Forslag til endring i forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv.

Endringer om sikkerhet for avanserte måle- og styringssystem (AMS)

Øyvind Anders Arntzen Toftegaard og Hanne Alette Hillestad

1
2018

HØRINGSDOKUMENT

Høringsdokument nr 1-2018
Forslag til endring i forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv.

Utgitt av: Norges vassdrags- og energidirektorat

Redaktør: Guro Grøtterud

Forfattere: Øyvind A. Arntzen Toftegaard og Hanne Alette Hillestad

Trykk: NVEs hustrykkeri
Opplag: 20
Forsidefoto: NVE v/Arnt E. Bjøru
ISBN 978-82-410-1657-8
ISSN 1501-2840

Sammendrag: Teknologien i digitale informasjons- og kommunikasjonssystemer er i stadig utvikling, og sikkerhetsrisikoen knyttet til slike systemer endrer seg over tid. NVE har derfor sett behov for å oppdatere og tydeliggjøre kravene til sikkerhet i AMS. Endringene som er foreslått omfatter i hovedtrekk nye definisjoner av AMS og brytefunksjonalitet, mindre endringer i krav til funksjonalitet, ny bestemmelse om krav til sikkerhet i AMS og overtredelsesgebyr ved brudd på sikkerhetsbestemmelsen.

Emneord: Avanserte måle- og styringssystemer, AMS, IKT-sikkerhet, brytefunksjonalitet, regulering, måleverdier

Norges vassdrags- og energidirektorat
Middelthunsgate 29
Postboks 5091 Majorstua
0301 OSLO

Telefon: 22 95 95 95
Internett: www.nve.no

Innhold

Forord

Norges vassdrags- og energidirektorat (NVE) sender med dette på høring forslag til bestemmelser og endringer i forskrift av 11. mars 1999 nr. 301 om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettjenester (heretter forkortet avregningsforskriften). Formålet er å tydeliggjøre hvilke krav som stilles til sikkerhet i avanserte måle- og styringssystemer (AMS). Samtidig er kravene oppdatert i samsvar med utviklingen innen sikkerhetsteknologi, virksomhetenes organisering og annet regelverk. Forslaget er utarbeidet og høres i henhold til bestemmelsene i forvaltningsloven kapittel VII, jf. også utredningsinstruksen.

Vi ber om at kommentarer til dette forslaget sendes til NVE senest 21. mai 2018. Elektronisk oversendelse til nve@nve.no foretrekkes. Vi gjør oppmerksom på at høringsuttalelser normalt publiseres.

Etter høringsfristen vil NVE vurdere de innkomne høringsuttalelsene og eventuelle behov for å gjøre endringer i forslaget. Det tas sikte på at forskriften vedtas i august 2018, og at forskriften vil tre i kraft fra 1. januar 2019.

Oslo, februar 2018

Per Sanderud
vassdrags- og
energidirektør

Ove Flataker
avdelingsdirektør

1. Innledning

Den 24. juni 2011 vedtok NVE at installering av AMS, inkludert utrulling av digitale elektrisitetsmålere, skulle gjennomføres. Nettselskapene skal ha installert AMS i alle målepunkt innen 1. januar 2019. Det er stilt krav til funksjonaliteten[1] til AMS, inkludert generelle krav til sikkerhet. NVE foreslår nå endringer for å stille tydeligere krav til hva plikten til å sikre AMS innebærer.

Endringsforslagene omfatter bestemmelser i kapittel 1, 4 og 9. NVE har gjort en vurdering av administrative og økonomiske konsekvenser knyttet til forslagene. For at det skal være enkelt å se hvilke endringer vi foreslår, er forslag til nye bestemmelser og ny tekst ved endring av bestemmelser, satt i kursiv. Tekst som utgår ved endring av bestemmelser, er overstrøket.

NVE er delegert forskriftskompetanse etter energiloven § 10-6 og energilovforskriften § 9-1. De foreslåtte bestemmelsene og endringene gjelder sikkerhet i tilknytning til måling og avregning. NVE har derfor hjemmel i energilovforskriften § 9-1 bokstav i til å vedta de foreslåtte endringene.

I denne forbindelse bemerker vi at Stortinget per dags dato behandler proposisjon 5 L (2017-2018) på bakgrunn av implementering av EUs tredje energimarkedspakke. Det er foreslått at deler av reguleringsmyndigheten legges til Reguleringsmyndighet for energi (RME), som egen enhet. Da proposisjonen ikke har blitt behandlet, er formelt sett NVE riktig myndighet for foreliggende endringsforslag. Vi gjør likevel oppmerksom på at dersom, og eventuelt når, proposisjonen vedtas, vil trolig RME bli riktig vedtaksmyndighet for endringsforslagene i avregningsforskriften.

1.1. Bakgrunn

NVE publiserte i 2012 en veileder til sikkerhet i AMS som skal hjelpe nettselskapene med å oppfylle de krav til sikkerhet som følger av gjeldende § 4-2 bokstav g i avregningsforskriften. Høsten 2016 foretok SINTEF Energi AS (SINTEF) en gjennomgang av denne veilederen på oppdrag fra NVE.[2] Målet med oppdraget var blant annet å evaluere sikkerhetskravene i veilederen, vurdere nye problemstillinger, og gi anbefalinger til forbedringer av innholdet i veilederen.[3] Det fremkommer i rapporten at det er behov for å stille tydeligere krav til sikkerhet i AMS, blant annet knyttet til innebygd sikkerhet og sikkerhetstesting. SINTEF viser også til viktigheten av at forskriftskrav ikke hindrer nettselskapenes innhenting av nettnyttedata[4].

I tillegg gjennomgikk NVE eget regelverk på IKT-sikkerhet i løpet av høsten 2016 og våren 2017.[5] Målet med gjennomgangen var å vurdere behovet for endringer i regelverket for IKT-sikkerhet i energiforsyningen. Vi konkluderte med at det var behov for mer spesifikk regulering av sikkerhet for AMS. Særlig så NVE behov for å stille krav til beskyttelse av brytefunksjonaliteten. Av hensyn til sikkerhet foreslo vi i tillegg å oppheve visse krav til funksjonalitet i AMS, se punkt 2.3.1.

[1] Funksjonalitet forteller noe om hva et produkt kan gjøre.
[2] NVE Rapport 44/2017: Evaluering av NVEs veileder til sikkerhet i AMS.
[3] Les mer om rapporten og arbeidet på NVEs nettsider: https://www.nve.no/nytt-fra-nve/nyheter-elmarkedstilsyn/evaluering-av-nves-veileder-til-sikkerhet-i-ams/.
[4] Med nettnyttedata menes her informasjon fra sensorer i AMS som samles inn fordi informasjonen kan ha nytteverdi for kraftnettet.
[5] NVE Rapport 26/2017: Regulering av IKT-sikkerhet.

1.2. Rettslig utgangspunkt

AMS er et informasjonssystem som i likhet med andre informasjonssystemer må sikres mot uønskede hendelser. Informasjonssikkerhet handler om konfidensialitet[6], integritet[7] og tilgjengelighet[8]. Formålet med å sikre AMS i avregningsforskriften er å få en helhetlig beskyttelse av måleverdikjeden, og da spesielt måleverdier[9]. Sikring av konfidensialitet, integritet og tilgjengelighet av måleverdier har vært utgangspunktet ved utforming av sikkerhetskrav til AMS. Det er viktig å beskytte både AMS som system, og informasjonen som behandles i systemet. Beskyttelse av AMS er nødvendig for at det potensialet AMS åpner opp for, nemlig effektiv drift av nettet og riktig avregning og fakturering, utnyttes fullt ut.

Der konfidensialitet, integritet eller tilgjengelighet sikres tilstrekkelig gjennom annet regelverk, er det ikke nødvendig å stille ytterligere krav. På denne måten unngår vi dobbeltregulering. Vi viser til en nærmere redegjørelse av annet regelverk under punkt 1.3.

1.3. Relevant regelverk

Under følger en liste over gjeldende og foreslått regelverk av relevans for sikkerhet i AMS. Listen er ikke uttømmende. Regelverk som kun er foreslått, vil kunne bli endret før ikrafttredelse. NVE vurderer likevel at eventuelle materielle endringer i foreslått eller gjeldende regelverk, trolig ikke vil berøre de endringene som nå foreslås i avregningsforskriften.

