GDPR in The Energy Sector

UTILITY RECOMMENDATIONS FOR LONG-TERM ROADMAP

Jan Forslow | W231 | 04/18/2018

Table of Contents

Introduction

The General Data Protection Regulation - GDPR [1] is due to come into force in the European Union on May 25th, 2018. The GDPR is fundamentally concerned with the issue of protecting the privacy of individuals and enabling them to exercise their rights in this regard. To this end, the GDPR establishes a set of the most stringent global requirements imposed on service providers in terms of protection of privacy. These requirements govern how service providers must manage and protect the personal data of individuals in the EU while respecting their individual choices, no matter where the data is processed, stored, or sent.

The wide-spread use of smart grids facilitates mass collection of detailed consumer information. Smart meter data collection at 15-minute intervals can give a detailed insight into a person's life. It can determine times when a user is at home or at work as well as eating, sleeping or watching television. This extensive user data allows establishing a link with a particular individual, and therefore, the processing of data within smart grids is subjected to the EU data protection framework, now updated by the GDPR.

While service providers in the Financial and Media sectors have relatively new technology platforms and can offer plenty of incentives for consumers to opt-in to custom privacy policies, this is not the case in the Energy sector. The Energy sector is often thought of as a commodity provider using often older systems that were never designed to meet the needs described in the GDPR. Meeting the standards as defined in GDPR will mean significant investments and process changes, but these changes are ultimately expected to make the sector more transparent, trustworthy and open up for a more meaningful one-on-one conversation with its customer base.

GDPR – What Is It?

Without going into too much detail, it is considered best to introduce a few of the key terminology in the GDPR [2] before delving into the main part of the paper.

PERSONAL DATA REDEFINED

GDPR defines Personal Data as "any information relating to an identified or identifiable natural person". It doesn't just include data that directly identifies an individual, it also includes other identifiers, or information that can be used to identify a living person.

In the energy trading world, data processed by devices such as smart meters and connected devices will be considered "personal data" and will therefore be subject to additional rights and obligations. The scope now includes a Meter Subscriber Number (MSN) and a Meter Point Administration Number (MPAN) as well as an IP address, a

Meter Serial Number or a Customer Reference Number as those can also identify a human person and his location when, e.g., associated with the address.

SUBJECTS ACCESS RIGHTS

The GDPR intends to give people more control over how their personal data is managed by companies. For this reason, the GDPR introduces two new rights for customers vs. the Data Protection Directive 95/46/EC [3], which it replaces: the right to be forgotten and the right of data portability. The right to be forgotten allows customers to have their data deleted. The right of data portability implies that companies might be required to transfer the customer data to another provider when a client decides to switch provider. Here is a short description of all subject access rights in the GDPR:

- **The right to be informed** (ask what information is held)
- **The right of access** (access or be provided with the information stored is a guaranteed right)
- **The right to erasure** (the right to have all data deleted)
- **The right to portability** (to move data, in readable, useable format)
- **The right to rectification** (to update incorrect or incomplete data)
- **The right to restriction** (to restrict what can be done with the data)
- **The right to object** (to object to use of the data, while still requesting basic service)
- **Rights in relation to automated decision making and profiling** (to be informed of this type of processing and to object to it)

ROLES AND RESPONSIBILITIES

GDPR defines Data Controllers and Processors. Data Subjects can exercise their rights as per above at any time and both Controllers and Processors must ensure it can meet those.

The Utility is a Controller:

- Defines the legal basis for collecting data
- Decides which items of personal data to collect, i.e. the content of the data
- Decides the purpose or purposes the data are to be used for
- Decides which individuals to collect data about
- Decides whether to disclose the data, and if so, who to

- Decides whether subject access and other individuals' rights apply
- Decides how long to retain the data or whether to make non-routine amendments

A Utility Vendor is a Processor:

- Does not have overall control of the data
- Are told what they can do with the Personal Data via contract from the Controller
- Processors often decide the security arrangements for the data
- Stepping outside of the terms of a contract could amount to an infringement of Data Subjects rights and subsequently, the law

Both Controllers and Processors are subject to the requirements of GDPR regardless of data ownership. Controllers dictate, via contracts, what Processors may do with the Personal Data they provide. It is the Controllers responsibility to gather consent, then tell the Processor what can done with the Personal Data. Controllers and Processors can both be held accountable for the same breach.

GDPR READINESS STATUS

Forrester Research published a report in January 2018 called "The State of the GDPR Readiness" [4]. It took stock of the current GDPR compliance state by industry and geography. At the time of the Forrester Research report, only 30% of the respondents confirmed that they were GDPR ready and even this number is thought to be high given the self-assessment nature of the exercise.

The local Data Protection Authorities (DPAs) are not ready yet either. In a press release earlier this year called "GDPR is not Y2K" [5], the Information Commissioner's Office (ICO) [6], the DPA in the UK, softened the compliant requirements for May 25, 2018 stating that as long as a company can show a time plan and an active project then this is acceptable for now. It is expected though that ICO will be more stringent by the end of 2018.

When it comes to the different verticals' status, the Forrester Research report shows that utilities are in the middle of the pack in terms of GDPR readiness with 33% considering themselves fully compliant and 19% partially compliant. While the utilities were behind the financial services and health care sectors in terms of GDPR readiness, they were ahead of retail and media sectors.

