EDPS
TECHDISPATCH

Issue No 2 | 2019

Smart Meters in Smart Homes

To tackle climate change, the European Union has set itself a target to ensure that 80% of EU consumers are using *smart meters* by 2020. This should accelerate the move towards cleaner energy and reduce energy consumption. The European Commission issued a Recommendation on preparations for the roll-out of smart metering systems in 2012. Today, there are an increasing number of *smart meters* being used across the EU and integrated with other *smart home* appliances.

1. What are smart meters? What are smart homes?

A *smart meter* is an electronic device that records energy consumption and exchanges consumption data with energy suppliers, which is used for monitoring and billing. While this TechDispatch focuses on electricity smart meters, smart meters can also measure the consumption of other resources, such as natural gas or water.

A *smart home* is a home with a system that connects with certain appliances to automate specific tasks. It is typically remotely controlled. A smart home system can be used to program sprinklers, set and monitor home security systems and cameras, or control appliances like refrigerators, or air conditioning and heating.

Households are equipped with electricity meters which measure the consumption of electricity. The distribution and diversification of centralised electricity supply, due to the small-scale generation of (renewable) electric power by households and communities for example, requires closer monitoring of consumer electricity consumption. *Smart grids*, electrical power grids equipped with measures to control the production and distribution of electricity, also rely on close monitoring of electricity consumption.

Figure 1: Advanced Metering Infrastructure (AMI). Source: Wikimedia (cc by-sa 3.0)

Traditionally, individuals manually collect and transfer only one meter value to the supplier per billing period, which could be once per year. In contrast, *smart meters* provide more information than a conventional meter, enable automated meter reading (AMR) and transfer the readings at regular intervals, perhaps hourly or even more frequently, to the supplier. Some smart meters (see Figure 1) provide for an *advanced metering infrastructure* (AMI). This enables two-way communication. Such smart meters can receive instructions from the supplier, including time-based pricing information, demand-response actions, or remote supply disconnects.

Smart meters can be connected to smart home devices, such as energy monitors, to enable the tracking of individual appliances, to improve control and save energy.

ACER reported that, in 2017, Spain, Italy, Sweden, Finland and Estonia had already reached the EU's target of 80% electricity smart meter rollout for household consumers.

2. What are the data protection issues?

The monitoring of the energy consumed in short intervals can help to increase the efficiency and safety of electricity distribution, but also allows those who have access to the data to draw conclusions about the behaviour of energy consumers. In 2012, both the European Data Protection Supervisor (EDPS) (Opinion on smart metering systems) and the former Article 29 Working Party of Data Protection Supervisory Authorities (Opinion 12/2011) identified certain risks to the protection of personal data that were previously unknown to the energy sector. Since then, researchers, policy makers and regulators have systematically assessed and addressed privacy risks, both at EU and at national level. The EU's 2019 amended electricity Directive specifically requires smart meters to comply with the EU's data protection rules.

Potential risks due to conclusions drawn from consumption data

Smart meters record the measured consumption over a given measurement interval and transfer recorded values individually, or in block, in a transfer interval. The European Commission recommended in 2012 to keep both intervals under 15 minutes to "allow the information to be used to achieve energy savings". Figure 2 shows an overview of maximum measurement intervals in 2017.