1.3.1. Beredskapsforskriften

I løpet av høsten 2017 startet en revidering av forskrift av 7. desember 2012 nr. 1157 om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften). NVE sendte forslag til endringer på høring i desember 2017.[10]

Et tydelig skille mellom regulering av AMS-sikkerhet i beredskapsforskriften og avregningsforskriften, var sentralt i dette arbeidet. Gjeldende beredskapsforskrift stiller krav til varsling av sikkerhetshendelser i AMS og regulerer eventuell integrasjon mellom AMS og driftskontrollsystemer. I revidert versjon er det foreslått bestemmelser som stiller krav til et minimums sikkerhetsnivå gjennom grunnsikring av IKT-systemer. Kravene til grunnsikring fremgår av beredskapsforskriften § 6-9 og inkluderer AMS. Det er i forslaget stilt krav som ivaretar konfidensialitet, integritet og tilgjengelighet. I tillegg er det inkludert beskyttelse av brytefunksjonaliteten i AMS i revidert versjon av forskriften § 6-10.[11]

1.3.2. Personvern

Lov om behandling av personopplysninger (personopplysningsloven) av 14. april 2000 nr. 31 og forskrift om behandling av personopplysninger (personopplysningsforskriften) av 15. desember 2000 nr. 1265 stiller krav til sikring av personopplysninger. General Data Protection Regulation (heretter forkortet GDPR)[12] som stiller nye krav til behandling og sikring av personopplysninger, trer i kraft i EU 25. mai

---

[6] Konfidensialitet handler om å beskytte informasjon mot at uønskede får tilgang til den.
[7] Integritet handler om hvorvidt en kan stole på at informasjon er korrekt (at den ikke uønsket har blitt endret).
[8] Tilgjengelighet handler om i hvilken grad informasjon er tilgjengelig for rettmessige brukere når de trenger det.
[9] Med måleverdier menes her målt strømforbruk i sluttbrukers målepunkt i AMS-måler.
[10] NVE Høringsdokument 6/2017: Forslag til endringer i beredskapsforskriften.
[11] Les mer om høringsforslaget på https://www.nve.no/om-nve/regelverk/lov-og-forskriftsendringer-pa-horing-ikke-konsesjonssaker/horing-endringer-i-regelverket-for-beredskap-i-energiforsyningen/.
[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1518982762991&from=EN.

2018. Forordningen er ansett som EØS-relevant, og vil derfor nødvendigvis medføre endringer i personopplysningsloven.

Måleverdier gir opplysninger om strømforbruket til personer som bor i boligen måleverdiene er knyttet til. Datatilsynet har uttalt at personopplysningsloven stiller krav til hvordan slike data skal behandles og sikres. Nettnyttedata som på tilsvarende vis kan si noe om hva enkeltpersoner gjør i hjemmet, vil også falle inn under definisjonen av personopplysninger. Det følger av GDPR at personopplysninger skal sikres slik at blant annet konfidensialitet, integritet og tilgjengelighet ivaretas.

NVEs formål med å sikre opplysninger i AMS er ikke å sikre personopplysninger. NVEs formål er å sikre avregningen og måleverdikjeden. Regler om sikkerhet i AMS vil likevel dekke flere krav som stilles til sikring av personopplysninger. Vi understreker at NVE ikke har foretatt en vurdering av om kravene som vi foreslår også oppfyller kravene i GDPR. Det er den enkelte virksomhet og Datatilsynet som er ansvarlig for å følge opp personvernregelverket.

1.3.3. Krav til elektrisitetsmålere

Forskrift av 20. desember 2007 nr. 1723 om målenheter og måling stiller krav til måleredskaper og målinger, jf. forskriften § 1. Forskrift av 28. desember 2007 nr. 1753 om krav til elektrisitetsmålere (heretter forkortet elmålerforskriften) fastsetter mer spesifikke krav for elektrisitetsmålere[13], jf. forskriften § 1. Forskriftene implementerer krav til måleinstrumenter etter direktiv 2014/32/EU om harmonisering av medlemslandenes lovgivning om markedsføring av måleinstrumenter, som erstattet direktiv 2004/22/EC om måleinstrumenter.

Målerne skal beskyttes mot manipulering og feil, slik at berørte parter har tillit til at måledata er korrekt, jf. elmålerforskriften §§ 3 og 19. Blant annet skal komponenter og programvare med avgjørende betydning for målerens måletekniske egenskaper, sikres. Videre kreves det at måledata som lagres eller overføres, skal være beskyttet på hensiktsmessig vis mot endringer. NVE forstår dette slik at data som overføres fra AMS-måleren til nettselskapets sentralsystem, skal beskyttes. Det er nettselskapene som er ansvarlig for at forskriftens bestemmelser er oppfylt.

NVE vurderer at elmålerforskriften i tilstrekkelig grad stiller krav til beskyttelse mot manipulering av måleverdier i AMS i svindeløyemed. Slik svindel kan være at uvedkommende påvirker måleren slik at den registrerer et lavere strømforbruk enn hva som er reelt, eller kobler seg på kommunikasjonsinfrastrukturen i AMS for å sende falske måleverdier til sentralsystemet. NVE anser det ikke nødvendig å stille ytterligere krav til beskyttelse mot manipulering av måleverdier i AMS. Det er Justervesenet som er ansvarlig for å følge opp krav i forskriftene.

1.3.4. Annet EU-regelverk

EU har fokus på utvikling av sikkerhetsregelverk. Ulike forslag og regelverk kan ha betydning for sikring av AMS.

<u>Elmarkedsdirektivet</u>

Av sist oppdatert posisjon fra Rådet av 20. desember 2017 til revidert direktiv om felles regler for det indre marked for elektrisitet (heretter forkortet Elmarkedsdirektivet[14]) Art. 20 bokstav b, følger det at

[13] Elmålerforskriften § 2 bokstav a definerer elektrisitetsmåler som en innretning som måler aktiv elektrisk energi som forbrukes i en krets, herunder måler som i tillegg måler reaktiv elektrisk energi. Målere som bare måler reaktiv energi omfattes ikke av definisjonen i forskriften.

[14] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on common rules for the internal market in electricity (recast), saksnr. 2016/0380, dokumentnr. 15886/17: http://data.consilium.europa.eu/doc/document/ST-15886-2017-INIT/en/pdf.

AMS skal være sikret i tråd med annet europeisk sikkerhetsregelverk, og at man skal sikre høyeste grad av cybersikkerhet.[15] Videre følger det av bokstav c at personvern skal sikres.[16] Det er opp til medlemslandene å spesifisere i sitt nasjonale regelverk, krav som sikrer oppfyllelse av dette sikkerhetsnivået[17].

Videre er "smart metering system" foreslått definert i Art. 2 punkt 18, til … an electronic system that can measure energy consumption or the amount of electricity put into the grid, providing more information than a conventional meter, and can transmit and receive data for information, monitoring and control purposes, using a form of electronic communication …" Denne definisjonen vurderes nærmere under punkt 2.2.1.

Cybersecurity Act og Grensehandelforordningen

Det er foreslått en forordning om cybersikkerhetssertifisering av informasjons- og kommunikasjonsteknologi (Cybersecurity Act[18]), som legger opp til utvikling av felles sikkerhetssertifiseringsordninger. Dette betyr at det på europeisk nivå kan bli utviklet en felles rutine for sertifisering også for AMS. Det synes å være frivillig om medlemslandene ønsker å sertifisere, men dersom man først har en sertifiseringsordning er det obligatorisk å bruke den europeiske løsningen.

I tillegg er det i sist oppdatert posisjon fra Rådet av 20. desember 2017 til revidert forordning om det indre marked for elektrisitet (forkortet Grensehandelforordningen[19]) Art. 55 nr. 1 bokstav o, foreslått en nettkode på cybersecurity. En slik nettkode kan få betydning for sikkerhetskrav til AMS, men fordi det ennå ikke er avklart om en slik nettkode skal utarbeides eller hva innholdet vil være, kan vi ikke ta hensyn til dette på nåværende tidspunkt.

Videre er det foreslått å opprette en EU DSO Entity blant nettselskapene, som blant annet skal ha ansvar for cybersikkerhet og databeskyttelse.[20] Det er per dags dato usikkert hva dette ansvaret innebærer, og om det vil påvirke krav til sikkerhet i AMS.

NIS-direktivet

Direktiv 2016/1148 om tiltak for et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU (heretter forkortet NIS-direktivet[21]) stiller krav til at medlemslandene sikrer sine IKT-systemer på et

---

[15] "Where smart metering is positively assessed as a result of cost-benefit assessment referred to in Article 19(2), or systematically rolled out, Member States shall implement smart metering systems in accordance with … the following principles: … (b) the security of the smart metering systems and data communication is ensured in compliance with relevant Union security legislation having due regard of the best available techniques for ensuring the highest level of cybersecurity protection whilst bearing in mind the costs and principles of proportionality…"

[16] "… (c) the privacy and data protection of final customers is ensured in compliance with relevant Union data protection and privacy legislation …"

[17] Smart-Grid Task Force Stakeholder Forum publiserte i 2016 en "Best Available Techniques Analysis" som kan brukes for å få et bedre overblikk om hva som menes med dette kravet: https://ec.europa.eu/energy/sites/ener/files/documents/bat_wp3_bat_analysis.pdf.

[18] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") COM(2017) 477: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0477R(01)&from=DA.

[19] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the internal market for electricity (recast) saksnr. 2016/0379, dokumentnr. 15879/17: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the internal market for electricity (recast).

[20] Jf. forordningens Art. 51: «1. The tasks of the EU DSO entity shall be the following: … (e) data management, cyber security and data protection; …»

[21] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures for a high common level of security: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&qid=1516095255417&from=EN.

minimumsnivå. Medlemslandene er blant annet forpliktet til å utvikle en nasjonal sikkerhetsstrategi for IKT-systemer, opprette responsmiljøer og samarbeidsgrupper mellom disse, og utvikle systemer for nettverks- og informasjonssikkerhet hos operatører av essensielle tjenester og digitale tjenesteytere.[22]

NIS-direktivet Art. 14 og 16 stiller krav til at leverandører av essensielle tjenester og digitale tjenesteytere skal etablere tekniske og organisatoriske sikkerhetstiltak. Direktivet har en risikobasert tilnærming, og har i utgangspunktet et overordnet fokus på hendelseshåndtering og varslingsplikt om IKT-hendelser gjennom responsmiljøene.[23] Samtidig krever direktivet at medlemsland påser at tjenesteytere etablerer både forebyggende og skadebegrensende sikkerhetstiltak. Videre oppfordrer direktivet i Art. 19 til bruk av europeiske eller andre internasjonale sikkerhetsstandarder og -spesifikasjoner. Per dags dato er det usikkert hvordan dette regelverket vil bli implementert i Norge, og eventuelt hvilken betydning det vil få for sikkerhet i AMS.

