Vejledning om persondata for vandselskaber

DANVA vejledning nr. 100, ver. 4

Vandhuset · Godthåbsvej 83 · 8660 Skanderborg · Tlf.nr.: 7021 0055
· Fax: 7021 0056
danva@danva.dk · www.danva.dk

DANVA
Dansk Vand- og Spildevandsforening

ISBN: 978-87-92651-21-1

Titel: Vejledning om persondata for vandselskaber

Udgiver: DANVA
Vandhuset
Godthåbsvej 83
8660 Skanderborg

Udarbejdet af:
Horten og DANVA

Finansiering:
Vejledningen er finansieret af
DANVA

Granskning og høring:
Susanne Vangsgård, DANVA
Lars Gadegaard, DANVA

Version 4, August 2023

Indholdsfortegnelse

1 Introduktion

Med denne vejledning gives et overblik over de væsentligste[1] persondataretlige regler og problemstillinger, som har en betydning på forsyningsområdet. Vejledningen beskriver reglerne i hovedtræk og er derfor ikke et udtryk for en fuldstændig gennemgang af persondatalovgivningens bestemmelser. Spørgsmål om behandling af personoplysninger kan rettes til Datatilsynet. Den fuldstændige lovtekst kan findes på www.retsinformation.dk.

Vejledningen tager udgangspunkt i databeskyttelsesforordningen[2] og den danske databeskyttelseslov[3]. NIS-direktivet og NIS2-direktivet[4], der vedrører sikkerhedsniveauet for net- og informationssystemer og underretningspligt ved sikkerhedshændelser, er alene kort omtalt i denne vejledning.

Formålet med nærværende vejledning er at sikre, at der blandt DANVAs medlemmer er en fælles forståelse for, hvordan de eksisterende regler for behandling af personoplysninger efterleves.

Emnerne i vejledningen er udvalgt for at hjælpe DANVAs medlemmer med vurderingen af, hvilken betydning de persondataretlige regler har ved varetagelse af opgaver på vand- og spildevandsforsyningsområdet.

Denne afgrænsning indebærer, at der ikke er en særskilt beskrivelse af, hvilke persondataretlige krav, der gælder ved personaleadministration. Der er ikke her forskel på vand- og spildevandsforsyningsområdet og personaleadministration på andre områder. Det skal således alene bemærkes, at de generelle principper for behandling af personoplysninger, et retligt grundlag for behandlingen og opfyldelse af oplysningspligten også gælder i forhold til personaleadministration.

Der henvises desuden til DANVAs persondatasite, hvor DANVA har udgivet vejledninger og skabeloner, der med fordel kan benyttes med henblik på at efterleve persondatalovgivningen.

Afgørelserne, som er nævnt i vejledningen, kan findes ved at søge på journalnummeret, som står i vejledningen, på Datatilsynets hjemmeside.[5]

---

[1] Vejledningen er ikke udtryk for en udtømmende oplistning af persondataretlige problemstillinger på forsyningsområdet. Endvidere hører emnet ikke til DANVA sekretariatets spidskompetenceområder. Vejledningen tager desuden ikke stilling til virksomheders håndtering af personoplysninger i forbindelse med personaleadministration.

[2] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse

[3] Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

[4] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen og EU's direktiv, 2022/2555 (NIS2-direktivet), som blev vedtaget den 14. december 2022 og skal være implementeret i dansk ret senest den 17. oktober 2024, se også afsnit 9.6

[5] https://www.datatilsynet.dk/afgoerelser

2 Introduktion til reglerne om persondata

2.1 Hvornår gælder reglerne om persondata?

Databeskyttelsesforordningen er den primære retskilde for, hvornår og hvordan personoplysninger kan og skal behandles, som suppleres af databeskyttelsesloven (i denne vejledning benævnt "persondatalovgivningen").

Persondatareglerne gælder for alle former for behandling af personoplysninger, samt hvis personoplysningerne er eller vil blive indeholdt i et register.[6]

I praksis vil de fleste situationer være omfattet af databeskyttelsesreglerne. Det gælder f.eks., når en medarbejder modtager en e-mail om/fra en kunde[7], når en person ansøger om et job, eller hvis der tages et billede af deltagerne til et arrangement.

Fravigelse af persondatalovgivningen kan kun ske ved lov, og det skal specifikt fremgå af selve loven, at der sker en fravigelse af persondatalovgivningen. I forhold til vand- og spildevandssektoren er der ikke foretaget fravigelser af persondatalovgivningen. Vandforsynings- og spildevandsforsyningsselskabers ("forsyningsselskaber") behandling af persondata skal altid have hjemmel i persondatalovgivningens bestemmelser.

Det bemærkes herved, at forsyningsselskaber og serviceselskaber – uanset om de er del af en koncern, eller der er tale om eksterne eller delvist ejede serviceselskaber – formelt er selvstændige juridiske personer. Det indebærer, at en videregivelse af oplysninger er en behandling, som kræver hjemmel, opfyldelse af oplysningspligten osv.

Dette kan give en række udfordringer, som i et vist omfang kan løses ved indgåelse af databehandleraftaler, se afsnit 8.

Når et serviceselskab i en forsyningskoncern behandler personoplysninger om kunder i de enkelte forsyningsselskaber, der også er en del af koncernen, skal der indgås en databehandleraftale. Dette gælder f.eks. også eksterne serviceselskaber, uanset om forsyningsselskabet er medejer af det eksterne serviceselskab eller ej.

Databeskyttelsesforordningen gælder både for offentlige myndigheder og private, jf. artikel 1, stk. 1. Databeskyttelsesforordningen er således knyttet til selve behandlingen af personoplysninger.

---

[6] Dette følger af Databeskyttelsesforordningen artikel 2. Dog er der visse situationer, hvor persondatareglerne ikke finder anvendes, f.eks. ved behandling af personoplysninger som en fysisk person foretager som led i rent personlige eller familiemæssige aktiviteter, *eller* hvis behandlingen alene sker i journalistisk øjemed.

[7] Begreberne "kunde" og "forbruger" er anvendt synonymt i denne vejledning.

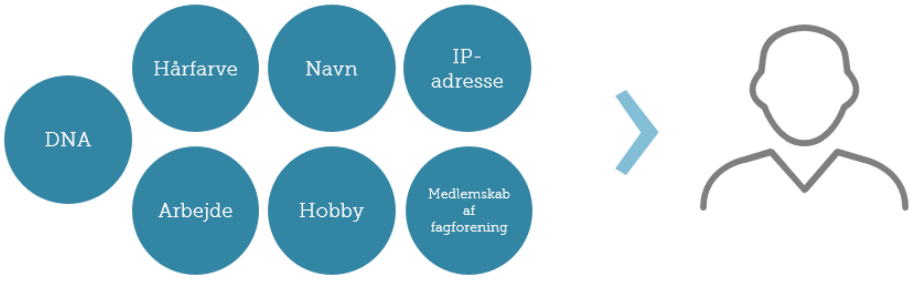
Det er tidligere blevet afklaret, at forsyningsselskaber skal betragtes som private i forhold til reglerne for behandlingen af personoplysninger[8].

2.2 Definitioner

Med **"personoplysninger[9]"** menes enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«)

En **"identificerbar person"** er en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator, som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet. Også selvom det kun er muligt for særligt indviede at forstå, hvem oplysningen vedrører. Helt anonymiserede oplysninger er ikke omfattet.

Dvs. at persondatareglerne gælder for alle oplysninger om fysiske personer, som direkte eller indirekte kan identificeres.[10]



Billedet viser eksempler på, hvilke personoplysninger, der kan relateres til en fysisk person.

[8] Det følger af den kommenterede persondatalov (som vedrørte den gamle persondatalov) at når det skal klarlægges, om et organ eller en institution skal anses for privat eller offentligt, så skal der lægges vægt på den organisatoriske placering. Hvis der er tvivl, kan der lægges vægt på de funktioner, som organet udfører. For så vidt angår vandforsyningsselskaber er de organisatorisk placeret uden for kommunens organisation, idet de er udskilt og selskabsgjort. Derudover afgrænsedes den offentlige forvaltning efter den gamle persondatalov på samme måde som afgræsningen finder sted efter offentlighedslovens § 2. Afgræsningen er herefter således: "Loven finder anvendelse på al virksomhed, der udøves af myndigheder inden for den offentlige forvaltning" Da vandforsyningsselskaber ikke er en del af den offentlige forvaltning, er de dermed ikke omfattet af persondatareglerne efter afgrænsningen i offentlighedsloven. Dette understøttes af beskrivelsen i den kommenterede persondatalov, hvorefter organer/institutioner, der er organiseret i selskabsform, herunder fx aktieselskaber, er at betragte som private efter persondatareglerne. Dette gælder uanset, at vandsektorlovens § 14 fastslår at vandforsyningsselskaber, der er omfattet af vandsektorlovens § 2, nr. 2, i øvrigt er omfattet af offentlighedsloven.)

[9] Databeskyttelsesforordningens artikel 4, nr. 1.

[10] Dette følger af databeskyttelsesforordningens artikel 4, nr. 1, som nævner flere eksempler på personoplysninger, f.eks. et navn, identifikationsnummer, lokaliseringsdata og en onlineidentifikator.

Virksomhedsoplysninger, dvs. oplysninger om juridiske personer, så som aktieselskaber og anpartsselskaber, er ikke omfattet af databeskyttelsesreglerne, da der ikke er tale om personoplysninger. Oplysninger om enkeltmandsvirksomheder og I/S'er anses dog som personoplysninger. Oplysninger om kontaktpersoner eller ansatte i virksomheder vil også være personoplysninger.

Definitionen - og dermed lovgivningen om databeskyttelse - omfatter ikke anonyme oplysninger. Der skal dog meget til, før en personoplysning er tilstrækkelig anonymiseret, da det kræver, at personen bag heller ikke kan identificeres ved brug af hjælpemidler. Det må derfor vurderes konkret, om en personoplysning er effektivt anonymiseret.

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

Et **"samtykke"** er enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling. Der er særlige krav til et samtykke i Databeskyttelsesforordningens artikel 7.

3 Behandlinger af personoplysninger på forsynings-området

Der er en forsyningspligt inden for oplandet i spildevandsplanen, jf. miljøbeskyttelseslovens § 32 b. I forhold til vand fremgår forsyningspligten af vandforsyningslovens § 45.

Som et naturligt led i varetagelsen af forsyningsopgaver eller indgåelse og opfyldelse af aftaler om forsyning (hvor der ikke er forsyningspligt) indsamler og behandler forsyningsselskaber personoplysninger relateret til den enkelte kunde.

Det drejer sig om helt sædvanlige personoplysninger til brug for administration af det løbende kunde-/aftale-forhold, såsom navn, adresse, e-mail, telefonnummer og evt. andre relevante identifikationsoplysninger.

Forsyningsselskaber indhenter herudover efter behov kundens samtykke til behandling af kundens cpr-nr. Behandlingen af sådanne almindelige personoplysninger skal ske i overensstemmelse med databeskyttelses-forordningens bestemmelser.

Adgang til at få oplyst cpr-nr. er herudover reguleret i gældsinddrivelsesloven § 2, stk. 9 og 10. Det fremgår bl.a., at hvis en kommunalt ejet forsyningsvirksomhed (eller den, der på dennes vegne opkræver) overdrager fordringen (det vil sige den manglende betaling) til restanceinddrivelsesmyndigheden (som normalt er Gælds-styrelsen), skal skyldnerens cpr-nr. oplyses, og der er derfor ret til at indhente cpr-nr. efter denne bestemmelse. Hvis gælden oversendes til privat inkasso, vil behandlingen normalt være nødvendig for at kunne fastlægge eller gøre et retskrav gældende. Behandlingsgrundlaget ved oversendelse til privat inkasso vil derfor normalt være databeskyttelseslovens § 11, stk. 2, nr. 4. Se også de sædvanlige databeskyttelsesretlige regler for behandling af cpr-nr. i afsnit 6.1.5.

Et typisk forsyningsselskab indhenter desuden personoplysninger som led i afbrydelsesprocessen og måler-data hos den enkelte kunde til brug for afregning.

Der henvises i øvrigt til en nærmere gennemgang af typiske behandlinger af personoplysninger i DANVAs behandlingsoversigt, se afsnit 4.2.

3.1 Forsyningsselskaber som dataansvarlig på forsynings-området

Forsyningsselskaber er efter databeskyttelsesforordningen dataansvarlige for de personoplysninger, der be-handles hos det enkelte forsyningsselskab, hvilket i praksis er driftsselskabet, hvorimod et serviceselskab er databehandler på vegne af driftsselskabet. Det er derfor det enkelte forsyningsselskab, der skal sikre, at alle de forpligtelser, der følger af databeskyttelseslovgivningen, overholdes, herunder fx pligten til at ajourføre de indhentede personoplysninger og opfyldelse af oplysningspligten.

Forsyningsselskaber forpligtes desuden til at træffe passende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til risiciene ved behandling af personoplysningerne, herunder at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lovgivningen. Se mere herom nedenfor under afsnit 9 om tekniske og organisatoriske sikkerhedsforanstaltninger.

3.2 Fælles dataansvar

Ved samarbejde om en opgave mellem flere forsyningsselskaber skal parterne være opmærksomme på, at der kan opstå et fælles dataansvar. Databeskyttelsesforordningens artikel 26 angiver, at der opstår et fælles dataansvar, hvis "*to eller flere dataansvarlige i fællesskab fastlægger formålene med og hjælpemidlerne til behandling*".

Hvis der er fælles dataansvar, er det vigtigt, at der ikke er tvivl om, hvem af de dataansvarlige der har ansvaret for hvad, så den fælles behandling lever op til reglerne. Fælles dataansvarlige har derfor også en pligt til at indgå en aftale om fælles dataansvar, som navnlig skal indeholde en fordeling af parternes ansvar, herunder ansvar i forhold til hvad angår udøvelsen af de registreredes rettigheder, og deres respektive pligter til at overholde oplysningspligten over for den registrerede.[11] Datatilsynet har udarbejdet en skabelon til aftale om fælles dataansvar.[12] Bemærk, at uanset hvad der aftales om fælles dataansvar mellem de fælles dataansvarlige, kan de registrerede dog altid henvende sig til enhver af de dataansvarlige for at udøve deres rettigheder. Fælles dataansvarlige hæfter solidarisk i forhold til et evt. erstatningskrav fra de registrerede.

Der er i nyere praksis flere eksempler på, at EU-Domstolen har valgt at statuere fælles dataansvar, herunder særligt dommene i sag C-210/16 og C-40/17, som begge vedrørte Facebook.

EU-Domstolen kom i dommen C-210/16 frem til, at Facebook og administratoren af en fanside på Facebook havde et fælles dataansvar for behandlingen af personoplysninger indhentet via cookies, som blev indsamlet i forbindelse med besøg på den pågældende fanside med henblik på at vise statistikker over de besøgende.

I dommen C-40/17 kom EU-Domstolen desuden frem til, at Facebook og en hjemmesideejer havde et fælles dataansvar for behandlingen af personoplysninger indhentet via et integreret plug-in med Facebooks "synes godt om"-knap på hjemmesiden. Plug-in'net medførte, at oplysninger om den besøgendes IP-adresse og User Agent (oplysninger som identificerer browseren og styresystemet) blev indsamlet og videregivet til Facebook.

[11] Pligten følger af databeskyttelsesforordningens artikel 26

[12] Aftalen kan tilgås på Datatilsynets hjemmeside: https://www.datatilsynet.dk/Media/637696319926241925/Datatilsynet_skabelon%20til%20en%20aftale%20vedr%C3%B8rende%20f%C3%A6lles%20dataansvar%20-%20dansk%20version.docx

Datatilsynet har udarbejdet en vejledning om dataansvarlige og databehandlere. I vejledningen er der eksempler på, hvornår man er dataansvarlig, databehandler eller fælles dataansvarlig.[13]

[13] Vejledningen kan tilgås på Datatilsynets hjemmeside: https://www.datatilsynet.dk/Media/7/6/Dataansvarlige%20og%20databehandlere.pdf

4 Overblik over persondata og fortegnelser

4.1 Overblik over persondata og behandlingen heraf

DANVA anbefaler – med henblik på at kunne dokumentere persondatacompliance – at forsyningsselskaberne skaber sig et overblik over de persondata, der behandles, samt løbende opdaterer denne information for at afspejle den aktuelle behandling af oplysninger i selskabet. Dette overblik kan også bruges til at udarbejde de fortegnelser, som er lovpligtige efter databeskyttelsesforordningen, jf. nedenfor.

Overblikket kan skabes ved, at virksomheden stiller sig selv nogle helt grundlæggende spørgsmål vedrørende håndtering af persondata, herunder navnlig[14]:

- Hvilke personoplysninger bliver behandlet?
- Hvilke typer af teknologier anvendes? (Fx forskellige databaser)
- Hvordan foregår indsamlingen af personoplysninger?
- Til hvilket formål behandles personoplysningerne?
- På hvilket retligt grundlag foretages behandlingen? Samtykke? Retlig forpligtelse?
- Hvilken behandling finder sted? (Fx opbevaring, videregivelse)
- Hvem har adgang til data? (Fx hvilke personalegrupper)
- Videregives data til andre? (Herunder uden for forsyningsselskabet, fx til et serviceselskab eller lign.)
- Hvem har ansvaret for personoplysningernes sikkerhed? (Tegn evt. et flowdiagram over, hvor oplysningerne ligger, og hvem der kan tilgå dem)

Nogle af spørgsmålene vil være nemmere at tage stilling til efter læsning af nærværende vejledning.

4.2 Fortegnelser

Forsyningsselskaberne er forpligtede til at udarbejde fortegnelser for deres behandlingsaktiviteter i overensstemmelse med databeskyttelsesforordningens artikel 30, som bl.a. skal indeholde oplysninger om formålet med behandlingen, kategorien af personoplysninger og tidsfristerne for sletning.

Formålet med fortegnelserne er at give et overblik over den behandling af personoplysninger, som sker hos selskabet.

Datatilsynet kan kræve at få udleveret fortegnelserne, og forsyningsselskaberne er ansvarlige for at opdatere fortegnelserne, når der foretages ændringer i behandlingen. Datatilsynet har tidligere ført tilsyn med udarbejdelsen af fortegnelser i tre forskellige kommuner. I den ene sag (2018-423-0018) udtalte Datatilsynet bl.a., at

[14] Inspirationen til disse spørgsmål er fundet i DI's vejledning om persondataforordningen. Spørgsmålene danner derfor også et godt afsæt for virksomhedens efterlevelse af databeskyttelsesforordningen.

det skal specificeres, hvilke typer af følsomme oplysninger, der behandles. Det er derfor ikke tilstrækkeligt at anføre i fortegnelsen, at der behandles følsomme oplysninger – det skal konkret angives, hvilke typer følsomme oplysninger, der behandles.

Der henvises i øvrigt til DANVAs persondatasite "Vejledninger og skabeloner fra DANVA", der indeholder skabeloner for fortegnelse over behandlinger af HR- og kundedata.

Datatilsynet har udarbejdet en vejledning om fortegnelse over behandlingsaktiviteter, som uddyber reglerne for fortegnelsen.[15]

[15] Vejledningen kan tilgås på Datatilsynets hjemmeside: https://www.datatilsynet.dk/Media/E/5/Fortegnelse%20(3).pdf

5 Generelle principper for behandling af personoplysninger og dokumentation

5.1 De generelle principper

I databeskyttelsesforordningens artikel 5, stk. 1 er der fastsat seks principper, som altid skal overholdes ved behandling af personoplysninger. Bl.a. følger det af disse principper, at personoplysninger aldrig må behandles længere, end det er nødvendigt af hensyn til formålet med behandlingen, og at behandlingen skal være gennemsigtig, således at enhver information er lettilgængelig og afgivet i et klart og enkelt sprog.

Herudover følger det af databeskyttelsesforordningens artikel 5, stk. 2, at den dataansvarlige er ansvarlig for og skal kunne påvise, dvs. dokumentere, at de seks ovennævnte principper overholdes.

