet for og gevinstene av slik bruk, har Helse- og omsorgsdepartementet og Klima- og miljødepartementet publisert nye «Nasjonale mål for vann og helse med gjennomføringsplan».

Nasjonalt mål 8 krever at lekkasje av drikkevann skal reduseres. Andelen lekkasje av ferdig produsert drikkevann fra det enkelte vannforsyningssystem som ikke når forbrukeren, skal være under 25 % innen 2033.⁶²⁾ For å nå dette målet, er det essensielt at bransjen gis anledning til å innhente nøyaktige og kontinuerlige data om vannforbruk fra digitale vannmålere, som kan brukes til å identifisere lekkasjer.

Nasjonalt mål 9 krever at distribusjonssystemet for drikkevann skal fornyes, ikke forfalle.⁶³⁾ Digitale vannmålere spiller en viktig rolle i denne fornyelsen, ved å gi nøyaktig og oppdaterte data som kan brukes til å overvåke tilstanden til distribusjonssystemet og identifisere områder med høy lekkasje, som krever umiddelbar oppmerksomhet.

I bakgrunnsinformasjonen til de nasjonale målene peker departementene på at kommunene i liten grad har oversikt over utslippsmengder som lekker ut fra ledningsnett og at kunnskap om dette bør bedres.⁶⁴⁾ Digitale vannmålere kan gi bedre oversikt og kontroll ved å gi nøyaktige data om vannforbruk og lekkasjer, noe som kan brukes til å forbedre vedlikehold og planlegging.

9.5. Prosjektets anbefaling

Basert på prosjektets dialog med Datatilsynet og andre offentlige myndigheter, de nasjonale målene for vann og helse, og kommuner og selskapers behov, anbefaler prosjektet å gå i dialog med lovgiver for å etablere dedikerte lovhjemler for lekkasjesøk og andre bruksområder for personopplysninger innhentet gjennom digitale vannmålere.

61) Se rapportens pkt. 4.

62) [Nasjonale mål for vann og helse med gjennomføringsplan - regjeringen.no](#), s. 20.

63) *Ibid.*

64) *Ibid.*, s. 30.

Dedikerte lovhjemler vil sikre mer forutsigbarhet for både abonnenter, kommuner og selskap, samt kunne redusere de administrative byrdene ved å måtte etablere andre former behandlingsgrunnlag. Lanseringen av de nye nasjonale målene synes å være et godt tidspunkt for lovgiver å komme på banen for å sikre at kommuner og selskaper har effektive verktøy for å kunne oppfylle disse målene.

10. Referanser

Ofte, J., Windt, P. og Farestveit, T. (2011) *Tilsyn med utslipp fra avløpsanlegg innen kommunens myndighetsområde*. Norsk Vann Rapport 184/2011.

Røstum, J., Gilje Jaatun, M. (2018) *Informasjonssikkerhet i skybaserte tjenester for vannbransjen*. Norsk Vann Rapport 238/2018.

Datatilsynets maler for protokoll over behandlingsaktiviteter. (sist endret: 2024) [Datatilsynets hjemmeside](#): Protokoll over behandlingsaktiviteter.

Datatilsynet om automatisk strøm- og vannmåling. (sist endret: 2023) [Datatilsynets hjemmeside](#): Automatisk strøm- og vannmåling.

Helse- og omsorgsdepartementet, Klima- og miljødepartementet. (2024). *Nasjonale mål for vann og helse med gjennomføringsplan: Målsettinger og tiltak under Protokollen for vann og helse*.

Vejledning om persondata for vandselskaber. (2023). DANVA vejledning nr. 100, ver. 4.