Beredskap i elektrisitetssektoren

Det er foreslått en forordning om beredskap i elektrisitetssektoren som er ment å dekke forebygging og håndtering av kriser i elektrisitetssektoren.[24] Blant annet stiller forordningen krav om at det skal foretas risikovurdering av ondsinnede angrep. Forordningen synes derfor mest relevant for forsyningssikkerhet, som reguleres i beredskapsforskriften.

1.4. Avgrensning av forslaget

Måleverdikjeden omfatter hele den måletekniske verdikjeden, fra de elektriske målerne til oversendelse av disse dataene til Elhub, jf. avregningsforskriften § 3-10. AMS er bare en del av denne kjeden, og omfatter systemet fra og med elektrisitetsmåleren, til og med nettselskapets sentralsystem, inkludert kommunikasjonsdelen mellom disse. Vi har vurdert om det er tilstrekkelig å kun sikre AMS, eller om det også er behov for å sikre infrastrukturen som overfører måleverdier videre fra nettselskapets sentralsystem til Elhub.

Nettselskapet vil kunne innhente både måleverdier og nettnyttedata ved bruk av AMS. Det er imidlertid kun måleverdier som sendes videre i måleverdikjeden fra nettselskapet til Elhub. Måleverdier som tilhører husholdningskunder vurderes som personopplysninger. Nettselskapene må i henhold til personvernregelverket etablere tiltak for å sikre at disse måleverdiene kun er tilgjengelig for dem de er tiltenkt, at måleverdiene er riktige, og at de er tilgjengelig når det er behov for dem.

For måleverdier som tilhører næringskunder, er sikkerhetsregelverket noe mer fragmentert. Krav til tilgjengelighet følger av avregningsforskriften § 6-17, som trer i kraft fra den tid NVE bestemmer, hvor måleverdier skal være tilgjengelig innen kl. 9 første kalenderdag etter driftsdøgnet. For kraftsensitiv informasjon etter beredskapsforskriften § 6-2, stilles det krav om konfidensialitet.

I beredskapsforskriften er det også foreslått endringer i § 6-9 som stiller krav til grunnsikring av informasjonssystemer. Dette inkluderer nettselskapets informasjonssystem for overføring av måleverdier til Elhub. Samtidig stiller avregningsforskriften § 6-21, som trer i kraft fra den tid NVE bestemmer, blant

[22] NIS-direktivet Art. 1. For mer informasjon: http://www.europalov.no/rettsakt/tiltak-for-nettverks-og-informasjonssikkerhet/id-6118.
[23] Computer security incident response teams (CSIRTs), jf. NIS-direktivet Art. 9.
[24] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on risk-preparednedd in the electricity sector and repealing Directive 2005/89/EC, COM(2016) 862: https://ec.europa.eu/energy/sites/ener/files/documents/1_en_act_part1_v7.pdf.

annet krav til at Statnett som avregningsansvarlig skal sørge for at all informasjonsutveksling i henhold til Ediel[25] er kryptert. Dette betyr at nettselskapets utgående kommunikasjon må sikres, samtidig som Statnett må påse at meldinger de mottar i Elhub er kryptert.

Det foreligger derfor sikkerhetskrav ved overføring mellom nettselskapets sentralsystem og Elhub som ivaretar konfidensialitet, integritet og tilgjengelighet. Samtidig er disse IKT-systemenes kompleksitetsnivå lavere enn for AMS, og kommunikasjonen er hovedsakelig begrenset til overføring av måleverdier. Etter NVEs vurdering ivaretar gjeldende og foreslått regelverk et tilstrekkelig sikkerhetsnivå for den resterende delen av måleverdikjeden som ikke er del av AMS.

I tillegg til at AMS-målerne kommuniserer til nettselskapet, er det lagt til rette for annen funksjonalitet mot kunden. For eksempel skal andre type målere kunne kobles til, og kommunisere gjennom, AMS-målere. AMS-målere skal også ha grensesnitt for å sende måleverdier lokalt til sluttbruker (HAN-port). NVE anser selve grensesnittet hvor eksternt utstyr kobles til AMS, som del av AMS. Samtidig vil tilkoblet utstyr verken regnes som del av måleverdikjeden eller AMS. Selv om slik tilkobling kan ha betydning for sikkerheten i AMS, har eierne av de tilkoblede enhetene selv ansvaret for sikkerheten i disse enhetene. Nettselskapet må i stedet påse at AMS beskyttes mot slike tilkoblede enheter, og at sikkerheten ikke forringes ved tilkobling av eksterne enheter. Les mer under punkt 2.4.1.

[25] Ediel: Standard for elektronisk kommunikasjon som kraftbransjen er pålagt å benytte for meldinger, jf. avregningsforskriften § 1-4.

2. Forslag til forskriftsendringer

2.2. Endring i § 1-3. Definisjoner

2.2.1. Bakgrunn

NVE er kjent med at nettselskap har lagt inn AMS-funksjonalitet i systemer de har definert som utenfor AMS. Vi ser det også som sannsynlig at flere tredjepartstjenester med kobling mot AMS vil tilbys i markedet i fremtiden. Det er derfor behov for å definere AMS, også for å avklare grensene for nettselskapets forpliktelser. Det vil stilles krav til at tilkoblede systemer som ikke er del av AMS, for eksempel driftskontrollsystem (SCADA) og kundesystem (KIS), ikke skal forringe sikkerheten i AMS, se punkt 2.4.1.

For å oppnå en praktisk og anvendbar definisjon av AMS, har NVE valgt en teknisk innfallsvinkel. Alternativet hadde vært en formålsrettet definisjon som forklarer hva AMS brukes til. Sist oppdatert posisjon fra Rådet til revidert Elmarkedsdirektiv har i Art. 2 punkt 18 valgt en formålsrettet definisjon, se punkt 1.3.4. Vi mener en slik definisjon i praksis blir både vanskeligere å etterleve, og å føre tilsyn med.

AMS består av kommuniserende elektrisitetsmålere, nettselskapets sentralsystem som blant annet samler inn måleverdier, og et toveis kommunikasjonssystem mellom disse enhetene. Vi viser til definisjonen av elektrisitetsmåler i elmålerforskriften § 2 bokstav a. Den foreslåtte definisjonen av AMS betyr at målere uten kommunikasjonsegenskaper, eller målere som kun kan kommunisere én vei, vil falle utenom definisjonen. Dette betyr også at nettselskap må oppgradere til toveiskommuniserende målere i de målepunkt hvor AMS skal installeres. Uavhengig om måleren er plassert eksempelvis hjemme hos en forbruker, hos en næringskunde, eller i tilknytning til avregning mellom to områder, vil systemet som installeres defineres som AMS, så lenge det oppfyller kravene i definisjonen. Det presiseres at målere i nettet som ikke benyttes til avregningsformål, for eksempel målere på nettstasjoner som utelukkende benyttes med det formål å overvåke status i nettet, ikke omfattes av definisjonen av AMS.

NVE er kjent med at flere nettselskap kjøper tjenester av leverandører, som betyr at hele eller deler av sentralsystemet kan være plassert og driftet hos leverandør, eller hos en av leverandørens leverandører. Uavhengig av hvor sentralsystemet er plassert og driftet, er nettselskapets sentralsystem del av AMS, og skal sikres på samme nivå som resten av systemet.

NVE har også sett et behov for å definere brytefunksjonalitet. Brytefunksjonalitet omfatter alle løsninger som kan benyttes for å fjernstyre inn- og utkobling av strømuttaket i målepunktet til AMS-målere. Dette inkluderer løsninger som utnytter brytefunksjonaliteten for å begrense effekt- eller energiuttak i målepunktet, ettersom slike løsninger vil kunne gi tilgang til å styre eller manipulere brytefunksjonaliteten.

2.2.2. Forslag til to nye definisjoner i § 1-3

§ 1-3. Definisjoner

Avanserte måle- og styringssystem (AMS): Toveis informasjons- og kommunikasjonssystem fra og med elektrisitetsmålere benyttet til avregning for de enkelte målepunkt, til og med sentralsystemet hos nettselskap eller nettselskapets leverandør.

Brytefunksjonalitet: System for fjernstyrt inn- og utkobling av strømuttaket i målepunktet til AMS-målere.

2.2.3. Økonomiske og administrative konsekvenser

Med definisjonen av AMS er det et ønske om å tydeliggjøre den forståelsen av begrepet som allerede har vært lagt til grunn i praksis. Det følger av avregningsforskriften § 4-1, som trer i kraft fra 1. januar 2019, at nettselskap skal installere AMS i alle målepunkt. Når AMS nå defineres, kan det stilles spørsmål ved om plikten til å installere AMS utvides. Det vil kunne medføre en større økonomisk byrde for nettselskapene dersom de må oppgradere og bytte ut et økt antall målere. NVE viser til at definisjonen i seg selv ikke medfører en utvidet plikt for nettselskapene. Det er §§ 4-1 og 4-5 som forplikter nettselskapene til å installere AMS i deres konsesjonsområde, og denne plikten er uforandret. NVE bemerker at bestemmelsene også åpner for at det i særlige tilfeller kan gis dispensasjon fra plikten til å installere AMS. NVE vurderer derfor at definisjonen av AMS ikke vil medføre økonomiske eller administrative konsekvenser. Samtidig bemerker vi at installering av toveis kommunikasjon mellom måler og sentralsystem må ansees som en helhetlig modernisering som skal sikre mer effektiv drift av nettet.