Disse principper kan oplistes således:

Princip:	Indhold:
Lovlighed, rimelighed og gennemsigtighed	Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.
Formålsbegrænsning	Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål.
Dataminimering (proportionalitet)	Personoplysningerne skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.
Rigtighed	Personoplysninger skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges.
Opbevarings-begrænsning	Personoplysninger skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles.
Integritet og fortrolighed	Personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger.
Ansvarlighed	**Den dataansvarlige er ansvarlig for og skal kunne påvise, at de 6 ovennævnte grundprincipper overholdes.**

Disse principper indebærer bl.a., at der bliver nødt til at blive fastsat interne retningslinjer og procedurer for ajourføring af data og sletning heraf.

Princippet om opbevaringsbegrænsning indebærer, at forsyningsselskaberne skal fastsætte slettefrister for personoplysningerne på baggrund af formålene med behandlingerne, samt kunne dokumentere de slettefrister, der fastlægges f.eks. ved udarbejdelsen og efterlevelsen af en slettepolitik.

Der vil ofte være lovmæssige krav, der påvirker perioden for personoplysningernes opbevaring, f.eks. kravene i bogføringsloven, som forsyningsselskaberne skal tage højde for ved fastsættelsen af slettefrister.

Ved sletning af persondata skal det sikres, at alle kopier af oplysningen slettes permanent:

- Ved på elektroniske medier skal oplysningerne ikke kunne genskabes.
- Ved fysiske kopier skal oplysningerne makuleres eller på tilsvarende vis destrueres.
- Ved sletning af e-mail skal mailen slettes i såvel afsenders udbakke/modtagers indbakke samt efterfølgende i papirkurven.
- Husk også at slette sikkerhedskopier/back-ups, som indeholder oplysningerne, såfremt det er teknisk muligt. Hvis det ikke er teknisk muligt at slette oplysningerne, skal forsyningsselskabet sikre sig, at personoplysningerne fjernes, hvis backuppen genetableres. Datatilsynet har anført på sin hjemmeside, at det kan være nødvendigt at foretage en logning over foretagne sletninger til dette formål (Loggen bør dog ikke indeholde direkte personhenførbare oplysninger af hensyn til princippet om dataminimering).[16]

Datatilsynet har anført på sin hjemmeside[17], at en sletteprocedure skal inkorporere både tekniske og organisatoriske overvejelser, herunder om sletningen skal ske manuelt eller automatisk, hvordan systemerne løbende undersøges for oplysninger, der har nået de for de pågældende oplysninger gældende slettefrist, samt hvilke konkrete datafelter i et system der vil blive påvirket af sletningen.

Datatilsynet anfører endvidere, at der bør implementeres en procedure for opfølgning på sletning for at sikre, at sletning forløber som forventet.

Datatilsynet har i en række sager indstillet virksomheder til bøder på baggrund af princippet om opbevaringsbegrænsning.

I en sag fra 22. juni 2022 blev virksomheden Gyldendal A/S indstillet til en bøde på 1.000.000 kr. for at opbevare oplysninger om 685.000 personer i en såkaldt "passiv database" i mere end 10 år efter, at personerne havde meldt sig ud af bogklubben. Anklagemyndigheden har endnu ikke taget stilling til tiltalte spørgsmålet, og der er derfor endnu ikke afsagt dom.

I sag 2020-431-0116 blev Danske Bank indstillet til en bøde på 10 mio. kr., fordi banken i en række it-systemer ikke kunne dokumentere, at de havde slettet personoplysninger i overensstemmelse med databeskyttelsesreglerne. Bødeindstillingens størrelse skulle bl.a. ses i lyset af, at princippet om opbevaringsbegrænsning er et grundlæggende princip, og den manglende overholdelse af princippet berørte et meget stort antal registrerede. Anklagemyndigheden har endnu ikke taget stilling til tiltalte spørgsmålet, og der er derfor endnu ikke afsagt dom.

I sag 2018-41-0015 udtalte Datatilsynet alvorlig kritik af virksomheden IDdesign A/S (nu Ilva A/S) og indstillede til bødefordi virksomheden ikke havde fastlagt, hvilke frister der skulle gælde for sletning af personoplysninger

[16] Teksten findes under afsnittet "sletning af personoplysninger", som kan tilgås på dette link: https://www.datatilsynet.dk/emner/person-datasikkerhed/sletning/

[17] Teksten findes under afsnittet "sletning af personoplysninger", som kan tilgås på dette link: https://www.datatilsynet.dk/emner/person-datasikkerhed/sletning/

i et system. Virksomheden blev i byretten idømt en bøde på 100.000 kr.[18] Sagen er anket til landsretten.Herudover følger det af principperne, at forsyningsselskabet skal sørge for, at der alene behandles oplysninger om den enkelte kunde, der er relevante og nødvendige for det enkelte kundeforhold. Det er vigtigt, at der ikke registreres personoplysninger "bare fordi". Der skal være et sagligt formål, dvs. registreringen skal være lovlig, relevant og nødvendig.

Det betyder også, at forsyningsselskabet bør være opmærksom på eventuelle fritekstfelter og lignende, hvor personoplysninger, fx fra telefonsamtaler med kunder, nedfældes[19]. Brug af sådanne fritekstfelter bør minimeres mest muligt, og personoplysninger, der ikke falder i kategorien navn, adresse, e-mail, telefonnummer, cpr-nr. eller lignende samt målerdata, bør ikke registreres eller opbevares, medmindre der er et behandlingsgrundlag hertil, jf. afsnit 6.

Derfor er det også vigtigt, at der internt i virksomheden foretages en ajourføring og kontrol af oplysninger således, at vildledende eller urigtige oplysninger kan blive slettet eller rettet.

Formålet med indsamlingen af en kundes personoplysninger på vand- og spildevandsforsyningsområdet vil typisk være varetagelse af forsyningsforpligtelsen, herunder evt. indgåelse af aftalen om levering, levering af ydelsen, registrering af forbrug og opkrævning af forbrugsafgift.

Oplysninger, der ikke længere er relevante – det vil sige, hvor der ikke længere er en saglig begrundelse for at behandle dem – skal slettes[20] eller anonymiseres[21]. Datatilsynet har over for et forsyningsselskab udtalt sig om netop sletteplig ten i en sag om opbevaring af afsluttede supportsager, som ikke var nødvendigt at opbevare længere.[22]

---

[18] Dommen kan læses på Retten i Aarhus' hjemmeside: https://www.domstol.dk/aarhus/aktuelt/2021/2/selskab-idoemt-en-boede-paa-100000-kr/

[19] Vandselskaber, der ikke træffer myndighedsafgørelser, har ikke en notatpligt, som der skal tages hensyn til. Reglerne om notatpligt vil derfor sjældent være relevante, men der skal til gengæld tages hensyn til f.eks. sager om aktindsigt, hvor det er nødvendigt at tage notat af mundtlige oplysninger om væsentlig sagsbehandlingsskridt, f.eks. hvis selskabet mundtligt oplyser den, der har søgt aktindsigt om, at 7-dages fristen ikke overholdes.

[20] Sletning af personoplysninger betyder i praksis, at personoplysninger uigenkaldeligt fjernes fra alle de lagringsmedier, hvorpå de har været lagret, og at personoplysninger på ingen måde kan genskabes. Dette gælder for samtlige lagringsmedier, der har været i anvendelse i forbindelse med den pågældende databehandling, det vil sige, at der også sker sletning i den bagvedliggende database jf. Datatilsynet

[21] Der skal være tale om en uigenkaldelig anonymisering. Det skal vurderes konkret, om en anonymisering er tilstrækkelig, eller om personen stadig er identificerbar. Det kommer an på de faktiske omstændigheder, jf. Datatilsynet

[22] Datatilsynets afgørelse af 3. juli 2015 i j.nr. 2013-631-0053. https://www.datatilsynet.dk/afgoerelser/historiske-afgoerelser/2015/jul/sikkerhedsbrud-og-optagelse-af-kundesamtaler-hos-natur-energi-as

Datatilsynet havde i år 2022 særligt fokus på forsyningsselskabers håndtering af anmodninger om sletning (og indsigt). Datatilsynet havde jævnligt modtaget henvendelser fra borgere, der klagede over forsyningsselskabernes besvarelse af anmodninger om indsigt i eller sletning af de personoplysninger, som selskaberne behandlede.[23] Datatilsynet har imidlertid ikke offentliggjort nogle afgørelser på baggrund af deres udmelding.

DANVA anbefaler, at virksomheder løbende – og med et passende interval – foretager en gennemgang af registrerede persondata med henblik på ajourføring af relevante personoplysninger samt eventuel sletning af forældede data. Regler om minimumsopbevaringstid i lovgivningen skal overholdes, og der vil derfor sagligt kunne (og skulle) opbevares personoplysninger i dette tidsrum.

5.2 Krav til dokumentation

Det følger af Databeskyttelsesforordningens artikel 5, stk. 2, og artikel 24, at den dataansvarlige og databehandlere skal kunne påvise, at de overholder reglerne om databeskyttelse.

Det følger derfor af disse bestemmelser, at det er nødvendigt, at der laves dokumentation, som viser, at reglerne overholdes løbende.

Forsyningsselskaberne skal bl.a. kunne dokumentere, at der løbende foretages opdatering/ajourføring af selskabets dokumenter, politikker og overblik over databehandlingen. Der kan derfor med fordel udarbejdes et årshjul, hvorefter det skal dokumenteres, at de aktiviteter, som fremgår af årshjulet, er udført.

Forsyningsselskaberne skal ligeledes kunne dokumentere, at alle medarbejdere, som behandler personoplysninger er blevet instrueret om behandlingen f.eks. gennem en intern politik, og at de relevante medarbejdere løbende orienteres om ændringer/opdatering til politikkerne og lovgivningen.

Der skal føres en log over henvendelser fra registrerede samt besvarelse heraf, samt en sikkerhedsbrudslog.

5.3 Krav til samtykke

Det følger af databeskyttelsesforordningens artikel 4, nr. 11, at et samtykke skal være en frivillig, specifik, informeret og utvetydig viljestilkendegivelse. Det bør altid vurderes konkret, om samtykke er det bedst egnede behandlingsgrundlag.

I sag 2019-41-0038 udtalte Datatilsynet, at det er uhensigtsmæssigt, hvis behandlingen af personoplysninger sker på baggrund af samtykke, hvis den dataansvarlige i stedet kan basere behandlingen på andre relevante bestemmelser. Det kan f.eks. overvejes, om artikel 6, stk. 1, litra c (om retlig forpligtelse) eller artikel 6, stk. 1, litra f (interesseafvejning) kan benyttes som behandlingsgrundlag i stedet for samtykke.

[23] Datatilsynet offentliggør hvert år deres særlige fokusområder for dele af deres tilsynsaktiviteter. Læs mere om Datatilsynets særlige fokusområder for 2022 på Datatilsynets hjemmeside: https://www.datatilsynet.dk/afgoerelser/generelt-om-tilsyn/saerlige-fokusomraader-for-datatilsynets-tilsynsaktiviteter-i-2022. Fokusområderne for 2023 kan ses her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/feb/datatilsynets-fokusomraader-i-2023

Hvis samtykke dog vurderes at være det korrekte behandlingsgrundlag, har Datatilsynet udarbejdet en vejledning om samtykke, hvor kravene til samtykke gennemgås nærmere.[24] Vejledningen indeholder også en tjekliste, som forsyningsselskaberne kan bruge til at tjekke, om et samtykke er på linje med kravene i persondatalovgivningen.

I vejledningen udtaler Datatilsynet, at et samtykke skal være granulært i den forstand, at den dataansvarlige skal indhente særskilt samtykke for hvert enkelt formål med behandlingen af personoplysninger. Datatilsynet udtaler, at indhentelsen af flere samtykker i praksis kan ske i en samlet erklæring, hvor den registrerede særskilt kan markere, hvilke formål vedkommende vil acceptere.

I vejledningen fremgår det desuden, at et samtykke som minimum skal indeholde følgende oplysninger:

- Den dataansvarliges identitet,
- formålet med den påtænkte behandling,
- hvilke oplysninger, der behandles, og
- retten til at trække samtykket tilbage.

Samtykketeksten skal dog altid tilpasses til den konkrete situation, så den registrerede får fyldestgørende informationer om den konkrete behandling.

Anmodningen om samtykke skal være i en letforståelig og lettilgængelig form samt i et klart og enkelt sprog. Ligeledes skal den dataansvarlige kunne dokumentere, at den registrerede har givet samtykke.

Før samtykke indhentes, bør forsyningsselskaberne altid overveje, om samtykke er det mest passende behandlingsgrundlag, eller der kan været et andet retsgrundlag for behandlingen (se nærmere om de forskellige behandlingsgrundlag for almindelige og følsomme oplysninger i afsnit 6).

Den registrerede har altid ret til at trække sit samtykke tilbage, jf. databeskyttelseslovens artikel 7, stk. 3.

Der henvises i øvrigt til DANVAs persondatasite "Vejledninger og skabeloner fra DANVA", der indeholder et eksempel på en samtykkeerklæring.

5.3.1 Muligheden for at videregive oplysninger på baggrund af fuldmagt

En fuldmagtshaver (det vil sige en tredjemand som fx en ejendomsmægler eller lignende) kan handle på vegne af den registrerede. Det skal dog sikres, at fuldmagtshaveren er bemyndiget

[24] Datatilsynets vejledning om samtykke kan tilgås her: https://www.datatilsynet.dk/Media/0/C/Samtykke%20(3).pdf

5.3.2 Mulighed for at videregive oplysninger på baggrund af værgemål (Børn & unge under 18 år)

Forsyningsselskaber kan opleve at få en anmodning om personoplysninger fra en person, der er værge for et ungt menneske under 18 år, der er flyttet hjemmefra. Ligeledes kan der også komme anmodninger fra andre personer med relation til det unge menneske: Socialrådgiver, støtteperson, handicaphjælper m.fl.

Det kan eksempelvis dreje sig om;

- forespørgsler om forbrug og kopier af fakturaer og årsopgørelser.
- henvendelser om ret til indsigt.
- henvendelser om afgivelse af stemme i forbindelse med forbrugervalg til selskabets bestyrelse.
- hjælp til afgivelse af stemme i forbindelse med forbrugervalg til selskabets bestyrelsen.
- dialog om ikke betalte fakturaer.
- oprettelse af betalingsaftaler (afdragsordninger).

Når et samtykke er påkrævet for at videregive oplysninger, følger det af Datatilsynets vejledning om samtykke, at den dataansvarlige skal overveje, om barnet ud fra en modenhedsvurdering selv kan give samtykke, eller samtykket skal indhentes hos forældremyndighedsindehaveren. Det fremgår af vejledningen, at et barn på 15 år normalt vil være tilstrækkelig moden til at give samtykke.

Samme modenhedsvurdering skal anvendes, når et barn anmoder om indsigt i sine oplysninger efter databeskyttelsesforordningens artikel 15.

Hvis en forældremyndighedsindehaver henvender sig på barnets vegne og anmoder om at få udleveret oplysninger om barnet, skal den dataansvarlige foretage en vurdering af, hvorvidt forældremyndighedsindehaveren kan anmode om indsigt på barnets vegne. Selvom barnet er under 18, kan der forekomme tilfælde, hvor kun det barn, hvis oplysninger behandles, men ikke værgen/forældrene, bør kunne begære indsigt.

Datatilsynet har i en tidligere sag udtalt, at hovedreglen er, at en forældremyndighedsindehaver kan få indsigt i oplysninger om vedkommendes barn uden at skulle fremvise fuldmagt.[25] Det påhviler dog i det tilfælde den dataansvarlige at sikre, at den pågældende person er berettiget til at handle på vegne af barnet.

Datatilsynet har i en anden sag fra 2019 udtalt, at formålet med at anmode om indsigt i behandlingen af oplysninger om en forældremyndighedsindehavers barn er at kontrollere oplysningernes rigtighed med henblik på en eventuel berigtigelse og vurdering af nødvendigheden af opbevaringen samt kontrol af behandlingens

[25] Datatilsynets afgørelse af 21. marts 2017, j.nr. 2015-218-0195

lovlighed. I sagen var forældremyndighedsindehaverens formål med indsigtsanmodningen i datterens oplysninger hos en idrætsforening alene løbende at få information om datterens dansetræning. Idrætsforeningen var derfor berettiget til at afslå indsigtsanmodningen.[26]

Såfremt den dataansvarlige udleverer oplysninger til uvedkommende, vil der være tale om et sikkerhedsbrud.

Datatilsynet har tidligere udtalt, at det er den dataansvarlige, som afgør, hvorledes repræsentanten skal godtgøre, at vedkommende er berettiget til at optræde som repræsentant for den registrerede.[27] Det kan afhængig af omstændighederne f.eks. ske ved at forlange dokumentation for forældremyndigheden. Der henvises desuden til afsnit 7.3 og Datatilsynets vejledning om de registreredes rettigheder, som indeholder nærmere tekst om legitimationskravene generelt ved retten til indsigt.

5.3.3 Mulighed for at videregive oplysninger på baggrund af værgemål (Voksne) eller andre repræsentanter

Som anført i afsnit 5.3.2, skal den dataansvarlige sikre sig, at en person, der påstår at være repræsentant for den registrerede, faktisk er berettiget til at handle på vegne af vedkommende, herunder modtage oplysninger efter retten til indsigt.

Det gælder også for voksne personer under værgemål eller i den situation, hvor en person vælger at lade sig repræsentere af en anden f.eks. en ægtefælle, handicaphjælper eller en støtteperson. I disse tilfælde skal den dataansvarlige således sikre sig, at repræsentanten er berettiget til at handle på den registreredes vegne, f.eks. ved at forlange dokumentation af fuldmagtsforholdet og legitimation.

Den dataansvarlige er ikke forpligtet til at opbevare personoplysninger alene for at kunne reagere på mulige anmodninger, jf. præambelbetragtning nr. 64 i databeskyttelsesforordningen. Afgiven dokumentation kan imidlertid opbevares med formål at dokumentere, at den dataansvarlige har sikret sig, at vedkommende var berettiget til at handle på vegne af den registrerede, såfremt opbevaringen lever op til de almindelige principper og regler om behandling af personoplysninger.

[26] Datatilsynets afgørelse af 19. november 2019, j.nr. 2018-31-0972

[27] Datatilsynets afgørelse af 25. januar 2012, j.nr. 2012-211-0040

6 Hvornår må personoplysninger behandles?

Hvis der behandles personoplysninger, skal der være et behandlingsgrundlag. Det betyder, at det skal stå i databeskyttelsesforordningen eller databeskyttelsesloven, at man har lov til at behandle personoplysningerne. Behandlingsgrundlaget afhænger bl.a. af, hvilke kategorier af personoplysninger, der behandles. Derfor beskrives først kategorierne af personoplysninger og i afsnit 6.1 - 6.3 beskrives de specifikke regler for, hvornår personoplysninger må behandles afhængigt af hver kategori.

