dataskydd.net
ORG.NR 802495-4797 – HTTPS://DATASKYDD.NET – INFO@DATASKYDD.NET

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

Miljö- och energidepartementet
103 33 Stockholm

Stockholm 2018-01-28

Remissyttrande över Funktionskrav på smarta elmätare – Ei R2017:08 (M2017/02657/Ee)

Vi avstyrker funktionskrav 3, och funktionskrav 1,4 och 5 i den omfattning funktionskrav 3 består. Vi avstyrker funktionskrav 6 och 7 av säkerhetsskäl. Vi tillstyrker funktionskrav 2. Energimarknadsinspektionen (EI) har fortfarande inte gjort någon bra utredning av informationssäkerhets- och dataskyddsaspekter i smarta elmätare. Integritetsanalysen har gjort en felaktig bedömning av proportionalitet och missförstått samtyckesbegreppet. Utredningen gör tekniska förbiseenden som skadar både datasäkerhet och dataskydd. Inspektionen framhåller fortfarande spekulativa fördelar som inte visat sig i forskning ha förutsättningar att införlivas som främsta skäl för sina förslag.

Innehållsförteckning:

Är de smarta elmätarna smarta?

> Smart meters put pressure not only on informational privacy, but also on the right to inviolability of the home and the right to respect for family life. For these reasons, the report performed a strict privacy-compliance test as laid down in art. 8 ECHR.
>
> – Cuijpers och Koops i European Data Protection Coming of Age, 2013.[1]

I vårt förra remissyttrande lyfte vi att det inte var klart att de smarta elmätarna har möjlighet att bidra till uppfyllandet av de politiska målsättningar som EI påstår att de kan bidra till att uppfylla.[2] Det gäller framför allt de smarta elmätarnas möjlighet att bidra till mer miljömedveten energikonsumtion bland slutkonsumenter.

Till stöd för detta påstående åberopade vi en studie genomförd vid Umeå universitet på uppdrag av EI.[3] I EI:s förra rapport om framtidens funktionskrav på elmätare gavs rapporten mycket sparsamt utrymme[4] men i innevarande studie har studien helt trollats bort – trots att den ger skäl att ifrågasätter premisserna för de flesta fördelar EI föreställer sig ska införlivas genom deras förslag! I stället upprepar EI gång på gång att konsumenter kommer att förändra sitt beteende om de utsätts för mer mätning.[5]

Ingen tjänar på att myndigheter och politiker hittar på nyttor med övervakningsåtgärder som inte är verkliga eller till och med osannolika. Det finns tillräckligt med verklighet att förankra beslut i för att politiken inte ska behöva bedrivas utifrån falsarier.

Fördelarna med de smarta elmätarna förefaller tillkomma uteslutande elnätleverantörer, i det att de slipper anställa personal som kan genomföra fältbesök[6] och att de kan utveckla nya tjänster de tror att konsumenterna vill ha, utan att fråga konsumenterna först.[7] Till skillnad från vad EI påstår[8] är smarta elmätare inte viktig för smarta elnät, vilket enklast inses av att man i Tyskland arbetar för att genomföra smarta elnät med hjälp av så kallade smarta *gateways*, som inte

---

[1] Collette Cuijpers och Bert-Jaap Koops. Smart Metering and Privacy in Europe: Lessons from the Dutch Case, European Data Protection: Coming of Age Gutwirth, Leenes, de Hert, Poullet (red.), s. 269–295. Springer Verlag, 2013.

[2] Dataskydd.net, remissyttrande över Ei R2015:09.