11. Vedlegg

Informasjon som må gis til de registrerte	Person- opplysninger samlet inn fra den registrerte	Person- opplysninger samlet inn fra andre kilder
Navn og kontaktinformasjon til kommunen eller selskapet	✓	✓
(Dersom relevant) Navn og kontaktinformasjon til representant for kommunen eller selskapet	✓	✓
Navn og kontaktinformasjon til personvernombudet	✓	✓
Formålene med behandlingen	✓	✓
Behandlingsgrunnlaget for behandlingen	✓	✓
(Dersom relevant) de berettigede interessene som forfølges av kommunen eller selskapet	✓	✓
Kategoriene av personopplysninger som behandles		✓
Mottakere/kategorier av mottakere av personopplysninger	✓	✓
Informasjon om eventuell overføring av personopplysninger til land utenfor EU/EØS	✓	✓
Lagringstiden for personopplysningene	✓	✓
De registrertes rettigheter	✓	✓
Retten til å trekke tilbake et samtykke	✓	✓
Retten til å klage til en tilsynsmyndighet	✓	✓
Hvor personopplysningene er innhentet fra	✓	✓
Om det foreligger et lovfestet eller avtalefestet krav om å gi personopplysninger til kommunen/selskapet	✓	
Forekomsten av og detaljer rundt automatiserte avgjørelser, herunder profilering	✓	✓