NVE vurderer også at definisjonen av brytefunksjonalitet ikke medfører økonomiske og administrative konsekvenser.

2.3. Endring i § 4-2. Funksjonskrav

2.3.1. Bakgrunn

Vi foreslår å endre overskriften for å klargjøre at bestemmelsen regulerer krav til funksjonalitet, det vil si egenskaper AMS skal ha. Dette har ingen materielle konsekvenser. I tillegg foreslår vi å legge inn en presisering av at nettselskapet er ansvarlig for at AMS har disse funksjonalitetene.

I avregningsforskriften er det ikke differensiert mellom elektrisitetsmålere for ulike typer målepunkt, og hvilken funksjonalitet de skal ha. Både elektrisitetsmålere brukt til avregning i lavspentnettet og høyspentnettet, uavhengig av om de er tilknyttet sluttbruk, produksjon eller utveksling, omfattes av den foreslåtte definisjonen av AMS i § 1-3.

Avregningsforskriften § 4-1, som trer i kraft fra 1. januar 2019, og § 4-5 stiller krav om installering av AMS i alle målepunkt. En problemstilling er om nettselskapet er forpliktet til å installere AMS-målere med funksjonalitetene listet opp i § 4-2 i alle målepunkt brukt for avregning, uavhengig av hvor målepunktet er plassert. Ordlyden taler for at plikten til å installere AMS hverken avhenger av om målepunktet er plassert i høyspent- eller lavspentnettet, eller om det er knyttet til sluttbruk, produksjon eller utveksling. NVE har likevel i vår oppfølging av utrullingen av AMS fokusert på sluttbrukere. Det synes i tillegg av merknadene til forskriftsendringene, at NVEs intensjon var å sikre installasjon av AMS i målepunkt hos sluttbrukere. Dette kan derfor tolkes dithen at det kun var AMS-målere i målepunkt hos sluttbruker som var ment å oppfylle kravene til funksjonalitet i § 4-2.

Statnett som systemansvarlig har vist til at det vil være nyttig for driften av kraftsystemet å innføre en avregningsperiode på 15 minutter. Det synes også at de andre nordiske systemansvarlige er enige i at 15 minutters avregningsperiode bør innføres, med tilsvarende endring av oppløsning i balansemarkedet. Dersom kommisjonsforordningen 2017/2195 om retningslinjer for balansering av elkraftsystemet[26] innlemmes i norsk rett, vil det i tillegg kunne forplikte NVE til å innføre en avregningsperiode på 15 minutter innen utgangen av 2020. Med bakgrunn i dette har NVE startet å vurdere konsekvenser av en

[26] COMMISSION REGULATION (EU) 2017/2195 of 23 November 2017 establishing a guideline on electricity balancing: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R2195&from=EN.

eventuell innføring av en avregningsperiode på 15 minutter, og behov for forskriftsendringer. Dette arbeidet er planlagt ferdigstilt i løpet av 2018. Foreløpige vurderinger tilsier at dersom 15 minutters avregningsperiode skal innføres i Norge, vil det trolig være nødvendig at alle målere tilknyttet større sluttbruk, produksjon og utveksling, må kunne lagre måleverdier med en registreringsfrekvens på 15 minutter.

I dag er et av funksjonalitetskravene til AMS-målere at de skal kunne stilles om til å registrere målinger hvert 15. minutt, jf. § 4-2 bokstav a. Sett i sammenheng med at AMS-målere skal installeres i alle målepunkt, kan dette forstås dithen at alle elektrisitetsmålere plassert i målepunkt brukt for avregning, skal kunne stilles om til å registrere målinger hvert 15. minutt. I lys av at NVE i oppfølgingen av AMS-utrullingen har hatt fokus på målere for sluttbrukere, samt merknader til forskriftsendringene, anerkjenner NVE at det kan være noe ulik praksis blant nettselskapene knyttet til kravene til funksjonalitet til elektrisitetsmålere for produksjon og utveksling. I tillegg anerkjenner NVE at det er noe usikkerhet knyttet til nettselskapenes forståelse av gjeldende funksjonalitetskrav for elektrisitetsmålere knyttet til sluttbrukere på høyere nettnivåer. Eksempelvis om slike elektrisitetsmålere kan stilles om til å lagre måleverdier med en registreringsfrekvens på minimum 15 minutter.

Som del av NVEs vurdering av nødvendige tilpasninger ved innføring av 15 minutters avregningsperiode, vil NVE kartlegge nettselskapenes praktisering av funksjonalitetskravet til å kunne omstille til en registreringsfrekvens på minimum 15 minutter for ulike typer målepunkt, som produksjon, utveksling og sluttbruk på høyere nettnivåer. Dersom NVE avdekker behov for å presisere kravene til funksjonalitet for målere i ulike typer målepunkt, vil NVE påse at bransjen blir gitt nødvendig tid til å omstille seg endringene.

NVE presiserer imidlertid at den foreslåtte definisjonen i avregningsforskriften ikke er ment å pålegge nettselskapene ytterligere forpliktelser enn de har i dag, med hensyn til installering og krav til AMS-målernes funksjonalitet.

NVE foreslår å oppheve sikkerhetskravene i § 4-2, da de dekkes i ny § 4-2a. Dagens § 4-2 bokstav d om å sikre at lagrede data ikke går tapt ved spenningsavbrudd, dekkes av krav til tilgjengelighet som del av grunnsikring, jf. forslagets § 4-2a annet ledd annet punktum. Gjeldende § 4-2 bokstav g om krav til sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner, dekkes av det generelle kravet til sikring i ny § 4-2a annet ledd første punktum. Som konsekvens av at to bokstaver flyttes ut av § 4-2, vil rekkefølgen forskyves. Dette har ingen materielle konsekvenser, inkludert for dispensasjoner som er gitt fra visse funksjonalitetskrav.

I NVEs Rapport 26/2017[27], hvor vi gjennomgikk vårt eget regelverk på IKT-sikkerhet, ble det foreslått å oppheve § 4-2 bokstav f og § 4-4 annet ledd i avregningsforskriften. Dagens § 4-2 bokstav f stiller krav om at AMS skal kunne sende og motta informasjon om kraftpriser og tariffer, mens § 4-4 annet ledd, som trer i kraft fra 1. januar 2019, sier at kraftleverandør og nettselskapet skal kunne sende henholdsvis prisinformasjon og tariffinformasjon til displayet. Grunnen til at disse bestemmelsene ble foreslått slettet, var at det ville være enklere og sikrere å sende tariffinformasjon over kundens egen internettkobling. Jo mer funksjonalitet AMS har, jo mer utsatt vil systemet være for risiko.

Per dags dato er det imidlertid usikkert hvilken løsning som mest effektivt sikrer sluttbrukere tilgang på prisinformasjon. Smart Grid Task Force Stakeholder Forum[28] anbefaler at AMS støtter avanserte

[27] NVE Rapport 26/2017: Regulering av IKT-sikkerhet.
[28] Smart Grid Task Force ble etablert av EU-kommisjonen i 2009 for å gi råd om temaer relatert til etablering av smart grid.

tariffsystemer.[29] NVE vurderer at enkleste måte å etablere slike systemer på, potensielt kan være med en felles kommunikasjonskanal gjennom AMS. Derfor velger vi å beholde § 4-2 bokstav f og § 4-4 annet ledd slik de står. Det er også foreslått at sikkerheten skal opprettholdes eller bedres ved tilkobling av tredjeparter, som inkluderer kraftleverandører i denne type tilfeller, jf. nytt krav i § 4-2a tredje ledd.

2.3.2. Forslag til endring av § 4-2

§ 4-2. ~~Funksjonskrav~~ *Krav til funksjonalitet*

Nettselskapet er ansvarlig for at AMS skal:

a) lagre måleverdier med en registreringsfrekvens på maksimalt 60 minutter, og kunne stilles om til en registreringsfrekvens på minimum 15 minutter,

b) ha et standardisert grensesnitt som legger til rette for kommunikasjon med eksternt utstyr basert på åpne standarder,

c) kunne tilknyttes og kommunisere med andre typer målere,

~~d) sikre at lagrede data ikke går tapt ved spenningsavbrudd,~~

d) ~~e)~~ kunne bryte og begrense effektuttaket i det enkelte målepunkt, unntatt trafomålte anlegg,

e) ~~f)~~ kunne sende og motta informasjon om kraftpriser og tariffer samt kunne overføre styrings- og jordfeilsignal, og

~~g) gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner og~~

f) ~~h)~~ registrere flyt av aktiv og reaktiv effekt i begge retninger.

Norges vassdrags- og energidirektorat kan etter søknad i særlige tilfeller gi dispensasjon fra enkelte ~~funksjons~~krav.

2.3.3. Økonomiske og administrative konsekvenser

NVE vurderer at endringene ikke får noen økonomiske eller administrative konsekvenser.