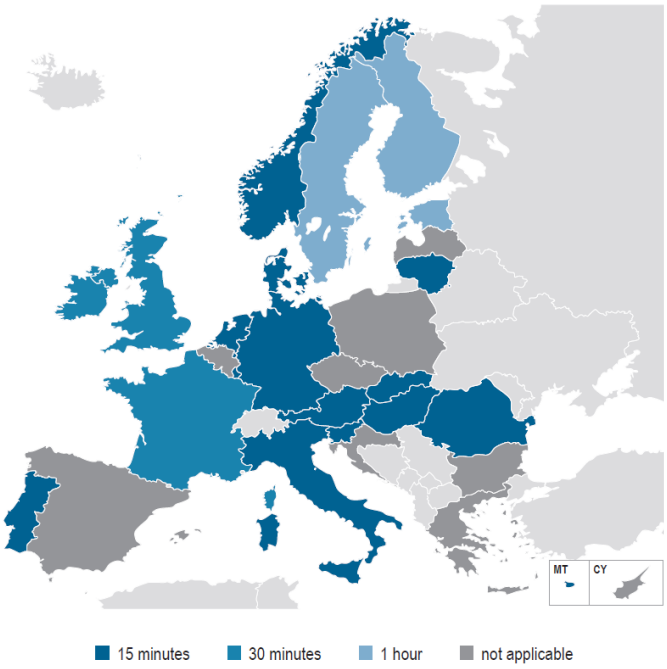

Figure 2: Max measurement intervals in smart meters in 2017. Source: ACER 2018

However, the smaller the measurement intervals, the more detail is revealed about the consumption profile, allowing various conclusions to be drawn about the household and its members. For instance, with the 15-minute interval smart meter data of residential households taken during a period of around one year, researchers could:

- infer holiday periods of residents (Eibl et al., 2018),
- infer religious practises from the time shifts in daily routines during Ramadan (Cleemput, 2018),
- detect the use of household appliances such as refrigerators or lighting; bathroom and housework activities can be inferred with intervals of under 60 seconds (Eibl et al., 2015).

Power data usage patterns obtained from smart meters can reveal much more than how much power is being used: the use of household appliances is an indicator of human behaviour, and allows for the identification of individuals. The operation of smart meters therefore entails the processing of 'personal data' and needs to be in line with the EU's General Data Protection Regulation (GDPR).

Lack of control and transparency

The implementation of smart meters gives rise to complex personal data processing operations. Most data subjects will be unaware of the nature of these operations, of which organisations are using of their data and of the potential impact this could have on their privacy. Certainly, if they are not aware of the personal data processing then it is impossible for them to make informed decisions about it. In practice, once a smart meter is installed with enabled connectivity, it may be difficult for consumers to prevent the accumulation of meter data.

Electricity suppliers deploy smart meters for an expected lifetime of 14 years on average (EC Benchmark, 2014). Even where consumers have initially understood the implications of newly deployed devices, the

processing of meter data may evolve throughout the meter's lifetime and may eventually become an essential part of smart homes. This may increase the complexity of the processing even more. Moreover, future research and analysis may make it possible to draw more detailed conclusions about an individual's activities, using past and future meter data.

Potential for profiling and mass surveillance

Information about real-time energy consumption can have high commercial value. Unless adequate safeguards are established to ensure that only authorised third parties may access and process data for clearly specified purposes and in compliance with applicable data protection law, the use of smart metering may lead to tracking the everyday lives of people in their own homes and building detailed profiles of all individuals based on their domestic activities.

Under certain circumstances, profiles might be enriched with personal data drawn from smart homes and other online and offline sources. These profiles could then be used for many other purposes, including for marketing and advertisement. Law enforcement agencies, tax authorities, insurance companies, landlords, employers, and other third parties may also be interested in accessing personal energy consumption information.

A network of smart meters with two-way communications enabled could also become part of an infrastructure of mass surveillance. This could technically be achieved with a mere firmware update to shorten the measurement and transfer intervals. Smart meters connected to smart home appliances are more vulnerable to breaches of meter data.

Generic risks common to IoT devices

Smart meters and smart home appliances fall into the category of Internet of Things (IoT) devices as they have network connectivity, sensors and controls to interact with their local environment. In consequence, smart meters and homes also share the risks originating from IoT devices or networks. Generally, the risks increase with the number of connected devices integrated in the smart home, especially if those devices allow for connectivity with insecure networks.

Where smart meters are connected to smart home appliances or the internet, and they are compromised, they could harm or infect other vulnerable or sensitive devices or services, such as mobile phones, computers, security cameras, smart locks, or public web services. Conversely, unauthorised access to smart meters via other devices in a smart home could compromise smart meter functionalities, including the provision of energy. Smart meters with network connectivity may be subject to unauthorised access. Malicious actors may extract consumption data or compromise the firmware to systematically record false consumption values, for example. To protect consumers and the power grid as critical infrastructure, some EU countries demand comprehensive certifications for smart meters and related components.

To ensure a high level of security, smart meters and home appliances must be regularly updated with security fixes and upgrades throughout their entire product lifecycle.