As per Forrester Research, the reason for this is that the traditionally highly regulated sectors did not have to define new teams for the GDPR compliance journey, while this was the case for the others. Given the complexity of GDPR, expertise from a large part of the organization is required and that takes time to coordinate and get spun up:

- Legal Team
- Security Team
- Chief Data Officer
- Digital Team (IT)
- Marketing Team
- Customer Experience Team
- Human Resources
- Procurement / Vendor Management

GDPR FRAMEWORKS

Building a team is one aspect! Having the necessary tools is another! There are more than six vendors and an array of consultants that are eager to support a utility with a framework for the GDPR compliance process. A few vendors, such as Proteus-Cyper [7], provide a one-stop-shop solution. Their GDPR Ready Software includes modules for data discovery (questionnaires to detect what data is held where and with which security implementation), maps (visualizations showing relationships among the datasets) and Data Protection Impact Assessment (DPIA) templates (documents to be filled out and submitted to the GDPR Supervisory Authority in the EU country where the utility has its main operating entity).

Figure 1 – GDPR Ready Software; Proteus-Cyber [7].

This report is not targeted to replicated these frameworks, but rather to fill a void in terms of strategic utility roadmap considerations based on the GDPR. It will review Privacy-Enhancing Techniques (PET) that utilities should contemplate to introduce and different forms of organizational alignments that can be beneficial in order to not only ensure compliance but also strengthening customer relationships and building a competitive GDPR-driven roadmap year after year.

GDPR - The Regulation

In this main part of the paper, we will go through the GDPR article-by-article and recommend approaches to build a comprehensive roadmap for the articles deemed most open-ended in the regulation.

DATA PROTECTION PRINCIPLES

Article 6(1) – Lawfulness of processing

> "Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes."

Over the last few years, improvements in low-cost interval metering and communication technology have started to enable load disaggregation through non-intrusive load monitoring (NILM) technologies, which estimate and report energy consumption of individual end-user loads. These technologies have the potential to enable many utility and customer facing applications but are at the same time also raising new privacy concerns.

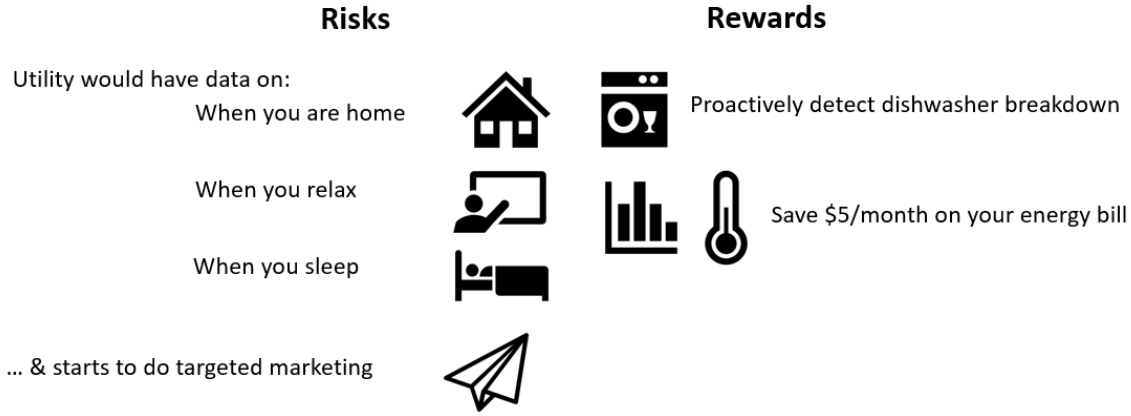

Figure 2 – Consumer Viewpoint on Load Disaggregation Services.

As mentioned in the introduction to this paper, information may be gleaned from this type of monitoring of electricity consumption that can disclose the approximate number of occupants, when they are present, as well as when they are awake or asleep. For many, this will resonate as a 'sanctity of the home' issue, where such intimate details of daily life should not be accessible. Utilities that are considering to add load disaggregation services in their long-term roadmap, are therefore recommended to validate the benefits of this service to the consumers vs. the privacy concerns they create before proceeding with any investments. It is worth noting that no high-uptake has been demonstrated so far in the market.

Article 7(3) – Conditions for consent

> "The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent."

The requirement on conditions for consent has been one of the least studied within the Smart Grids Task Force [8] that was formed within the European Commission. It has, however, implications on one of the common practices within utilities, i.e. the one "to refuse to serve" in case a customer decides to opt-out during a smart metering rollout. While it is true that most opt-out requests so far have been related to RF exposure risks from communicating smart meters, the increased attention to privacy is likely to make it a new reason for opt-out. In this sense, GDPR will require utilities to give users more real choices and not have a "take it or leave it"-attitude. One privacy-enhancing technique that could be considered as a more reasonable alternative to those who decide to opt-out for privacy reasons is Homomorphic Encryption (HE). HE would allow the utility to perform computations on the data while still protecting its confidentiality. For more details on this and other privacy-enhancing techniques, see page 16.

Article 7 also requires utilities to use clear and plain language to explain how they will use their users' personal details. The companies must provide information about what other kinds of entities users' data will be shared with**.** The digital platform part of the utility must obtain consent [9] from individuals for each use of their personal data. When a utility wants to use individuals' data for a new purpose, they must explain that new purpose and obtain users' permission again. When reviewing the frameworks that are available today for handling such granular consent processing, the User Managed Access (UMA) [10] standard stands out.

UMA supports a very user-friendly method for managing access control over personal data. It makes it easy to grant consent, share data and revoke consent at a granular level.