[3] Thomas Broberg, Runar Brännlund, Andrius Kazukauskas, Lars Persson, Matthias Vesterberg Handelshögskolan Umeå Universitet, Centrum för Miljö- och Naturresursekonomi ‚En elmarknad i förändring - Är kundernas flexibilitet till salu eller ens verklig?, 2014, s. 31:

> *I den här rapporten har vi försökt närma oss frågan vad vi kan förvänta oss av framtidens elkunder, i synnerhet vad gäller benägenheten att reagera på prissignaler och att anpassa beteende efter effektsituationen i elsystemet. Smarta elmätare och en effektivare prissättning av el har lyfts fram som viktiga reformer för att öka efterfrågeflexibiliteten på elmarknaden. I grunden finns en förväntan om att elkunderna tar till sig relevant information och reagerar på den. Vår analys tyder på att de ekonomiska incitamenten att avtala om timpriser är förhållandevis små för hushåll och att man därför inte kan vänta sig någon större efterfrågeflexibilitet. Våra beräkningar pekar på att hushåll som drastiskt flyttar om sin elkonsumtion sparar mindre än en krona om dagen, givet dagens prisvariation på elspotmarknaden. Vår analys tyder också på att hushåll i allmänhet har liten kunskap om kostnaden för att förbruka el och att man således inte tar till sig den information som faktiskt finns tillgänglig via elräkningen etc. En slutsats av detta är att den starka tilltro till efterfrågeflexibilitet som ibland ges uttryck för grundar sig på en naiv föreställning om hushållens anpassningsbarhet och vilja.*

[4] Enda omnämnandet sker i fotnot 42 på s. 46 i Ei R2015:09.

[5] Se tabell på s. 6 i Ei R2017:08, särskilt angående funktionskrav 1, 2 och 5.

[6] *Ibid.*, angående funktionskrav 6 och 7, men jämför även funktionskrav 3.

[7] Ei R2017:08, s. 78.

[8] *Ibid.*, s. 6.

är placerade i hushåll utan aggregerar information från flera olika hushåll inom samma område.[9]

Ingen integritetsanalys för tekniska krav

EI har fallit i fällan att de vill se dataskydd som enbart en juridisk fråga. Artikel 32 i dataskyddsförordningen sveps förbi i all hast i säkerhetsanalysen med konstaterandet att den kräver ”lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.”[10] Samtidigt anser EI att tekniska krav inte kräver någon integritetsanalys.[11]

Olika tekniska lösningar lånar sig mer eller mindre bra till dataskydd. Smarta elmätare som fenomen lånar sig rätt dåligt till dataskydd. Det är därför mer än hälften av alla de mått (*metrics*) för bra IT-säkerhet och dataskydd som ingick i en tysk översikt från 2015[12] rör smarta elmätare: attackvektorerna är helt enkelt många, och relationerna mellan olika parter i nätverken som på olika sätt kan utgöra en dataskydds- eller säkerhetsrisk ännu fler.

Dataskydd.net hävdar att myndigheter och företag *särskilt* vid utformningen av tekniska krav måste tänka igenom integritetsaspekter. Det hävdar också dataskyddsförordningens art. 25 (inbyggt integritetskydd).

***Art. 25 (Inbyggt integritetsskydd) ***

EU:s lagstiftare har godtagit att den tekniska utformningen av ett system påverkas dess förmåga att ge ett gott dataskydd. Därför kräver dataskyddsförordningen att utvecklare, tillhandahållare och leverantörer av tekniska apparater ska ha inbyggt integritetsskydd.

Samtycke som rättslig grund för insamling och behandling

EI drar slutsatsen att samtycke kommer vara den huvudsakliga grunden för insamling av uppgifter.[13] Men samtycke ska vara fritt givet, specifikt, tidsbegränsat och individen ska ha en rimlig möjlighet att förutse konsekvenserna av sitt samtycke.[14] Det kan inte anses gälla för den sortens användningsområden EI

[9] Frank Pallas. Beyond Gut Level – Some Critical Remarks on the German Privacy Approach to Smart Metering, European Data Protection: Coming of Age, Gutwirth, Leenes, de Hert, Poullet (red.), s. 313–347. Springer Verlag, 2013.