Persondatareglerne inddeler overordnet personoplysninger i to typer:

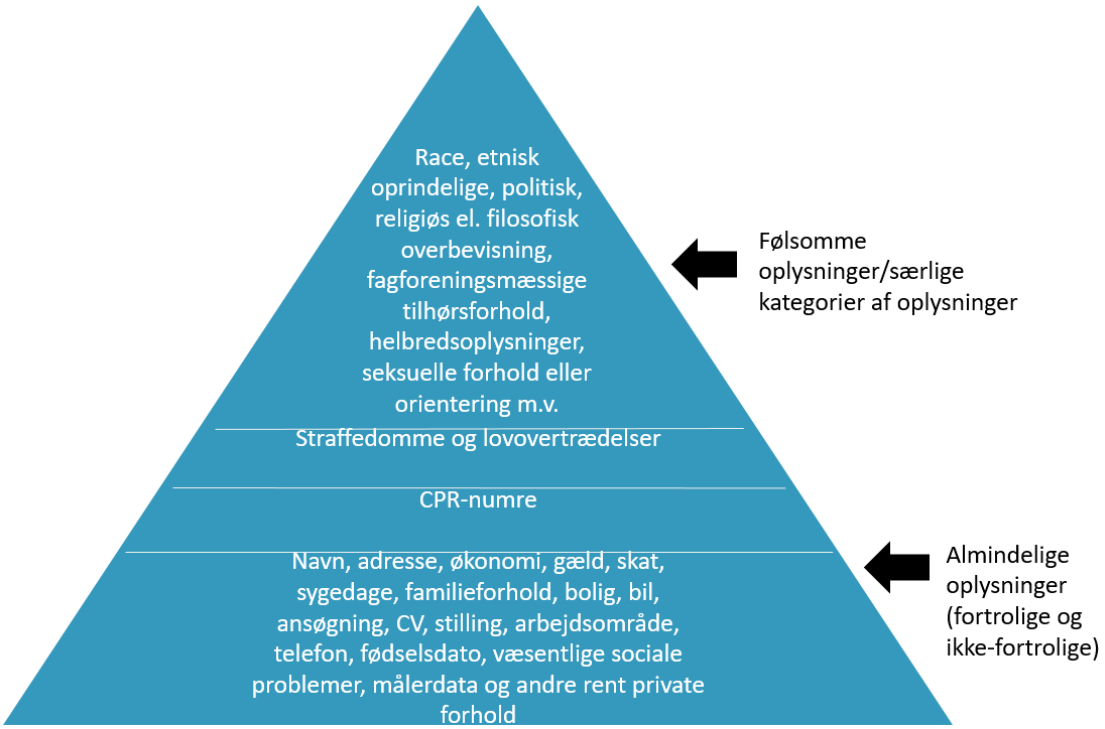
- **Følsomme oplysninger** (særlige kategorier af personoplysninger): De følsomme oplysninger er udtømmende opregnet i databeskyttelsesforordningens artikel 9 og omfatter: Personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold (f.eks. medlemskab af en bestemt fagforening) samt genetiske data og biometriske data samt helbredsoplysninger samt oplysninger om en fysisk person seksuelle forhold eller seksuelle orientering.

- **Almindelige oplysninger**: Det er alle andre personoplysninger, som ikke er følsomme. Det kan f.eks. være navn, alder, arbejde, hårfarve, økonomiske forhold, IP-adresse, målerdata eller andre tænkelige oplysninger, der kan henføres til en person. Fortrolige oplysninger, som ikke er følsomme oplysninger, hører under kategorien almindelige oplysninger.

Denne forskel i typen af data kan illustreres ved tegning nedenfor. Derudover gælder der en særregulering i databeskyttelsesloven af personoplysninger om straffedomme og lovovertrædelser samt cpr-numre[28], hvorfor disse almindelige personoplysninger er fremhævet.

Jo højere oppe i trekanten personoplysningen er placeret, desto strengere betingelser gælder for behandlingen af oplysningen.

[28] Disse personoplysninger reguleres af databeskyttelseslovens § 8 (straffedomme og lovovertrædelser) og § 11 (cpr-numre).



Fortrolige oplysninger: Omfatter de oplysninger, som efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab. De følsomme personoplysninger (de oplysninger, som er nævnt i artikel 9, det vil sige race, religion, helbredsoplysninger osv.) er også fortrolige oplysninger. Ikke-følsomme personoplysninger kan i visse situationer være fortrolige.. En fortrolig oplysning, som ikke er følsom, kan f.eks. være oplysning om, at en person modtager sociale ydelser eller har været udsat for en ulykke. Fortrolige oplysninger er efter omstændighederne også oplysninger om f.eks. indtægts- og formueforhold (f.eks. oplysninger om en persons manglende betaling), arbejds-, uddannelses- og ansættelsesmæssige forhold, oplysning om beskyttet/hemmelig adresse. Det samme gælder oplysninger om interne familieforhold, herunder for oplysninger om for eksempel selvmordsforsøg og ulykkestilfælde, jf. https://www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber/hvad-er-personoplysninger. Databeskyttelsesforordningen indeholder ikke særbestemmelser for fortrolige oplysninger og hører derfor under kategorien "almindelige personoplysninger", medmindre andet er fastsat i lovgivningen. Det vil sige, at forsyningsselskaber har ret til at behandle fortrolige oplysninger, så længe der er et behandlingsgrundlag, og oplysningerne ikke videregives til uvedkommende. De fortrolige oplysninger bør dog give anledning til ekstra opmærksomhed ved fastsættelse af særlige sikkerhedsforanstaltninger, f.eks. i forhold til kryptering. Se vejledningens afsnit 9.2 om kravene til kryptering ved afsendelse af bl.a. fortrolige oplysninger via e-mail.

6.1 Almindelige personoplysninger

Almindelige personoplysninger kan fx være identifikationsoplysninger (navn, adresse, telefonnummer, e-mail mv.), oplysninger om, hvor stort et vandforbrug den enkelte husstand har (og på hvilket tidspunkt af døgnet), kundeforhold eller andre lignende ikke-følsomme oplysninger.

Behandling af almindelige personoplysninger, det vil sige identifikationsoplysninger såsom fx navn, adresse, e-mail, tlf.nr. samt målerdata, må finde sted, hvis en af følgende relevante betingelser i databeskyttelsesforordningen, jf. databeskyttelseslovens § 6, stk. 1, er opfyldt:

- Den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål (artikel 6, stk.1, litra a).
- Behandlingen er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt (artikel 6, stk.1, litra b).
- Behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige, så som fx forsyningsselskabets forpligtelse til at indhente målerdata[29] (artikel 6, stk.1, litra c).
- Behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt (artikel 6, stk.1, litra e).
- Behandlingen er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser (artikel 6, stk.1, litra d).
- Behandlingen er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor (artikel 6, stk.1, litra f) – også kaldet interesseafvejningsreglen. Reglen gælder ikke for offentlige myndigheder.

Selvom en af ovenstående betingelser er opfyldt, må behandlingen kun finde sted, såfremt den ikke strider imod principperne i databeskyttelsesforordningens artikel 5, herunder fx at der ikke må behandles flere persondata end højst nødvendigt og ikke i længere tid end nødvendigt og kun til det/de formål, forsyningen på forhånd har angivet. Se nærmere herom i afsnit 5.

Behandlingen af almindelige oplysninger på forsyningsområdet sker typisk i forbindelse med og som følge af forsyningsselskabets forsyningspligt (artikel 6, stk. 1, litra c) og/eller indgåelse af en forsyningsaftale med kunden (artikel 6, stk. 1, litra b). Det bemærkes i den forbindelse, at der inden for vandsektoren normalt ikke anvendes skriftlige, gensidige aftaler om levering af en forsyningsydelse, og "aftalen" foreligger i form af en indirekte aftale baseret på forsyningsforpligtigelsen, leveringsvilkår i form af myndighedsgodkendt regulativ/betalingsvedtægt, myndighedsgodkendt takstblad og tilmed et reelt forsyningsforhold (typisk) i form af brug af service og betaling herfor.

[29] Se afsnit 2.2.

Det må dog antages, at hjemmelshenvisningen for behandlingen af personoplysninger primært har hjemmel i artikel 6, stk.1, litra b, fordi behandlingen er "nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt".

6.1.1 Navn og adresse mv.

Det lægges til grund, at forsyningsselskabets behandling af identifikationsoplysninger såsom navn(e), adresse, e-mail og telefonnummer er nødvendige af hensyn til opfyldelse af leveringsforpligtelsen over for den enkelte. Selvom leveringen sker på grundlag af forsyningsselskabets almindelige leveringsbetingelser, må det antages, at der består et aftaleforhold mellem forsyningsselskabet og kunden, og at behandlingen bl.a. er nødvendig for at opfylde denne aftale, som den registrerede er part i, jf. databeskyttelsesforordningens artikel 6, stk.1, litra b. Såfremt behandlingen baserer sig på forsyningspligt, vil behandlingen dog også have hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra c.

6.1.2 Afbrydelser

Vandforsyningsselskaber har i visse situationer ret til at få forsyningen af et forbrugssted afbrudt.

Som led i opkrævningsfasen er der mulighed for at afbryde vandforsyningen. Muligheden fremgår af leveringsbetingelserne/regulativet, der på dette punkt også vil være i overensstemmelse med Normalregulativet, jf. vejl. 9289/2014 og branchevejledningen fra 2020. I forhold til spildevand sker der i praksis ingen afbrydelse, da dette forventes hurtigt at ville give hygiejnemæssige problemer, hvilket der er krav om at modvirke[30].

I forbindelse med afbrydelsesprocessen kan det forekomme, at vandforsyningsselskabet indsamler, behandler og videregiver personoplysninger af følsom karakter, såsom fx oplysninger om helbredsforhold. Behandlingen af følsomme oplysninger skal i denne forbindelse ske i overensstemmelse med databeskyttelsesforordningens bestemmelser, jf. afsnit 6.2.

I afbrydelsessituationer kan det ligeledes blive relevant for forsyningen at overveje at videregive (person)oplysninger om udlejer til lejer, hvis udlejer af en ejendom kontraherer med forsyningen. Hvis eksempelvis udlejeren (som kan være en juridisk eller privat person) ikke har betalt, og forsyningen ønsker at lukke for vandet efter udløbet af rykkeprocessen, kan der opstå den situation, at lejeren i forbindelse med, at forsyningens ansatte møder op for at foretage afbrydelsen, gerne vil have lov til at betale regningen og derefter afregne med udlejeren.

---

[30] Hovedreglen er, at inddrivelse alene skal ske via Gældsstyrelsen. Med hensyn til opkrævningsfasen, der går frem til overdragelsen til Gældsstyrelsen, vil der være en rykkerprocedure baseret på lokal praksis – ligesom inkassovirksomheder/advokatfirmaer kan være involveret. Reguleringen har ændret sig, dec 2019, således at forsyningsselskaber kan vælge privat inddrivelse. Se https://www.danva.dk/nyheder/2020/privat-inddrivelse-er-en-ny-mulighed/ og pkt. 15.1.2.1 i DANVA vejledning 106 /regulativ (en kommunal forsyning kan vælge mellem privat inddrivelse og fortsat gøre brug af Gældsstyrelsen som inddrivelsesmyndighed)

Såfremt udlejer er en juridisk person, er der som det klare udgangspunkt ikke tale om personoplysninger.

Hvis udlejer er en privat person, vil oplysningerne udgøre en personoplysning (om størrelsen af en gæld). Forsyningen vil formentlig i en sådan situation – efter en konkret vurdering – kunne videregive oplysningerne til lejer (vedrørende gælden for forbrug på den ejendom, som lejeren lejer) med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra d (om beskyttelse af lejers vitale interesser, hvis der vurderes at være et sådant behov) eller artikel 6, stk. 1, litra f (om lejers legitime interesser i at have adgang til vand).

Bemærk at forsyningen ikke skal blande sig i forholdet mellem udlejer og lejer; hvis en udlejer ikke betaler vandregningen, og der sker en afbrydelse -, så kan lejeren kontakte kommunen og bede om at sikre, at forsyningen genoptages, jf. lejelovens § 95 og lov om boligforhold § 19.

6.1.3 Kreditoplysninger

Kreditoplysninger er under den nye persondatalovgivning almindelige oplysninger, som kan behandles efter artikel 6 i databeskyttelsesforordningen. De vil dog normalt udgøre fortrolige oplysninger, som kræver iagttagelse af særlige sikkerhedsforanstaltninger.

Normalt ligger vandforsyningsselskaber ikke inde med oplysninger om kundernes økonomi, men i særlige situationer er selskabet forpligtiget til at indgå afdragsordninger, hvorved kreditoplysninger behandles. Det kunne eksempelvis være den situation, hvor forsyningsselskabet er forpligtiget til at indgå i en afdragsordning i forhold til betaling af tilslutningsbidrag, jf. bekendtgørelse 108/2015 om afdragsordninger, fristfastsættelse for spildevandshåndtering og tilslutningsbidragets forfaldstidspunkt. I tilfælde, hvor selskabet er forpligtet til at behandle kreditoplysningerne, kan behandlingen ske med hjemmel i databeskyttelsesforordningens artikel 6, stk.1, litra c (retlig forpligtelse).

6.1.4 Målerdata

Målerdata(forbrug) indhentes, jf. databeskyttelsesforordningens artikel 6, stk.1, litra c, som led i forsyningsselskabets overholdelse af en retlig forpligtelse til afregning efter målt forbrug[31].

I forhold til vandforsyning er der med hjemmel i vandforsyningslovens § 55, stk. 6, i bekendtgørelse 525/1996 udstedt regler om indhentelse af vandmålerdata og betaling efter målt forbrug. Med hensyn til spildevand sker afregning efter målt forbrug via vandmåler, jf. lov om betalingsregler for spildevandsforsyningsselskaber § 2a,

[31] Se kapitel 2.2.

stk. 4. Indhentelsen af disse data har hjemmel i § 7b. I praksis indhenter spildevandforsyningsselskaberne dataene én gang årligt, og der er som udgangspunkt ikke brug for løbende data.

Hos vandforsyningsselskaber er det almindeligt at indhente data løbende via fjernaflæsning med henblik på at optimere driften af forsyningen. Herudover anvender forsyningsselskabet målerdata til brug for optimering og drift af nettet.

Energistyrelsen udmeldte i januar 2018, 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, men at det var centralt, at de grundlæggende principper i artikel 5 i databeskyttelsesforordningen blev overholdt. En sådan behandling kan dermed ske med hjemmel i databeskyttelsesforordningens artikel 6, stk.1, litra c (retlig interesse), artikel 6, stk. 1, litra e (nødvendig af hensyn til udførelse af en opgave i samfundets interesse) eller artikel 6, stk. 1, litra f (nødvendig for at dataansvarlig kan forfølge en legitim interesse).

Forsyningsselskabets behandling af målerdata er endvidere nødvendig af hensyn til opfyldelse af leveringsforpligtelsen over for den enkelte kunde og den heraf følgende fakturering af kunden, jf. databeskyttelsesforordningens artikel 6, stk.1, litra b.

Målerdata må således anses for almindelige personoplysninger, der kan behandles med hjemmel i databeskyttelsesforordningens artikel 6. Det er dog anbefalingen, at målerdata sikkerhedsmæssigt behandles, som var det fortrolige oplysninger. Det vil sige, at selvom Datatilsynet ikke umiddelbart stiller krav til kryptering af e-mails indeholdende forbrugsdata på kvartals-/årsniveau, er det forsyningen som dataansvarlig, der med udgangspunkt i sin risikovurdering, skal vurdere hvilket sikkerhedsniveau der er passende. Ud fra et forsigtighedsprincip, herunder en formodning om at mange forbrugere opfatter forbrugsdata som værende af privat karakter samt det øgende fokus på it-sikkerhed (NIS2) kan forsyningen her vælge at følge Datatilsynets krav om TLS 1.2 (eller højere) kryptering ved fremsendelse af e-mails med fortrolige eller følsomme oplysninger via internettet. En betragtning, der deles af DANVAs GDPR-netværk. Se mere om kryptering i afsnit 9.2.

Det bemærkes endvidere, at i hvert fald oplysninger om energiforbrug antages at være en oplysning, som ikke kan videregives til private eller offentliggøres uden samtykke. Det er uafklaret, om dette også gælder forbrugsoplysninger, som vedrører vand og spildevand og ikke energi.

Det er DANVAs opfattelse, at oplysninger om forbrug i forhold til vand og spildevand ikke kan videregives til private eller offentliggøres uden samtykke. Efter omstændighederne kan det dog vurderes, at der er et andet passende behandlingsgrundlag. Det kan for eksempel være, hvis oplysningerne skal videregives for at overholde en retlig forpligtelse, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra c.

Oplysninger om forbrug i forhold til vand og spildevand er ikke følsomme personoplysninger, men hensynene til, at det ikke skal være muligt for udenforstående at kende den enkelte husstands forbrug, gør, at disse

oplysninger har en privat karakter og således ikke kan omfattes af interesseafvejningsreglen i databeskyttelsesforordningens artikel 6, stk. 1, litra f.[32] Oplysninger om forbrug bør således som udgangspunkt ikke offentliggøres eller videregives uden den enkelte kundes samtykke.

Muligheden for at aflæse målerdata ved fjernaflæsning ændrer ikke på, at der stadig er tale om en behandling af almindelige ikke-følsomme oplysninger, der kan behandles med hjemmel i databeskyttelsesforordningens artikel 6, selvom fjernaflæsning gør det muligt at foretage en meget hyppigere aflæsning end en manuel aflæsning. Aflæsningshyppigheden skal dog overholde databeskyttelsesforordningens artikel 5, jf. Energistyrelsens udmelding herom[33].

Det er dog en forudsætning, at oplysningerne behandles til forsyningsformål – herunder forsyningspligt, driftssikkerhed, optimering af drift, forsyningsøkonomi og miljøhensyn – eller f.eks. statistik og forskning i forsyningens interesse.[34]

Hvor ofte der kan ske fjernaflæsning til forsyningsformål, afhænger af det konkrete projekt/formål, og hvor ofte det her er sagligt nødvendigt at foretage fjernaflæsning sammenholdt med den integritetskrænkelse, det kan indebære for den enkelte kunde. Der skal således foretages en konkret vurdering af behovet for aflæsning af målerdata, idet aflæsningen skal være i overensstemmelse med artikel 5.

En løbende dataindsamling/aflæsning af målerdata med henblik på monitorering af en ejendom vil dog formentlig kræve samtykke – specielt hvis der er tale om hyppig registrering – fordi en profil baseret på mange, hyppige målerdata går tæt på kundens persondataretlige integritet.

I forhold til tilknyttede-aktivitets-selskaber (jf. bekendtgørelse 1227/2016) og deres forhold til forsyningsselskabet, må det antages, at der i tilknyttede-aktivitets-selskaber behandles personoplysninger til andre grundlæggende formål end i et vandselskab. Det indebærer bl.a., at de ovenfor anførte grundlag for at indhente målerdata ikke finder anvendelse i forhold til et tilknyttede-aktivitets-selskabs behandling af målerdata.

Generelt vil de særlige hensyn til varetagelse af forsyningsformål og de særlige bestemmelser herom således ikke have betydning for behandling af personoplysninger i forbindelse med tilknyttede aktiviteter. Tilknyttede-aktivitets-selskaber skal derfor vurderes konkret ud fra de almindelige krav til behandling af personoplysninger.

---

[32] Dette er også lagt til grund i den tidligere persondatalovs forarbejder (svar på spørgsmål nr. 63 L 44 fremsat 8. oktober 1998) forhold til elforbrug. Det er endvidere lagt til grund i Datatilsynets høringssvar i forhold til BBR-loven (L 47 fremsat 29. oktober 2009) i forhold til energiforbrug generelt.

[33] http://www.mynewsdesk.com/dk/energistyrelsen/news/dansk-afklaring-om-fjernaflaesning-i-forhold-til-databeskyttelsesforordningen-291497.

[34] Oplysningerne indhentet via fjernmålere vil ligeledes kunne blive behandlet med hjemmel i artikel 6, stk. 1, litra c, hvis forsyningsselskabet bliver pålagt at udlevere oplysninger på baggrund af en retlig forpligtelse, jf. afsnit 11.

6.1.5 Cpr-nummer

Der gælder særregler vedrørende behandlingen af cpr-numre, som efter den danske databeskyttelseslovs § 11 medfører, at selskaber som udgangspunkt kun må behandle disse oplysninger, når det følger af lovgivningen, eller den registrerede har givet sig samtykke hertil.

Herudover har § 11, stk. 2, nr. 4 i databeskyttelsesloven dog også givet mulighed for at behandle cpr-numre, hvis betingelserne i databeskyttelseslovens § 7 er opfyldt. Sidstnævnte indebærer, at cpr-numre kan behandles, hvis betingelserne i databeskyttelsesforordningens artikel 9, stk. 2, litra a, c, d, e eller f, er opfyldt.

Forsyningsselskabets behandling af kundens cpr-nr. sker p.t. primært på grundlag af kundens samtykke, jf. databeskyttelseslovens § 11, stk. 2, nr. 2[35], som fx indhentes ved en elektronisk aftale i forbindelse med aftaleindgåelsen – og/eller på grundlag af adgangen til at få oplyst cpr-nr. uden samtykke er reguleret i inddrivelsesloven § 2, stk. 9 og 10, jf. databeskyttelseslovens § 11, stk. 2, nr. 1.