2.4. Ny § 4-2a. Krav til sikkerhet i AMS

2.4.1. Bakgrunn

Det stilles i dag krav til sikkerhet i AMS i avregningsforskriften § 4-2. Det er i tillegg foreslått nye sikkerhetskrav i beredskapsforskriften. Vi viser til redegjørelsen i punkt 1.3, som inkluderer oversikt over regelverk med betydning for sikring av AMS.

[29] Best available techniques reference document for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems 7/11/2016: https://ec.europa.eu/energy/sites/ener/files/documents/bat_wp4_bref_smart-metering_systems_final_deliverable.pdf.

Etter forslagets første ledd skal nettselskap vurdere sikkerhet ved oppstart og gjennomføring av endringsprosesser. Kravet skal forstås i tråd med prinsippet om innebygd sikkerhet **(**security by design). Nettselskapet må kunne dokumentere at sikkerhetsrisikoen har vært vurdert under livssyklusen til alle prosjekter, tjenester og produkter, fra oppstart til avvikling. Kravet skal bidra til bevisstgjøring rundt sikkerhet i AMS, og er viktig for å oppnå et så kostnadseffektivt sikkerhetsnivå som mulig.

Etter annet punktum skal nettselskapet foreta en avveining mellom ulike løsninger med betydning for sikkerhet i AMS. Kravet skal forstås i tråd med prinsippet om sikkerhet som førstevalg (security by default). Løsninger kan eksempelvis være produkter, programvareinnstillinger, organisering eller sikkerhetstiltak. Nettselskapet skal velge løsningen som gir høyest sikkerhetsnivå, med mindre løsningen vil medføre en urimelig ulempe, sett i sammenheng med kostnadsnivå og risikoen den forebygger. Dette betyr at det er rom for at nettselskapet foretar en bedriftsøkonomisk vurdering ved valg mellom ulike løsninger med betydning for sikkerhet. NVE ber om tilbakemelding fra høringsinstansene om de mener dette kommer tydelig nok frem i den foreslåtte forskriftsteksten.

Avveining mellom ulike løsninger med betydning for sikkerhet, kan utføres som en del av vurderingen av sikkerhet etter første punktum. NVE presiserer likevel at sikkerhet som førstevalg også er et selvstendig krav, som skal utføres ved valg mellom ulike løsninger, uavhengig av eventuelle endringsprosesser. Dette betyr at avveining mellom ulike løsninger med betydning for sikkerhet, kan være nødvendig også utenom konkrete endringsprosesser hos nettselskapet.

Forslagets annet ledd slår fast at nettselskapet er pliktsubjekt for sikring av AMS, selv om de skulle sette ut visse oppgaver til leverandører. Systemet må beskyttes på en helhetlig måte mot alle typer trusler for å sikre at nettselskapet mottar riktig data til riktig tid.

Krav til grunnsikring er foreslått i beredskapsforskriften.[30] Dette inkluderer både tekniske og organisatoriske sikkerhetskrav. Det følger av forslagets første ledd at grunnsikring skal sikre at digitale informasjonssystemer beskyttes, slik at konfidensialitet, integritet og tilgjengelighet ivaretas. Av hensyn til konfidensialitet er det viktig å hindre at data kommer på avveie dersom noen skaffer seg tilgang til systemkomponenter eller infrastruktur. Av hensyn til integritet, er det viktig å beskytte både lagrede og overførte data mot uautoriserte endringer. Samtidig er det viktig at tilgjengelighet sikres, slik at informasjon ikke går tapt ved eksempelvis spenningsbrudd.

Det følger videre av forslaget i beredskapsforskriften at sikkerhetsløsninger skal baseres på anerkjente standarder. Når det gjelder krypteringsløsninger for AMS, fremhever NVE spesielt at løsninger som er FIPS-godkjent[31] eller tilsvarende, ansees som et minimumsnivå. Nasjonal sikkerhetsmyndighet (NSM) har også publisert relevante sikkerhetsveiledere for AMS.[32]

For å gi AMS et høyere sikkerhetsnivå enn grunnsikringsnivået, er det foreslått syv tilleggskrav:

Bokstav a
For å hindre at falske AMS-målere eller andre falske enheter kommuniserer til eller i AMS, skal alle enheter godkjennes før de gis tilgang til systemet. Godkjenning kan gjennomføres i AMS eller i tilkoblede systemer. Slik godkjenning kan eksempelvis gjennomføres ved at AMS-målere og sentralsystem utveksler meldinger kryptert med unike forhåndsdelte krypteringsnøkler, hvor bare enheten som er opphavet til nøkkelen kan dekryptere og bekrefte meldingen (også kalt PKI[33]). Slike

[30] NVE Høringsdokument 6/2017 (grunnsikring omtales i kap. 9.6): Forslag til endringer i beredskapsforskriften.
[31] FIPS 140-2 Security Requirements for Cryptographic Modules 25/5/2001 (Change Notice 2, 12/3/2002): https://csrc.nist.gov/publications/detail/fips/140/2/final.
[32] NSM veiledning for systemteknisk sikkerhet: https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet/.
[33] Public Key Infrastructure.

krypteringsnøkler kan legges inn i AMS-målerne tidlig i produksjonsprosessen, men det vil være nettselskapet eller nettselskapets leverandør som gjennomfører eller følger opp selve godkjenningen ved innkobling av nye enheter i AMS.

Kravet om godkjenning gjelder kun enheter som kommuniserer til eller i AMS. Slike enheter inkluderer elektrisitetsmålere, og enheter benyttet av servicepersonell for tidsbegrenset tilkobling til AMS-måleren lokalt. Enheter som ikke kommuniserer i eller til AMS, er eksempelvis sluttbrukerens private utstyr som kobles til HAN-grensesnitt, men som kun kommuniserer ut til kunden. NVE presiserer her at enheter som kommuniserer ved hjelp av nettverk fysisk adskilt fra AMS, ikke må godkjennes i systemet. Dette er fordi enhetene da hverken er del av AMS, eller koblet til AMS etter dette forslagets tredje ledd. Dette betyr at i tilfeller hvor en vannmåler er tilkoblet AMS, og dens kommunikasjonsløsning kun er logisk adskilt fra AMS, må vannmåleren godkjennes. Dersom nettselskapet ikke ønsker at vannmåleren skal godkjennes i selve AMS-løsningen, kan tredjepart og nettselskapet i stedet avtale særskilt at vannmåleren godkjennes i en logisk adskilt del av systemet under kontroll av nettselskapet eller nettselskapets leverandør. NVE ønsker imidlertid tilbakemelding fra høringsinstansene på om forslaget gir en tydelig nok avgrensning av hvilke enheter som må godkjennes i systemet, og hvilke deler av systemet enhetene kan godkjennes i.

Programvare, det vil si dataprogram som benyttes i datasystemer, skal godkjennes før den installeres i AMS. Slik godkjenning kan gjennomføres ved at nettselskapet eller nettselskapets leverandør kontrollerer at et sammendrag av programkoden (sjekksum), samsvarer med tilsvarende sammendrag fra programvareleverandøren.

Bokstav b
For å hindre at uvedkommende får innsyn i data, må kommunikasjonen i AMS sikres fra ende-til-ende. Ende-til-ende-sikkerhet betyr at sikkerheten skal opprettholdes i alle ledd i kommunikasjonsflyten i AMS. Et eksempel på slik ende-til-ende-sikkerhet er kryptering hele veien mellom AMS-målerens dataprogram og tilsvarende dataprogram benyttet i sentralsystemet (applikasjonsnivå[34]). Data som skal beskyttes er ikke begrenset til personopplysninger underlagt personvernlovgivning eller brytekommandoer regulert i forslag til endringer i beredskapsforskriften. Det er også viktig å sikre konfidensialitet for informasjon om AMS-måler og programvare med betydning for måleverdikjeden. Slik informasjon kan eksempelvis være oversendelse av programvareoppdateringer eller krypterings- og tilgangsnøkler.

Bokstav c
Det er alltid en risiko for at programvare har feil eller svakheter (sikkerhetshull), som kan gjøre det digitale systemet sårbart. Når produsenter oppdager slike sikkerhetshull, gjør de vanligvis tilgjengelig programvareoppdateringer for å lukke sikkerhetshullet. Det er derfor viktig at programvare i AMS til enhver tid er oppdatert, for å motvirke at AMS-målere og andre enheter i AMS forblir sårbare dersom sikkerhetshull oppdages. Dette krever nødvendigvis at også AMS-målere og andre viktige enheter må kunne oppdateres.

Bokstav d
Et sikkerhetsbrudd i AMS, som skjer andre steder enn i nettselskapets sentralsystem, skal ikke kunne få betydning for andre deler av, eller hele AMS. Dersom for eksempel krypteringsnøkler for en AMS-måler kommer på avveie, skal ikke dette medføre tilgang til andre AMS-målere eller sentralsystemet.

NVE er oppmerksom på at ordlyden i forslaget i stor grad samsvarer med forslag til ny § 6-10 bokstav e i beredskapsforskriften.[35] Forslaget i avregningsforskriften er likevel ment å sikre en mer helhetlig beskyttelse av AMS, mens beredskapsforskriftens forslag har beskyttelse av brytefunksjonaliteten i fokus.

[34] Applikasjonsnivå: Abstraksjonsnivået nærmest brukeren i OSI-referansemodellen for datakommunikasjon.
[35] NVE Høringsdokument 6/2017: Forslag til endringer i beredskapsforskriften.