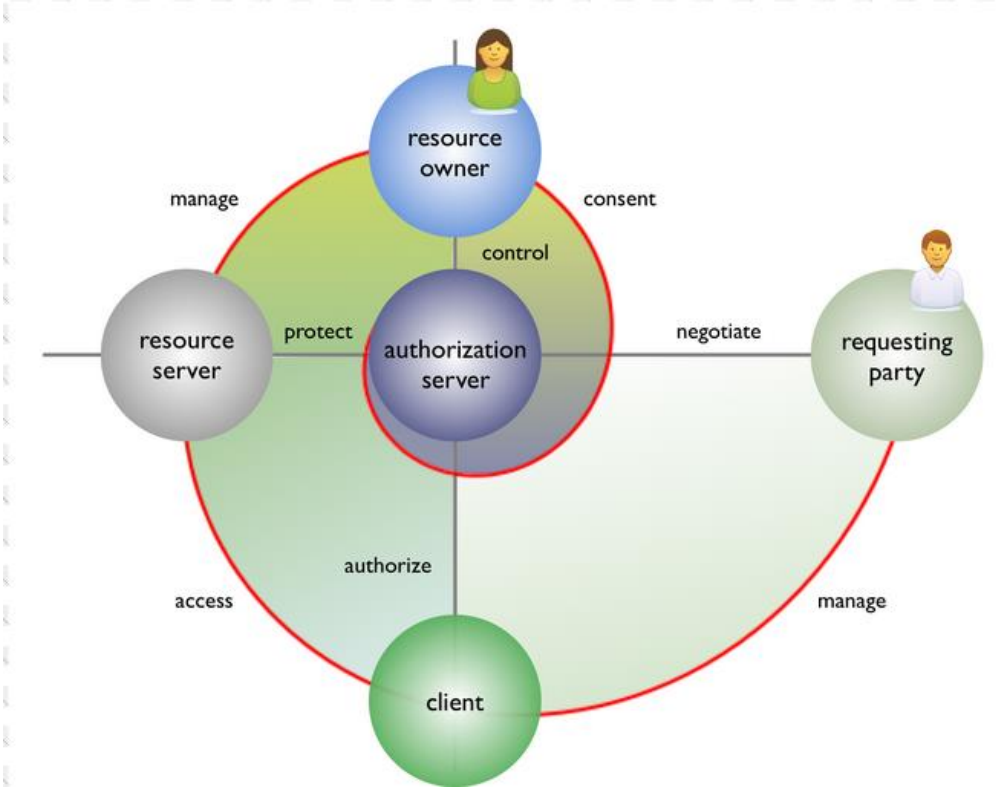

Figure 3 – High-level overview of the entities involved in the UMA framework; Kantara [10].

UMA is based on OAuth [11], the constrained delegation to apps and federation. It adds cross-party sharing for delegation and consent in the following ways:

- Share: Ahead of time
- Monitor: Anytime
- Withdraw: Anytime
- Opt-in: At run time
- Approve: After the fact

Article 9(1, 4) – Processing of special categories of personal data

> "1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited
>
> 4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health."

Even if utilities today do not process data included in the special categories of personal data in Article 9, it is important to be aware given that vendors most likely will come with products using, e.g., biometrics authentication in the future. It is also important to note that this article opens up for national legislation as well. So far nothing specific for the utility industry has been identified, but this is important to watch. Two leading DPOs are:

- the third generation of the UK Data Protection Bill [12]; and
- in Germany, the New Federal Data Protection Act, Bundesdatenschutzgesetz (BDSG New) [13].

Article 15(3) – Rights of access by the data subject

> "The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form."

Before we dive into the resolution to Article 15 and its rights of access to personal data, it is important to clarify that this definition includes any data that can be linked to Personal Identifiable Information (PII) and that the data include not only what the utility has obtained from the user and associated meter directly but also from third parties and the web.

A 74-page report from the European Commission Smart Grids Task Force Expert Group 1 was produced in 2016 to assess a unified compliance path to Article 15. The report is called "My Energy Data" [14] and it reviews related ongoing initiatives from ten Member States,

as well as the North American Green Button initiative. The following figure from the report, shows the scope.