Hjemlen til behandling af cpr-nummer i inddrivelsesloven gælder kun i forhold til inddrivelse. I øvrige situationer kræver behandling som udgangspunkt samtykke. DANVA har udarbejdet et eksempel på en samtykkeerklæring, den fremgår af DANVAs persondatasite "Vejledninger og skabeloner fra DANVA"

Gældsinddrivelseslovens § 2, stk. 9-10, som giver mulighed for behandling af cpr-nummer, er sålydende:

"Stk. 9. Ved overdragelse af fordringer til restanceinddrivelsesmyndigheden skal en kommunalt ejet forsyningsvirksomhed eller den, der på dennes vegne opkræver fordringen, oplyse skyldnerens personnummer. Hvis forsyningsvirksomheden ikke er i besiddelse af skyldnerens personnummer, skal forsyningsvirksomheden eller den, der på dennes vegne opkræver fordringen, inden overdragelsen af fordringen skriftligt anmode skyldneren om inden for en nærmere angiven frist at oplyse sit personnummer. Anmodningen skal indeholde oplysning om adgangen til at indhente skyldnerens personnummer fra Det Centrale Personregister efter fristens udløb, jf. stk. 10.

Stk. 10. Har skyldneren ikke oplyst sit personnummer inden for den angivne frist, eller foreligger der begrundet tvivl om rigtigheden af skyldnerens oplysning herom, kan forsyningsvirksomheden eller den, der på dennes vegne opkræver fordringen, ved henvendelse til en kommunalbestyrelse efter forudgående entydig identifikation af skyldneren få oplyst skyldnerens personnummer fra Det Centrale Personregister. Kommunalbestyrelsen skal behandle anmodningen senest 10 hverdage efter modtagelsen heraf."

I nogle situationer er der indgået en gensidig aftale mellem forsyningsselskabet og kunden. Dette kan være ved kontrakt mellem spildevandsforsyningsselskabet og en kunde på landet, hvorefter forsyningsselskabet etablerer, driver og vedligeholder en renseløsning i forhold til husspildevand på privat ejendom (helårsbebo-

[35] En række forsyningsselskaber har fået kunders cpr-nr. ved en elektronisk aftale, hvorved der kan være opnået et samtykke som grundlag for behandlingen, jf. § 11, stk. 2, nr. 2. Sigtet har typisk været at sikre en hurtig og automatisk tilbagebetaling af for meget acontobetaling.

else). Der kan i sådanne aftaler være aftaler om overførsel af cpr-nr. fra kunde til selskab. Det er en forudsætning, at der er tale om et udtrykkeligt samtykke, der opfylder definitionen for et samtykke, og det er således ikke tilstrækkeligt, at kunden giver oplysningerne til forsyningen, jf. afsnit 2[36].

Det skal bemærkes, at den registrerede altid kan tilbagekalde sit samtykke, jf. herved databeskyttelsesforordningens artikel 7.

Uanset om indhentelse af CPR-nummer sker ved et samtykke eller med hjemmel i lovgivning, skal forsyningsselskaberne også være opmærksomme på at overholde databeskyttelsesforordningens artikel 5 (der henvises til vejledningens afsnit 5.1). Det indebærer bl.a., at CPR-nummer kun skal indhentes, hvis det er nødvendigt i forhold til formålet, og ikke må opbevares i længere tid end nødvendigt.

Se nærmere om Datatilsynets anbefalinger vedrørende datasikkerhed ved behandling af cpr-nr. under afsnit 9.

6.1.6 Videregivelse til statistiske eller videnskabelige formål

Almindelige personoplysninger kan behandles til videnskabelige eller statistiske formål uden den registreredes samtykke med hjemmel i databeskyttelsesforordningens § 6, stk. 1, litra e. Det vil sige, at forsyningsselskabet kan udlevere kunders målerdata til brug for videnskabelige og statistiske formål, uden at målerdata er anonymiseret, hvis udleveringen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse. Det kunne fx være udlevering/overladelse af målerdata i forbindelse med analyser for optimering af forsyningsnettet. Den typiske situation vil nok være, at der sker analysearbejde efter instruks fra en forsyning eller i forbindelse med større projekt med relation til eksempelvis VUDP (Vandsektorens forening til forbedring af vandsektorens effektivitet og kvalitet).)[37]

Persondatalovgivningens bestemmelser skal naturligvis iagttages (dvs. fx sikre, at oplysningerne ikke falder i de forkerte hænder), men Datatilsynet skal ikke godkende projektet.

Til gengæld gælder det, at videregivelse til tredjemand af oplysninger (dvs. til en ny dataansvarlig), der er behandlet med videnskabeligt eller statistisk formål, imidlertid i visse situationer kræver forudgående tilladelse fra Datatilsynet. Og dette krav om forudgående tilladelse til videregivelse gælder både i forhold til følsomme og ikke-følsomme personoplysninger, så som fx forbrug. Datatilsynet kan stille nærmere vilkår for videregivelsen[38].

---

[36] Persondatalovens § 11, stk. 2, nr. 2, og § 3, nr. 8.

[37] Hvis der er tale om analysearbejde "efter instruks" fx fra et forsyningsselskab, som leverer dataene, vil den, der laver analysearbejdet, muligvis blot være databehandler for dataene. I et sådan tilfælde vil der skulle udfærdiges en databehandleraftale. Det vil være en konkret vurdering.

[38] Se databeskyttelseslovens § 10.

Det må i den forbindelse antages, at selvom fjernaflæsning af forbrug med korte intervaller kan bruges til at danne præcise profiler, så vil der som udgangspunkt ikke være tale om følsomme oplysninger. Dette forudsætter imidlertid, at det konkret er sagligt og nødvendigt, at der sker en så hyppig registrering, og at fjernaflæsningen ikke sker med henblik på monitorering af den enkelte kunde.

6.2 Følsomme personoplysninger

Behandling af følsomme oplysninger så som fx oplysninger om helbredsmæssige forhold kan på forsyningsområdet ske, hvis en af de relevante betingelser er opfyldt i databeskyttelsesforordningen artikel 9, jf. databeskyttelseslovens § 7, stk. 1. Det omfatter bl.a. følgende behandlingsgrundlag:

- Den registrerede har givet udtrykkeligt samtykke til behandling (artikel 9, stk. 2, litra a).
- Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser i tilfælde, hvor den registrerede fysisk eller juridisk ikke er i stand til at give samtykke (artikel 9, stk. 2, litra c).
- Behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares (artikel 9, stk. 2, litra f).

Derudover er det efter Datatilsynets opfattelse tillige nødvendigt at identificere et lovligt grundlag for behandlingen i databeskyttelsesforordningens artikel 6 vedrørende ikke-følsomme personoplysninger (der henvises til opregningen af behandlingsgrundlag i artikel 6 i afsnit 6.1). Der er således et dobbelt hjemmelskrav for følsomme oplysninger, da den dataansvarlige skal sikre, at behandlingen både opfylder én af betingelserne i databeskyttelsesforordningens artikel 9 og opfylder én af betingelserne i artikel 6.

Selvom ovenstående betingelser er opfyldt, må behandlingen kun finde sted, såfremt den ikke strider imod principperne i databeskyttelsesforordningens artikel 5, herunder fx, at der ikke må behandles flere persondata end højst nødvendigt og ikke i længere tid end nødvendigt.

Behandling af oplysninger om helbredsmæssige forhold sker fx, når forsyningsselskabet bliver opmærksom på, at en kunde virker senil eller på anden vis udviser en hjælpeløs adfærd, og dette registreres.

En sådan helbredsoplysning kan være relevant at registrere og videregive fra forsyningsselskabet i forbindelse med afbrydelse af den pågældende kunde for at sikre, at en afbrydelse ikke får uhensigtsmæssige konsekvenser for den pågældende.

I et sådan tilfælde vil det ofte ikke være muligt at indhente kundens samtykke. Behandlingen antages imidlertid at være nødvendig for at beskytte kundens vitale interesser, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra c, og artikel 6, stk. 1, litra d.

I de afbrydelsessituationer, hvor forsyningsselskabet får kendskab til, at der gælder særlige forhold i forhold til en kunde, og der er behov for at videregive en sådan følsom oplysning, bør et udtrykkeligt samtykke til behandlingen af oplysningen i første omgang forsøges indhentet. Dette kan f.eks. være i forhold til trusler mod

forsyningsmedarbejdere eller børn, der er i risiko for omsorgssvigt. Kan dette ikke lade sig gøre, må det vurderes, om behandlingen af oplysningen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares, hvilket vurderes at kunne være tilfældet i en afbrydelsessag, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra f, og artikel 6, stk. 1, litra d eller f.

6.3 Straffedomme og lovovertrædelser

Behandling af straffedomme og lovovertrædelser kan ske, hvis kunden har givet sit udtrykkelige samtykke hertil, eller hvis behandlingen er nødvendig til varetagelsen af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede, jf. databeskyttelseslovens § 8, stk. 3.

Dette kunne fx være oplysninger om truende adfærd på en ejendom, som giver anledning til, at politiet skal kontaktes, eller som i hvert fald giver anledning til agtpågivenhed, når en tekniker skal ud på adressen og fx foretage en afbrydelse. I et tilfælde, hvor en kunde udviser truende adfærd i forbindelse med en afbrydelse, der foretages fysisk på adressen, vil det ofte ikke være muligt at indhente kundens samtykke. Behandlingen af oplysningen om, at kunden udviser truende adfærd, må derfor baseres på en afvejning af hensynet til den registrerede og hensynet til selskabets ansatte, jf. databeskyttelseslovens § 8, stk. 3. Alt afhængigt af de konkrete omstændigheder bør en sådan afvejning falde ud til fordel for selskabets ansatte, hvorfor oplysningen om fx truende adfærd godt kan behandles.

Tyveri af vand forekommer også. Der er i disse tilfælde tale om overtrædelse af straffeloven og bestemmelser i leveringsvilkårene, der kan resultere i politisager[39].

I sager om tyveri af vand, hvor forholdet er anmeldt til politiet og derfor håndteres efter straffeloven, må det antages, at oplysninger om den pågældende kundes målerdata og andre oplysninger i relation hertil vil kunne kategoriseres som oplysninger om strafbare forhold, der kan behandles uden samtykke fra kunden i medfør af databeskyttelseslovens § 8, stk. 3-5[40].

I sag 2003-42-0523 udtalte Datatilsynet sig om brug af videoovervågning i S-togene. Datatilsynet udtalte bl.a., at DSB-tog A/S havde ret til at videoovervåge passagerer i S-togene med henblik på at forbedre trygheden blandt passagererne og for at kunne bruge optagelserne som led i efterforskning ved kriminelle handlinger og som bevismateriale i eventuelle retssager. Datatilsynet udtalte, at DSB-tog A/S uden samtykke kunne videre-

[39] Hjemlen dertil er at hente i VFL § 84. Se Normalregulativet (2014) pkt. 17 for en oplistning, og hvor pkt. 9.2, 1 sætning er nævnt. Se også DANVA og Danske Vandværker, 2020, Regulativ for almene vandforsyninger, branchevejledning (DANVA vejledning nr. 106).

[40] Om der kan ske videregivelse af sådanne oplysninger, fx til politiet i forbindelse med den pågældende sag, må eventuelt vurderes efter interesseafvejningsreglen i databeskyttelsesforordningens artikel 6, stk. 1, litra f, og i det hele taget efter dansk retsregler om bevisførelse.

give oplysninger fra optagelser i et S-tog af konkrete hændelser, der afslørede oplysninger om strafbare forhold, til politiet, forudsat, at det var til brug for en strafferetlig efterforskning af forhold over en vis bagatelgrænse.

Også uautoriseret arbejde på vandinstallationer og indgreb i målere kan resultere i bødestraf[41].

Ligesom andre har forsyninger også en forpligtigelse efter dyreværnsloven. Det kan være vanskeligt for vandforsyningens personale at vurdere, om afbrydelsen af vand i et konkret tilfælde udløser vanrøgt af en hel dyrebesætning, men manglende vand vil hurtigt kunne få konsekvenser for dyrene. En eventuel mistanke om vanrøgt kan derfor godt føre til en konkret anmeldelse til politiet, som herefter må foretage en vurdering af de faktiske omstændigheder.

Der er i databeskyttelsesforordningen en bestemmelse om, at oplysninger vedrørende straffedomme og lovovertrædelser kun må behandles under kontrol af en offentlig myndighed, eller hvis behandlingen har hjemmel i lovgivningen[42], hvilket som anført ovenfor kan være i databeskyttelseslovens § 8.

6.3.1 Tv-overvågning

Behandling af personoplysninger i forbindelse med tv-overvågning er reguleret i databeskyttelsesretten og i tv-overvågningsloven.

Behandlingen kan kun finde sted, hvis de grundlæggende behandlingsprincipper om bl.a. lovlighed, rimelighed og gennemsigtighed, formålsbegrænsning og opbevaringsbegrænsning er opfyldt. Se vejledningens afsnit 5.1 om de grundlæggende principper.

Behandling af personoplysninger skal ud over at leve op de grundlæggende principper ske inden for rammerne af behandlingsreglerne i databeskyttelsesforordningen eller databeskyttelsesloven. Se afsnit 6 om behandlingsreglerne.

Billed- og lydoptagelser med personoplysninger, som stammer fra tv-overvågning i kriminalitetsforebyggende øjemed, skal som hovedregel slettes 30 dage efter, at de er blevet optaget.[43]

---

[41] Se bekendtgørelse om kontrol med vandmålere.

[42] Artikel 10.

[43] Det følger af tv-overvågningslovens § 4 c, stk. 4. Efter tv-overvågningslovens § 4 c, stk. 5, kan optagelserne dog under særlige omstændigheder opbevares i et længere tidsrum end 30 dage efter, at optagelserne er foretaget.

Private og offentlige myndigheder, der foretager tv-overvågning af steder eller lokaler, hvor der er almindelig adgang til, eller af arbejdspladser, skal ifølge tv-overvågningsloven ved skiltning eller på anden tydelig måde oplyse om overvågningen.[44]

Datatilsynet har lavet en side om tv-overvågning, som beskriver nærmere om reglerne.[45]

[44] Det følger af tv-overvågningslovens §§ 3 og 3 a.

[45] https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/optagelser-og-overvaagning/tv-overvaagning

7 Den registreredes (kundens) rettigheder

7.1 Oplysningspligten

Når personoplysninger indsamles, skal den dataansvarlige give den registrerede meddelelse om følgende[46]:

- den dataansvarliges identitet og kontaktoplysninger.
- kontaktoplysninger for en eventuel databeskyttelsesrådgiver.
- formålene med den behandling, som personoplysningerne skal bruges til, og retsgrundlaget for behandlingen.
- de berørte kategorier af personoplysninger.
- hvilken kilde personoplysningerne hidrører fra, og eventuelt hvorvidt de stammer fra offentligt tilgængelige kilder.
- de legitime interesser, som forfølges af den dataansvarlige eller en tredjemand, hvis behandlingen er baseret på artikel 6, stk. 1, litra f).
- eventuelle modtagere eller kategorier af modtagere af personoplysningerne.
- hvor det er relevant, at den dataansvarlige agter at overføre personoplysninger til et tredjeland eller en international organisation, og om hvorvidt Kommissionen har truffet afgørelse om tilstrækkeligheden af beskyttelsesniveauet, eller i tilfælde af overførsler i henhold til artikel 46 eller 47 eller artikel 49, stk. 1, andet afsnit, litra h), henvisning til de fornødne eller passende garantier, og hvordan der kan fås en kopi heraf, eller hvor de er blevet gjort tilgængelige.

Herudover bør der gives følgende oplysninger:

- det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum.
- retten til at anmode den dataansvarlige om indsigt i og berigtigelse eller sletning af personoplysninger eller begrænsning af behandling vedrørende den registrerede eller til at gøre indsigelse mod behandling samt retten til dataportabilitet.
- retten til at trække samtykke tilbage på ethvert tidspunkt, uden at dette berører lovligheden af behandling, der er baseret på samtykke, inden tilbagetrækning heraf.
- retten til at indgive en klage til en tilsynsmyndighed.
- meddelelse af personoplysninger er lovpligtigt eller et krav i henhold til en kontrakt eller et krav, der skal være opfyldt for at indgå en kontrakt, samt om den registrerede har pligt til at give personoplysningerne og de eventuelle konsekvenser af ikke at give sådanne oplysninger.

[46] Databeskyttelsesforordningens artikel 13. I en sådan situation, hvor forsyningsselskabet ikke får personoplysninger fra den registrerede selv, vil det være databeskyttelsesforordningens artikel 14, der gælder for oplysningspligten.

- forekomsten af automatiske afgørelser, herunder profilering, og i disse tilfælde som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede.

DANVA har udarbejdet et udkast til en skabelon for en privatlivspolitik, der opfylder oplysningspligten. Den fremgår af DANVAs persondatasite "Vejledninger og skabeloner fra DANVA"

Privatlivspolitikken skal i henhold til databeskyttelsesforordningens artikel 12 være lettilgængelig. Datatilsynet har i sin podcast-serie udtalt, at en privatlivspolitik på en hjemmeside skal være placeret således, at den er en integreret del af hjemmesiden samt er tilgængelig på eventuelleundersider, så den registrerede hele tiden har mulighed for at tilgå den. Det er ikke tilstrækkeligt, at den kun fremgår under fanen "om os" eller lignende.[47]

Hvis oplysningerne er indsamlet hos den registrerede selv, skal oplysningerne ovenfor gives samtidigt med indsamlingen af oplysningerne, jf. artikel 13, stk. 1. Hvis oplysningerne ikke er indsamlet hos den registrerede, skal oplysningspligten opfyldes inden for en rimelig frist efter indsamlingen af personoplysningerne, men senest inden for én måned under hensyn til de specifikke forhold, som personoplysningerne er behandlet under, jf. artikel 14, stk. 3.[48]

Det er Datatilsynets opfattelse, at de oplysninger, som den dataansvarlige er forpligtet til at give, skal være tydeligt adskilt fra andre oplysninger – og tydeligt fremhævede – og fra start giver den registrerede et klart overblik. Dette skyldes, at der er krav om, jf. artikel 12, at oplysningerne skal gives til den registrerede på en tydelig, kortfattet og letforståelig måde.

Herudover følger det af databeskyttelsesforordningens artikel 21, stk. 4, at den registrerede har ret til at få meddelelse om oplysninger om retten til at gøre indsigelse over behandling af personoplysninger i artikel 21, stk. 1 og 2, klart og adskilt fra alle andre oplysninger.

Oplysningerne skal gives direkte til den registrerede, herunder evt. som aktivt link til en privatlivspolitik, hvor oplysningspligten er opfyldt. Herudover bør privatlivspolitikken også være på selskabets hjemmeside.

DANVA anbefaler at forsyningsselskabet i dialogen omkring afbrydelsen informerer om at forsyningsselskabet i forbindelse med afbrydelsen kan behandle personoplysninger samt kundens rettigheder efter databeskyttelseslovgivningen. Det kan for eksempel være ved i dialogen med kunden at henvise til forsyningsselskabets privatlivspolitik på hjemmesiden eller ved at vedhæfte privatlivspolitikken i forbindelse med dialogen.]. I praksis skal forsyningsselskabet i forbindelse med tilslutning af nye kunder sikre sig, at disse kunder sammen med information om leveringsvilkår (regulativ, betalingsvedtægt) og takster også modtager oplysninger om privat-

[47] Podcastet benævnt "Podcast: #4 - Hvordan laver man en god persondatapolitik?". Det kan tilgås på Datatilsynets hjemmeside: https://www.datatilsynet.dk/hvad-siger-reglerne/podcast/hvordan-laver-man-en-god-persondatapolitik

[48] Hvis personoplysningerne skal bruges til at kommunikere med den registrerede, senest på tidspunkt for den første kommunikation, og hvis personoplysningerne er bestemt til videregivelse til en anden modtager, senest når personoplysningerne videregives første gang, jf. artikel 14, stk. 3, litra a) og b).

livspolitikken (som kan være et bilag til leveringsvilkår) – evt. ved brug af et aktivt link i et elektronisk velkomstbrev. Hvis velkomstbrevet er fysisk, bør privatlivspolitikken/opfyldelse af oplysningspligten fremgå af dette brev, men med særskilt overskrift, således at oplysninger er adskilt fra andre oplysninger. Oplysningerne må således ikke blandes ind i leveringsvilkårene – men kan dog formentlig være et bilag hertil med særskilt overskrift.