> *this boils down to a modular measurement system where one or more electronic meters falling within the scope of European regulation are connected to a “smart metering gateway” falling within the scope of national legislation (see Fig. 14.2). The detailed legal as well as technical elaboration of the German data protection framework for smart metering then rests upon four main concepts. These are:*
>
> - *a paradigm of star-shaped end-to-end communication between gateway and market actors, replacing the established concept of chain-formed communication,*
> - *mainly local storage of measurement data with access being granted to the different market actors on the basis of locally enforced, receiver-specific access profiles,*
> - *different kinds of local preprocessing of measurement data being executed on the gateway before sending data to external parties, including local tariffing, and, finally,*
> - *a complete ex-ante definition of legitimate data uses given in national energy law, declaring any collection, processing and use of personal data from the measurement system beyond this set of data uses illegitimate.*

[10] Ei R2017:08.

[11] *Ibid.*, s. 71, 73.

[12] Isabel Wagner och David Eckhoff, Technical Privacy Metrics: a Systematic Survey, arXiv, december 2015.

[13] Ei R2017:08, s. 79.

[14] Se dataskyddsförordningen, art. 4.11 och 7.4.

> *Art 2.11 samtycke av den registrerade: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne,*
>
> *Art. 7.4 Vid bedömning av huruvida samtycke är frivilligt ska största hänsyn bland annat tas till huruvida genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet.*

föreslår, och som bland annat innefattar att nätleverantörer och elbolag kan ha ”behov”. EI förutsätter dessutom att uppgifter kommer spridas vidare till energitjänstföretag, andra företag som ingår i samma koncern som elnätsföretaget och deras samarbetspartners.[15] Den pedagogiska utmaningen i att göra allt detta förutsägbart för en slutkonsument vid tillfället då slutkonsumenten försöker tillgodose sitt behov av att kunna få varmt vatten, eller tända lampor i det egna hemmet, är uppenbar.

För att en elleverantör ska kunna uppfylla avtal om elleveranser till slutkonsument krävs inte alls den omfattning på uppgiftsinsamling som EI föreslår. Denna rättsliga grund kommer bara i mycket begränsad utsträckning kunna åberopas av elföretag som vill läsa av och analysera kunder.

Slutsatsen EI borde ha dragit är att NÄT 2012 K (rev) inte uppfyller dataskyddsförordningens villkor på vad som utgör ett samtycke, och borde ses över. I stället har EI använt NÄT 2012 K (rev) för att undergräva privatpersoners nya rättigheter enligt dataskyddsförordningen.

✻ NÄT 2012 K (REV) ✻

NÄT 2012 K (rev) förefaller inte, enligt Energimarknadsinspektionens beskrivning, överensstämma väl med dataskyddsförordningens principer och regler. Därför borde avtalet ses över, och justeras så att det respekterar privatpersoners rättigheter enligt förordningen.

Proportionaliteten i insamlingen

EI skriver att ”*för kunden att delta aktivt på marknaden samt möjliggöra en effektivare drift av elnätet och möjliggöra styrning av elanvändarnas elanläggningar krävs att information om ström, spänning, aktiv och reaktiv effekt och energiförbrukning kan göras tillgängliga för kunden i nära realtid via kundgränssnittet.*”[16] Detta förklarar inte varför elnätsleverantören behöver tillgång till uppgifterna, och således har EI inte motiverat varför det är proportionerligt att uppgifterna specifikt ska kunna spridas till elnätleverantören efter elnätsleverantörens eget tycke och behag (jfr. krav på distansavläsning).

Inspektionen fortsätter sedan med att ”*[f]ör elnätsföretagen är de utökade möjligheterna att få information om kundernas förbrukning nödvändiga för att förbättra driften av elnätet.*”[17] Detta motsägs av att EI inte producerat annat än spekulativa fördelar för elnätföretagen av datainsamlingen (se nedan, avsnittet *Krav 3: Avläsning på distans*) samt att den tyska erfarenheter talar emot denna bedömning (se ovan, avsnittet *Är de smarta elmätarna smarta?*).

