GUIDELINE: PRIVACY AND DATA PROTECTION

Abstract

In this guideline we provide information on how to deal with issues relating to privacy, data protection, and personal data storage. This guideline provides an overview of recommended methods and measures that would preserve the user's data protection rights. The guideline is intended for smart grid service providers, e.g. DSOs and retailors at installation of smart meters and offering various functionalities. For the reader it is recommended to have some basic IT knowledge to understand the content.

What is it?

Privacy is a constitutional standard in contemporary European democracies. Non-compliance with privacy criteria might have an adverse effect on smart grid deployment in a given electricity market. The frequency of the measurement collection is close to real time on the level of the individual consumer with smart meters and this enables the operator a very detailed overview of the consumer energy behaviour. With long term collection, the patterns of the consumer life style behaviour may be visible, which could have an impact on its privacy and security. For this reason such energy consumption data are considered to be personal data. The operator and/or utility needs to take measures to protect the nature and contents of these data in order to safeguard the privacy of the consumer. Therefore the privacy issues in IT further implies protection procedures, which put restrictions on data handling. This has the goal of minimizing the security risk and building towards trust from the consumer.

This guideline is mainly sourced from Directive 95/46/EC and Consumer protection, Recommendation to the European Commission documents (Smart Grids Task Force, 2011). In the near future a new General Data Protection Regulation (GDPR), which is planned to replace the existing Directive 95/46/EC, will be introduced to define the rights of the data subjects (consumers) regarding processing their personal data:

- the right to be informed about processing their personal data in a clear and understandable language,
- the right to access their own personal data,
- the right to rectify any wrong or incomplete information,
- the right, in some cases, to object to the processing on legitimate grounds,
- the right not to be subject to an automated decision intended to evaluate certain personal aspects relating to the data subjects such as their performance at work, creditworthiness, reliability, etc.,

- the right to judicial remedy and to receive compensation from the data controller for any damage suffered (so not a vis major),
- the right to the erasure of data replaces the right to be forgotten in the upcoming GDPR. Provided that the data subject has the right to request erasure of personal data related to him.

These data subjects' (consumer) rights correspond to the data controllers' (service provider) obligations to:

- ensure the data subjects' rights are correctly observed,
- ensure observance of the data minimisation principle,
- ensure observance of the criteria for making the data-processing legitimate (e.g. consent or performance of the contract),
- safeguard confidentially of processing,
- safeguard security of processing,
- notify processing of personal data to the national data protection authority (DPA).

These obligations imply that service providers by law have to design a "Privacy impact assessment" (PIA) - a tool for identifying and assessing privacy risks throughout the development life cycle of a program or system. The tool contains technical and organisational measures to protect privacy and data of the end users.

This guideline provides an overview of recommended methods and measures that would preserve the data subject's user's data protection rights listed above.

Handling privacy and data protection issues, one must also take care about the security (security of data, appliances, network, etc.). The subject of security is too wide to be described in this guideline, but the reader is invited to get more info in the reference (Smart Grids Task Force, 2011).

When to use?

It is recommended that a service provider takes specific measures to ensure the adequate protection of personal data not only in smart metering but also in data handling at smart homes and smart cities projects. The fact is that smart metering, which is necessary for the society as a whole, should not suffice to override the fundamental right to protection of privacy. Any solution must comply with the law on data protection and privacy.

DSOs and energy suppliers acting as enablers of demand side response need to maintain information hubs. The responsibility for administration of verified and validated master data currently lies with the DSO in most European countries. The role of the DSO is to ensure data privacy and security within their scope of

responsibilities: ensure data security and privacy at the LAN level (communications through the national grid between smart meters and distribution transformer controllers (DTC)) and the WAN level (communication of the DTCs to the DSO central systems).

From the moment the DSO delivers the meter data to each of the retailers, the responsibility of further data privacy and security lies exclusively with the retailers. Therefore it is recommended that a retailor is obligated to put the privacy statements into the consumers electricity supply contract. The decision regarding privacy should be stated as optional by the end user and should follow the recommendations described in the next section; “what do you need to do?”.