The use of the Data Protection Impact Assessment (DPIA) Template for Smart Grid and Smart Metering Systems as an evaluation and decision-making tool may further support smart grid operators.

Data protection by design and by default

Article 25 of the GDPR on data protection by design and by default requires that controllers implement appropriate technical and organisational measures – both at the time when the means for processing is determined and at the time of the processing itself.

The possibility for users to choose large measurement intervals could reduce the accuracy of conclusions drawn using smart meter data. Consumers could also be given the option to disable and enable certain smart features of their smart meter in some circumstances.

Moreover, deploying privacy-enhancing technologies (PETs) may reduce the risks originating from drawing conclusions from the data without changing the measurement interval. Examples are:

- *encryption* of meter data – different temporal resolutions could be encrypted with different keys to serve different purposes of varying accuracy requirements and distributed on a need to know basis,
- *masking protocols* that allow for secure aggregation of meter data to hide the meter data of individual households in the sum of a number of households (Knirsch et al., 2018),
- *homomorphic encryption* to aggregate the meter data of multiple households (Li et al., 2010),
- mesh networks to aggregate encrypted meter data hierarchically (Tonyali et al., 2018),
- privacy-preserving linkable *anonymous credential* protocols (Diao et al., 2015).

3. Recommended Reading

- European Commission overview on 'Smart grids and meters' (2019)
- Agency for the Cooperation of Energy Regulators (ACER), 'Annual Report of 22 October 2018 on the Results of Monitoring the Internal Electricity and Natural Gas Markets in 2017 - Consumer Empowerment Volume' (2018)
- European Commission 'Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems' (2012)
- EDPS opinion on 'Smart metering systems' (2012)
- Article 29 Data Protection Working Party, 'Opinion 12/2011 on smart metering', WP 183 (2011).
- European Commission: 'Benchmarking smart metering deployment in the EU-27 with a focus on electricity' (2014)
- Dario Carluccio and Stephan Brinkhaus: 'Smart Hacking For Privacy' (2011)
- Cleemput, S.: 'Secure and privacy-friendly smart electricity metering' (PhD thesis, 2018)
- Diao, F., Zhang, F., & Cheng, X. 'A Privacy-Preserving Smart Metering Scheme Using Linkable Anonymous Credential' In IEEE Transactions on Smart Grid, 6(1), 461–467 (2015)
- Eibl, G., Burkhart, S., & Engel, D. 'Unsupervised Holiday Detection from Low-Resolution Smart Metering Data' In Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018 (pp. 477–486). SciTePress (2018)
- Eibl, G., & Engel, D. 'Influence of Data Granularity on Smart Meter Privacy' In IEEE Transactions on Smart Grid, 6 (2), 930–939. (2015)
- Frédéric Simon: 'Smart meter woes hold back digitalisation of EU power sector' (2019)
- Knirsch, F., Eibl, G., & Engel, D. 'Error-resilient Masking Approaches for Privacy Preserving Data Aggregation' In IEEE Transactions on Smart Grid, 9 (4), 3351–3361 (2018)
- Li, F., Luo, B., & Liu, P. 'Secure Information Aggregation for Smart Grids Using Homomorphic Encryption' In Proceedings of First IEEE International Conference on Smart Grid Communications (pp. 327–332). Gaithersburg, Maryland, USA (2010)
- Tonyali, S., Akkaya, K., Saputro, N., Uluagac, A. S., & Nojoumian, M. 'Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems' In Future Generation Computer Systems, 78, 547–557. (2018)

This publication is a brief report produced by the Information Technology Policy Unit of the European Data Protection Supervisor (EDPS). It aims to provide a factual description of an emerging technology and discuss its possible impacts on privacy and the protection of personal data. The contents of this publication do not imply a policy position of the EDPS.

Author of this issue: Dr. Robert Riemann
Editor: Thomas Zerdick
Contact: techdispatch@edps.europa.eu

HTML	ISBN 978-92-9242-425-1	ISSN 2599-932X	https://data.europa.eu/doi/10.2804/27855	QT-AD-19-002-EN-Q
PDF	ISBN 978-92-9242-426-8	ISSN 2599-932X	https://data.europa.eu/doi/10.2804/87340	QT-AD-19-002-EN-N