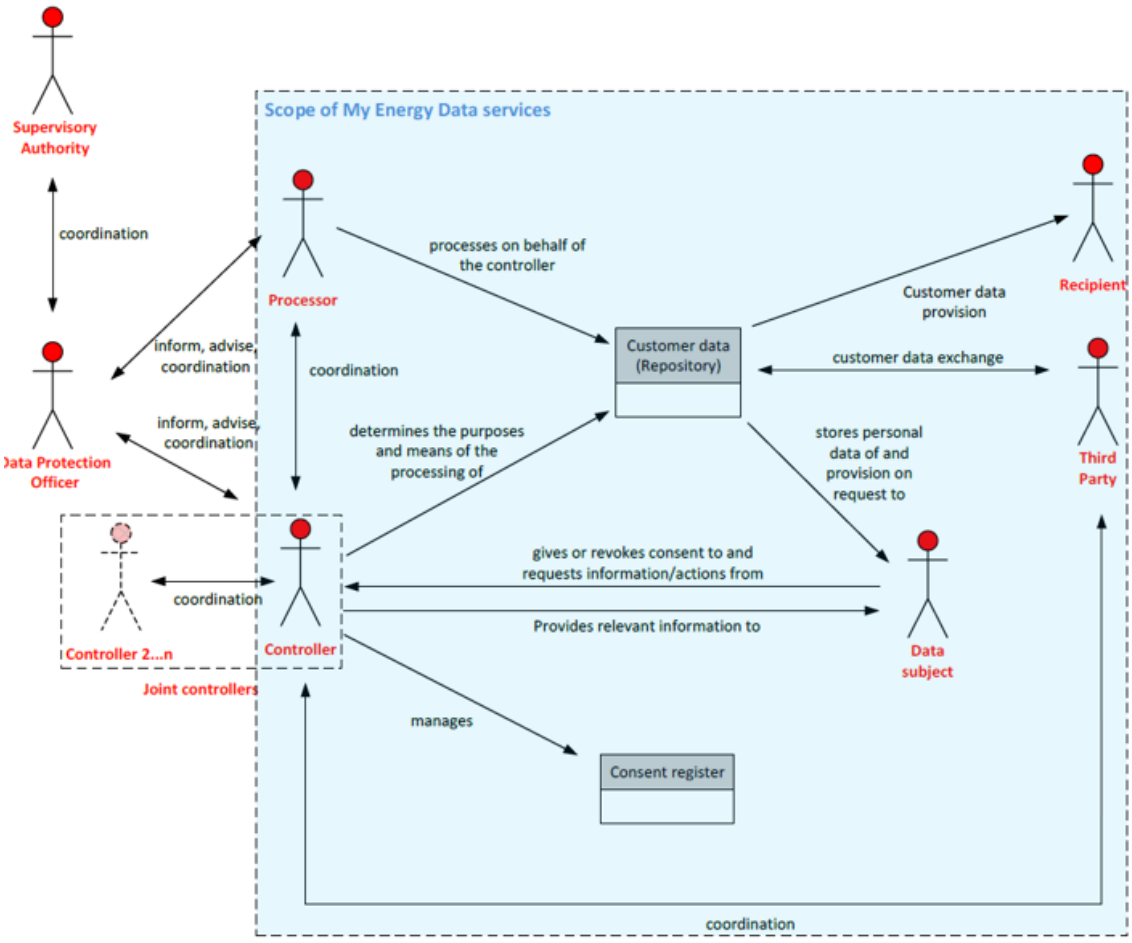

Figure 4 – Interaction model of GDPR roles in scope of "My Energy Data" services; EC Smart Grids Task Force [14].

The report points out the challenges for utilities with services that will need near real-time answers, and possibly with many requests in a short amount of time. The dynamic visualization of a load curve would for example require as many requests as the customers change the scope of the visualization. The utility industry has struggled with selecting the appropriate approach for this requirement. On the one hand, the utility network bandwidth is not enough for the refresh rates required for a truly interactive web portal. On the other hand, a deployment of in-home displays has been hard to rollout and maintain. A long-term strategy in this area does most likely include a third option where the user can get access to real-time smart meter data using a smartphone app and leveraging a local Wi-Fi network.

RIGHTS OF THE DATA SUBJECT

Article 20(2) – Right to data portability

> "In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible"

In order to allow users to swap energy supplier, most utilities within a country already have some type of capability to exchange data among each other as part of prior local regulations. However, as the Smart Grids Task Force Expert Group 1 discovered in its "My Energy Data" review, the protocols and object formats vary greatly from country to country. A common format could have a number of benefits including:

- Alignment and co-operation with international partners on equipment procurement.
- Bring more motivation for developers and as such more novel services.
- Facilitate service interoperability: a service developed in one national market could easily be sold in other markets.
- Facilitate the development of energy market services.

For this purpose, the Smart Grids Task Force has decided to form a Working Group on Electricity and Gas Data Format and Procedures [15] with the overall task to setup a common framework concerning format and procedures for electricity and gas data access and exchange in the EU-28. They will take into account the initial reflections on this issue captured in the interim report on "My Energy Data". While a final report is expected at the end of 2018, we can already conclude based on the "My Energy Data" report that two broad categories of data formats/models will need to be taken into consideration:

1. A human-friendly format (like CSV/XLS/PDF), that the end user can access to view or download his smart metering data and use with common IT tools (Download My Data service).

2. A machine-friendly format (like XML/JSON/CSV) that is used to exchange energy data with other 3rd parties (Share My Data service).

The 'My Energy Data' report lists the following minimum requirements for both:

- The format should be compatible with relevant European standards used in Member States smart meter rollout programs. This would facilitate interoperability of energy services across Europe.

- The format should be adaptable to handle different data time resolutions (like daily, hourly, 30 min, 15 min, 1 min, seconds data, or others adopted by Member States) or variable time resolutions.
- It should be flexible enough to support any type of variables and units (like for example aggregated energy consumption, Active & Reactive Energy, Gas, Energy Production or heat), to be able to address the different use cases implemented by each Member State.
- Scalability and expandability should be guaranteed from the start in regards to the incorporation of new variables/data in the future.
- The format should be easy to implement in the energy market with working knowledge that already is available.

In case a utility has plans to invest in this area already in 2018, then the Common Information Model (CIM), as standardized in IEC-61968, -61970 and-62325, is the recommended alternative to use as it is already the base for the US Green Button initiative and is being deployed in the Netherlands as well.

Article 22(2-3) – Automated individual decision making, including profiling

> "2. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
>
> 3. In the cases where this does not apply due to necessity for performance of contract or based on explicit consent, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision"

In combination with other technologies, Artificial Intelligence (AI) has the potential to deliver the active management that will be required for the grid of the future. Powerful intelligence will be able to balance grids, manage demand, negotiate actions, enable self-healing and facilitate a host of new products and services. Indeed, AI, will not just lend itself to the transition into a transactive energy market, it will also enable more efficient utility operations by helping to analyze unstructured data in the organization.

However, the state-of-the-art Machine Learning models are generally opaque, non-intuitive and difficult for people to understand, Article 22 and its prohibition of decision-making solely based on automated processing is therefore a real challenge. For this purpose, the US Defense Advanced Research Projects Agency (DARPA) has started a

multi-year program with several universities on Explainable Artificial Intelligence [16]. The program aims to enable human users to be able to understand, appropriately trust, and effectively manage the Machine Learning models. This is one approach to tackle Article 22 in the long-term. Some promising results have already been shown for Neural Networks by, e.g., adding a second Deep Learning algorithm to generate explanations.

