DANVA
Dansk Vand- og Spildevandsforening

DATO: 29. november 2018
PROJEKTNR.: 7016

NOTAT

Vedr.: Kryptering af forbrugsrelaterede data sendt via e-mail

Datatilsynet offentliggjorde sommeren 2018 en udtalelse om skærpet praksis i forhold til krypteret e-mail, og budskabet er, at efter Datatilsynets opfattelse, at vil det normalt være en passende sikkerhedsforanstaltning – for både offentlige og private aktører – at anvende kryptering ved transmission af fortrolige og følsomme personoplysninger med e-mail via internettet Kryptering kan ske på forskellig vis, og tilgangen til emnet skal ske ud fra en risikovurdering.

I det nærværende er der primært fokus på **forbrugsrelaterede data**, som vandselskaber ønsker at gøre tilgængelige for kunden.

Sikkerhed omkring personoplysninger, som vi finder i persondataforordningens artikel 32, omtales, ligesom vi vil behandle fortrolighedsbegrebet. For at kvalificere fortrolighedsbegrebet laver vi nogle vurderinger om "private forhold", som aktindsigtsregler lægger op til.

Selvom nogle forsyninger sender/formidler forbrugsrelateret data – ikke mindst faktura – via PBS (Pengeinstitutternes BetalingsService), via e-Boks efter aftale med kunden eller kundeportaler, så er det DANVAs indtryk, at der er forsyninger, der anvender almindelig e-mail-kommunikation i den forbindelse.

DANVAs bedste vurdering og anbefaling

Der er på nuværende tidspunkt ingen juridisk afklarede udmeldinger i forhold til, om forbrugsdata – i et eller andet omfang – kan fremsendes via ukrypteret e-mail til eksterne folk uden for forsyningen.

Med "risiko" for at overimplementere persondatareglerne tilsiger et forsigtighedsprincip, at kunders data omgås med stor varsomhed – og at forsyningerne arbejder for, at personhenførbare data videreformidles via beskyttede kanaler.

For indeværende er det DANVAs bedste vurdering, at forbrugsdata og fakturaer, der typisk udsendes kvartalsvis, af kunderne generelt opleves som værende af privat karakter. Dette peger følgelig i retning af, at de kan anses som værende fortrolige data i persondatasammenhæng. Dette betyder, at hvis en forsyning på lovlig vis har e-mailadressen til kunden og ønsker at sende sådanne data, så bør der ske en kryptering.

Det er dog DANVAs bedste vurdering, at det i dag ikke er en realistisk, generel løsning at anvende kryptering af e-mails som en sikker måde at behandle persondata på. Anbefalingen er at anvende mere centraliserede løsninger over enten PBS, e-Boks eller kundeportaler – og en midlertidig løsning kan være brevpost.

Anbefalingen lægger således op til, at forsyningen italesætter sikkerhed over for kunderne.

Uddybning

Aktindsigt

De kommunalt ejede vand- og spildevandforsyninger (vandselskaber) er i vidt omfang omfattet af offentlighedsloven, se § 14.1 i vandsektorloven. Når kryptering diskuteres, så vil det ikke give mening, hvis der var en generel aktindsigt i en kundes forbrugsdata, og der samtidigt blev krævet kryptering.

En vilkårlig person, der anmoder om aktindsigt i forbrugsdata hos en eller flere kunder, vil typisk blive mødt med et afslag, hvor begrundelsen er, at dette kræver et dataudtræk, hvilket vandselskabet ikke er forpligtiget til at foretage, se vandsektorloven § 14.1. Vandselskabet kan overveje meroffentlighed – men i den forbindelse er DANVAs bedste vurdering, at en sådan aktindsigt skal afvises efter § 30 i Offentlighedsloven.

§ 30 har nemlig følgende ordlyd:
Retten til aktindsigt omfatter ikke oplysninger om
1) enkeltpersoners private, herunder økonomiske, forhold og
2) tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el.lign., for så vidt det er af væsentlig økonomisk betydning for den person eller virksomhed, oplysningerne angår, at anmodningen ikke imødekommes.

Hvorvidt en oplysning vedrører et "privat forhold", er tilknyttet en vurdering af, om oplysningen ud fra en generel betragtning efter sin karakter vedrører oplysninger om enkeltpersoners private, herunder økonomiske, forhold. Om oplysningens hemmeligholdelse har konkret betydning, er derfor uden betydning. Det betyder, at særlig følsomme oplysninger om den private er omfattet af bestemmelsen, hvorimod oplysninger af objektiv karakter falder udenfor.