Därtill hävdar inspektionen att det inte sker någon förändring för de privatpersoner som väljer att inte tillgodogöra sig uppgifterna i kundgränssnittet.[18] Detta är uppenbarligen fel, eftersom privatpersonerna påverkas så till vida att elnätsleverantörerna får tillgång till uppgifterna.

---

och jämför med Datainspektionens riktlinjer för samtycke under nuvarande lagstiftning:

> *Samtycket ska vara individuellt. /.../ Att ett samtycke ska vara frivilligt kan sägas innebära att den enskilde i praktiken måste ha ett fritt val att avgöra om hans eller hennes uppgifter ska få behandlas.*
>
> *Här måste den personuppgiftsansvarige göra en bedömning av läget. Samtycke kan ju vara en förutsättning för att den registrerade ska få något som han eller hon önskar eller behöver, till exempel ett telefonabonnemang, en semesterresa, en livsnödvändig sjukvårdsbehandling, anställning, bostadsbidrag, etcetera. Om den registrerade i praktiken inte kan avstå kan samtycket inte gärna vara ”frivilligt”.*

[15] Ei R2017:08, s. 79, 81.
[16] *Ibid.*, s. 81.
[17] *Ibid.*, s. 83.
[18] *Ibid.*

Krav för krav

Dataskydd.net avstyrker funktionskravet om distansavläsning, mot bakgrund både av den bristfälliga proportionalitetsbedömningen och att elkonsumenter inte har någon reell möjlighet att invända eller undanhålla sitt samtycke från vidaredelningen av uppgifter. Övriga funktionskrav underkänns i den utsträckning funktionskrav 3 om distansavläsning består. Vi är tveksamma över utformningen på funktionskrav 6 om fjärruppdateringar och funktionskrav 7 om fjärrfrånkoppling av säkerhetsskäl, men också på grund av att vi anser att privatlivets helgd innefattar rimliga möjligheter för en konsument att utöva kontroll över och uppskatta förändringar i hemmiljön när dessa sker.

Vår alternativa kravlista

1. Mätdata ska inte göras tillgänglig för elnätleverantören utan konsumentens specifika, tidsbegränsade godkännande.
2. Avbrottsregistreringar ska inte göras tillgängliga för elnätleverantören utan konsumentens specifika, tidsbegränsade godkännande.
3. Elmätare ska utrustas med mjukvara som gör det möjligt för slutkonsumenter att definitivt begränsa inkommande anslutningar från elnätleverantören.

Krav 1: Utökad mätdata

Vi ifrågasätter nyttan av den utökade mätdatan för privatkonsumenter. Möjligheterna för kunder som EI beskriver förefaller vara sådana som kräver sådan analyskapacitet hos slutkund att privatpersoner i typfallet inte borde antas besitta analyskapaciteten eller, om kapaciteten finns där, önskan om att ödsla sin fritid på att genomföra en sådan.

De privatpersoner som ändå vill genomföra sådana analyser kan ges möjligheten att göra det, genom att smarta elmätare med detta funktionskrav görs frivilliga för privatpersoner att köpa och installera i sina hushåll. Om privatkonsumenter anser att utökad mätdata har stort värde för dem, kommer de frivilligt köpa och installera produkter som tillhandahåller sådan mätdata, utan att EI gör en föreskrift som gör utökad mätdata obligatoriskt.

Detsamma gäller privatpersoner som vill ägna sig åt mikroproduktion av el. I förhållande till det totala antalet privatpersoner som är uppkopplade mot ett elnät, är denna grupp liten. De flesta privatpersoner är nöjda med att el produceras av någon annan än dem själva och anländer till deras egna hushåll "färdigpaketerat". En del av den stora effektivisering och produktivitetsförbättring samhället genomlevde i industrialiseringen, genomlevdes just för att olika delar av samhället överlät på specialiserade enheter att utföra sådana saker som tidigare hade genomförts per hushåll.