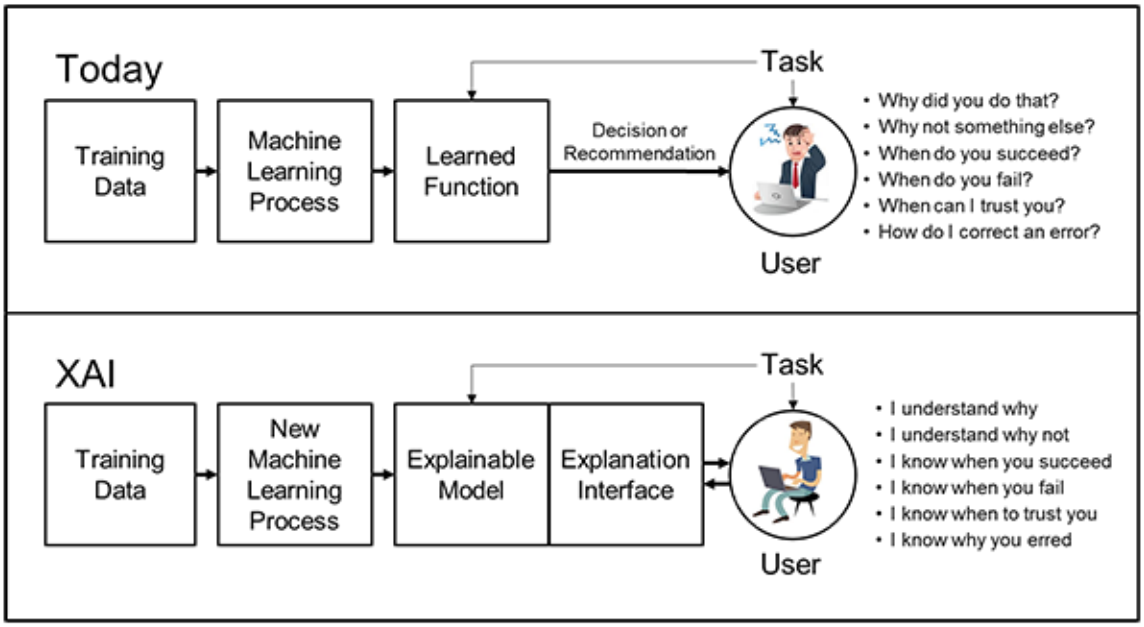

Figure 5 – Introduction to the Explainable AI Initiative; DARPA [16].

There will also be many instances where vendors and 3rd party service providers will encourage the utility to outsource the advanced processing to them and hand-over Personal Identifiable Information (PII) data. Given the ramifications in Article 22, it is not recommended to take that route too often. There should be justifiable reason to send PII data outside of the utility. If still required, ways to restrict this include to, e.g., offer pseudonymized query access only to the 3rd party service provider while still holding the data (and the PII mapping) within the utility domain.

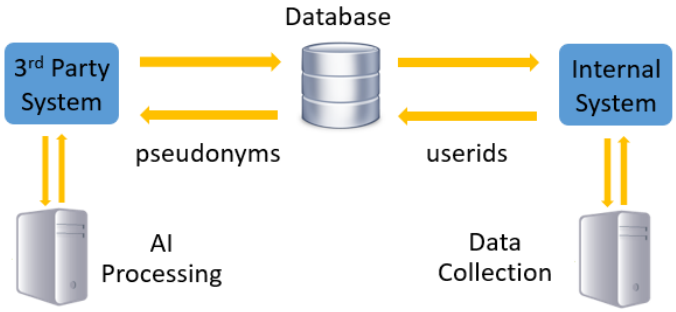

Figure 6 – Use of Pseudonymization when Outsourcing Advanced Processing.

CONTROLLER AND PROCESSOR

Article 25(2) – Data Protection by Design and by Default

> "The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

A 2016 report [17] from security ratings company BitSight Technologies ranked utilities as the worst prepared industry in the private sector for cyberattacks and data breaches that frequently make high profile headlines.

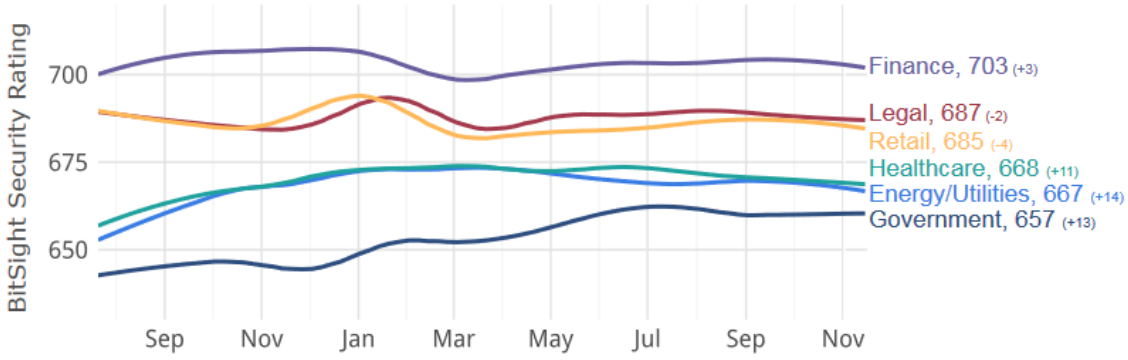

Figure 7 –Security Rating per Industry Sector in 2015-2016 including 2,841 Energy/Utilities from around the World; BitSight [17].