TIDLIGERE UTGITTE RAPPORTER

2025	291	Kompetansekrav knyttet til drift av vann- og avløpsanlegg
	B28	Kompetansekrav knyttet til drift av vann- og avløpsanlegg
2024	290	Veiledning for oljeutskilleranlegg
	289	Vannbehandlingsbarrierer, vannverkslam og returstrømmer – BARRINOR og SLAMINOR
	288	Veiledning for dimensjonering av mindre avløpsanlegg
	287	Veiledning for design og drift av nanofilteranlegg
	286	Veiledning i bruk av infiltrasjon i vannforsyning
	C17	Ny kunnskap om filterdrift og mikrobiologisk liv i ozonering-biofiltreringsanlegg
	285	Kartlegging og inndeling av sprinkleranlegg i farekategorier
2023	284	Mikroforurensninger i avløpsvann – resultater fra innløp- og utløpsvann fra 19 norske avløpsrenseanlegg
	283	Organiske miljøgifter i norsk avløpsslam – resultater fra undersøkelsen i 2022/2023
	282	Taknedløp fra kompakte tak – mulighet for utkast til terreng
	281	Mulige organisasjonsformer for den kommunale vann- og avløpssektoren
	280	Fremtidens vann- og avløpssystem
	279	Overvåkning av vannkvalitet på distribusjonsnett – Erfaringer fra bransjen
	278	LOSINOR – Lukt- og smaksproblemer i norsk drikkevann
	C16	Stikkledninger i varerør
	277	Nasjonal strategi for behandling og disponering av avløpsslam
	276	Lange pumpeledninger for avløp på land og i sjø
2022	275	Mikroforurensninger og legemidler i avløpsvann
	274	Korrosjonsbeskyttelse – erfaring og ny kunnskap
	273	Veileder i samfunnsøkonomiske analyser for vannbransjen
	272	Sikker utforming av åpne overvannsløsninger
	271	Åpen fordøyning – Etablering av anlegg for permanente og midlertidige vannspeil med dybde over 20 cm
	C15	Digitalisering av VA-sektoren i Norge – status, utfordringer og behov
	270	Helsemessig sikker drift av vannledningsnett – prosedyrer og anbefalinger
	269	Risikovurdering av bergsprengte drikkevannsmagasiner
	268	PFAS i råvann og drikkevann fra Norge
	267	Veiledning for utarbeidelse av kommunale forskrifter på avløpområdet
2021	266	Vannbransjens erfaringer med kommune-sammenslåinger
	265	MEMINOR: Membranfiltrering for fjerning av Naturlig Organisk Materiale i Nordiske drikkevann
	264	Alternativ til akkreditert prøvetaking
	263	Trykkoptimalisering på vannledningsnett – beste praksis
	B27	Forurensning i overvann fra urbane flater – vannmiljø og rensesilt
	262	Undersøkelser som grunnlag for valg av avløpsløsning
	261	Omfyllingsmasser
	260	Innovative anskaffelser i vannbransjen
2020	259	Kommunalt finansieringsbehov i vannbransjen 2021 – 2040
	258	Rekutteringsbehov i vannbransjen – status og prognoser 2020 – 2050
	257	Etablering og drift av mindre avløpsanlegg
	256	Veiledning for dimensjonering av avløpsrenseanlegg
	255	Bærekraftig fremmedvannsandel – Modell for vurdering av riktig nivå
2019	254	Forvaltning av nedbørsfelt for overflatevannkilder
	B26	Kunnskapsbehov innen overvann og klimatilpasning
	B25	Forprosjekt – Digital Vannstatistikk
	253	Mikroplast i avløpsvann, avløpsslam og jord
	252	Kummer – Klassifisering og tilstandsvurdering
	B24	Primærrens – Status og renseeffekter 10 år etter
	C14	Bærekraftig fornyelse av ledningsnett
	251	Klimagassutslipp, veiledning for vannbransjen
	250	Kommunens roller, rettigheter og fremgangsmåter i private utbyggingsområder
	249	Veiledning i nød vannforsyning
2018	B23	Evaluerer av Norsk Vanns prosjektsystem
	248	Organic Pollutants in Norwegian Wastewater Sludge
	247	Beste praksis for HMS-arbeid i vannbransjen
	246	Regulering og organisering av vann- og avløpssektoren i utvalgte europeiske land
	245	Veiledning for tilstandsvurdering av infiltrasjonssystemer
	244	Veiledning i utarbeidelse av prøvetaksplan for drikkevann
	243	Verdiforvaltning av vann- og avløpsinfrastruktur
	242	Praktiske råd ved valg av ledningsmateriale
	241	Mapping microplastic in Norwegian drinking water
	240	UV-desinfeksjon av drikkevann
2017	B22	Vann og avløp i arealplanlegging og byggesaker
	239	Beregning av bærekraftig lekkasjenivå
	238	Informasjonssikkerhet og skybaserte tjenester
	237	Dataflyt for GIS-informasjon i VA-prosjekter
	236	Akseptkriterier – Vurdering av nye og nyrenoverte avløpsledninger ved rørinspeksjon
	235	Dataflyt
	234	Rørinspeksjon av hovedledninger for vann og avløp
	233	Veiledning for bruk av betongrør og kummer
	232	Plastrør for vannforsyning og avløp: Hvordan skal vi oppnå minst 100 års levetid?
	231	NOMINOR: Natural Organic Matter in drinking waters within the Nordic Region