Krav 2: Öppet kundgränssnitt

För de kunder och konsumenter som valt att ingå i EIs tilltänkta system, stödjer vi att kundgränssnittet är öppet snarare än slutet.

*** Konsumenter kan välja ***

Om en viss funktionalitet är väldigt bra och eftertraktansvärd för konsumenter, kommer de själva välja att köpa och installera produkter med sådana funktionaliteter i sina hem. Det behövs inte statliga tvång för funktionaliteter som är bra. Bara om funktionaliteterna är oönskvärda och egentligen dåliga, eller i alla fall meningslösa, för konsumenter behöver staten gå in och skapa tvingande regler för funktionaliteterna.

Krav 3: Avläsning på distans

I sin behandling av funktionskrav 1 (utökad mätdata) beskriver inte EI vilka tider som ska gälla för lagring av data, eller för insamling.[19] Inte heller i avsnittet om avläsning på distans görs någon sådan bedömning.

Nyttorna med distansavläsning beskrivs i hypotetiska ordalag: avläsningen skulle ”kunna vara till hjälp för nätföretagen i deras drift av elnätet”,[20] men om avläsningen faktiskt *är* till hjälp lämnas osagt. Trots att EI bevisligen haft mycket kontakt med näringslivet och borde ha kunnat tillgodogöra sig information om nyttan med avläsningen om någon sådan hade funnits.

Det är, för det första, uppenbart att privatpersoner inte har något fullgott skydd för sin integritet och att det görs intrång på privatpersoners dataskydd, om de inte kan motsätta sig avläsning på distans. Det bör alltså vara ett krav att privatpersoner kan motsätta sig avläsning på distans, särskilt då EI redan dragit slutsatsen att uppgifterna som avläses är personuppgifter.[21]

För det andra behöver EI ställa krav på med vilken frekvens avläsningar på distans kan och får genomföras. Eftersom det finns forskning som visar att man genom frekventa avläsningar av energikonsumtion i ett hushåll kan få fram mycket detaljerad information om hushållet och göra inferenser på bas av dessa (till exempel om när en familj är nära skilsmässa,[22] vad de tittar på på TV,[23] och andra saker), är det uppenbart att frekvensen för avläsningarna spelar roll.

För det tredje bör det införas gränser för hur länge bolagen som genomför distansavläsning får spara uppgifterna. Eftersom nyttan med distansavläsningen för bolagen är ytterst oklar (inspektionen talar om möjligheten att utveckla tjänster[24], kostnadsbesparingar jämfört med att avläsa mätare manuellt[25] och att elbolagen kan ha ”behov” eller falla under regelverk som tvingar dem att avläsa mätare[26]), men de tilltänkta användningsområdena många, behövs det en specifik begränsning i föreskriften om funktionskraven, eftersom föreskriften specificerar ändamål som inte lämpar sig för någon naturlig lagringsminimering på det sätt som föreskrivs i dataskyddsförordningen.

Hur ska en privatperson förstå lagringsminimering[27] i förhållande till att lagringen av uppgiften kan fortgå så länge elföretaget upplever sig ha ett ”behov”? Vilket behov? Meningen med dataskyddsreglerna är att insamling, behandling och lagring av uppgifter ska vara förutsägbart för varje privatperson. De föreslagna reglerna uppnår inte det syftet.

---

[19] Ei R2017:08, s. 52.
[20] *Ibid.*, s. 61.
[21] *Ibid.*, s. 49.
[22] Ross Anderson och Shailendra Fuloria, Cambridge University, Smart meter security: a survey, 2011:

> *The spikes in the energy trace can often be mapped to appliances such as electric showers and cookers; by noting the time and size of the spikes, an observer can deduce how many people there are in a house, when they get up, when they eat and when they go to bed. This information could be valuable not only to Google and home appliance vendors, but to burglars and maybe even divorce lawyers*

[23] Dario Carluccio och Stephan Brinkhaus, Smart Hacking for Privacy, 2011 (video).
[24] Ei R2017:08, s. 78.
[25] *Ibid.*, s. 62.
[26] *Ibid.*, s. 63.
[27] Dataskyddsförordningen, art. 5.1.e.