It should be ensured that consumers have control over their data usage as data protection and other legislation specifies; this includes what data is read from the meter, who is collecting it for what purpose, and the period of archiving. Personal data should under no circumstances be saved or shared with other market actors beyond national law or without explicit consent between consumer, energy provider or third parties contracted by the consumer.

The same thing is valid about value added services. These services can be presented by the DSO to the retailers or can be presented by the retailers to their clients. The clients have the same control over their data that might be stored with these new services.

Bad terminology provoked privacy issues (OSCAR, CH)

An interesting case facing the privacy issues was provided by Swiss utility BKW Energie AG, which in the project OSCAR opened customer energy saving portal. Over 10.000 consumers registered to the portal entering their consumption data. The utility supplied the user data privacy statement but the privacy complaints raised since the consumption data were presented in the form ”your consumption versus consumption of your neighbour”. The information with that accompanying text was understood that the utility is revealing the participants location data and that actual consumption of the neighbours is exposed. This was later resolved via web forum explanations, that the participants were compared to averages and not to the specific consumption of the neighbour.
More information on https://oscar.bkw-fmb.ch/de/

What do you need to do?

The following main elements that should enter the PIA of the service provider to preserve the privacy and data protection rights:

- *Privacy by design and by default:* Privacy should be centered as core functionality in the design and architecture of Smart Grid systems and practices, where appropriate measures and a high level of protection of personal data are considered as default. Privacy by design basically consists

of 7 technical and organisational principles like “Proactivity and Preventability”, “Default setting”, “Visibility and Transparency” and others described at ‘privacy by design’.

- *Data retention:* There are a several reasons identified for the retention of personal and technical data within smart metering like network maintenance, billing, etc. The details concerning the scope and length of data retention and entities involved are explained in (Smart Grids Task Force, 2011) and in the Table 1 here below, which summarizes some of them.
  For example, billing customers have a legal period in which they can challenge their bills (consumer redress). It is usually around 3-5 years from the ‘due date’ – date of payment required by the creditor, yet country dependent (i.e. statute of limitation for periodic payments). From the consumer’s point of view, data should be stored only for that period of time.

Purpose	Scope	Length	Kept by
Network maintenance	Personal/anonymised/aggregated	strictly necessary / national law	Utility
Billing and payments	summed up usage	around 12-13 months / national law	Utility and energy market supplier
Billing complaints	detailed personal data	national law	consumer
Taxation – tax records	summed up usage	national law	utility
Taxation – tax breaks	detailed personal data		consumer
Value added services	upon consent	upon consent	any interested
Policy making	anonymised/aggregated	unlimited	public authorities

Table 1: Recommendation for scope and length of data retention (Smart Grids Task Force, 2011)

- **Smart services as option**: The services which apart from energy supply are provided by the utility and/or third parties on a commercial basis. These are of business-related high importance for distributors and suppliers and provide benefits like energy savings, but may also have significant impact on private lives. In order to live up to the data protection principles, the acceptance of these commercial services by the consumer should be only optional.

  The customers need to explicitly agree (opt-in) to provide their own data for these specific services. The use and collection of data and by whom it is collected needs to be clearly specified, as well as the specific purpose of collection and where the data will be stored. This agreement would also define the retention period, which should be justified by the specific use case

and should be agreed upon by the responsible national data protection authority (DPA).
The customer should have a right to withdraw consent easily, i.e. the customer's consent can be withdrawn at any time, without any reasoning.

- **Data anonymization**: Data that is anonymised is usually considered non-personal because the data subject can no longer be identified. But on the other hand it is almost impossible to ensure full anonymization since advanced data-mining methods enable "re-identification" or "de-anonymization" of individuals. For example, studies showed that more than 80% of the population may be uniquely identified by the combination of gender, birth date and postal code. Therefore it is recommended to use new advances in cryptographic techniques which allow building systems that do not require the sharing of personal information.