Det skal i den forbindelse nævnes, at DANVA tidligere har tilkendegivet[1], at oplysningerne om forbrug i forhold til vand og spildevand ikke kan videregives til private eller offentliggøres uden samtykke. Der er ikke tale om 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.[2]

I det nærværende, hvor der er fokus på aktindsigt, tænkes der på såvel de situationer, hvor der er tale om opsummeringer af forbrug på kvartals- eller årsbasis, som situationer hvor der ønskes adgang til evt. hyppige forbrugsmålinger, som måtte foretages lovligt via smart meters (fjernaflæsningsmålere). Dette kunne lægge op til en graduering i vurderingen afhængig af, hvor præcis en profilering/adfærdsbeskrivelse, du vil kunne lave med afsæt i de modtagene forbrugsdata.

I vores aktuelle vurdering lægger vi derudover vægt på:

- Der er i de seneste år en øget bevidsthed omkring brug af persondata[3], ligesom der også synes at være en øget, kritisk tilgang til overvågning af privatsfæren[4].

[1] DANVA vejledning nr. 100, Vejledning om persondata for vandselskaber

[2] Dette er også lagt til grund i persondatalovens 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.

[3] EU's Persondataforordning og dens implementering har affødt opmærksomhed om persondata og brugen heraf.

[4] Sommeren 2018 viste der sig at være en voldsom modstand i offentligheden i forhold til de politiske partiers aftaleforhandling om kontrol af snyd med sociale ydelser. Beskæftigelsesministeren trak lovforslaget

- Det er en udbredt holdning hos kunderne, at de ikke ønsker at få offentliggjort, hvor meget eller hvor lidt de bruger; det kan nemlig problematiseres når kunden bruger "for meget" vand (ressource-svineri), ligesom det vel også kan problematiseres, når en kunde bruger for lidt (hygiejne-perspektivet). Ingen ønsker at indgå i en evt. "name and shame" artikel i lokalavisen.
- Klimaforandringerne vil øge risikoen for, at vandforsyningen mange steder i perioder kommer under pres – hvilket sommeren 2018 var et godt eksempel på. Det betyder, at ovenstående problematisering alt andet lige er endnu mere relevant.
- Indblik i en ejendoms vandforbrug – selv på årsbasis – indikerer hvor mange mennesker, der bor i ejendommen, eller hvor meget de måtte være på ferie. Denne information kan være nyttig viden for personer, der vil finde indbrudsegnede hjem i et område.

På denne baggrund vil der kunne argumenteres for, at der vil være en udbredt/generel opfattelse af, at forbrugsdata af enhver art, der kan henføres til en bestemt kunde, anses som værende af privat karakter. Og at en 3. persons anmodning om aktindsigt som udgangspunkt vil kunne afvises med hjemmel i § 30 offentlighedsloven.

Det skal dog understreges, at vi ikke har kendskab til nogen afgørelser eller udtalelser fra myndigheder om emnet.

Følsomme og fortrolige oplysninger

Afsættet er, at der er en almindelig opfattelse af, at kunders forbrugsdata er persondata i persondatalovgivningens forstand.

Når der er fortrolige eller følsomme personoplysninger i en mail, skal der ske kryptering, se artikel 32 kombineret med Datatilsynets udmeldinger om fortolkning heraf.

De følsomme personoplysninger genfinder vi i oplistningen i forordningens artikel 9; "*… race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering er forbudt*".

Men begrebet fortrolig er ikke så klart. Datatilsynet skriver således:

"*Fortrolige oplysninger er en særlig kategori af oplysninger, der ikke nævnes udtrykkeligt i databeskyttelsesreglerne, men hvor særlige beskyttelsesbehov kan have betydning ved anvendelsen af databeskyttelsesreglerne. Fortrolige oplysninger vil endvidere ofte være underlagt særregulering i anden lovgivning. Personnummer (CPR-nummer) er en fortrolig oplysning, der er særskilt reguleret i databeskyttelsesloven.*

Det afgørende for, om en oplysning skal anses for fortrolig, vil være en vurdering af, om oplysningen efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab, jf. straffelovens § 152 sammenholdt med forvaltningslovens § 27. Følsomme

---

tilbage. Disse forhandlinger angik ifølge pressen en løbende overvågning af el-forbrug. Det skal bemærkes, at der allerede eksisterer regler i CPR-loven og retssikkerhedsloven, hvorefter kommunalbestyrelsen ved konkret mistanke om snyd med sociale ydelser kan indhente data fra forsyninger.