Oplysningsforpligtigelsen gælder naturligvis også overfor eksisterende kunder. Opfyldelse af oplysningspligten over for disse kan f.eks. ske ved på/i forbindelse med en faktura – klart og adskilt fra fakturaoplysningerne – at gøre opmærksom på, at selskabet har udarbejdet/ændret sin privatlivspolitik, der angår de personoplysninger, som selskabet indsamler, opbevarer og behandler. Såfremt de eksisterende kunder endnu ikke har fået en orientering om deres rettigheder, er det nødvendigt, at selskaberne opfylder oplysningspligten over for disse – evt. i forbindelse med førstkommende faktura, idet det dog bemærkes, at opfyldelse af oplysningspligten skal ske i forbindelse med, at indsamlingen af oplysningerne er sket, jf. artikel 13 (hvis oplysningerne er indsamlet hos den registrerede selv).

7.2 Andre rettigheder

Databeskyttelsesforordningen kapitel III indeholder regler, som giver den registrerede (kunden) en række rettigheder over for de dataansvarlige virksomheder, som behandler personoplysninger.

Det bemærkes, at omfanget og rækkevidden af rettighederne på en lang række områder endnu er uklare. Der henvises til Datatilsynets vejledning om de registreredes rettigheder for en nærmere gennemgang.

Kundens rettigheder omfatter navnlig følgende:

7.2.1 Ret til indsigt i de oplysninger, der behandles

Den registrerede har ret til at se de personoplysninger, som selskabet behandler om vedkommende ved at modtage en kopi heraf. Derudover har den registrerede ret til at modtage en række oplysninger om den behandling, som selskabet foretager, fx formålet med selskabets behandling af personoplysningerne og slettefrister.

Anmodninger om indsigt behøver ikke indeholde henvisninger til databeskyttelsesreglerne eller indeholde brug af ordet "indsigt", hvis det på anden måde er klart, at den registrerede ønsker indsigt. Anmodninger om indsigt skal besvares uden unødig forsinkelse og senest en måned efter, at anmodningen er modtaget. Denne periode kan forlænges med yderligere to måneder, hvis det er nødvendigt på grund af anmodningernes kompleksitet og antal. Det vil sige, at der er en absolut frist for besvarelse af anmodninger på tre måneder.

I sag 2019-31-1713 udtalte Datatilsynet kritik af, at en virksomhed var ca. fem måneder om at besvare en anmodning om indsigt, og at den registrerede først fik svar på anmodningen efter, at den registrerede klagede til Datatilsynet.

Der gælder dog visse undtagelser til reglen, men Datatilsynet har i en afgørelse udtalt, at der altid skal foretages en konkret vurdering af, om indsigt kan afslås efter undtagelsesreglerne.[49] Den konkrete vurdering skal indeholde en afvejning af, om den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv, jf. databeskyttelseslovens § 22. Der gælder ikke regler i forhold til at begrænse eller afslå anmodningen, hvis behandlingen nødvendiggør et uforholdsmæssigt ressourceforbrug eller lignende. Det vil sige, at selvom det fx vil tage lang tid og være forbundet med store omkostninger, kan dette ikke i sig selv begrænse den registreredes ret til indsigt efter databeskyttelsesreglerne.

Datatilsynet har i tilsynsager anbefalet, at der udarbejdes retningslinjer, procedurer m.v. for efterlevelsen af retten til indsigt samt skabeloner til besvarelse af indsigtsanmodninger.[50]

7.2.2 Ret til berigtigelse af urigtige oplysninger

Den registrerede har ret til, uden unødig forsinkelse, at få berigtiget urigtige personoplysninger og få fuldstændiggjort ufuldstændige oplysninger.

Det bemærkes, at den dataansvarlige selv har en forpligtelse til at registrere korrekte og ajourførte data og foretage ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, som de behandles til, straks slettes eller berigtiges, jf. databeskyttelsesforordningens artikel 5, litra d.

7.2.3 Ret til sletning af oplysningerne under nærmere omstændigheder

Den registrerede har ret til at anmode om at få slettet personoplysninger af den dataansvarlige, hvis:

1) Behandling ikke længere er nødvendig til at opfylde de formål, oplysningen blev indsamlet eller behandlet til,
2) Den registrerede trækker eventuelt samtykke tilbage, og behandlingen ikke kan ske med anden hjemmel,
3) Den registrerede har en berettiget indsigelse, jf. artikel 21,
4) Behandlingen er ulovlig,
5) Sletning er nødvendig for at opfylde lovkrav, eller
6) Oplysningen er blevet indsamlet i forbindelse med udbud af informationssamfundstjenester som omhandlet i artikel 8, stk. 1.

---

[49] Datatilsynets afgørelse af 18. november 2019, Journalnummer: 2019-31-1424. Afgørelsen kan tilgås på Datatilsynets hjemmeside: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2019/nov/indsigt-i-laegekonsulentvurderinger

[50] Datatilsynets afgørelser af 26. februar 2020, Journalnummer: 2019-421-0027 og: 2019-423-0202. Afgørelserne kan tilgås på Datatilsynets hjemmeside: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/nye-afgoerelser-tilsyn-med-retten-til-indsigt/

Der gælder en række undtagelser til den registreredes ret til sletning, som gælder i det omfang behandlingen er nødvendig:

1) for at udøve retten til ytrings- eller informationsfrihed.
2) for under visse omstændigheder at overholde en retlig forpligtelse, udføre en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.
3) af hensyn til samfundsinteresser på folkesundhedsområdet.
4) til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål under visse omstændigheder, eller
5) for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

Undtagelserne følger af databeskyttelsesforordningens artikel 17, stk. 3. Datatilsynet beskriver også undtagelserne i deres vejledning om de registreredes rettigheder.[51]

7.2.4 Ret til begrænsning af behandlingen under nærmere omstændigheder

Databeskyttelsesforordningen giver den registrerede ret til at opnå begrænsning af behandlingen i følgende situationer:

1) Den registrerede bestrider rigtigheden af personoplysninger (begrænsningen gælder indtil indsigelsen er undersøgt).
2) Behandlingen er ulovlig, men den registrerede ønsker ikke sletning, kun begrænsning af behandlingen af oplysningerne.
3) Den dataansvarlige har ikke længere brug for personoplysningerne, men disse er nødvendige for, at et retskrav kan fastlægges, gøres gældende eller forsvares.
4) Den registrerede har gjort indsigelse mod behandlingen i henhold til artikel 21, stk. 1 (midlertidig begrænsning, mens indsigelsen behandles).

Uanset om behandlingen er blevet begrænset, for så vidt angår visse oplysninger, er der dog visse muligheder for at behandle disse oplysninger alligevel, fx hvis et retskrav skal fastlægges, jf. nedenfor.

[51] Datatilsynets vejledning om de registreredes rettigheder kan tilgås her: https://www.datatilsynet.dk/Media/C/0/Registreredes%20rettigheder.pdf

7.2.5 Ret til at gøre indsigelse

Den registrerede har overordnet ret – af grunde, der vedrører den pågældendes særlige situation – til at gøre indsigelse over for den dataansvarliges behandling af personoplysninger, hvis:

1) Behandlingen baseres på artikel 6, stk. 1, litra e) eller f), om hhv. behandling, som er nødvendig for at udføre en opgave i samfundets interesse, og behandling på baggrund af interesseafvejningsreglen (legitim interesse), herunder hvis der sker profilering.

   Den dataansvarlige må i tilfælde af en indsigelse ikke længere behandle personoplysningerne, medmindre den dataansvarlige påviser vægtige legitime grunde til behandlingen, som går forud for registreredes interesser, rettigheder og frihedsrettigheder, eller behandlingen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares.

2) Behandlingen indebærer direkte markedsføring[52], herunder profilering til brug for markedsføring. Den dataansvarlige må efter indsigelse mod behandling af personoplysninger til direkte markedsføring ikke længere behandle oplysningerne til dette formål.

7.2.6 Ret til at modtage oplysningerne i et struktureret, almindeligt anvendt og maskinlæsbart format (dataportabilitet)

Dataportabilitet betyder

1) At den registrerede har ret til at modtage persondata om sig selv, som vedkommende selv har givet til den dataansvarlige, hvis behandlingen er sket automatisk, og har baseret sig på samtykke eller på kontrakt*, i et struktureret, almindelig anvendt og maskinlæsbart format*, og

2) Den registrerede har ret til at overføre disse oplysninger til en anden dataansvarlig. Personoplysningerne skal kunne flyttes, kopieres og overføres fra ét IT-miljø til et andet uden hindring, hvis det er teknisk muligt.

Den registrerede anses for at have givet oplysningerne selv, både når oplysningerne er givet direkte til den dataansvarlige, og når de er genereret ved brug af elektroniske anordninger, som selskabet er dataansvarlig for. Dette indebærer formentligt, at den registrerede har ret til oplysninger, som er indsamlet via fjernaflæste målere. Dog kan en del af oplysningerne, som er indsamlet til brug for formålet som forsyningssikkerhed mv., og som kan anses som nødvendigt for at udgøre en opgave i samfundets interesse formentlig undtages, jf. artikel 20, stk. 3.

52 Vand- og spildevandsforsyningerne må ikke bruge takstmidler til at lave markedsføring i sædvanlig forstand. Der kan måske være behov for overvejelser i datterselskaber, hvor der udøves tilknyttet aktivitet, såfremt der laves direkte markedsføring.

7.3 Besvarelse af henvendelse fra de registrerede

Hvis der er rimelig tvivl om identiteten af den fysiske person, der fremsætter en anmodning om udøvelse af sine rettigheder som registreret, skal den dataansvarlige efter databeskyttelsesforordningens artikel 12, stk. 6, anmode om yderligere oplysninger, der er nødvendige for at bekræfte den registreredes identitet.

Ved modtagelse af en henvendelse skal forsyningsselskabet således sikre sig, at vedkommende er den person, som han/hun giver sig ud for at være. Det kan f.eks. ske ved at anmode om legitimation i form af pas, kørekort eller anden ID, hvis det vurderes nødvendigt.

I sag 2019-441-3399 udtalte Datatilsynet alvorlig kritik af, at BroBizz A/S ad flere omgange havde videregivet personoplysninger (herunder oplysninger om lokation) til uvedkommende. I sagen udleverede virksomheden bl.a. oplysninger om lokationsdata (fra BroBizz-senderen) til en ekskæreste, som over for virksomheden havde oplyst telefonnummer på den registrerede og herefter fik udleveret oplysningerne. Datatilsynet fandt, at det var i strid med databeskyttelsesreglerne om, at den dataansvarlige skal anmode om yderligere oplysninger, der er nødvendige for at bekræfte den registreredes identitet, hvis der hersker tvivl om identiteten af den fysiske person, der fremsætter en anmodning. Vurderingen af, om det giver anledning til yderligere undersøgelser for at fastslå identiteten, skal forsyningsselskabet foretage konkret i hver enkelt situation. Datatilsynet har i en afgørelse udtalt, at en generel procedure, hvorefter der uden undtagelse stilles krav om ID-validering i forbindelse med behandling af anmodninger om udøvelse af registreredes rettigheder, ikke er i overensstemmelse med databeskyttelsesforordningens artikel 12, stk. 6, og artikel 5, stk. 1, litra c.[53]

Den dataansvarlige skal besvare en anmodning om udøvelse af rettigheder uden unødig forsinkelse og senest 1 måned efter modtagelsen af anmodningen. Denne periode kan forlænges med to måneder, hvis det er nødvendigt, under hensyntagen til anmodningernes kompleksitet og antal. Den dataansvarlige skal i så fald underrette den registrerede om en sådan forlængelse senest en måned efter modtagelsen af anmodningen sammen med begrundelsen for forsinkelsen.

Det er DANVAs forventning, at med det stadigt stigende fokus på behandling af personoplysninger, vil omfanget af kundehenvendelser med anmodning om indsigt stige.

Det er derfor vigtigt, at forsyningsselskabet har en i forvejen fastlagt ”køreplan” for, hvordan en sådan henvendelse behandles, og at ansatte i virksomheden er informeret om, at kunderne har disse rettigheder.

DANVA har udarbejdet en skabelon for, hvordan en sådan procedure kan se ud, kaldet "registreredes rettigheder", og den fremgår af DANVAs persondatasite "Vejledninger og skabeloner fra DANVA"

[53] Datatilsynets afgørelse af 25. oktober 2019, Journalnummer: 2018-7320-0166. Afgørelsen kan tilgås via Datatilsynets hjemmeside: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2019/okt/id-validering-ifm-anmodninger-om-udoevelse-af-registreredes-rettigheder

8 Databehandlere

Det er vigtigt at være opmærksom på, om der benyttes en databehandler, som behandler personoplysninger. Hvis det er tilfældet, stiller databeskyttelsesreglerne bl.a. krav til, at der skal indgås en databehandleraftale, og der skal føres tilsyn med databehandleren. Datatilsynet har udarbejdet en vejledning om dataansvarlige og databehandlere, som også beskriver reglerne generelt.[54]

Et forsyningsselskab eller et serviceselskab kan vælge at lade en ekstern aktør, fx et IT-firma, til lønsystem, afregning eller lignende. Kendetegnende for cloud-løsninger er, at det er standardiserede it-ressourcer, der tilgås via internettet. Cloudservices kan for eksempel være lønsystemer, der danner lønsedler eller et økonomisystem, der bruges til at sende og opkræve fakturaer. Datatilsynet har udarbejdet en vejledning om cloud, som beskriver reglerne for brug af cloud.[55]

I en sådan situation behandler den eksterne aktør personoplysningerne på vegne af forsyningsselskabet og bliver således databehandler[56].

Hvis en dataansvarlig anvender en databehandler, skal der indgås en databehandleraftale mellem disse to parter. Databehandleraftalen skal opfylde alle kravene i databeskyttelsesforordningens artikel 28, stk. 3. Der skal således bl.a. stilles krav om, at databehandleren træffer de passende tekniske og organisatoriske foranstaltninger efter databeskyttelsesforordningens artikel 32 for at sikre et sikkerhedsniveau, der passer til risicierne. Disse nye skærpede krav til databehandleraftaler gælder både for aftaler indgået før og efter 25. maj 2018, hvor den nye databeskyttelseslovgivning fik virkning fra.

Datatilsynet har udarbejdet en skabelon til en standarddatabehandleraftale, som overholder kravene i databeskyttelsesforordningens artikel 28. Skabelonen har karakter af standardkontraktsbestemmelser, hvilket indebærer, at Datatilsynet ikke vil efterprøve det allerede fastlagte indhold nærmere fx i forbindelse med et tilsynsbesøg. Forsyningsselskaberne kan dermed med fordel benytte eller søge inspiration i den seneste version af standarddatabehandleraftalen, når nye databehandleraftaler skal indgås eller fornys.[57]

Den dataansvarlige skal aktivt kontrollere databehandleren, herunder sikre, at de krævede sikkerhedsforanstaltninger overholdes hos databehandleren. Datatilsynet har udarbejdet en vejledning om tilsyn med databehandlere.[58] I vejledningen beskrives en vejledende model bestående af en pointskala, som skal ses som et

---

[54] Datatilsynets vejledning om dataansvarlige og databehandlere kan tilgås her på Datatilsynets hjemmeside: https://www.datatilsynet.dk/Media/7/6/Dataansvarlige%20og%20databehandlere.pdf

[55] Vejledningen kan tilgås på Datatilsynets hjemmeside: https://www.datatilsynet.dk/Media/637824109172292652/Vejledning%20om%20cloud.pdf

[56] Ofte vil en databehandler have en standarddatabehandleraftale, der kan anvendes som udkast. Det er dog fortsat forsyningsselskabets ansvar, at der indgås en sådan aftale, og at kravene i denne i øvrigt overholdes. Datatilsynet har også udviklet en skabelon for en databehandleraftaler, som kan findes på Datatilsynets hjemmeside.

[57] I skrivende stund kan den seneste version af teksten findes på Datatilsynets hjemmeside under vejledninger: https://www.datatilsynet.dk/Media/637696299321948979/Datatilsynet_skabelon-til-databehandleraftale-dansk.docx

[58] Vejledningen kan tilgås på Datatilsynets hjemmeside: https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet_Vejledning%20om%20tilsyn%20med%20databehandlere_oktober-2021.pdf

udtryk for, hvor risikofyldt behandlingen af personoplysninger er. I tilknytning hertil foreslår Datatilsynet seks tilsynskoncepter, som gradvist stiller større og større krav til gennemførelsen af tilsynet med databehandleren i takt med, at risikoen stiger. Det vil sige, at jo mere der kan gå galt ved behandlingen hos databehandleren, jo større krav stilles der til den dataansvarliges tilsyn med databehandleren.

For eksempel indebærer det første tilsynskoncept , at der ikke skal gøres noget, medmindre den dataansvarlige bliver opmærksom på, at der er noget galt hos databehandleren. Hvis dataansvarlig stiller større krav til tilsynet med databehandleren, er et andet tilsynskoncept, at der indhentes en årlig revisionserklæring fra en uafhængig tredjepart; til det formål har FSR – forenede revisorer efter samarbejde med Datatilsynet udarbejdet en revisionserklæring, ISAE 3000, til at hjælpe de dataansvarlige i forhold til at føre det fornødne tilsyn med deres databehandlere.[59] Det mest omfattende tilsynskoncept – det vil sige det sjette tilsynskoncept efter Datatilsynets vejledning om tilsyn med databehandlere – er, at den dataansvarlige selv foretager et komplet tilsyn hos databehandleren. Der kan læses om alle tilsynskoncepterne i Datatilsynets vejledning.

Når der i en forsyningskoncern behandles personoplysninger om kunder i de enkelte forsyningsselskaber i serviceselskabet, skal der indgås en databehandleraftale mellem service- og forsyningsselskabet. Dette gælder f.eks. også eksterne serviceselskaber, uanset om forsyningsselskabet er medejer af det eksterne serviceselskab eller ej.

Det bemærkes, at Datatilsynet har stort fokus på, at virksomheder, der behandler personoplysninger, får indgået korrekte databehandleraftaler, såfremt den dataansvarlige benytter sig af eksterne samarbejdspartnere, der herved kommer til at behandle personoplysninger på vegne af den dataansvarlige virksomhed, og at der føres tilstrækkeligt tilsyn med databehandleren. Datatilsynet indledte bl.a. i efteråret 2021 tilsyn med seks statslige myndigheders tilsyn med deres databehandlere.[60]

DANVA har udarbejdet en tjekliste til indgåelse af databehandleraftalen. Den fremgår af DANVAs persondatasite "Vejledninger og skabeloner fra DANVA".

Herudover skal det fremhæves, at der ikke er behov for, at der indgås en databehandleraftale, når der overføres personoplysninger fra vandforsyning til spildevandsselskaber, idet denne overførsel sker i henhold til lovgivningen, jf. https://www.danva.dk/viden/spoergsmaal-svar/persondataforordningen/overdragelse-af-maaler-data-samtykke-og-databehandleraftaler/. Linket forudsætter login på DANVAs hjemmeside.

[59] Datatilsynets pressemeddelelse om erklæringen kan tilgås her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/feb/ny-erklaering-skal-hjaelpe-med-kontrol-af-databehandlere/

[60] Læs om sagerne i Datatilsynets nyhed fra den 17. januar 2023: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jan/tilsyn-med-statslige-myndigheders-tilsyn-med-databehandlere

9 Tekniske og organisatoriske sikkerhedsforanstaltninger

Det følger af databeskyttelsesforordningens artikel 32, at dataansvarlige og databehandlere skal træffe de passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til risici, under hensyntagen til:

- det aktuelle tekniske niveau.
- implementeringsomkostningerne.
- behandlingens karakter, omfang, sammenhæng og formål.
- samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Det er væsentligt at holde sig for øje, at kravet om passende tekniske og organisatoriske sikkerhedsforanstaltninger både relaterer sig til beskyttelse af oplysninger indeholdt i et manuelt register (f.eks. et kartotek) såvel som ved elektronisk behandling. Det indebærer også, at der foretages tilstrækkelig beskyttelse mod fysiske farer så som brand, oversvømmelse eller uvedkommendes adgang.