Meanwhile, at the core of GDPR is the concept of Privacy by Design [18], i.e. that all data identified as private must be protected in transit and at rest, and that the principle of these protections should be embedded in systems from inception. Some of the main considerations for utilities to integrate into future development programs, therefore, include:

- System architecture to adhere to the Confidentiality, Integrity and Availability of personal information in GDPR.
- Privacy as the default setting, granular access controls and use of data minimization/minimal retention in design.
- Security to be included in project definitions and risk assessments.

- Security analysis and penetration testing of common and not so common threats to Personal Data.
- Definition of mitigations to reduce risk.
- Identification of documentation to be retained.

If utilities can keep a clear separation between the Automatic Metering Infrastructure (AMI) and the Distributed Automation (DA) inside the company, they are likely to be able to handle the GDPR requirement better. The reason is that the metering data for AMI operations is usually of low frequency (hourly or even daily) but need to be associated to PII for billing purposes. Meanwhile, the metering data for DA operations require high frequency (second to minute level) but can be anonymized or aggregated per transformer feeder line to avoid location and behavioral usage patterns (see page 16 for more details on these Privacy-Enhancing Techniques). A process for this can be defined as per below.

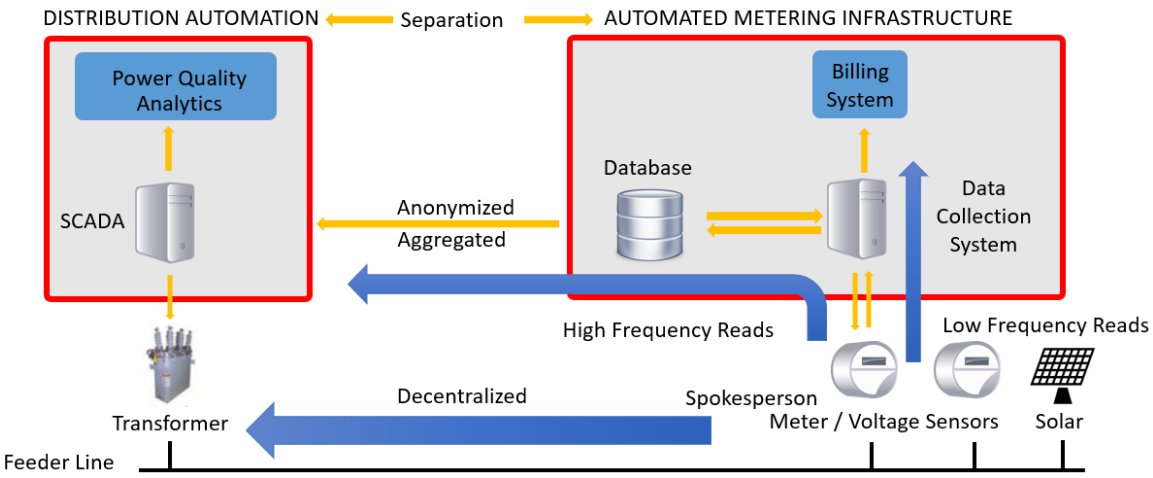

Figure 8 – Separation of AMI and DA Operations with Anonymized Data Interface.

Note that due to the high bandwidth requirements with bringing back high frequency voltage data it is recommended to consider a direct smart meter to power grid component communication out on the feeder line in a decentralized fashion. This would require to move the anonymization/aggregation function down to the meters and in a round-robin fashion elect a spokesperson for the smart meters to maintain anonymity.

Article 32(1-2) – Security of processing

> "1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
>
> 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed."

We divide this analysis in new and old (legacy) systems as the approach differs for each.

New systems

The EC Smart Grids Task Force Expert Group 2 has during the last two years been working on a Best Available Technique Analysis [19] for privacy, data protection and cyber-security in the smart grids environment and mapped those to the 10 most fundamental utility services: billable data readings, energy efficiency data readings, remote readings, two-way communications for maintenance, network planning readings, advanced tariff systems, remote off/on controls, secure data communications, fraud prevention and detection, import/export and reactive metering. In the work, they used the following reference architecture.