2016	230	NOMINOR: Naturlig Organisk Materiale i Nordiske drikkevann
	229	Sikring av vannforsyning mot tilsiktede uønskede hendelser
	228	Tilførsel av industrielt avløpsvann
	227	Beregning av forurensningsutslipp fra avløpsanlegg
	226	Tømming av slam
	225	Trykkavløp i spredtbygd og urbane strøk
	224	Eierskap til stikkledninger
	223	Finansieringsbehov i vannbransjen 2016 – 2040
	222	Dokumentasjon av utslipp fra avløpsnett
	221	Smart ledningsfornyelse – bruk av NoDig-metoder
2015	B21	Utvikling av studietilbud i bachelor i vann- og miljøteknikk
	B20	Norske tall for vannforbruk med fokus på husholdningsforbruk
	220	Kritiske ledninger for vann og avløp – klassifisering og tiltaks vurdering
	219	Eksempler på implementering av bærekraft i vannbransjen
	218	Vann til brannsløkking og sprinkleranlegg
	217	Videreutvikling av beregningsmetodikk for gjenanskaffelsesverdi og investeringsbehov
	215	Tilbakestrømssikring – veiledning til vannverkseiere
	214	Forslag til ny sektorlov for vanntjenester
	213	Sikkerhetsstyring for vannbransjen
	212	Veiledning for dimensjonering av vannbehandlingsanlegg
2014	211	Erfaringer med ozon-biofiltrering for behandling av drikkevann
	210	Veiledning for praktisering av selvkost
	209	Veiledning i mikrobiell barriere analyse
	208	Sikring av kvalitet på ledningsanlegg
	207	Stikkledninger – ansvar og teknisk utforming
	206	Biostabilitet i drikkevannsnett
	205	Bærekraftig forvaltning av VA-tjenestene
	204	Åpne flomveger i bebygde områder
2013	203	Fra driftsassistanter til regionale vannassistanter
	202	Microbial barrier analysis (MBA) – a guideline
	201	Anskaffelser i vannbransjen
	200	Håndtering av overvann fra urbane veger
	199	Etablering av gode VA-løsninger i spredt bebyggelse
	198	Organiske miljøgifter i norsk avløpsslam – Resultater fra undersøkelsen i 2012/13
	197	Avløpsanlegg Vurdering av risiko for ytre miljø
	196	Veiledning i tilstandskartlegging og fornyelse av VA-transportssystemer
	195	Sikkerhet og sårbarhet i driftskontrollsystemer for VA-anlegg
	B19	Varmepumper i drikkevannsforsyningssystem
2012	B18	Kranvannets kokebok for kommunikasjon
	B17	Investeringsbehov i vann- og avløpssektoren
	194	Energiriktig design og prosjektering av avløpsrenseanlegg
	193	Veiledning i dimensjonering og utforming av VA-transportsystem
	192	Veiledning for valg av riktige sensorer og måleutstyr i VA-teknikken
	191	Rettigheter til uttak av vann til allmenn vannforsyning
	190	Klimatilpasningstiltak innen vann og avløp i kommunale planer
	188	Veiledning for drift av koaguleringsanlegg
	C8	Omdømmeplattform og -strategi
	187	Kommunal overtakelse av vannverk organisert som andelslag eller samvirkeforetak
2011	186	Veiledning i omorganisering av andelsvannverk til samvirkeforetak
	185	Fett i avløpsnett. Kartlegging og tiltaksforslag
	184	Tilsyn med utslipp fra avløpsanlegg innen kommunens myndighetsområde
	183	Veiledning om regulering av VA-tjenester til næringsmiddelindustri
	182	Prøvetaking av avløpsvann og slam
	181	Veiledning i bygging og drift av drikkevannsbasseng
	180	Fjernavlesning av vannmålere
	179	Veiledning i utarbeidelse av kommunale gebyrfskrifter for vann og avløp
	B16	Veiledning for kartlegging av energibruk i VA-sektoren
	B15	Vannforskriftens økonomiske konsekvenser for kommunesektoren og avløpsanleggene
2010	C7	Forvaltningspraksis ved norsk damsikkerhet
	178	Grunnundersøkelser for infiltrasjon – mindre avløpsanlegg
	177	Drikkevannskvalitet og kommende utfordringer – problemoversikt og status
	176	Statlige gebyrer og avgifter på de kommunale VAR-tjenestene
	175	Vann og avløp for nye i bransjen – læreplan. E-læring og samlinger
	174	Hygienisering av avløpsslam. Langtidslagring og enkel rankekompostering. Resultater fra 3 års valideringstesting
	173	Veiledning for bruk av støpejernsrør
	B14	Klimatilpasningstiltak i VA-sektoren – forprosjekt
	B13	Silslam – mengder, behandlingsløsninger og bruksområder. Forprosjekt.
	172	Trykktap i avløpsnett
2009	171	Erfaringer med lekkasjekontroll
	170	Veileder til god desinfeksjonspraksis
	169	Optimal desinfeksjonspraksis fase 2
	168	Veiledning for dimensjonering av avløpsrenseanlegg
	167	Veiledning for kjøp av VA-kjemikalier
	166	Tiltak for å bedre fosforfjerningen på kjemiske renseanlegg
	165	Innsamlingsverktøy for vedlikeholdsdata
	B12	Drikkevatt i media



Norsk Vann BA, Vangsvegen 143, 2321 Hamar
Tlf: 62 55 30 30 E-post: post@norsk vann.no
www.norsk vann.no