Krav 4: Timregistrering

I avsnittet *Är de smarta elmätarna smarta?* ovan motiverar vi varför det här funktionskravet är onödigt. Med det sagt finns det ingenting som förhindrar försäljare av smarta elmätare att redan idag tillverka och sälja smarta elmätare med den här funktionaliteten.

Om funktionaliteten är viktig och attraktiv för konsumenter och kunder, kommer de att köpa smarta elmätare som har den här funktionaliteten. Det behövs inget statligt krav på att funktionaliteten ska finnas i alla smarta elmätare.

Krav 5: Avbrottsregistrering

Problemet motsvarar det som beskrivits för avläsning på distans och utökad mätdata.

Krav 6: Fjärruppdatering

Vid funktionskravet för fjärruppdateringar berättar EI att de ska återkomma till djupare övervägningar i kapitel 5.2 om säkerhetsanalys.[28] Denna djupare bedömning består av följande mening:[29]

> Fjärruppgradering i form av säkerhetsuppdateringar är en viktig del i att behålla en hög säkerhetsnivå som står emot intrångsförsök och också en anledning till att fjärruppgradering bör ställas som ett funktionskrav.

Vid Totalförsvarets forskningsinstitut har två forskare emellertid kommit fram till att problemformuleringen gällande säkerhetskraven måste vara åtminstone dubbel:[30]

> Säkerhetsbrister i installerade produkter åtgärdas sällan då det i många fall är en komplex procedur att installera uppdateringar och att detta måste göras manuellt av konsumenten. Dessutom är det vanligt att produkterna fortfarande används flera år efter att tillverkaren slutat släppa säkerhetsuppdateringar, något som gör det omöjligt för konsumenten att undvika säkerhetsbrister.

Frågan uppenbarar sig vad man gör ifall en antagonistisk attack innebär att alla smarta elmätare tar emot en bit kod som dels stänger av elmätare eller påverkar dess funktion, och dels instruerar elmätaren att inte längre ta emot fjärruppdateringar. Energimarknadsinspektionen skulle behöva fundera på det här en vända till.

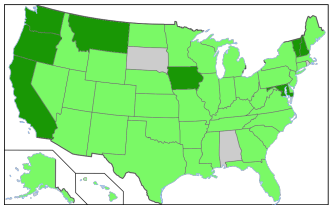
Dataskydd.net hade velat se krav på bättre information om säkerhet till konsumenter:

- vilka uppdateringar sker,
- varför sker uppdateringarna (vilket problem är det som åtgärdas?),
- vid vilka tillfällen sker uppdateringarna (veckovis? månadsvis?) och
- vad ska man som konsument göra ifall en uppdatering inte sker, eller om någonting med apparatens mjukvara inte fungerar som det ska?

[28] Ei R2017:08, s. 71.
[29] *Ibid.*, s. 91.
[30] FOI, Särtryck ur strategisk utblick 7, Daniel Eidenskog och Farzad Kamrani, Internet of Things – En IT-säkerhetsmässig mardröm, november 2017.

Det här är information som självklart skulle ges till konsumenter i till exempel USA, där hela 48 delstater har lagstiftning som tvingar företag att rapportera personuppgiftsläckor och säkerhetsincidenter till berörda invånare i delstaten, men som saknas i alla EU-länder och specifikt i Sverige.