November 2018 kom lovforslag L 98, der også viser, at forbrugsdata skal håndteres varsomt. I lovforslaget foreslås det, at der gives kommunerne en klar hjemmel til at få adgang til at indhente oplysninger fra forsyningsselskaber – herunder vand. Denne information kan kommunerne bruge til at håndhæve bopælspligten.

personoplysninger vil utvivlsomt være fortrolige oplysninger. Omvendt er en fortrolig oplysning ikke altid følsom.

Ikke-følsomme personoplysninger kan i visse situationer være fortrolige. Det gælder efter omstændighederne oplysninger om indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold. Det samme gælder oplysninger om interne familieforhold, herunder oplysninger om for eksempel selvmordsforsøg og ulykkestilfælde. Oplysninger, der kan henføres til bestemte personer, og som ikke kan nægtes udleveret efter offentlighedsloven, vil ikke være af fortrolig karakter. Det gælder f.eks. oplysninger af rent objektiv karakter, såsom oplysninger om udstedelse af pas, kørekort, jagttegn osv."

Begrebet fortrolighed som forvaltet efter straffe- og forvaltningsloven

Dette emne er relevant at vurdere på, da Datatilsynet tidligere har omtalt begrebet fortrolighed og sammenhængen til straffe- og forvaltningsloven.

Disse bestemmelser har fokus på tavshedspligt i den offentlige forvaltning og selvejende institutioner, der er oprettet på privat initiativ, hvis institutionen i øvrigt udøver offentlig virksomhed af mere omfattende karakter og i den forbindelse er undergivet intensiv offentlig regulering, tilsyn og kontrol.

I straffelovens § 152 stk. 3 står:
En oplysning er fortrolig, når den ved lov eller anden gyldig bestemmelse er betegnet som sådan, eller når det i øvrigt er nødvendigt at hemmeligholde den for at varetage væsentlige hensyn til offentlige eller private interesser.
Forbrugsdata er ikke fortrolige grundet en eksplicit formulering i en lovbestemmelse. Men fanges vi af fortrolighedsbegrebet grundet vendingen "hemmeligholdes for at varetage væsentlige hensyn til offentlige eller private interesser"?
Når vi ser nærmere på forvaltningslovens § 27, lyder den som så:
Den, der virker inden for den offentlige forvaltning, har tavshedspligt, jf. straffelovens § 152 og §§ 152 c-152 f, med hensyn til oplysninger om

1. *enkeltpersoners private, herunder økonomiske, forhold …*

I bemærkningerne er det angivet, at bestemmelsen svarer til § 30 i offentlighedsloven (aktindsigtsundtagelsen).

Spørgsmålet er, om der for en personoplysning omfattet af undtagelsesbestemmelsen § 30 i offentlighedslov definitivt skal sættes lighedstegn med fortrolighedsbegrebet, som det skal anvendes i persondataregi. Det synes at pege i den retning.

Krav til behandlingssikkerhed

Artikel 32 - der ikke er let at læse, og som synes at være en gummi-paragraf - lyder:

1. *Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:*
    a. *Pseudonymisering og kryptering af personoplysninger*

   b. *Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester*
   c. *Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse*
   d. *en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
3. *Overholdelse af en godkendt adfærdskodeks som omhandlet i artikel 40 eller en godkendt certificeringsmekanisme som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af kravene i nærværende artikels stk. 1.*
4. *Den dataansvarlige og databehandleren tager skridt til at sikre, at enhver fysisk person, der udfører arbejde for den dataansvarlige eller databehandleren, og som får adgang til personoplysninger, kun behandler disse efter instruks fra den dataansvarlige, medmindre behandling kræves i henhold til EU-retten eller medlemsstaternes nationale ret.*