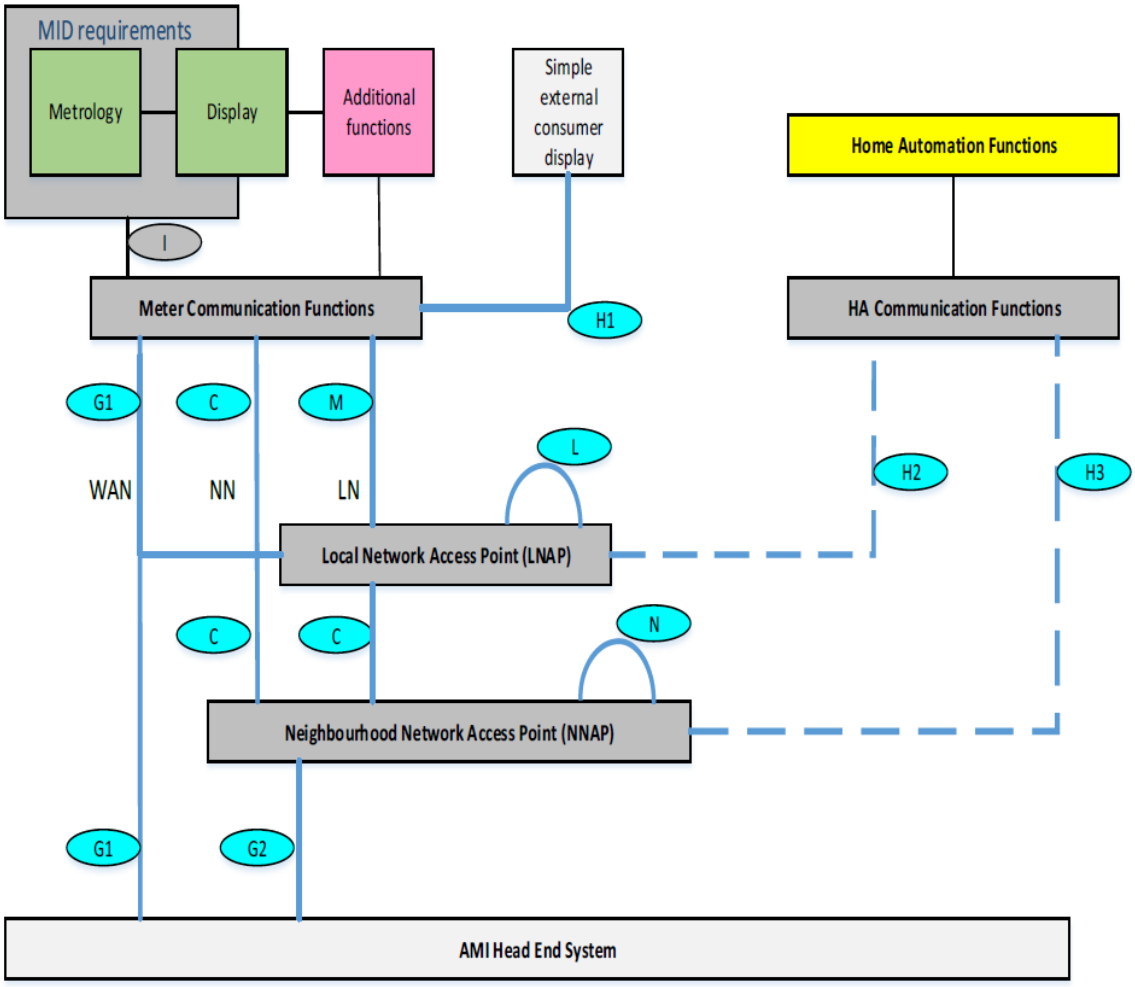

Figure 9 - Smart Metering Reference Architecture; EC Smart Grids Task Force [19].

While a lot of techniques were considered to improve cyber-security, a short subset was seen as having any real impact on privacy and data protection. The final list of Privacy-Enhancing Techniques (PETs) is shown in the table below with their individual ratings pertaining to the following criteria (2 being highest score):

- **Anonymity** allows the production of anonymized data.
- **Data Minimization** is considered in a privacy by design approach. A minimal set of personal data is used to implement the technique. No other technique can realize the same minimum functionality with a lesser amount of personal data.
- **Data Control** allows the data owners to have total control over the data collected unless strictly not possible to provide the service.
- **Data Access** allows the data subject to have total access over personal data collected.

- **Data Retention** is considered in a privacy by design and by default approach. No data is retained longer than what is strictly needed to make services available according to what is lawfully established and it is effectively deleted when not required. Data is only stored locally.

DOMAIN	TECHNIQUE	Anonymity	Minimization	Control	Access	Retention
(O*) Access Control / Consumer Use Case	Username/Password sent in clear to a server					0
	Username/Password stored and verified in tamper resistant module					2
	OTP					2
	2 factors Authentication					2
(O*) Access Control / Op. and 3rd Party Use Cases	Username/Password			0		
	OTP					2
	2 factors Authentication					2
(O*) Monitoring and alarming	(any technique)			0	0 or 2	
(O*) Security Architecture	Private location				1	
Component C* (applicable components)	Retention for data stored locally in meter or after contract has ended					2
	Daily transmission of interval data (CD, CF, OB, OD, OA)		2	0		
	1 second local intervals and bi-monthly readings		2	2		
	Aggregation (O*, P*)	2	2	2		2
Component P* (applicable components)	Aggregation (Px)	1	2			
	Multi-factor authentication (Px)			0		
	One-time password (Px)					2

Table 1 – Validity of Techniques for Privacy and Data Protection; EC Smart Grids Task Force [19].

Password stored and verified locally in a tamper resistant module gets a score of 2 in data retention if user is in control of the data collected. **One-time-password** provides additional security compared to regular password authentication in a sense that replay attacks have no effects and compromised passwords become ineffective. One specific use case identified for one-time-password is for use on smart meters, whereby the meter generates a code on the display that can be used to identify the consumer when assisting remotely. Finally, **2-factor authentication** gets 2 in retention as well because the user information is checked and stored locally.

Monitoring and Alarming can be achieved with any technique and gets a good score of 2 in terms of access if material is made available to the consumer.

Private location gets 1 in data access rating if the smart metering devices are mounted on the private property of the consumer and are not (legally) physically accessible by others.

Retention is also a technique in itself. The retention period for the storage of personal data must be in accordance to the European Data Protection framework and is split into:

- Max retention for data after the contract has ended (30 days as per GDPR).
- Max retention for data reading and logs stored locally in the meter as per individual local regulations (normally 30 days).
- Minimum reading and transmission frequency for making the time-based advanced tariffs possible (normally hourly interval data with user consent).
- Max six bi-monthly values for network planning purposes of 15-minute interval values and 1 second for local interface.

Aggregation for network planning purposes is considered in effect if more than 5 households are aggregated under the consent of the consumers. The high frequency used for these readings from the smart meter divulges information about an individual/household. Thus, privacy requirements are strict and this technique is considered mandatory to implement in order to make sure the data collection is appropriate. Data that are aggregated and anonymized for statistic and scientific research can normally be on monthly data and across a minimum of 10 households and without any references to individual meters. Note that the exact procedures may vary among EU countries as controlled by the national regulator. In the UK as an example, this is handled by the Information Commissioner's Office (ICO) [6]. For European research projects, the ICO provides meter serial number and occupancy of house today. This is considered PII as per GDPR and it is up to ICO to take corrective action. ICO has discussed to hold serial numbers in one system and user PII in another system with special credentials needed to have access to both. Some further anonymization before providing data to EU research projects is also expected.