Kravene til sikkerhed indebærer også, at det ved kassering af fysiske medier så som dvd'er, videobånd, mobiltelefoner, bærbare computer skal sikres, at alle kopier af oplysningerne på mediet er destrueret sikkert og permanent, så uvedkommende ikke kan få adgang til oplysningerne, jf. afsnit 5.1 om krav til sletning.

Det fremgår ikke specifikt af databeskyttelsesforordningen, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger den dataansvarlige bør træffe, men der er dog i artikel 32, stk. 1, litra a-d, nævnt nogle eksempler på sikkerhedsforanstaltninger. Der henvises til Datatilsynets vejledning om behandlingssikkerhed.[61] Vejledningen redegør nærmere for, hvilke overvejelser i forhold til beskyttelsesbehov og risikovurdering, som den dataansvarlige skal igennem for at opfylde kravet om beskyttelse af personoplysningerne, og indeholder også en praktisk hjælpeguide til overholdelse af kravene.

I en sag fra 29. september 2021 har Datatilsynet oplyst[62], at de har anmeldt Kræftens Bekæmpelse til politiet og indstillet til en bøde på 800.000 kr. efter gentagne problemer med utilstrækkelig beskyttelse af bl.a. kræftsyge borgeres helbredsoplysninger. Kræftens Bekæmpelse havde selv – efter at være blevet udsat for hackerangreb – vurderet, at de burde øge beskyttelsen gennem multifaktor-autentifikation (dvs. at man bruger to

[61] https://www.datatilsynet.dk/Media/637689328983143992/Behandlingssikkerhed%20og%20databeskyttelse%20gennem%20design%20og%20standardindstillinger_2018.pdf

[62] Datatilsynet har skrevet om anmeldelsen til politiet og indstillingen til bøde på deres hjemmeside: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/kraeftens-bekaempelse-indstillet-til-boede

eller flere faktorer til at logge på systemet o.l.), men dette blev ikke implementeret. Efterfølgende blev de udsat for brud endnu engang, og mindst 1.448 personers oplysninger blev kompromitteret.

Risikoanalyser
For at kunne træffe de passende tekniske og organisatoriske sikkerhedsforanstaltninger er det nødvendigt, at der udarbejdes risikoanalyser forud for, at sikkerhedsforanstaltningerne fastlægges.

Datatilsynet og Rådet for Digital Sikkerhed har udarbejdet en vejledende tekst om risikovurdering[63], som er en praktisk orienteret hjælpetekst i forhold til udarbejdelsen af risikoanalyser.

Det følger bl.a. af den vejledende tekst, at en risikovurdering typisk vil indeholde en konsekvensvurdering, en trusselsvurdering, en sårbarhedsvurdering samt en vurdering af risikobilledet på baggrund af de forudgående vurderinger.

Den vejledende tekst henviser desuden til en skabelon, som skal benyttes til at lave risikovurderinger. Skabelonen er udarbejdet af Erhvervsstyrelsen og Rådet for Digital Sikkerhed.[64]

Det bemærkes, at kravene til sikkerhed generelt vil være strengere ved behandling af følsomme og fortrolige oplysninger, herunder cpr-nummer, idet risiciene ved behandlingen af sådanne oplysninger vil være større.

Datatilsynet har udarbejdet en vejledning om behandlingssikkerhed og databeskyttelse gennem design og indstillinger, som der henvises til.

Sikkerhedsforanstaltninger
Der kan søges inspiration i den i medfør af den forhenværende persondatalov udstedte bekendtgørelse og en tilhørende vejledning om sikkerhedsforanstaltninger til beskyttelse af personoplysninger[65]. Således anfører Datatilsynet i sin vejledning, at hvis en eller flere af de foranstaltninger, der var en del af sikkerhedsbekendtgørelsen – efter en konkret vurdering – fortsat er relevante, vil det være oplagt at fortsætte med at gøre brug af dem. Og det nævnes, at det f.eks. kunne være kravene om autorisation, kontrol med afviste adgangsforsøg eller logning.

Sikkerhedstjekket.dk
Herudover har Rådet for Digital Sikkerhed i samarbejde med Erhvervsstyrelsen udarbejdet et værktøj (www.sikkerhedstjekket.dk), der kan hjælpe virksomheder med at få et overblik over IT-sikkerheden i virksomheden. Ved svar på en række spørgsmål kan virksomheden få et fingerpeg om, hvor fokus bør være i virksomhedens fremadrettede sikkerhedsindsats.

---

[63] Den vejledende tekst kan tilgås på Datatilsynets hjemmeside: https://www.datatilsynet.dk/Media/4/8/Risikovurdering.pdf

[64] Skabelonen kan tilgås her: https://sikkerdigital.dk/virksomhed/test-og-vaerktoejer/

[65] Se https://www.retsinformation.dk/Forms/R0710.aspx?id=1002 og Håndbog om IT-sikkerhed i forsyningsbranchen, DANVA vejledning nr. 94

Strategi for cyber- og informationssikkerhed i vandsektoren
Regeringen lancerede i december 2021 en ny national strategi for cyber- og informationssikkerhed. Strategien afløser den tidligere strategi fra 2018. Den nye strategi hæver ambitionsniveauet for cybersikkerheden med 34 hovedinitiativer, der i endnu højere grad sætter fokus på beskyttelsen af Danmarks digitale infrastruktur og it-systemer. En række sektorer – herunder vandsektoren – har skullet lave delstrategier, som et led i den nationale strategi. Miljøstyrelsen har derfor, i samarbejde med vandsektoren, udarbejdet Strategi for cyber- og informationssikkerhed i vandsektoren 2023-2025. Delstrategien fremgår af dette link Strategi for cyber- og informationssikkerhed i vandsektoren 2023-2025. .

Center for cybersikkerhed (CFCS)
Center for cybersikkerhed (CFCS), er den nationale IT-sikkerhedsmyndighed og CFCS har en række anbefalinger, vejledninger og materiale som selskaberne bør holde sig orienteret om og bruge, hvilket fremgår af dette link www.CFCS.dk.

SektorCERT
For at styrke vandselskabernes IT- og cybersikkerhed samt databeskyttelse, er DANVA i 2023 blevet partner i SektorCERT.

SektorCERT har blandt andet et sensornetværk, med netværksmonitering installeret hos forsyningsselskaber, bredt i den kritiske danske infrastruktur. SektorCERT analyserer indsamlede data med henblik på at kunne informere og alarmere det enkelte SektorCERT-medlem ved relevante sikkerhedshændelser.

SektorCERT har ligeledes uddannelser og faciliterer videndeling om IT- og cybersikkerhed samt databeskyttelse. SektorCERTs ydelser, rapporter og anbefalinger fremgår af dette link www.SektorCERT.dk.

DANVAs håndbog om IT-sikkerhed
DANVA har endvidere udgivet "Håndbog om IT-sikkerhed i forsyningsbranchen, DANVA vejledning nr. 94", der beskriver IT-sikkerhed, generelle sikkerhedsforhold samt fysisk sikkerhed omkring overvågning og adgangskontrol.

Digitaliseringsstyrelsens guide til implementering af ISO 27001
Endeligt henvises til Digitaliseringsstyrelsens guide til implementering af ISO 27001.

Databeskyttelsesforordningen har indført en række nye bestemmelser om behandlingssikkerhed, herunder bl.a. om brug af pseudonymisering og dataminimering som led i privacy by design og default, tilslutning til adfærdskodekser eller certificeringsmekanismer, anmeldelse til Datatilsynet af brud på sikkerheden, konsekvensanalyser og databeskyttelsesrådgiver (DPO). Visse af disse bestemmelser vil blive omtalt nedenfor.

9.1 Udarbejdelse af IT-politik

Databeskyttelsesforordningen stiller ikke eksplicit krav om, at en virksomhed, der behandler personoplysninger, har udarbejdet en IT-politik. På baggrund af dokumentationskravene, kravet om at træffe passende organisatoriske sikkerhedsforanstaltninger samt databeskyttelsesforordningens krav om instruks til medarbejdere

om behandling af personoplysninger, anbefaler DANVA, at forsyningsselskabet udarbejder en intern IT-politik (fx som en del af en personalehåndbog), der sikrer, at medarbejdernes brug af IT ikke bliver en risikofaktor i forhold til, at de personoplysninger, som virksomheden ligger inde med, falder i de forkerte hænder.

DI har udarbejdet syv gode råd om IT-sikkerhed samt en skabelon for en IT-politik, som kan tjene til inspiration, ligesom der formentlig vil kunne søges inspiration i den vejledning om behandlingssikkerhed, som Datatilsynet og Justitsministeriet har varslet vil blive udsendt.

9.2 Krav om kryptering ved overførsel af cpr-nr., følsomme og fortrolige oplysninger

Datatilsynets stiller krav om kryptering ved transmission af fortrolige og følsomme personoplysninger med e-mail via internettet, da det anses som en passende sikkerhedsforanstaltning til at beskytte indholdet af e-mails mod uvedkommende.

Datatilsynet har desuden i sin vejledning om behandlingssikkerhed m.v. anført følgende:

"Det vil fortsat være sådan, at du ikke må sende følsomme (og fortrolige) personoplysninger ukrypteret over netværk, som den dataansvarlige ikke har fuld kontrol over, f.eks. ukrypterede e-mail på internettet. I disse situationer skal du således anvende en sikker løsning, herunder f.eks. Digital Post eller bruge en forbindelse, der krypterer det overførte indhold under hele transporten."

Der er således et krav om kryptering af e-mails, som sendes eksternt, hvis de indeholder følsomme eller fortrolige oplysninger, herunder f.eks. CPR-nr., oplysninger om manglende betaling og oplysninger om beskyttet adresse. Se vejledningens afsnit 6.1 om fortrolige oplysninger.

Der er mulighed for at implementere forskellige grader af kryptering. Datatilsynet har på sin hjemmeside oplistet forskellige former for kryptering i form af overkategorierne "kryptering på transportlaget" og "end-to-end kryptering".[66] End-to-end kryptering er som udgangspunkt en "stærkere" kryptering end kryptering på transportlaget.

Efter Datatilsynets opfattelse skal kryptering på transportlaget betragtes som et minimumsniveau for sikkerheden, når der fremsendes fortrolige eller følsomme personoplysninger via e-mail over åbne netværk. Kryptering på transportlageret kan foretages ved såkaldt TLS kryptering (Transport Layer Security kryptering), som sikrer kryptering af selve overførslen af mailen. End-to-end kryptering er en mere omfattende løsning, som krypterer selve indholdet af mailen. End-to-end kryptering vil være passende, hvis der er en høj risiko for de registrerede f.eks., hvis der er helbredsoplysninger om et stort antal personer.

[66] Datatilsynets tekst om transmission af personoplysninger via e-mail, som kan tilgås her: https://www.datatilsynet.dk/emner/persondatasikkerhed/transmission-af-personoplysninger-via-e-mail/

Datatilsynet har bl.a. udtalt sig om TLS kryptering i to forskellige sager.

I sag 2019-31-1263 havde en virksomhed sendt fortrolige oplysninger (skyldige restancer) ved at anvende en opportunistisk TLS 1.2-kryptering ved fremsendelsen. Det vil sige, at mails kun bliver krypteret under transporten til modtageren, hvis dette understøttes, men ukrypteret såfremt det ikke understøttes. I den konkrete sag fandt tilsynet, at der ikke var grund til at udtale kritik, men bemærkede generelt, at når der behandles e-mail med følsomme og/eller fortrolige oplysninger, opfordres den dataansvarlige til at sætte sin mailserver op til, at der gennemtvinges TLS (Forced TLS), som minimum i version 1.2.

I sag 2021-442-11601 udtalte Datatilsynet alvorlig kritik af, at Silkeborg Kommune sendte en e-mail, som indeholdt en liste med bl.a. cpr-nummer for 12.915 skoleelever. Afsendelsen skete muligvis med kryptering på transportlageret med TLS 1.1. Datatilsynet udtalte, at TLS 1.1 ikke kunne anses som passende sikkerhed til kryptering på transportlageret i den konkrete situation. Tilsynet udtalte, at der vil være typer af behandlinger, hvor kryptering af payload, såkaldt end-to-end kryptering vil være passende, såfremt der konkret er en højere risiko ved behandlingen, fx ved afsendelse af personoplysninger af fortrolig og/eller følsom karakter om et stort antal registrerede. Beslutningen om krypteringsform skal foretages af forsyningsselskaberne på baggrund af en risikovurdering. Det følger desuden af principperne i artikel 5 i databeskyttelsesforordningen, at det altid skal vurderes, om der virkelig er et behov for at sende følsomme eller fortrolige oplysninger i e-mails.

DANVA anbefaler, at forbrugsdata og fakturaer, der typisk sendes kvartalsvis, anses for at være fortrolige data i persondatasammenhæng, da de af kunden generelt opleves som værende af privat karakter, og at forsyningsselskabet dermed krypterer sådanne data, hvis de sendes via e-mail til kunden.[67] Se også afsnit 6.1.4 om målerdata.

Datatilsynet har endvidere udtalt vedrørende SMS-beskeder, at transmission via SMS af følsomme og fortrolige oplysninger indebærer en betydelig risiko for de registreredes rettigheder og frihedsrettigheder. Sådanne oplysninger bør derfor ikke sendes som SMS, da risikoen for fortroligheden under transport kun i meget begrænset omfang kan formindskes ved tiltag iværksat af den dataansvarlige selv.[68]

9.3 Indbygget databeskyttelse - privacy by design og default

Databeskyttelsesforordningens artikel 25 stiller krav om, at den dataansvarlige skal beskytte personoplysningerne gennem design og standardindstillinger (på engelsk privacy by design og privacy by default).

[67] Danvas udtalelse af 29. november 2018, som kan tilgås her: https://www.danva.dk/media/5056/20181204-final-danva-notat-kryptering-af-mail-med-forbrugsdata.pdf

[68] Datatilsynets udtalelse om transmission af personoplysninger via SMS, som kan tilgås her: https://www.datatilsynet.dk/emner/persondatasikkerhed/transmission-af-personoplysninger-via-sms/

Privacy by design indebærer, at der ved udvikling, tilrettelæggelse og brugen af midlerne til at behandle personoplysningerne skal tages højde for databeskyttelse, effektiv implementering af principperne i databeskyttelsesforordningens artikel 5 (herunder formålsbegrænsning og dataminimering), håndtering af de registreredes rettigheder og andre bestemmelser i databeskyttelsesforordningen, således at løsningen ved hjælp af passende tekniske og organisatoriske foranstaltninger bliver designet til at efterleve databeskyttelsesreglerne, og disse principper bliver integreret i behandlingen.

Den dataansvarlige har således en overvejelses- og håndteringspligt til at tænke databeskyttelse ind i designet af løsningen. Et eksempel kan være, at et IT-program er teknisk indrettet til at kunne pseudonymisere og har tilstrækkelige sikkerhedsforanstaltninger indbygget.

Privacy by default indebærer, at der ved den dataansvarliges tekniske og organisatoriske foranstaltninger, såsom IT-systemer og arbejdsgange, skal sikres den størst mulige databeskyttelse gennem standardindstillingerne. Det medfører f.eks., at mængden af oplysninger, som et system indsamler som standard, skal begrænses mest muligt, samt at konfigurérbare muligheder skal indstilles til det minimalt nødvendige for behandlingen af personoplysninger.

Hensynet bag de ovennævnte principper er, at den dataansvarlige så effektivt som muligt skal håndtere databeskyttelsesreglerne og således indtænke kravene allerede i udviklings- og indkøbsfasen af f.eks. IT-systemer, samt i disse systemers standardindstillinger og ved den organisatoriske forretningsunderstøttelse af behandlinger.

Datatilsynet anbefaler, at den dataansvarlige fører en logbog, der indeholder beskrivelserne og konklusionerne over de overvejelser, der er foretaget, med henblik på at kunne påvise overholdelsen af databeskyttelsesforordningens artikel 25.

Der henvises til Datatilsynets vejledning om databeskyttelse gennem design og standardindstillinger,[69] som også indeholder praktiske eksempler på tekniske og organisatoriske foranstaltninger, der kan tænkes ind i f.eks. et IT-system.

9.4 Konsekvensanalyse

Der er pligt til at gennemføre **forudgående konsekvensanalyse** (data protection impact assessment, som forkortes DPIA), når en type behandling "*navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, **sandsynligvis** vil indebære en **høj risiko** for fysiske personers rettigheder og frihedsrettigheder*", jf. databeskyttelsesforordningens artikel 35.

[69] https://www.datatilsynet.dk/Media/637689328983143992/Behandlingssikkerhed%20og%20databeskyttelse%20gennem%20design%20og%20standardindstillinger_2018.pdf

Datatilsynet har udarbejdet en liste over otte forskellige behandlingsaktiviteter, hvor det er obligatorisk at udarbejde konsekvensanalyser.[70] Det drejer sig bl.a. om følgende behandlingsaktiviteter:

- Behandling af lokationsdata i sammenhæng med mindst et yderligere kriterie fra Artikel 29-gruppens retningslinjer.
- Behandling ved brug af nye teknologier i sammenhæng med mindst et yderligere kriterie fra Artikel 29-gruppens retningslinjer.
- Behandling af personoplysninger om sårbare personer eller hvor der er tale om behandling af følsomme oplysninger (særlige kategorier), og hvor der benyttes profilering eller andre former for automatiserede afgørelser.

Datatilsynets liste henviser til kriterierne fra Artikel 29-gruppens retningslinjer (nu Det Europæiske Databeskyttelsesråd).[71] Retningslinjerne fastsætter ni kriterier, der kan hjælpe til at identificere de behandlinger, der vil kræve en konsekvensanalyse. Kriterierne omfatter bl.a. systematisk overvågning, følsomme oplysninger eller oplysninger af meget personlig karakter og oplysninger genstand for omfattende behandling.

Uafhængigt af, om behandlingsaktiviteten er på Datatilsynet liste, skal der foretages en konsekvensanalyse, såfremt det vurderes, at behandlingen vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Konsekvensanalysen skal foretages med henblik på at træffe passende foranstaltninger til at begrænse de påviste risici ved behandlingen og overholde forordningens krav. Er det ikke muligt at begrænse de påviste risici ved passende foranstaltninger, således at risikoen fortsat er høj, skal selskabet høre Datatilsynet forud for igangsættelse af den påtænkte behandling.

9.5 Databeskyttelsesrådgiver - DPO

Databeskyttelsesforordningen stiller krav om, at dataansvarlige i visse situationer skal udpege en databeskyttelsesrådgiver, DPO.

Kravet gælder for alle offentlige myndigheder og offentlige organer, samt for visse øvrige organisationer, som nærmere har angivet behandling af personoplysninger som kerneaktivitet.

Justitsministeriet[72] har imidlertid udtalt, at forsyningsselskaber ikke normalt kan anses for at behandle personoplysninger som kerneaktivitet, hvorfor forsyningsvirksomheder – som alene udfører forsyningsopgaver – normalt ikke vil skulle udpege en databeskyttelsesrådgiver.

---

[70] Listen kan tilgås her: https://www.datatilsynet.dk/Media/4/1/Datatilsynets%20liste%20over%20behandlinger%20der%20altid%20er%20underlagt%20kravet%20om%20en%20konsekvensanalyse%20(2).pdf

[71] WP248 vedtaget den 4. april 2017 med titlen: "Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679", som kan tilgås her: https://www.datatilsynet.dk/media/7826/konsekvensanalyser-vedroerende-databeskyttelse-dpia-wp248.pdf

[72] Betænkning 1565.

9.6 NIS2-direktivet

EU's direktiv, 2022/2555 (NIS2-direktivet) blev vedtaget den 14. december 2022 og skal være implementeret i dansk ret senest den 17. oktober 2024.

NIS2-direktivet indeholder dels krav rettet mod medlemsstaterne, dels krav rettet mod virksomheder og offentlige institutioner (bl.a. sikkerhedsledelses-, rapporterings- og ansvarsforpligtelser). Direktivets formål er at styrke og ensarte cybersikkerheden og modstandsdygtigheden overfor cybertrusler på tværs af EU. Særligt for virksomheder indenfor sektorer samt offentlige institutioner, der anses for at være kritiske for samfundet, herunder særligt infrastrukturer.