  Anonymization using the aggregation of personal data is context and data dependent. Some research indicates that the minimum number of users is around 7 to 8, but in many circumstances it will be more. It is easy to identify big devices like a washing machine, tea kettle, etc. from the smart meter readings. When aggregating data it has to be ensured that individual households and devices cannot be recognized.

- **Data storage location**: The data may be stored either on operator(s)-side, customer-side or both. The main difference between these options is whether data are stored using centralised or distributed (decentralised) method, or a combination thereof. From the view of personal data protection it is recommended to store the data with the highest possible security level compatible with national law.

- **Data mobility**: It has to be ensured that the data stays linked to the customer or is deleted in the case he moves to another location. In no case should one customer access detailed data from another one due to a location change.

- **Data Storage access**: It is recommended that the consumer has access to real time meter measurement and historic data. Consumers should be able to authorise anyone to access these data.

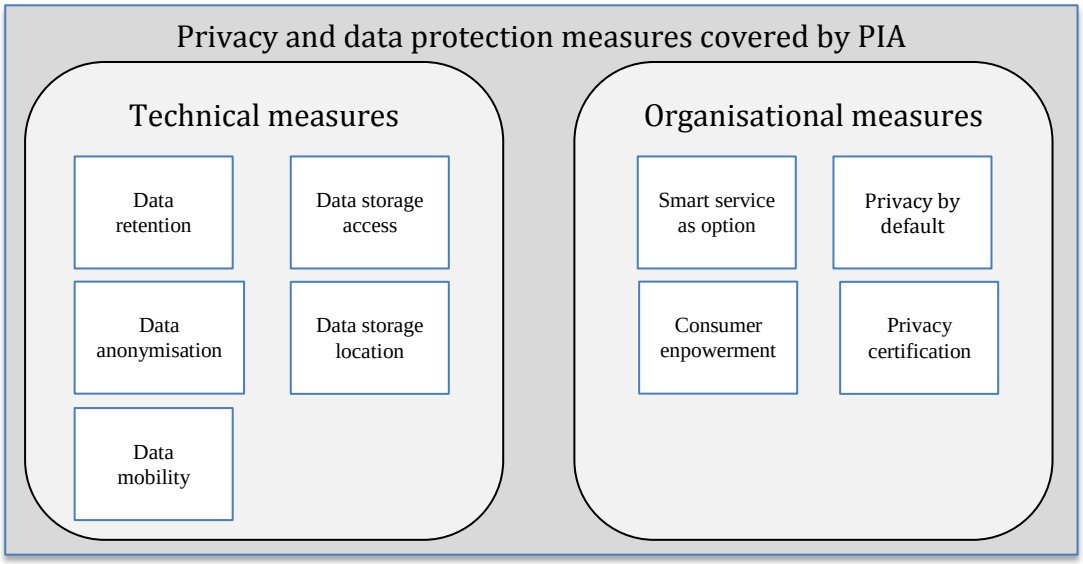

Figure 1: Privacy and data protection measures

- **Consumer empowerment**: The consumer empowerment is about giving a consumer more influence about personal data and decisions regarding privacy and data protection. The consumer should have an influence on issues like what data are to be collected, by whom, for what purposes, for how long, etc.

- **Privacy certification**: The data processing should meet certain principles and standards. Assurance on this subject may be provided by data protection audit, which identifies data processing weaknesses and maintains compliance with data protection requirements. A positive outcome of the audit may result in the privacy certification. A privacy certificate of compliance could be one way for organisations to show to consumers that they deal with the protection of their personal data with due care. An example of certification in the Netherlands is the Privacy Audit Proof certification[1]. Examples of certification delivery organization are EuroPriSe or TRUSTe.

Do's and don'ts

The following section outlines some specific recommendations when applying smart meter functionalities:

- **Ensure adequate protection level in foreign countries.** In case of the transfer to third countries (i.e. outside EU/EEA) – ensure that these countries

[1] https://www.privacy-audit-proof.nl/

provide adequate level of protection (in general), or in case of derogation ensure that the conditions of Article 26 of Directive 95/46/EC are met.