Centralt på en myndighet kan man så klart sitta och noja över riskerna med att vara öppen kring säkerhetsrisker i apparater[31] man förväntar sig ska finnas i varje svenskt hushåll, men för individerna som faktiskt ska bo i dessa hushåll är tillgången till information om säkerhetsrisker och strategier för att åtgärda, hantera eller reducera dessa risker livsviktig. Sverige behöver en öppnare säkerhetskultur, som i högre utsträckning involverar användarna (läs: medborgarna) av apparater i säkerheten.[32]



Incidentrapportering i USA. I USA har konsumenter rätt att få reda på om det skett en dataläcka i 48 delstater. Bara Alabama och South Dakota har inte lagstiftning som ger konsumenter och medborgare rätt att veta när myndigheter eller företag läckt deras uppgifter (gråfärgade på bilden). I åtta delstater (mörkgröna på bilden) publicerar delstaten alla incidentrapporter de fått in från företag och myndigheter. Typiskt sett ska delstatens myndigheter bara informeras om ett tillräckligt stort antal medborgare drabbats av en dataläcka. Om ett fåtal personer, oftast färre än femhundra eller ett tusental, drabbats av dataläckan behöver företaget eller myndigheten bara underrätta de direkt berörda, medborgarna själva.

Krav 7: Fjärrfrånkoppling

Problemen motsvarar de som har beskrivits för fjärruppgraderingar och distansavläsning. Fjärrfrånkoppling ger betydande, och särskilt för medborgaren, dolt inflytande över den egna hemmiljön till någon som kan befinna sig långt, långt bort och vara okänd för medborgaren. Detta behöver genomlysas ur perspektivet att privatpersoners hem och hushåll tillhör en normalt okränkbar, privat sfär.

Krav 8: Larm vid nollfel

Ingen kommentar.

Säkerhetsanalysen

EI medger att deras tidigare rapport, Ei R2015:09, fick kritik för den knapphändiga behandlingen av informationssäkerhetsfrågor och IT-säkerhetsfrågor.[33] I den nya rapporten vill de inte ställa allt för specifika krav, utan skriver[34]

> IT-säkerhet är ett område där det sker en snabb utveckling. Ei gör därför bedömningen att det vore olämpligt att exakt specificera hur aktörerna ska göra och vilken teknik de ska använda sig av för att se till så att elmätare och andra nödvändiga system är säkra. En utpekad teknisk lösning riskerar att snabbt bli

[31] Ei R2017:08, s. 91: "*Ei vill därför inte peka ut den teknik som ska användas för att upprätthålla säkerheten i elmätarna utan mer allmänt föreskriva att det ska vara tillräckligt säkert så att inte information kan hamna i fel händer och så att styrfunktionerna i elmätarna inte kan användas av obehöriga personer.*"

[32] Jfr. Ella Kolkowska *m. fl.*, *Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method*, Journal of strategic information systems, 6(1) p. 39-57, 2017:

> *Because of its military and technical origin, information security is sometimes reduced to "the techniques employed to maintain security within a computer system" (Gollmann, 1999). However, information security in the context of organisational governance is much broader. /.../*
>
> *The predominance of the command-and-control approach has a serious consequence when working with employees' information security behaviours. Employees are still seen as the biggest obstacle to information security. In many cases, their security behaviours are directed by poorly designed information security policies (Stahl et al., 2012). Moreover, most methods focus on changing employees' behaviours because they consider these behaviours to be irrational and wrong, while the information security policies themselves are "correct" and unchangeable. However, various studies (e.g. Mattia and Dhillon, 2003; Corbin, 2013) have shown that the inability of policy to reflect current work practices is one of the biggest reasons for non-compliance.*

[33] Ei R2017:08, s. 87.

[34] *Ibid.*, s. 91.

> omodern och öppna för nya säkerhetsrisker. Utöver detta så är det inte heller möjligt att fullt ut överblicka den lagstiftning som kommer framöver, bland annat som en följd av det kommande nya elmarknadsdirektivet. Av dessa anledningar bör myndighetsregleringar i möjligaste mån vara teknikneutrala.
>
> Ei vill därför inte peka ut den teknik som ska användas för att upprätthålla säkerheten i elmätarna utan mer allmänt föreskriva att det ska vara tillräckligt-säkert så att inte information kan hamna i fel händer och så att styrfunktionerna i elmätarna inte kan användas av obehöriga personer.