NIS2-direktivet et minimumsdirektiv. Selvom direktivet er vedtaget i EU, udestår udarbejdelse og vedtagelse af den danske lovgivning, der skal implementere direktivet i dansk ret. Der er derfor på nuværende tidspunkt (juli 2023) visse usikkerheder om de endelige danske regler. Særligt, da den konkrete implementeringsmodel ikke kendes endnu, og da direktivet er et minimumsdirektiv, som giver de enkelte medlemslande mulighed for at implementere skærpede krav i forhold til direktivet.

Det er angivet i NIS2-direktivet, at både drikke- og spildevandssektoren udgør særlig kritiske sektorer.[73] Virksomheder skal for at være omfattet af reglerne – som udgangspunkt – udgøre en "mellemstor virksomhed"[74] og virksomheden skal levere tjeneste eller udføre aktiviteter i EU. NIS2 vil dog også finde anvendelse på en række andre virksomheder uanset størrelse, herunder hvor:

- Virksomheden eller den tjeneste, som virksomheden leverer, er væsentlig for opretholdelse af kritiske samfundsmæssige eller økonomiske aktiviteter, offentlig sikkerhed, folkesundhed, udgør en systemisk risiko eller er betydende for sektoren.

- Virksomheden identificeres som en kritisk enhed i EU-direktiv 2022/2557.

Der er for nuværende for mange usikkerheder på området til, at man kan give et entydigt og helt konkret svar på hvilke af DANVA's medlemmer som omfattes af NIS2-direktivet. Det må dog forventes at en stor del af DANVA's medlemmer vil blive omfattet og underlægges de nye krav i NIS2-direktivet.[75]

Der er udover NIS2-direktivet også anden EU-retlig relevant lovgivning på vej ift. IoT-enheder i form af forordning om horisontale cybersikkerhedskrav til digitale produkter (på engelsk Cyber Resilience Act, som forkortes "CRA"[76]). Forordningen angår horisontale sikkerhedskrav til produkter med digitale elementer. Det er en kom-

[73] Leverandører og distributører at drikkevand som defineret i art. 2, nr. 1, litra a i EU direktiv 2020/2184 og virksomheder, der indsamler, bortskaffer eller behandler byspildevand, husspildevand eller industrispildevand som defineret i art. 2, nr 1), 2) og 3) i EU direktiv 91/271 EØF

[74] Tærsklerne for "mellemstore virksomheder" er defineret i art. 2 i bilaget til henstilling 2003/361/EF. Virksomheden skal have en samlet årlig balance på over EUR 10 mio. og have over 50 medarbejdere

[75] En evaluering af dette forventes at kunne udarbejdes ifm. den danske implementering af NIS2-direktivet.

[76] Forslaget kan tilgås på EU-Kommissionens hjemmeside: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

pleks forordning, der har til formål at indføre essentielle sikkerhedskrav (det vil sige produkternes cybersikkerhed) for enheder, som er koblet til internettet, og som sender og modtager data. Forordningen er imidlertid stadig under behandling i EU.

10 Sikkerhedsbrud

10.1 Registrering af brud

Et sikkerhedsbrud er i databeskyttelsesforordningen defineret som "et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet". Det kan f.eks. forekomme, hvis uvedkommende får adgang til oplysningerne eller oplysningerne tilintetgøres ved et uheld eller et hackerangreb. Ved konstateringen af et sikkerhedsbrud skal den dataansvarlige vurdere, hvorvidt der skal ske anmeldelse til Datatilsynet og underretning af registrerede, jf. afsnit 10.2 og 10.3.

Pligten efter databeskyttelsesreglerne omfatter en pligt til at anmelde til Datatilsynet og eventuelt underrette de registrerede. Den dataansvarlige har derfor ikke pligt til selv at foretage en anmeldelse til andre, fx politiet, alene på baggrund af et brud på persondatasikkerheden. Datatilsynet kan - fx på baggrund af et sikkerhedsbrud - foretage politianmeldelse og indstille til bøde, ligesom den registrerede (det vil sige den forurettede) kan foretage anmeldelse.

Selvom den dataansvarlige vurderer, at der ikke skal ske anmeldelse til Datatilsynet, skal sikkerhedsbruddet dokumenteres ved en intern dokumentation med henblik på, at Datatilsynet kan kontrollere oplysningerne ved et tilsyn. Pligten hænger også sammen med databeskyttelsesforordningens princip om ansvarlighed.

Datatilsynet har udtalt, at dokumentationen over alle brud på persondatasikkerheden (uanset om der skal ske anmeldes eller ej) i alle tilfælde skal indeholde information om dato og tidspunkt for bruddet, hvad der skete i forbindelse med bruddet, hvad der var årsagen til bruddet, hvilke (typer) personoplysninger, der var omfattet af bruddet, hvilke konsekvenser bruddet havde for de registrerede samt de trufne afhjælpende foranstaltninger.. Den interne dokumentation skal også indeholde en begrundelse for, hvorfor den dataansvarlige evt. har vurderet, at der ikke skal ske anmeldelse til Datatilsynet og underretning af de registrerede. Ovenstående oplysninger kan med fordel registreres i en log over sikkerhedsbrud.

Datatilsynets statistik for typer af brud på persondatasikkerheden viser, at cirka 79% af alle de anmeldte brud skete på baggrund af utilsigtede hændelser. Det vil sige primært menneskelige fejl, fx afsendelse af e-mail til forkerte modtager, utilsigtet offentliggørelse af personoplysninger, manglende anonymisering eller pseudonomisering og lignende. Statistikken viser også, at kun ca. 3% af alle brud var på baggrund af ondsindet aktivitet/misbrug, det vil sige IT-kriminalitet som fx phishing, svindelforsøg, målrettede angreb, overbelastningsangreb (DDos-agreb) og lignende.[77]

[77] Hele statistikken kan ses på Datatilsynets hjemmeside: https://www.datatilsynet.dk/sikkerhedsbrud/statistik-over-brud-paa-persondatasikkerheden/typer-af-brud

10.2 Anmeldelse til Datatilsynet

Databeskyttelsesforordningen fastsætter regler om anmeldelse af sikkerhedsbrud dels til Datatilsynet, dels underretning af den registrerede.

Det følger af disse regler, at på det tidspunkt, hvor den dataansvarlige bliver bekendt med, at der har været et brud på persondatasikkerheden, skal den dataansvarlige som udgangspunkt uden unødig forsinkelse og om muligt senest 72 timer herefter, anmelde bruddet til Datatilsynet jf. databeskyttelsesforordningens art. 33, stk. 1. Foretages anmeldelse ikke indenfor de 72 timer, skal der angives en begrundelse for forsinkelsen.

I sag 2020-442-6885 udtalte Datatilsynet alvorlig kritik og påbud om underretning af de registrerede, da Justitsministeriet sendte en e-mail med fortrolige oplysninger uden at anvende kryptering og først anmeldte bruddet over tre måneder efter, at Justitsministeriet blev informeret om et muligt brud. Datatilsynet henviste endvidere til muligheden for at foretage en foreløbig anmeldelse, der så kan uddybes, korrigeres eller berigtiges med yderligere oplysninger på et senere tidspunkt.

Såfremt det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for den fysiske persons rettigheder eller frihedsrettigheder, skal der ikke foretages en anmeldelse. Den dataansvarlige er dog forpligtet til at dokumentere, at der har fundet et brud sted, jf. afsnit 10.1. Vurderes det, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, skal der foretages en anmeldelse til Datatilsynet, som opfylder kravene til anmeldelse i databeskyttelsesforordningen art. 33, stk. 3.

Et brud på persondatasikkerheden vil indebære en risiko for fysiske personers rettigheder og frihedsrettigheder, hvis der på baggrund af bruddet f.eks. sker diskrimination, identitetstyveri eller -svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den registrerede.

I den konkrete vurdering af risikoen har Datatilsynet i deres vejledning om håndtering af brud på persondatasikkerheden[78] henvist til, at følgende forhold altid bør indgå:

- Typen af sikkerhedsbrud, herunder om der er sket tab af oplysninger, brud på fortroligheden eller en integritetskrænkelse.
- Oplysningernes art og omfang.
- Risikoen for at registrerede kan identificeres.
- Konsekvenser bruddet kan have for de registrerede.
- Hvorvidt bruddet omfatter særlige registrerede (f.eks. hvis der er tale om børn eller særligt udsatte).
- Antallet af berørte fysiske personer.

[78] Vejledningen kan tilgås på Datatilsynets hjemmeside: https://www.datatilsynet.dk/Media/637886298435856391/H%C3%A5ndtering%20af%20brud%20p%C3%A5%20persondatasikkerheden.pdf

Anmeldelse til Datatilsynet foregår digitalt via Virk.dk. Den dataansvarlige bør på forhånd have fastlagt en procedure, der skal følges ved sikkerhedsbrud, herunder udpege de medarbejdere, der skal anmelde sikkerhedsbruddet og efterprøve, at de kan logge ind på anmeldelsesløsningen med NemID på den dataansvarliges vegne.

DANVA anbefaler, at selskaber, der ikke selv har en databeskyttelsesrådgiver, kontakter en advokat eller IT-sikkerhedsspecialist, så den pågældende kan hjælpe med at analysere omfanget af skaden, inden der foretages anmeldelse til Datatilsynet. Datatilsynet vil dog også telefonisk kunne kontaktes (på anonym basis) for vejledning omkring anmeldelseskravet.

Datatilsynets vejledning om håndtering af brud på persondatasikkerheden indeholder en lang række illustrative eksempler i forhold til, om anmeldelse af/underretning om sikkerhedsbrud er påkrævet.[79]

I vejledningen nævnes bl.a. som eksempel, at anmeldelse til Datatilsynet ikke er nødvendigt, hvis en personalechef i en virksomhed på togturen hjem fra arbejde får stjålet sin taske, hvori der bl.a. ligger en ekstern harddisk indeholdende oplysninger om ansøgere til en opslået stilling i virksomheden. Virksomheden har sikret sig, at de harddiske, der udleveres til medarbejderne, er beskyttet med en stærk kryptering, der ikke umiddelbart vil være mulig for uvedkommende at dekryptere.

Et andet eksempel, som også nævnes, og hvor anmeldelse til Datatilsynet ikke er nødvendigt, er, hvis der ved en fejl uploades en fil med personoplysninger på en hjemmeside, men filen hurtigt bliver fjernet igen, og det kan konstateres ud fra it-afdelings logoplysninger, at der ikke har været besøgende på hjemmesiden i den tid, hvor filen var tilgængelig, og filen ikke er blevet kopieret af søgemaskiner.

Det skal også fremhæves, at det af ovenstående vejledning fremgår, at det er Datatilsynets opfattelse, at for at kunne sikre en effektiv efterlevelse af forpligtelsen til at anmelde brud på persondatasikkerheden til Datatilsynet og til at underrette de registrerede, er det helt afgørende, at den dataansvarlige (og databehandlere) udarbejder procedurer for håndtering af sikkerhedshændelser i organisationen.

10.3 Underretning af de registrerede

I medfør af databeskyttelsesforordningens art. 34 skal den registrerede underrettes uden unødig forsinkelse om bruddet på persondatasikkerheden, hvis bruddet sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

[79] Vejledningen kan tilgås på Datatilsynets hjemmeside: https://www.datatilsynet.dk/Media/637886298435856391/H%C3%A5ndtering%20af%20brud%20p%C3%A5%20persondatasikkerheden.pdf

Formålet med underretningen er bl.a. at give den registrerede mulighed for at træffe de fornødne forholdsregler i tilfælde af, at der er sket kompromittering af vedkommendes personoplysning.

Datatilsynets vejledning om håndtering af brud på persondatasikkerheden beskriver, at der ikke i databeskyttelsesforordningen findes en definition af begrebet "høj risiko". Men det må ved en vurdering af risikoens omfang lægges til grund, at jo mere alvorlige konsekvenser bruddet kan medføre, jo større vil risikoen være for de berørte personer. Tilsvarende vil en større sandsynlighed for, at et brud vil få konsekvenser for de registrerede ligeledes indebære en større risiko.

Det er ikke nødvendigt at underrette den registrerede, hvis

a) den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som f.eks. kryptering,
b) den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registreredes rettigheder og frihedsrettigheder sandsynligvis ikke længere er reel,
c) det vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

11 Udlevering af oplysninger til tredjepart

11.1 Udlevering af forbrugsoplysninger

Ikke sjældent modtager DANVA henvendelser fra medlemmer, der er blevet mødt af et krav fra fx politi eller kommune om udlevering af en bestemt kundes målerdata/forbrug på en bestemt adresse. Imidlertid kan forsyningsselskabet ikke uden videre udlevere sådanne oplysninger. Fælles for reglerne er, at der skal være et behandlingsgrundlag. Det vil sige, at forsyningsselskabet skal have lov til at videregive oplysningerne. Det kan være et behandlingsgrundlag, som følger af reglerne i databeskyttelsesforordningens artikel 6, eller det kan være særregler i anden lovgivning end databeskyttelseslovgivningen. Se også vejledningens punkt 6.1 hvor de forskellige behandlingsgrundlag står beskrevet.

Forsyningsselskabet bør være opmærksom på nedenstående:

11.1.1 Registerbaseret sagsbehandling og digitale sagsbehandlingsskridt mv. i den offentlige forvaltning

Det følger af lov om aktiv socialpolitik og af det generelle officialprincip (et princip, som ikke står i loven, men kan udledes af praksis m.v., som går ud på, at offentlige myndigheder har pligt til at undersøge sagen tilstrækkeligt, inden der bliver truffet afgørelse), at kommunen, når den træffer afgørelser om integrationsydelse, uddannelseshjælp og kontanthjælp, i videst muligt omfang skal indhente de nødvendige oplysninger fra elektroniske registre, som kommunen har adgang til.

De bestemmelser, som fremgår af lov om aktiv socialpolitik og det, som følger af officialprincippet, skal sikre, at sagsbehandlingen af sager om tilkendelse af kontanthjælp mv. bliver nemmere at administrere. På grund af disse regler kan oplysninger om en person, der allerede findes i et register, benyttes, i stedet for at der skal indhentes oplysninger fra den pågældende via fx lønsedler, oversigter over bankoplysninger, bopælsoplysninger mv.

Kommunen skal derfor som udgangspunkt basere sagsbehandlingen på de oplysninger, som allerede findes om en person. Hvis en person, som ansøger om kontanthjælp, i forbindelse med ansøgningen har givet kommunen oplysninger om forhold, som skal indgå i vurderingen af, om den pågældende er berettiget til kontanthjælp, kan kommunen anvende disse oplysninger i forbindelse med afgørelsen.

Indhentelse af oplysninger skal ske inden for rammerne af reglerne i såvel forvaltningsloven som persondatalovgivningen mv. om indhentelse af oplysninger, herunder reglerne om samtykke og partshøring. Kommunen skal derfor, inden den foretager en datasamkøring, orientere de berørte personer.

Rent praktisk kan et forsyningsselskab anmode kommunen om skriftligt at bekræfte, at denne fremgangsmåde er blevet fulgt, hvis der er tvivl herom.

11.1.2 Udlevering af forbrugsoplysninger til kommunen

Lov om boligforhold § 11[80] indeholder følgende hjemmel for kommunen til at indhente forbrugsoplysninger fra forsyningsselskaber med henblik på kontrol og tilsyn med bopælspligten:

"Kommunalbestyrelsen kan til brug for undersøgelse af en begrundet mistanke om overtrædelse af § 5, stk. 1, og § 7, stk. 1, om bopælspligt gøre følgende:

*1) Indhente oplysninger fra forsyningsselskaber om en konkret boligs samlede forbrug i en afgrænset periode på mindst 1 måned.*Bestemmelsen er en videreførelse af den forhenværende boligreguleringslovs § 52 e. Det fremgår af forarbejderne til denne bestemmelse, at forsyningsselskaberne har pligt til i konkrete sager at udlevere ikke-følsomme oplysninger på en bestemt bolig omfattende identifikation af navne, adresser og forbrug af el, vand, varme og gas, der skal have en længde på mindst en måned og vedrøre en afgrænset periode.

Det fremgår desuden, at "*Det er kommunalbestyrelsens ansvar, at betingelserne for at indhente forbrugsoplysninger i konkrete sager er opfyldt. Forsyningsselskabet har således pligt til at udlevere oplysningerne. Kommunalbestyrelsens indhentning og behandling af forbrugsoplysninger skal leve op til de almindelige principper og regler om behandling af personoplysninger, der følger af databeskyttelsesforordningens artikel 5.*"[81]

Bestemmelsen giver ikke kommunalbestyrelsen mulighed for at følge med i en husstands aktuelle forbrug ved at anmode om at modtage løbende forbrugsaflæsninger eller tegne en direkte adfærdsmæssig profil af husstandens forbrug og vaner.[82]

CPR-lovens § 10 indeholder desuden følgende bestemmelse vedrørende korrekt bopælsregistrering:

"En kommunalbestyrelse, der får formodning om, at en person ikke er korrekt bopælsregistreret, skal undersøge sagen for at rette eventuelle fejl. […]

Stk. 2. Kommunalbestyrelsen kan til brug for undersøgelsen af en persons bopælsforhold […] afkræve følgende oplysninger:

1) En nærmere redegørelse fra vedkommende selv […]

2) En erklæring […] om, hvem der bor eller opholder sig i ejendommen eller lejligheden.

3) Oplysninger fra […], private tele- og forsyningsselskaber, […] med henblik på at fastlægge vedkommendes bopælsforhold."

---

[80] Lovbekendtgørelse nr. 342 af 22/03/2022 (lov om boligforhold)

[81] Lovforslag nr. 98 2018/1 til Lov om ændring af lov om midlertidig regulering af boligforholdene

[82] Lovforslag nr. 98 2018/1 til Lov om ændring af lov om midlertidig regulering af boligforholdene

Af bemærkningerne til ovennævnte stk. 2, nr. 3 fremgår det, at:

"[…] De oplysninger, der kan kræves oplyst for at belyse en bopælssag, er den adresse, den pågældende har oplyst til andre at bo på, f.eks. til vedkommendes bank eller fagforening, og det samlede forbrug af el, vand, varme, gas samt telefon i en bestemt periode, samt navnene på en lejekontrakt. […]."

Bestemmelsen, der er møntet på kommunens pligt til at sikre korrekt bopælsregistrering af kommunens borgere efter lovens § 6, ses også forsøgt anvendt af kommuner i de såkaldte "dyneløftesager" til afdækning af eventuelle samlivsforhold, som kan have betydning for en persons ret til fx kontanthjælp. Imidlertid kan en kommune ikke med henvisning til CPR-lovens § 10 indhente de nævnte oplysninger til andre formål end undersøgelse af den pågældendes persons bopælsregistrering og -forhold. Forsyningsselskabet skal desuden holde sig for øje dels, at bopælsundersøgelsen alene vedrører den relevante adresse, dels at det kun er den pågældende persons forbrug, som kommunen undersøger, der kan og skal gives oplysninger omkring. At forsyningsselskabet fx også har registreret en anden persons navn på adressen, er ikke en oplysning, der er omfattet af bestemmelsen. Forsyningsselskabets udlevering af sådanne oplysninger vil i værste fald kunne føre til en overtrædelse af persondatalovgivningens bestemmelser.

Det anbefales, at forsyningsselskaber altid, forud for en udlevering af personoplysninger til en myndighed, beder om skriftlig angivelse af myndighedens hjemmel til at få oplysninger udleveret og dokumenterer dette på sagen. Forsyningsselskaberne bør også bede myndigheden forholde sig til, om udleveringen og behandlinger lever op til de almindelige principper og regler om behandling af personoplysninger, herunder artikel 5.

Forsyningsselskabet er som udgangspunkt forpligtet til at oplyse den registrerede om formålet med behandlingen og kategorierne af modtagere. I de konkrete tilfælde kan denne oplysningspligt vige for afgørende hensyn til offentlige interesser, f.eks. en konkret efterforskning. Af denne årsag anbefales det, at forsyningsselskaberne på forhånd oplyser i en privatlivspolitik, at oplysninger på skriftlig anmodning kan blive udleveret til de relevante myndigheder for at efterleve selskabets forpligtelser efter lovgivningen.