- **Set privacy as a default issue.** Smart meter integration should follow privacy as a default issue and not as an optional one. This means that the consumer has the right to get maximum privacy regarding data protection with no special requirements. Smart metering, while necessary for society as a whole, should not serve to override the fundamental right to protection of privacy.
- **Use transparent approach.** An information overload should be avoided for the consumer. The human habit is picking the default option, therefore this must be the standard option to choose regarding data protection. The consumer should be confronted clearly with the information on issues like what data are to be collected, by whom, for what purposes, for how long, etc. The statements that need the user's consent need to be exposed in such a meaningful way that the consumer can easily understand them.
- **Use local trustable authorities.** Involve or hire local authorities for marketing and propagation of new smart grid services. People generally have more trust in local organizations than in larger cooperations such as DSOs and TSOs due to conflicting interests.

Aggregation blurred personal profile (PET, NL)

The Privacy Enhancing Technology (PET) project presented an aggregation protocol designed to protect the privacy of smart meter data obtaining electricity usage data from a group of households without revealing privacy-sensitive information from a single household. The European Network for Cyber Security (ENCS), Alliander (a DSO) and Elster (smart meter producer) collaborated to conduct more in-depth integration and scalability tests on a set of 100 smart meters. The tests aimed to identify and resolve management, robustness, and performance issues and to minimize the effort to migrate to such a solution. ENCS also worked with Alliander to identify existing and potential use cases for smart meter data and to investigate alternative privacy approaches that are business-enabling.

More information on https://www.encs.eu/research/projects/privacy-enhancing-technology-project

Further reading

- Open meter project, http://www.openmeter.com/, Deliverable 3.2, Specification of Open Meter OSI layers and Multimetering Networking Interfaces, 2011
- Smart Grids Task Force, Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer protection, Recommendation to the European Commission, December 2011, https://ec.europa.eu/energy/sites/ener/files/documents/Recommendations%20regulatory%20requirements%20v1.pdf
- EC, Article 29 Data Protection Working Party, http://ec.europa.eu/justice/data-protection/article-29/index_en.htm, February 2010
- Directive 95/46/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
- General Data Protection Regulation [GDPR], http://en.wikipedia.org/wiki/General_Data_Protection_Regulation
- Privacy by design, *https://www.**privacybydesign**.ca/*

This guideline was developed in the S3C project, and is freely available from www.smartgrid-engagement-toolkit.eu.

S3C paves the way for successful long-term end user engagement, by acknowledging that the "one" smart consumer does not exist and uniform solutions are not applicable when human nature is involved. Beyond acting as a passive consumer of energy, end users can take on different positions with respective responsibilities and opportunities. In order to promote cooperation between end users and the energy utility of the future, S3C addresses the end user on three roles. The *smart consumer* is mostly interested in lowering his/her energy bill, having stable or predictable energy bills over time and keeping comfort levels of energy services on an equal level. The *smart customer* takes up a more active role in future smart grid functioning, e.g. by becoming a producer of energy or a provider of energy services. The *smart citizen* values the development of smart grids as an opportunity to realise “we-centred” needs or motivations, e.g. affiliation, self-acceptance or community.

S3C performed an extensive literature review and in-depth case study research in Smart Grid trials, resulting in the identification of best practices, success factors and pitfalls for end user engagement in smart energy ventures. The analysis of collected data and experiences led to the development of a new, optimised set of tools and guidelines to be used for the successful engagement of either Smart Consumers, Smart Customers or Smart Citizens. The S3C guidelines and tools aim to provide support to utilities in the design of an engagement strategy for both household consumers and SMEs. The collection of guidelines and tools describe the various aspects that should be taken into account when engaging with consumers, customers and citizens. More information about S3C, as well as all project deliverables, can be found at www.s3c-project.eu.