Problemet för leverantörer bör bli att de riskerar höga böter om de *inte* vidtar säkerhetsåtgärder,[35] och att det är oklart vad som är *tillräckligt* eller *rekommenderat*. Funktionskraven som specificeras är specifika: apparaterna ska uppfylla de specifika, tekniska krav som EI föreslagit, enligt EI. Om de inte uppfyller de specifika, tekniska kraven kan EI bestraffa tillverkarna. Men hur tillverkare och leverantörer ska bete sig för att slippa sanktioner enligt andra lagstiftningar, behagar EI inte tala om. Varför dessa olika policys för specifika tekniska krav på olika områden?

De specifika, och tekniskt icke-neutrala kraven som EI upprättat för smarta elmätare påverkar möjligheten att skapa bra informationssäkerhet, IT-säkerhet och starkt dataskydd. EIs beredskap att ställa specifika, tekniskt icke-neutrala krav påverkar därför leverantörers och tillverkares förmåga och möjlighet att uppfylla sina förpliktelser enligt annan lagstiftning. Trots det har inspektionen inte valt att underlätta för leverantörer och tillverkare att uppfylla sådana förpliktelser.

[35] Dataskyddsförordningen föreskriver böter på upp till 4% av årsomsättningen vid intrång i dataskyddet, och SOU 2017:36 om svensk implementation av nätverks- och informationssäkerhetsdirektivet föreskriver 10 miljoner kronor i böter vid otillfredsställande uppfyllande av krav.

Källförteckning

1. Thomas Broberg, Runar Brännlund, Andrius Kazukauskas, Lars Persson, Matthias Vesterberg Handelshögskolan Umeå Universitet, Centrum för Miljö- och Naturresursekonomi ‚En elmarknad i förändring - Är kundernas flexibilitet till salu eller ens verklig?, 2014. http://umu.diva-portal.org/smash/get/diva2:747928/FULLTEXT01.pdf
2. Dario Carluccio och Stephan Brinkhaus, Smart Hacking for Privacy, 2011. https://media.ccc.de/v/28c3-4754-en-smart_hacking_for_privacy
3. Collette Cuijpers och Bert-Jaap Koops. Smart Metering and Privacy in Europe: Lessons from the Dutch Case, European Data Protection: Coming of Age Gutwirth, Leenes, de Hert, Poullet (red.), s. 269–295. Springer Verlag, 2013. [ej nätresurs]
4. Dataskydd.net, remissyttrande över Ei R2015:09. https://dataskydd.net/sites/default/files/sou201525_remissyttrande_dataskyddnet.pdf
5. FOI, Särtryck ur strategisk utblick 7, Daniel Eidenskog och Farzad Kamrani, Internet of Things – En IT-säkerhetsmässig mardröm, november 2017. https://www.foi.se/report-search/pdf?fileName=D%3A%5CReportSearch%5CFiles%5C11f0fc26-5734-435f-9a39-aa28c72e8aae.pdf
6. Ella Kolkowska m. fl., *Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method* Journal of strategic information systems, 6(1) p. 39-57, 2017. http://oru.diva-portal.org/smash/get/diva2:1058091/FULLTEXT01.pdf
7. Energimarknadsinspektionen, Ei R2015:09, Funktionskrav på framtidens elmätare. https://www.energimarknadsinspektionen.se/Documents/Publikationer/rapporter_och_pm/Rapporter%202015/Ei_R2015_09.pdf
8. Frank Pallas. Beyond Gut Level – Some Critical Remarks on the German Privacy Approach to Smart Metering, European Data Protection: Coming of Age, Gutwirth, Leenes, de Hert, Poullet (red.), s. 313–347. Springer Verlag, 2013. [ej nätresurs]
9. Isabel Wagner och David Eckhoff, Technical Privacy Metrics: a Systematic Survey, arXiv, december 2015. https://arxiv.org/pdf/1512.00327.pdf