Sommeren 2018 skrev Datatilsynet følgende i vejledningen om behandlingssikkerhed:
"Behandlingssikkerhed reguleres i databeskyttelsesforordningens artikel 32 og handler overordnet om, at du som den ansvarlige for databehandlingen – dataansvarlig eller databehandler – tilvejebringer et tilstrækkeligt sikkerhedsniveau for den behandling af oplysninger, du foretager. Forordningen kræver, at du skal fastlægge sikkerhedsniveauet ud fra en samlet vurdering af det aktuelle tekniske niveau, implementeringsomkostninger og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Når du har taget hensyn hertil, skal du gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, bl.a. afhængigt af, hvad der er relevant i forhold til de foranstaltninger, som forordningen selv nævner, jf. nedenfor under vejledningens afsnit 3.2. Det er altså en forudsætning for at opnå den efter forordningen tilstræbte databeskyttelse, at der stilles nogle krav til dit sikkerhedsniveau, som modsvarer de risici, der er ved en given behandling af personoplysninger. I praksis betyder det, at du skal have et passende sikkerhedsniveau for at forhindre, at du behandler oplysninger i strid med forordningen, herunder at de personoplysninger, du behandler (f.eks. indsamler og opbevarer), enten hændeligt eller bevidst tilintetgøres, misbruges eller lignende."

Aktuelt sikkerhedsniveau

Det aktuelle sikkerhedsniveau hos forsyningerne i forhold til transport af forbrugsoplysninger/faktura er meget blandet. Der er forsyninger, der efter aftale med kunden anvender PBS eller e-Boks. Der er også forsyninger, der overvejer en kryptering af transporten via den såkaldte Forced TLS på ind- og udgående mail gældende for alle mails.

De kommunale forsyninger kan ikke tvinge sine kunder til at bruge e-Boks, hvilket Digitaliseringsstyrelsen har meddelt DANVA, 12.06.2018, at forsyningerne ikke er omfattet af Lov om offentlig digital post. Kunden er heller ikke forpligtiget til at modtage faktura via PBS med den sikkerhed, det giver.

Derudover er det DANVAs indtryk, at der er forsyninger, der benytter kundeportaler til kommunikation med mange af deres kunder.

Det vil sige, at der er en restgruppe af kunder, hvis omfang DANVA ikke har overblik over, hvor forsyningerne er tvunget til at anvende brev eller e-mail, såfremt e-mail adressen er angivet frivilligt af kunden. Af hensyn til kravet om økonomisk effektivisering er der ingen tvivl om, at disse forsyninger som udgangspunkt ønsker at anvende e-mail-kommunikation.

Implementeringsomkostninger

Vores overvejelser i forhold til implementeringsomkostninger er som udgangspunkt, at vi er enige i væsentligheden af, at korrekte oplysninger leveres til de rigtige personer, så sikkert som muligt. Deraf følger også, at data både under transport og i hvile, bør være beskyttet af passende beskyttelse.

Blandt IT-folk anses almindelig e-mail korrespondance ikke som værende en sikker måde at behandle persondata. Så ud fra det perspektiv, kan det nærmest hævdes, at Datatilsynet ved at acceptere ukrypteret e-mail korrespondance af persondata, så længe de ikke er fortrolige eller følsomme, med afsæt i artikel 32 accepterer en ekstrem lav/ingen beskyttelse af persondata. Hvis hovedformålet er, at kunden på en enkel måde skal kunne tilgå sine oplysninger, er det på nuværende tidspunkt ikke brugervenligt nok at anvende S/MIME eller PGP til kryptering af mails, hvis man tager udgangspunkt i det almene IT-kundskabsniveau hos en gennemsnitlig person. Denne vurdering finder bl.a. støtte hos DANVAs IT-netværk.

Krav om e-mailkryptering vil ikke blot betyde væsentlige implementeringsomkostninger hos den enkelte forsyning som afsender, men også placere en stor opgave hos den enkelte kunde, da korrekt anvendelse kræver installation på den enkelte kundes enhed (computer, telefon, tablet, etc.). I skrivende stund kræver sikker e-mail med NemID, at kunden først tilmelder sig personligt til løsningen, herefter installerer et program på sin computer i 6 trin[5], hvorefter der følger yderligere 6[6] trin for at tilpasse e-mail-programmet. Herefter følger 4 trin for hver sikker e-mail, der skal sendes. Den nuværende vejledning dækker desuden hverken Microsoft Windows 10 eller Microsoft Office 2016, som må forventes at være brugsscenarieet hos en stor mængde kunder.