Dette betyr at virkeområdet til beskyttelseskravet i beredskapsforskriften er noe mer snevert enn tilsvarende krav i avregningsforskriften.

Bokstav e
AMS skal for det første installeres med tilstrekkelig evne eller kapasitet for å til enhver tid kunne utføre tiltenkte oppgaver. Eksempelvis skal kommunikasjonsinfrastrukturen mellom AMS-måler og sentralsystem være dimensjonert slik at det er mulig å fjernoppdatere programvare. Et annet eksempel er at oversendelse av nettnyttedata ikke skal blokkere oversendelse av måleverdier.

For det andre skal enheter i AMS ikke ha funksjonalitet ut over det som er nødvendig for deres bruksoppgaver. Kravet er viktig fordi sikkerhetsrisikoen vil øke dersom AMS leveres med økt funksjonalitet. I kravet ligger det at funksjonalitet som nettselskapet har planer om, eller tror de vil komme til å benytte, kan inkluderes i systemet. Samtidig kan det være noen løsninger som nettselskapet ikke har planer om å bruke eller tilby. Når sikkerhetsrisikoen øker samtidig som funksjonaliteten ikke gir noen nytteverdi, er det bedre om funksjonaliteten ikke er tilstede. Kravet til nødvendighet legger derfor opp til en vurdering av sikkerhetsrisikoen som følger med funksjonaliteten, sett opp mot kostnaden av å ikke ha funksjonaliteten.

Bokstav f
Det stilles i forslagets tredje ledd krav til at sikkerheten i AMS ikke forringes ved at enheter og systemer i andre IKT-nettverk kobles til AMS. I tillegg hjemler bokstav f et krav om logisk eller fysisk skille mellom AMS, og andre IKT-nettverk nettselskapet eller nettselskapets leverandør benytter. Andre IKT-nettverk kan eksempelvis være nettverk for kontorstøttesystemer. Formålet med å stille særskilt krav om et slikt skille, er å forhindre at IKT-nettverk blir attraktive angrepsmål for uvedkommende som ønsker tilgang til AMS. Kvaliteten på eventuelle logiske skiller må samsvare med risiko forbundet med tilgang til de adskilte nettverkene.

Bokstav g
AMS-målere leveres med grensesnitt som display, HAN-port[36], blinkediode (S0-port) og M-Busport[37]. AMS-målere kan også i varierende grad leveres med andre grensesnitt, som eksempelvis et grensesnitt for servicepersonell (IR-port). Slike grensesnitt kan gi tilgang til enkeltkunders måleverdier, gjengitt med en hyppighet som kan si noe om aktiviteten i boligen. Datatilsynet har uttalt at personopplysningsloven stiller krav til hvordan slike data skal behandles, og at dataene derfor trenger en viss beskyttelse, enten fysisk eller ved kryptering.[38]

Offentlig tilgang til AMS-måleren og dets grensesnitt øker også faren for hærverk eller forsøk på datainnbrudd. Nettselskapene skal derfor innføre tiltak som begrenser tilgang til AMS-målerens grensesnitt. Nettselskapene kan selv vurdere hvilken løsning som er mest hensiktsmessig, basert på risiko og bedriftsøkonomiske vurderinger. AMS-måleren må kunne motstå en viss fysisk påvirkning, eksempelvis ved at én eller flere offentlig tilgjengelig AMS-målere beskyttes av et låst skap, eller at AMS-målerens fysiske porter er avslått, passordbeskyttet eller kryptert.

Etter forslagets tredje ledd skal nettselskapet påse at sikkerhetsnivået i AMS ikke reduseres som følge av at nettselskapet eller nettselskapets leverandør ønsker å koble enheter eller systemer til AMS.

---

[36] Home Area Network port: Grensesnitt for å kunne strømme blant annet måleverdier med 2-10 sekunders oppløsning til et eksternt display eller andre enheter hos strømkunden.
[37] M-Busport: Grensesnitt for å kunne tilknyttes og kommunisere med andre typer målere.
[38] NEK Høringsdokument 10/10/2017: Vedlegg 1 – HAN Personvern – et tillegg til utredningen «AMS + HAN – om å gjøre sanntid måledata tilgjengelig for forbruker».

Nettselskapet kan eksempelvis ønske at et kundesystem i administrasjonsnettverket har tilgang til noen typer funksjonalitet i AMS. Da må nettselskapet implementere sikkerhetstiltak som sikrer at det helhetlige sikkerhetsnivået i AMS fortsatt oppfyller kravene i § 4-2a.

Tilsvarende har nettselskap et ansvar for at sikkerhetsnivået bevares der tredjeparter eller sluttbrukere kobler enheter til AMS. Eksempler på slik tredjepartstilkobling er overføring av informasjon gjennom smarthjemsløsninger og boligalarmer. Sluttbrukere kan også ønske å koble enheter til AMS-målerens grensesnitt.

En konsekvens av at nettselskapet har ansvar for at tilkoblede enheter og systemer ikke skal forringe sikkerheten i AMS, kan være at nettselskap vil ønske å tilby færre tilkoblingsmuligheter for egne leverandører, tredjeparter og sluttbruker. Dette betyr at nettselskapet kan ønske å begrense sluttbrukers og tredjeparters mulighet til å utnytte det potensiale AMS har ved å koble seg til AMS-måleren eller systemet. NVE aksepterer en slik praksis så lenge funksjonaliteten til påkrevde grensesnitt opprettholdes. Vi ser at kommunikasjonsløsninger som ikke krever tilkobling til AMS, trolig vil bli tilbudt, til stadig rimeligere pris i markedet. For sluttbrukere og tredjeparter som ønsker å koble seg til grensesnittet, kan det likevel medføre en ekstrakostnad å påse at sikkerheten ikke forringes.

Etter fjerde ledd skal nettselskapet dokumentere oppfyllelse av sikkerhetskravene i et internkontrollsystem for informasjonssikkerhet. Formålet er å systematisere og dokumentere oppfølging av krav. Det stilles allerede krav til at nettselskap skal ha internkontrollsystem på ulike områder, eksempelvis for elektrisitetsmålere etter elmålerforskriften § 55 og for HMS i virksomheter etter forskrift om systematisk helse-, miljø-, og sikkerhetsarbeid i virksomheter (Internkontrollforskriften) av 6. desember 1996 nr. 1127. I tillegg pålegges nettselskapene internkontroll eller systematisk oppfølging både i beredskapsforskriften og personvernlovgivningen.

Internkontroll er sentralt innenfor sikkerhetsstyring og er omtalt av blant annet Direktoratet for forvaltning og ikt (Difi)[39], Datatilsynet[40] og NSM[41]. Internkontroll er et verktøy for å sikre at virksomheten oppfyller lovpålagte og selvpålagte sikkerhetskrav. Det er også et verktøy for å sikre kontinuerlig forbedring av sikkerhetsoppfølgingen i virksomheten, ved at nettselskapene skaffer seg oversikt over informasjon og informasjonssystemer de eier eller er ansvarlige for, samt risiko relatert til disse. Internkontroll for ulike områder, inkludert AMS, kan samkjøres for helhetlig internkontroll og kvalitetsstyring i virksomheten.

Noen nettselskap har søkt og fått innvilget tidsbegrenset dispensasjon fra enkelte av funksjonalitetskravene etter § 4-2 annet ledd. Ingen nettselskap har fått innvilget fritak fra sikkerhetskravene i dagens § 4-2 bokstav d og g. Dispensasjonene kan imidlertid medføre at enkelte nettselskap bruker eldre AMS-teknologi, som bare vil kunne oppfylle kravene i foreslått § 4-2a på et minimumsnivå. NVE antar dette spesielt vil gjelde krav om godkjenning av enheter og programvare, ende-til-ende-sikkerhet og krav til oppdatering av enheter. NVE aksepterer at alternativer til de mest anerkjente løsningene kan benyttes i perioden dispensasjonen gjelder for. Slike alternative løsninger kan være å holde spesialutviklet programvare for kommunikasjon hemmelig, å benytte fysiske sikkerhetsløsninger for å sikre informasjon ende-til-ende, og å manuelt oppdatere viktige enheter i AMS. NVE presiserer at vi forventer at nettselskap med dispensasjon vurderer hvordan alternative løsninger kan

[39] Difi Internkontroll i praksis - informasjonssikkerhet: http://internkontroll.infosikkerhet.difi.no/.
[40] Datatilsynet Internkontroll og informasjonssikkerhet: https://www.datatilsynet.no/regelverk-og-skjema/veiledere/internkontroll_informasjonssikkerhet/.
[41] Nasjonal sikkerhetsmyndighet Veileder Sikkerhetsstyring 10/03/2015: https://nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-sikkerhetsstyring--endelig.pdf.

gi tilsvarende sikkerhetsnivå som nyere AMS-løsninger. Nettselskap må innføre ytterligere sikkerhetstiltak dersom risikovurderinger avdekker at dette er nødvendig.

Vedlegg A viser hvilke anbefalinger og krav til sikkerhet vi har brukt som grunnlag i dette forskriftsarbeidet. Tabellen viser hvilke krav forslaget dekker, og hva som er, eller vil bli, dekket av annet regelverk.