11.1.3 Udlevering af oplysninger til udlejer

Forsyningsselskaber kan have interesse i at videregive oplysninger om forbrug til udlejer, f.eks. for at varsle udlejer i de situationer, hvor udlejer i sidste ende hæfter for lejers forbrug.

Forsyningsselskaber må kun videregive oplysninger, som er nødvendige for, at udlejer kan forsvare sig mod forsyningsselskabets eventuelle retskrav. Der kan derfor f.eks. ske videregivelse, hvis udlejer hæfter for drifts- eller vandafledningsbidraget samt eventuelle yderligere omkostninger. Der må først ske en videregivelse, når udlejers hæftelse aktualiseres, det vil sige, når forsyningsselskabet har ret til at afkræve udlejer betaling.

Rykkerskrivelser kan alene sendes til udlejer, hvis udlejer hæfter for rykkergebyrer og renter.

Videregivelse kan også ske til udlejer ved flytteafregning, hvis videregivelsen til udlejer i forbindelse med flytteafregning er nødvendig for, at udlejer kan tilbageholde et beløb svarende til restancen i depositummet.

11.1.4 Videregivelse af forbrugsoplysninger til politiet

Udlevering af forbrugsoplysninger til brug for politiets efterforskning i straffesager (fx sager om brandstiftelse) kræver som udgangspunkt en retskendelse (dommerkendelse). Men politiet har i medfør af regler i retsplejeloven relativt vidtgående beføjelser til i særlige tilfælde at gennemføre efterforskningsskridt uden først at indhente en kendelse.

DANVA anbefaler derfor, at selskaberne udviser forsigtighed og anmoder om dokumentation for at sikre sig, at politiet har den fornødne hjemmel til at få oplysninger (fx målerdata) udleveret, enten i form af en retskendelse eller i medfør af særlige regler om efterforskningsskridt, hvor en retskendelse ikke er påkrævet.

Videregivelse af billed- og lydoptagelser (som f.eks. videoovervågning) til politiet må ske, hvis det er i kriminalitetsopklarende øjemed.[83]

Se også afsnit 6.3 om behandling af oplysninger om strafbare forhold og om reglerne for videregivelse af sådanne oplysninger.

11.1.5 Aktindsigt

I forhold til anmodninger om aktindsigt efter offentlighedslovens har disse regler "fortrinsret" for persondatalovgivningen regler, jf. databeskyttelsesforordningens artikel 86. Dette gælder dog ikke, hvis der skal gives meroffentlighed i overensstemmelse med offentlighedslovens § 14. I sidstnævnte tilfælde skal databeskyttelsesforordningen iagttages i forbindelse med spørgsmålet om meroffentlighed. Forsyningsselskaberne kan ligeledes være forpligtet til at håndtere anmodninger om aktindsigt efter miljøoplysningsloven.

Såfremt et forsyningsselskab anmodes om aktindsigt – uden reference til en bestemt lov – skal forsyningsselskabet angive i svaret, at sagen er behandlet efter offentlighedslovens regler (eller miljøoplysningsloven). Alternativt kan den, der anmoder om aktindsigt, anmodes om at oplyse, efter hvilken lov anmodningen skal behandles.

Forsyningsselskabet skal dog være opmærksom på, at hvis en kombination af f.eks. offentlighedsloven/miljøoplysningslovens regler om aktindsigt og databeskyttelsesforordningens regler om indsigt giver den bedste retsstilling for den enkelte, skal begge regelsæt anvendes.[84]

---

[83] Det følger af tv-overvågningslovens § 4 c, stk. 1, nr. 3. Se også Datatilsynets side om tv-overvågning: https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/optagelser-og-overvaagning/tv-overvaagning

[84] Princippet følger bl.a. af Ombudsmandens praksis. Ligeledes fremgår det af Justitsministeriets betænkning nr. 1565 vedrørende databeskyttelsesforordningen, at afgørelser i forhold til egenaccess og aktindsigt skal træffes på det retsgrundlag, der er mest gunstigt for den pågældende.

Ved videregivelse af personoplysninger i forbindelse med anmodninger om aktindsigt, skal oplysningspligten over for de registrerede overholdes, medmindre én af undtagelserne i persondatalovgivningen finder anvendelse. Det anbefales derfor, at forsyningsselskaberne på forhånd oplyser om aktindsigt i deres privatlivspolitik.

11.2 Videregivelse af personoplysninger til brug for markedsføring

Databeskyttelsesloven indeholder særlige regler om videregivelse af oplysninger om forbrugere, dvs. kunder[85] (kundeoplysninger) til brug for andre virksomheders markedsføring[86].

Uden kundens udtrykkelige samtykke må en erhvervsdrivende kun videregive sådanne oplysninger, hvis der er tale om "generelle kundeoplysninger", som danner grundlag for inddeling i kundekategorier, og hvis interesseafvejningsreglen i databeskyttelsesforordningens artikel 6, stk. 1, litra f finder anvendelse.

Som eksempler på generelle kundeoplysninger, der vil kunne videregives uden samtykke, kan nævnes oplysninger om kundens navn, adresse, køn og alder. Det samme gælder generelle oplysninger som fx, at kunden er husejer, bilejer, computerejer og lignende. Der må således ikke være tale om detaljerede kundeoplysninger eller forbrugsvaner.

Oplysningerne må dog ikke videregives, hvis kunden har frabedt sig henvendelser i markedsføringsøjemed, herunder ved at få markeret i CPR-registret, at han eller hun ikke ønsker henvendelser i markedsføringsmæssigt øjemed (”Robinsonlisten”).

Reglerne om de registreredes indsigelsesret i databeskyttelsesforordningens artikel 21 finder desuden anvendelse på videregivelsen, hvilket indebærer, at den registrerede kan gøre indsigelse over for behandling af oplysninger med henblik på direkte markedsføring, og at den registrerede skal gøres opmærksom på denne rettighed.

Det skal bemærkes, at databeskyttelsesloven alene tager stilling til lovligheden af videregivelsen af personoplysninger til brug for markedsføring. Databeskyttelsesloven tager således ikke stilling til lovligheden af selve henvendelsen til kunden. Reglerne for, hvornår en virksomhed må henvende sig til en kunde i markedsføringsmæssigt øjemed, findes i markedsføringslovens § 10 om uanmodede henvendelser[87].

---

[85] Forbrugerbegrebet omfatter kun *privatpersoner*, ikke virksomheder, foreninger og myndigheder og heller ikke fysiske personer som erhvervsdrivende i personlig form (enkeltmandsvirksomhed).

[86] Se databeskyttelseslovens § 13. Datatilsynet har dog udtalt i en sag fra 2022, at det er tvivlsomt, om databeskyttelseslovens § 13, ligger inden for det nationale råderum, Det vil sige, at en dataansvarlig i hvert fald bør sikre, at der er behandlingsgrundlag til behandlingen efter artikel 6, f.eks. efter interesseafvejningsreglen i artikel 6, stk. 1, litra f.

[87] Se § 10 i markedsføringsloven https://www.retsinformation.dk/eli/lta/2022/866

11.3 Overførsel af personoplysninger til tredjelande

Hvis personoplysninger overføres til lande uden for EU/EØS eller til internationale organisationer, f.eks. ved outsourcing af it-systemer, skal den dataansvarlige iagttage reglerne for overførsler til tredjelande.

Hvis der sker overførsel til et sikkert tredjeland, kan dette ske efter de almindelige bestemmelser, det vil sige, når der er et sædvanligt behandlingsgrundlag – normalt enten i artikel 6 eller artikel 9 i databeskyttelsesforordningen. Hvis overførslen sker til et usikkert tredjeland, er der flere komplekse muligheder, fx ved at benytte de såkaldte standardkontraktsbestemmelser fra EU-Kommissionen (kaldes også for Standard Contract Clauses, forkortes SCC'er, som er kontrakter, der indgås med dataimportøren) og eventuelt indføre supplerende foranstaltninger (for eksempel tekniske sikkerhedsforanstaltninger såsom kryptering). Det er dog en konkret vurdering, om det er tilstrækkeligt til, at det vil være lovligt.

Reguleringen om overførsel til et tredjeland er komplekst og foranderligt, hvilket vil fremgå af nedenstående. DANVA anbefaler derfor, at vandselskabet er i tæt forbindelse med en advokat, der har særlig viden om GDPR.

11.3.1 Overførsel til et sikkert tredjeland

EU-Kommissionen har bl.a. godkendt Storbritannien, Færøerne og Israel som sikre tredjelande.[88]

USA er betegnet som sikkert tredjeland i forhold til overførsler til organisationer, som er certificeret under "EU-U.S. Data Privacy Framework" (forkortes DPF). Dette offentliggjorde EU-Kommissionen den 10. juli 2023, hvor de bekendtgjorde, at der nu var truffet en såkaldt tilstrækkelighedsafgørelse. Det vil sige, at der lovligt kan overføres til organisationer i USA, som er på listen over certificerede organisationer. Det omfatter såvel techgiganter som Microsoft og Google, som en række mellemstore og mindre virksomheder i USA. Listen over certificerede organisationer opdateres løbende og kan findes på Data Privacy Frameworkets hjemmeside.[89]

Det er vigtigt at være opmærksom på, at EU-U.S. Data Privacy Framework betragtes som en midlertidig løsning. Der er en stor sandsynlighed for, at løsningen bliver erklæret ugyldig af EU-Domstolen. Organisationen None Of Your Business (NOYB), som advokaten Max Schrems står bag, har allerede for længst meldt ud, at de ikke ser det som en holdbar og lovlig løsning, da en række af de retssikkerhedsmæssige garantier ikke overholdes. NOYB er derfor klar til at indbringe tilstrækkelighedsafgørelsen for EU-Domstolen, som de allerede har gjort to gange tidligere.

Det forventes derfor, at EU-Kommissionen stadig arbejder videre på en mere permanent løsning end den nuværende. Hvis EU-U.S. Data Privacy Frameworket bliver erklæret ugyldig, vil overførslerne skulle ske på andet grundlag, da EU-U.S. Data Privacy Frameworket ikke længere vil kunne bruges. Hvis der allerede er

[88] EU-Kommissionen offentliggør de sikre tredjelande på deres hjemmeside: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[89] https://www.dataprivacyframework.gov/s/participant-search

udarbejdet juridiske vurderinger (for eksempel SCC'er og TIA'er, som står for Transfer Impact Assessments, og normalt vil skulle udarbejdes ved overførsler til usikre tredjelande) fra før EU-U.S. Data Privacy Framework trådte i kraft, er det derfor en god idé at gemme disse vurderinger, så de kan benyttes, hvis EU-U.S. Data Privacy Frameworket bliver erklæret ugyldig.

Hvis vandselskabet har indgået SCC'er med organisationer i USA (og denne organisation nu er blevet certificeret), og vandselskabet vurderer, at SCC'erne er tilstrækkelige som overførselsgrundlag, kan vandselskabet beholde SCC'erne som overførselsgrundlag i stedet for det nye EU-U.S. Data Privacy Framework. Dermed behøver vandselskabet ikke skifte overførselsgrundlag igen, hvis EU-U.S. Data Privacy Frameworket bliver erklæret ugyldig.

Hvis vandselskabet har indgået SCC'er med organisationer i USA (og denne organisation nu er blevet certificeret), og vandselskabet vurderer, at de allerede indgået SCC'er ikke er tilstrækkelige som overførselsgrundlag, bør det nye EU-U.S. Data Privacy Framework i stedet benyttes som overførselsgrundlag, og de indgåede SCC'er bør opsiges.

Det er vigtigt løbende at sikre, at organisationen, som der overføres til, forbliver certificeret. Hvis organisationen ikke fremgår af listen over certificerede organisationer, skal det betragtes som en overførsel til et usikkert tredjeland.

EU-U.S. Data Privacy Framework gælder ikke for overførsler, som allerede er foretaget. Det vil sige, at hvis der er overført personoplysninger til en virksomhed i USA, eller det stadig sker, inden organisationen blev certificeret under EU-U.S. Data Privacy Framework, er man stadig ansvarlig for at have sikret essentielt samme beskyttelse for personoplysningerne i perioden inden EU-U.S. Data Privacy Framework. Hvis der modtages en klage, eller Datatilsynet kommer på besøg, kan man altså ikke forsvare lovligheden af tidligere overførsler før organisationen blev certificeret med henvisning til EU-U.S. Data Privacy Framework. Det vil sige, at hvis der for eksempel er udarbejdet TIA'er og SCC'er, skal disse gemmes som dokumentation for overførsler foretaget før EU-U.S. Data Privacy Framework trådte i kraft.

Hvis EU-U.S. Data Privacy Framework benyttes som overførselsgrundlag, skal det også afspejles i den databeskyttelsesretlige dokumentation. Det vil bl.a. sige, at det skal fremgå af privatlivspolitik (eller andre dokumenter, som bruges til at kunne opfylde oplysningspligten), fortegnelsen over behandlingsaktiviteter (artikel 30-fortegnelsen) og anden relevant dokumentation. Se i den forbindelse DANVAs udkast til privatlivspolitik om kundeoplysninger, som er opdateret med det nye EU-U.S. Data Privacy Framework.

11.3.2 Overførsel til et usikkert tredjeland

For de lande, som EU-Kommissionen har vurderet til at være usikre forhold til deres beskyttelse af personoplysninger (for eksempel Indien, Kina eller Vietnam), skal der findes et lovligt overførselsgrundlag i databeskyttelsesforordningens kapitel V, således at det garanteres, at der er et tilstrækkeligt beskyttelsesniveau for de overførte personoplysninger.

Det betyder, at der skal foretages en nærmere juridisk vurdering, hvis der overføres personoplysninger til et usikkert tredjeland.

Et sådant overførselsgrundlag kan f.eks. bestå i indgåelse af EU-Kommissionens standardkontrakter (kaldes også for SCC'er)[90] med aftalepartneren i usikre tredjelande. Denne aftale lever også op til kravene om databehandleraftale.

Hvis der allerede tidligere er blevet brugt standardkontrakter (SCC'er) som overførselsgrundlag til et usikkert tredjeland, skal man være opmærksom på, hvornår de blev indgået, og om man skal opdatere aftalerne, så det i stedet er de nye og "rigtige" standardkontrakter, som benyttes. Aftaler om overførsler til usikre tredjelande ved brug af EU-Kommissionens tidligere standardkontrakter, som blev indgået inden den 27. september 2021, har ikke kunnet benyttes siden 27. december 2022. I stedet skal EU-Kommissionens nye standardkontrakter benyttes. De nye standardkontrakter er dem, som på nuværende tidspunkt fremgår af EU-Kommissionens hjemmeside.

Udover at sørge for at indgå standardkontrakterne korrekt, er det et krav, at forholdene i det usikre tredjeland sikrer, at der sker en beskyttelse, som i det væsentlige svarer til det, som vi har i EU. Hvis det ikke er muligt, skal dataeksportøren enten bevise, at den problematiske lovgivning ikke er relevant for overførslen eller sørge for supplerende foranstaltninger, der afhjælper eventuelle utilstrækkeligheder i beskyttelsesniveauet. Hvis dataeksportøren ikke er i stand til at træffe supplerende foranstaltninger, som sikrer et beskyttelsesniveau, der i det væsentlige svarer til niveauet i EU-retten, skal dataeksportøren suspendere eller indstille overførslen af personoplysninger til det pågældende tredjeland.

EDPB (European Data Protection Board, som på dansk er benævnt Det Europæiske Databeskyttelsesråd eller blot Databeskyttelsesrådet) har udarbejdet en vejledning[91], som indeholder en beskrivelse af de trin, der skal følges for at afgøre, om dataeksportøren skal indføre supplerende foranstaltninger for lovligt at kunne overføre oplysninger til lande uden for EØS. Vejledningen indeholder også eksempler på supplerende foranstaltninger. Det vil være en konkret vurdering, hvorvidt der kan indføres tilstrækkelige supplerende foranstaltninger afhængigt af, hvilket land der er tale om, og hvilke personoplysninger der overføres.

Undtagelsesvist kan der ske overførsel til et ikke-sikkert tredjeland, selvom der ikke kan indgås standardbestemmelser og/eller ikke kan indføres supplerende foranstaltninger efter databeskyttelsesforordningens artikel 49. Det kan fx være, hvis samtykke til overførsel til et usikkert tredjeland indhentes. Et samtykke skal efter databeskyttelsesforordningens artikel 49, stk. 1, litra a, være udtrykkeligt, og den registrerede skal være blevet informeret om de mulige risici, som sådanne overførsler kan medføre for den registrerede på grund af manglen på et tilstrækkeligt beskyttelsesniveau for personoplysningerne. Det bør vurderes konkret om undtagelsesreglen i artikel 49 kan benyttes.

---

[90] EU-Kommissionens standardkontrakter kan tilgås EU-Kommissionens hjemmeside: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32021D0914&from=DA

[91] Vejledningen kan tilgås her: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_da.pdf

Datatilsynet har udarbejdet en vejledning om overførsel til tredjelande, hvor de forskelle overførselsgrundlag nærmere gennemgås[92], ligesom Datatilsynet også har udarbejdet en vejledning om cloud.[93]

[92] Vejledningen kan tilgås her: https://www.datatilsynet.dk/Media/637902777513932912/Vejledning%20om%20overf%c3%b8rsel%20til%20tredjelande.pdf

[93] https://www.datatilsynet.dk/Media/637824109172292652/Vejledning%20om%20cloud.pdf

12 Sanktioner

Datatilsynet påser af egen drift, eller efter klage fra en registreret, at en behandling finder sted i overensstemmelse med persondatalovgivningen. Ved overtrædelser kan Datatilsynet navnlig udtale kritik og alvorlig kritik og i særlige tilfælde udstede påbud eller forbud, ligesom Datatilsynet kan politianmelde og indstille til bøde, så overtrædelse kanstraffes med bøde eller fængsel op til 6 måneder.

Der er to forskellige grænser for den maksimale bødestørrelser afhængig af, hvilken bestemmelse, der overtrædes:

- Bøder på op til 10 000 000 EUR eller op til 2 % af en virksomheds samlede globale årlige omsætning i det foregående regnskabsår for overtrædelse af forpligtelser efter art. 8, 11, 25-39 og 42 og 43, herunder sikkerhedskrav.
- Bøder på op til 20 000 000 EUR eller op til 4 % af en virksomheds samlede globale årlige omsætning i det foregående regnskabsår for overtrædelse af de grundlæggende principper for behandling (art. 5, 6, 7 og 9), de registrerede rettigheder (art. 12-22), overførsel til tredjelande uden overførselsgrundlag eller manglende overholdelse af påbud m.v.

Databeskyttelsesloven lægger desuden op til, at visse overtrædelser kan straffes med fængsel i indtil 6 måneder, jf. lovens § 41, stk. 1. Det kan efter forarbejderne f.eks. være i tilfælde, hvor der sker en forsætlig offentliggørelse af følsomme oplysninger i et betydeligt omfang.

Bødeniveauet fastsættes efter databeskyttelsesforordningens art. 83, stk. 2, på baggrund af en række faktorer, herunder:

- Overtrædelsens karakter, alvor og varighed, antal registrerede, der er berørt og omfanget af den skade, som de har lidt.
- Hvorvidt overtrædelsen blev begået forsætligt eller uagtsomt.
- Foranstaltninger truffet for at begrænse skaden.
- Tidligere overtrædelser.
- Graden af samarbejde med Datatilsynet, og hvorvidt de blev underrettet om overtrædelsen.

Efter databeskyttelsesforordningens artikel 82, jf. databeskyttelseslovens § 40, har enhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af denne forordning, desuden ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren.

Der er efter den gamle persondatalov ikke domme i dansk retspraksis, hvor registrerede er blevet tilkendt erstatning for (dataansvarliges) overtrædelser af den tidligere persondatalov. Der findes dog en række situationer, der har været forelagt domstolene, og hvor det er blevet antaget, at der foreligger en persondataretlig krænkelse efter den gamle persondatalov, og der er tilkendt den krænkede part godtgørelse på op til kr. 25.000 efter erstatningsansvarslovens § 26 om godtgørelse for tort.