Derudover understøtter en mængde af de mest anvendte webmail-løsninger ikke sikker e-mail, hvorfor svar fra kunder i mange tilfælde ikke vil kunne sendes med samme sikkerhed, som det bl.a. kan ske ved brug af NemID-løsningen:
"Vær opmærksom på, at de fleste webmail-løsninger, som fx Hotmail, Gmail, Yahoo Mail osv., ikke giver mulighed for at benytte sikker e-mail."[7]

Øvrige løsninger kræver typisk oprettelse af konto hos yderligere 3. parts-leverandør, der også står for opbevaring af data.

Sagt med andre ord er det ikke muligt for forsyningen at sikre, at kunden svarer krypteret – eller sikre at kunden kan dekryptere en mail.

Dermed synes en realistisk tilgang til efterlevelse af behandlingssikkerheden at være en anden løsning end e-mail, men derimod mere centraliserede løsninger over enten PBS, e-Boks eller kundeportaler med brevpost som "nødløsning".

Opsamling og anbefaling

[5] https://www.nemid.nu/dk-da/kom_i_gang_med_nemid/sikker_e-mail/send_og_modtag_sikker_e-mail/installation_paa_windows/
[6] https://www.nemid.nu/dk-da/kom_i_gang_med_nemid/sikker_e-mail/send_og_modtag_sikker_e-mail/opsaetning_af_e-mail-program/windows_8/outlook_2013/
[7] https://www.nemid.nu/dk-da/kom_i_gang_med_nemid/sikker_e-mail/send_og_modtag_sikker_e-mail/

Der er på nuværende tidspunkt ingen juridisk afklarede udmeldinger i forhold til, om forbrugsdata – i et eller andet omfang – kan fremsendes via ukrypteret e-mail til eksterne folk uden for forsyningen.

Med "risiko" for at overimplementere persondatareglerne tilsiger et forsigtighedsprincip, at kunders data omgås med stor varsomhed – og at forsyningerne arbejder for, at personhenførbare data videreformidles via beskyttede kanaler.
Det er således DANVAs bedste vurdering, at en konkret kundes forbrugsdata/faktura er der ikke generel aktindsigt i, da der vil kunne gives afslag efter såvel vandsektorlovens § 14. 1 (dataudtræk) og offentlighedslovens § 30 (private forhold). Udmeldinger om begrebet fortrolighed fra Datatilsynet, hvor der refereres til begrebet fortrolighed i straffeloven og forvaltningsloven – der igen viser mod offentlighedslovens § 30, indikerer, at en kundes forbrugsdata/faktura er omfattet af begrebet fortrolighed, som fortolket af Datatilsynet.

Dette peger i retning af, at hvis en forsyning på lovlig vis har e-mailadressen til kunden og ønsker at sende sådanne data, så bør der ske en kryptering.

Det er dog DANVAs bedste vurdering, at det i dag ikke er en realistisk, generel løsning at anvende kryptering af e-mails som en sikker måde at behandle persondata på. Anbefalingen er at bruge mere centraliserede løsninger over enten PBS, e-Boks eller kundeportaler – og en "nødløsning" kan være brevpost. Dette lægger op til, at forsyningen italesætter sikkerhed over for kunderne.

Susanne Vangsgård med sparring fra Jes Eriksen
DANVAs IT-netværk har ligeledes givet deres bidrag.

Kilder:
Datatilsynets udtalelsen, 2018
https://www.**datatilsynet**.dk/presse-og-nyheder/nyhedsarkiv/2018/jul/skaerpet-praksis-ift-krypteret-e-mail/

Vejledning, 2018: Behandlingssikkerhed Databeskyttelse gennem design og standardindstillinger
https://www.datatilsynet.dk/media/6879/artikel25og32-vejledning.pdf

Tekst om sikkerhed ved transmission af personoplysninger via e-mail
https://www.datatilsynet.dk/emner/persondatasikkerhed/transmission-af-personoplysninger-via-e-mail/

Tekst om fortrolige personoplysninger
https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/

Persondataforordningen, 2016/679
https://eur-lex.europa.eu/legal-content/da/TXT/?uri=CELEX:32016R0679

Offentlighedslovens §30.1
https://aktindsigtshaandbogen.dk/aktindsigt-trin-for-trin/undtagelser-fra-aktindsigt/undtagelse-af-oplysninger/enkeltpersoners-private-forhold-30-nr-1/

Datatilsynet om personoplysninger og fortrolighed
https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/

Presse omkring samkøring af el-data og bopæl
https://fagbladet3f.dk/artikel/minister-opgiver-overvaage-borgeres-elforbrug