2.4.2. Forslag til ny § 4-2a.

***4-2a.** Krav til sikkerhet i AMS*

Nettselskapet er ansvarlig for at sikkerhet vurderes ved oppstart og gjennomføring av endringsprosesser tilknyttet AMS. Ved valg mellom ulike løsninger av betydning for sikkerhet i AMS, skal nettselskapet velge løsningen med høyest sikkerhetsnivå så lenge kostnaden ved gjennomføring er forsvarlig etter en kost/nytte-vurdering.

Nettselskapet er ansvarlig for å sikre AMS. Sikkerhetsløsninger i AMS, herunder krypteringsløsninger, skal oppfylle kravene til digitale informasjonssystemer i beredskapsforskriften. I tillegg skal følgende krav være oppfylt:

a) enheter som benyttes for kommunikasjon til eller i AMS, skal godkjennes i systemet av nettselskapet eller nettselskapets leverandør før tilgang gis. Tilsvarende skal programvare godkjennes før den installeres i AMS

b) det skal være ende-til-ende-sikkerhet i datautveksling mellom den enkelte AMS-måler og nettselskap

c) AMS-målere, sentralsystem og deler av kommunikasjonsinfrastrukturen som har funksjonalitet som kan påvirke sikkerheten i AMS, skal til enhver tid være oppdatert

d) hendelser som utfordrer sikkerheten i en AMS-måler eller dens kommunikasjon med sentralsystemet skal ikke utfordre sikkerheten i andre AMS-målere, deres kommunikasjon med sentralsystemet, eller sentralsystemet i seg selv

e) AMS-målere, sentralsystem og kommunikasjonsinfrastrukturen mellom disse enhetene, skal for å sikre tilgjengelighet, til enhver tid kunne utføre de oppgaver systemet er designet for. Enheter i AMS skal ikke ha funksjonalitet ut over det som er nødvendig for deres bruksoppgaver

f) det skal være et skille mellom AMS og andre IKT-nettverk for å hindre uautorisert tilgang til AMS gjennom slike nettverk og

g) tilgang til AMS-måleres grensesnitt skal begrenses for andre enn sluttbruker, nettselskap og andre aktører med legitimt behov.

Dersom nettselskapet eller nettselskapets leverandør kobler andre enheter eller systemer til AMS, skal sikkerhetsnivået i AMS opprettholdes eller forbedres. Tilsvarende gjelder dersom sluttbruker eller tredjepart kobler seg til AMS.

Nettselskapet skal dokumentere oppfyllelse av krav i første til tredje ledd i et internkontrollsystem.

2.4.3. Økonomiske og administrative konsekvenser

NVE vurderer at kravene som stilles til sikkerhet i ny § 4-2a stort sett samsvarer med krav som tidligere har vært hjemlet i §4-2 bokstav d og g, og som er nærmere presisert i NVEs veileder til sikkerhet i AMS[42]. Nettselskap som har overholdt kravene i gjeldende regelverk, vil stort sett allerede ha implementert de krav som foreslås.

Plikten til å begrense tilgangen til AMS-målerens grensesnitt i forslagets bokstav g, kan medføre en kostnad for nettselskapene. Forskrift om elektriske lavspenningsanlegg av 6. november 1998 nr. 1060 kapittel V stiller i dag krav om at mennesker og husdyr skal beskyttes mot elektriske støt fra deler av anlegg og utstyr. Det følger av veiledningen i forskriften at sikkerhetskrav spesifiseres i normen NEK 400. NEK 400 er ikke juridisk bindende. Likevel følger det av § 10 i forskriften at det skal dokumenteres tilsvarende sikkerhetsnivå dersom det velges en annen sikkerhetsløsning enn normen anbefaler. Gjeldende NEK 400 henviser til NEK 399-1 for elektriske installasjoner i boliger. Gjeldende NEK 399-1 stiller i kapittel 6.4 krav om at elmåler skal plasseres i låst skap som begrenser tilgangen for andre enn boligeier, bygningseier, elnetteier og ekomnetteier. Boligeier oppgis som ansvarlig for nødvendig låssystem i kapittel 5.1.3.

NVE vurderer derfor at det allerede i dag er stilt krav til en viss sikring av AMS-måleren. Kravet i bokstav g om at tilgang skal begrenses, vil trolig være oppfylt dersom nettselskapet allerede har fulgt opp anbefalingene i NEK 399-1. Samtidig finnes det eksempler på at skap montert før 2014 ikke har lås. Vi presiserer her at innføring av GDPR i norsk regelverk trolig vil medføre krav til en viss beskyttelse av AMS-målerens grensesnitt.

NVE anser derfor at endringene kun vil medføre mindre økonomiske eller administrative konsekvenser for nettselskapet.

2.5. Endring i § 9-1c. Overtredelsesgebyr

2.5.1. Bakgrunn

NVE kommer til å føre tilsyn med om nettselskapene følger kravene til sikkerhet stilt i ny § 4-2a. Dersom brudd avdekkes, vil NVE kunne gi pålegg om endring, jf. avregningsforskriften § 9-1, og pålegge tvangsmulkt til endringen er gjennomført etter energiloven § 10-3 første ledd.

Brudd på sikkerhetsbestemmelsene kan få store konsekvenser for hele måleverdikjeden. Sikring av AMS er essensielt for at nettselskapene mottar riktig data til riktig tid. Samtidig skal forbrukerne kunne stole på at de blir fakturert for sitt faktiske forbruk. Ettersom AMS er et så komplekst system kan også den helhetlige sikkerheten i AMS være avgjørende for både sikring av kraftforsyningen og ivaretakelse av personvern.

Ved brudd på kravene i ny § 4-2a kan eksempelvis datainnbrudd eller kommunikasjonssvikt allerede ha skjedd på det tidspunktet sikkerhetsbruddet avdekkes. Det er derfor behov for å forebygge eventuelle brudd på § 4-2a. Sikkerhet er ikke alltid et økonomisk lønnsomt valg, og det er derfor behov for andre virkemidler for å sikre overholdelse av bestemmelsen. I tillegg er brudd på sikkerhetsbestemmelsene en alvorlig overtredelse i seg selv. En overtredelse vil ikke nødvendigvis kun ha betydning for AMS hos nettselskapet, men kan også ramme andre tilkoblede enheter og tilsvarende systemer. Dette betyr at

[42] NVE Veileder til sikkerhet i avanserte måle- og styringssystem 7/2012: https://www.nve.no/Media/5525/veiledertil-sikkerhet-i-ams.pdf.

nettselskap som oppfyller kravene har interesse av at også andre nettselskap sikrer sine AMS-løsninger i samsvar med regelverket.

Vi kan ikke se at personlig straffansvar her er aktuelt etter energiloven § 10-5. NVE foreslår derfor at brudd på § 4-2a skal kunne sanksjoneres med overtredelsesgebyr.

2.5.2. Forslag til endring av § 9-1c.

§ 9-1c. Overtredelsesgebyr

Ved overtredelse av bestemmelsene i § 2-1a, § 2-2, § 3-3, § 3-7, § 3-8, § 3-10, *§ 4-2a*, § 6-12, § 8-1, § 8-1a og § 8-3 kan det ilegges overtredelsesgebyr.

2.5.3. Økonomiske og administrative konsekvenser

NVE vurderer at endringen ikke medfører noen økonomiske eller administrative konsekvenser.

3. Forslag til endringsforskrift

Forslag til forskrift om endring i forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv.

Fastsatt av Norges vassdrags- og energidirektorat xx.xx.2018 med hjemmel i forskrift av 7. desember 1990 nr. 959 om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energilovforskriften) § 9-1 bokstav i, jf. lov av 29. juni 1990 nr. 50 om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven) § 10-6.

I

I forskrift av 11. mars 1999 nr. 301 om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. gjøres følgende endringer:

§ 1-3 to nye definisjoner skal lyde:

§1-3. ***Definisjoner***

Avanserte måle- og styringssystem (AMS): Toveis informasjons- og kommunikasjonssystem fra og med elektrisitetsmålere benyttet til avregning for de enkelte målepunkt, til og med sentralsystemet hos nettselskap eller nettselskapets leverandør.

Brytefunksjonalitet: System for fjernstyrt inn- og utkobling av strømuttaket i målepunktet til AMS-målere.

§ 4-2 skal lyde:

§ 4-2. ***Krav til funksjonalitet***

Nettselskapene er ansvarlig for at AMS skal:

a) lagre måleverdier med en registreringsfrekvens på maksimalt 60 minutter, og kunne stilles om til en registreringsfrekvens på minimum 15 minutter,

b) ha et standardisert grensesnitt som legger til rette for kommunikasjon med eksternt utstyr basert på åpne standarder,

c) kunne tilknyttes og kommunisere med andre typer målere,

d) kunne bryte og begrense effektuttaket i det enkelte målepunkt, unntatt trafomålte anlegg

e) kunne sende og motta informasjon om kraftpriser og tariffer samt kunne overføre styrings- og jordfeilsignal, og

f) registrere flyt av aktiv og reaktiv effekt i begge retninger.

Norges vassdrags- og energidirektorat kan etter søknad i særlige tilfeller gi dispensasjon fra enkelte *krav*.

Ny § 4-2a skal lyde

§ 4-2a. Krav til sikkerhet i AMS

Nettselskapet er ansvarlig for at sikkerhet vurderes ved oppstart og gjennomføring av endringsprosesser tilknyttet AMS. Ved valg mellom ulike løsninger av betydning for sikkerhet i AMS, skal nettselskapet velge løsningen med høyest sikkerhetsnivå så lenge kostnaden ved gjennomføring er forsvarlig etter en kost/nytte-vurdering.

Nettselskapet er ansvarlig for å sikre AMS. Sikkerhetsløsninger i AMS, herunder krypteringsløsninger, skal oppfylle kravene til digitale informasjonssystemer i beredskapsforskriften. I tillegg skal følgende krav være oppfylt:

a) enheter som benyttes for kommunikasjon til eller i AMS, skal godkjennes i systemet av nettselskapet eller nettselskapets leverandør før tilgang gis. Tilsvarende skal programvare godkjennes før den installeres i AMS

b) det skal være ende-til-ende-sikkerhet i datautveksling mellom den enkelte AMS-måler og nettselskap

c) AMS-målere, sentralsystem og deler av kommunikasjonsinfrastrukturen som har funksjonalitet som kan påvirke sikkerheten i AMS, skal til enhver tid være oppdatert

d) hendelser som utfordrer sikkerheten i en AMS-måler eller dens kommunikasjon med sentralsystemet skal ikke utfordre sikkerheten i andre AMS-målere, deres kommunikasjon med sentralsystemet, eller sentralsystemet i seg selv

e) AMS-målere, sentralsystem og kommunikasjonsinfrastrukturen mellom disse enhetene, skal for å sikre tilgjengelighet, til enhver tid kunne utføre de oppgaver systemet er designet for. Enheter i AMS skal ikke ha funksjonalitet ut over det som er nødvendig for deres bruksoppgaver

f) det skal være et skille mellom AMS og andre IKT-nettverk for å hindre uautorisert tilgang til AMS gjennom slike nettverk og

g) tilgang til AMS-måleres grensesnitt skal begrenses for andre enn sluttbruker, nettselskap og andre aktører med legitimt behov.

Dersom nettselskapet eller nettselskapets leverandør kobler andre enheter eller systemer til AMS, skal sikkerhetsnivået i AMS opprettholdes eller forbedres. Tilsvarende gjelder dersom sluttbruker eller tredjepart kobler seg til AMS.

Nettselskapene skal dokumentere oppfyllelse av krav i første til tredje ledd i et internkontrollsystem.

§ 9-1c skal lyde:

§ 9-1c. *Overtredelsesgebyr*

Ved overtredelse av bestemmelsene i § 2-1a, § 2-2, § 3-3, § 3-7, § 3-8, § 3-10, *§ 4-2a*, § 6-12, § 8-1, § 8-1a og § 8-3 kan det ilegges overtredelsesgebyr.

Vedlegg A

Krav eller anbefalinger til sikkerhet fra dokumentasjon brukt i prosjektet	Referanse	Juridisk pålagt krav fra referanse?	Allerede dekket eller foreslått dekket hvor
AMS skal sikre at lagrede data ikke går tapt ved spenningsavbrudd.	Avregningsforskriften § 4-2 bokstav d.	Ja.	Beredskapsforskriften. Ny § 6-9 første ledd.
AMS skal gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner.	Avregningsforskriften § 4-2 bokstav g.	Ja.	Avregningsforskriften. Ny § 4-2a annet ledd første setning.
The security of the smart metering systems and data communication is ensured in compliance with relevant Union security legislation having due regard of the best available techniques for ensuring the highest level of cybersecurity protection.	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on common rules for the internal market in electricity (recast) COM (2016) 864, Article 20 (b).	Vil sannsynligvis bli det.	Avregningsforskriften. Ny § 4-2a.
The privacy and data protection of final customers is ensured in compliance with relevant Union data protection and privacy legislation.	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on common rules for the internal market in electricity (recast) COM (2016) 864, Article 20 (c)	Vil sannsynligvis bli det.	Personopplysningsloven m/forskrift og GDPR.
Provide secure data communication.	Smart Grid Task Force Stakeholder Forum, Best available techniques reference document, 10 minimum functional requirements of the Smart Metering Systems, 8.	Nei.	Avregningsforskriften. Ny § 4-2a bokstav a, b og c.
Fraud prevention and detection.	Smart Grid Task Force Stakeholder Forum, Best available techniques reference document, 10 minimum functional requirements of the Smart Metering Systems, 9.	Nei.	Elmålerforskriften § 3 og § 19.
All AMI components SHALL provide a log of security events.	SM-CG Task Force on Privacy and Security / ESMIG, Minimum security requirements for AMI components – European level	Nei.	Beredskapsforskriften. Ny § 6-9 bokstav c.

Krav eller anbefalinger til sikkerhet fra dokumentasjon brukt i prosjektet	Referanse	Juridisk pålagt krav fra referanse?	Allerede dekket eller foreslått dekket hvor
	requirements for Smart Metering, A.		
All data exchanges shall take place in a (end to end) secure manner.	SM-CG Task Force on Privacy and Security / ESMIG, Minimum security requirements for AMI components – European level requirements for Smart Metering, B.	Nei.	Avregningsforskriften. Ny § 4-2a bokstav b.
Availability of the system (AMI components and communication network) SHALL be sufficient to perform the use cases the system has been designed for.	SM-CG Task Force on Privacy and Security / ESMIG, Minimum security requirements for AMI components – European level requirements for Smart Metering, C.	Nei.	Avregningsforskriften. Ny § 4-2a bokstav e.
Crypto mechanism and key management SHALL be documented and be compliant with recognized/proven and approved open standards.	SM-CG Task Force on Privacy and Security / ESMIG, Minimum security requirements for AMI components – European level requirements for Smart Metering, C.	Nei.	Beredskapsforskriften. Ny § 6-9 tredje ledd. Avregningsforskriften. Ny § 4-2a fjerde ledd.
Every AMI component SHALL check the authorization of any entity requesting access to it and grant or deny access based on the result of that check.	SM-CG Task Force on Privacy and Security / ESMIG, Minimum security requirements for AMI components – European level requirements for Smart Metering, D.	Nei.	Avregningsforskriften. Ny § 4-2a bokstav a.
Data at rest SHALL be protected in all system components.	SM-CG Task Force on Privacy and Security / ESMIG, Minimum security requirements for AMI components – European level requirements for Smart Metering, E.	Nei.	Beredskapsforskriften. Ny § 6-9 første ledd.
AMI components SHALL be upgradable to incorporate new (security) functionalities.	SM-CG Task Force on Privacy and Security / ESMIG, Minimum security requirements for AMI components – European level requirements for Smart Metering, F.	Nei.	Avregningsforskriften. Ny § 4-2a bokstav c.

Krav eller anbefalinger til sikkerhet fra dokumentasjon brukt i prosjektet	Referanse	Juridisk pålagt krav fra referanse?	Allerede dekket eller foreslått dekket hvor
Functionalities in AMI components SHOULD be limited to the intended operational use cases and SHALL not be able to compromise security functions.	SM-CG Task Force on Privacy and Security / ESMIG, Minimum security requirements for AMI components – European level requirements for Smart Metering, G.	Nei.	Delvis dekket i avregningsforskriften. Ny § 4-2a bokstav e.
AMI components and the communications network SHALL be adequately protected against external disturbances and/or attacks and SHALL demonstrate resilience against attacks.	SM-CG Task Force on Privacy and Security / ESMIG, Minimum security requirements for AMI components – European level requirements for Smart Metering, H.	Nei.	Avregningsforskriften. Ny § 4-2a. Beredskapsforskriften. Ny § 6-9 og § 6-10. Energiloven § 9-2 og § 9-3.

Referanser til vedlegg A

Avregningsforskriften. Forskrift 11 mars 1999 nr. 301 om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. Tilgjengelig fra: https://lovdata.no/dokument/SF/forskrift/1999-03-11-301 (01.02.2018)

Energiloven. Lov 29 juni 1990 nr. 50 om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. Tilgjengelig fra: https://lovdata.no/dokument/NL/lov/1990-06-29-50?q=energiloven (02.02.2018)

European Commission (2017) Proposal for a directive on common rules for the internal market in electricity. Tilgjengelig fra: http://ec.europa.eu/energy/sites/ener/files/documents/1_en_act_part1_v7_864.pdf (31.01.2018)

European Parliament and Council (2016) Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Tilgjengelig fra: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (31.01.2018)

Forskrift om krav til elektrisitetsmålere. Forskrift 28 desember 2007 nr. 1753 om krav til elektrisitetsmålere. Tilgjengelig fra: https://lovdata.no/dokument/SF/forskrift/2007-12-28-1753?q=kravtilelektrisitetsmålere (02.02.2018)

Norges vassdrags- og energidirektorat (2017) Forslag til endringer i beredskapsforskriften. Tilgjengelig fra: http://webfileservice.nve.no/API/PublishedFiles/Download/201709983/2262758" (02.02.2018)

Smart Grid Task Force Stakeholder Forum (2016) Best available techniques reference document - for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems. Tilgjengelig fra: https://ec.europa.eu/energy/sites/ener/files/documents/bat_wp4_bref_smart-metering_systems_final_deliverable.pdf (25.06.2017)

SM-CG Task Force on Privacy and Security / ESMIG (2016) Minimum security requirements for AMI components – European level requirements for Smart Metering. Tilgjengelig fra: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/EnergySustainability/Management/SmartMeters/SMCG_Sec0109.pdf (25.06.2017)

Norges
vassdrags- og
energidirektorat

Norges vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 22 95 95 95
Internett: www.nve.no