In addition to the above software capabilities, hardware components such as **Switches and Meter Seals** for tamper detection are given a ranking of 2 in terms of privacy when the architecture provides means for the consumer to be aware of the data exchanged.

While the privacy enhancing techniques recommended by the Smart Grids Task Force are valuable and important, they are of the well-established kind. When looking to create a long-term roadmap, utilities may want to go beyond this list and a good source is then the survey that was performed by Eckhoff and Wagner in 2017 of privacy-enhancing techniques for smart cities [20]. In that paper, a set of data-oriented privacy techniques are reviewed that can enhance what the Smart Grids Task Force has proposed.

Differential Data Minimization can be derived from privacy by design. A specific challenge to data minimization is that more data is gathered and retained today by the smart meter than necessary for each task. The system should, therefore, preferably be

designed to limit and optimize data retrieval for the use case at hand. In smart metering, this would mean to allow different reading intervals per customer and service (e.g. separating out customers that use time-of-day tariffs for more frequent interval data collection).

Advanced Data Anonymization using k-Anonymity or Differential Privacy is aimed at preserving the privacy of individuals when releasing metering data for network planning or statistic/scientific research by providing both anonymity and unlinkability. In the case of k-Anonymity, the utility database that contains both identifying information (e.g. the names of individuals) and sensitive information (e.g. high-frequency, behavioral energy usage information) is split so that columns with identifying information are automatically removed before publication. k-Anonymity groups the database rows into equivalence classes based on transformer feeder line location with at least k rows being indistinguishable with respect to their quasi-identifiers. In the case of Differential Privacy, privacy is guaranteed instead by adding a small amount of random noise to the results of a database query. Regardless of principle chosen, the benefit is the same. The utility can now use high-frequency readings from smart meters for network planning purposes while not disclosing individual subscribers' behaviors to this personnel group.

Pseudonymization is a procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field. The purpose is to render the data record less identifying and therefore lower customer objections to its use. Data in this form is suitable for extensive analytics and processing by 3rd party systems that the utility subsequently can map back to the userid and as such avoid to disclose the PII to the 3rd party.

Encryption was not explicitly identified as a privacy-enhancing technique by the Smart Grids Task Force, but there are several variants that can protect the confidentiality of messages. Identity-based encryption and even attribute-based encryption are two such specializations, but the one mostly being associated to smart metering is Homomorphic Encryption. This is a cryptographic method that allows computations on encrypted data and thus protects confidentiality during data processing. The appeal of homomorphic encryption in utility applications is that it can be used to allow parties to process sensitive data without getting to know all the inputs for the computations.

Zero-Knowledge Proofs are a cryptographic method that allows one party (the prover) to prove their knowledge of some fact to another party (the verifier), without revealing the fact or any other information. Zero-knowledge proofs ensure that a cheating prover who does not know the fact cannot convince the verifier (the soundness property), and that a cheating verifier does not learn any other information (the zero-knowledge property). Zero-knowledge proofs provide confidentiality and privacy-preserving accountability. For example, they can be used for authentication, allowing the user to prove that they know

the password without revealing it. This technique has already been proposed in research for designing solutions for smart metering.

Secure Multi-Party Computation is a cryptographic method that allows two or more parties to jointly compute the value of a public function without revealing the parties' private inputs, and without relying on a trusted third party. This can have applicability for utilities that want to act as a broker in the transactive energy paradigm where users are both producers and consumers of energy and trade. The secure multi-party computations provide confidentiality and unlinkability. They are computationally expensive, but real-world applications have already been reported, for example to realize auctions where the final price can be computed without revealing individual bids. This has parallels to blockchain where no trusted third party is required. We caution, though, utilities to deploy blockchain as part of creating a transactive energy market until it has received a proper privacy framework.

Legacy systems

Whilst utilities can plan and apply the prescribed controls of anonymization, pseudonymization and encryption for new systems, older legacy systems are not as easy to update. The recommendation in this case is to apply a layered "onion" strategy to wrap the system with security controls and certify the setup to ISO27001 [21] in order to demonstrate compliance. In many cases, this means to host the application on a local server instead of in the cloud; to have it on its own network segment with additional firewalling; and to restrict access levels to the specific duties pertaining to each role (i.e. no power accounts). Additional training and employee NDAs may also be pertinent.

Article 33(1) – Notification of a personal data breach to the supervisory authority

> "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

Whilst a number of EU data protection authorities currently encourage controllers to report breaches, the Data Protection Directive 95/46/EC [3], which the GDPR replaces, does not contain a specific personal data breach notification obligation and therefore such a requirement is new for many organizations. The GDPR now makes notification mandatory for all controllers unless a breach is unlikely to result in a risk to the rights and freedoms of individuals [22]. Incidents can lead to notices, prosecution and / or fines as per below:

- Serving of improvement notices.
- Prosecution resulting in fines, reputation damage, loss of customers, increased insurance premiums, etc.
- Lesser infringement: 2% of global annual turnover or €10M (whichever is higher).
- Full infringement: 4% of global annual turnover €20M (whichever is higher).

Figure 10 shows the technical security incident conditions for which a breach notification is considered mandated. As can be seen, this covers a broad scope and need to be taken into account in the monitoring and reporting procedures inside the utility.

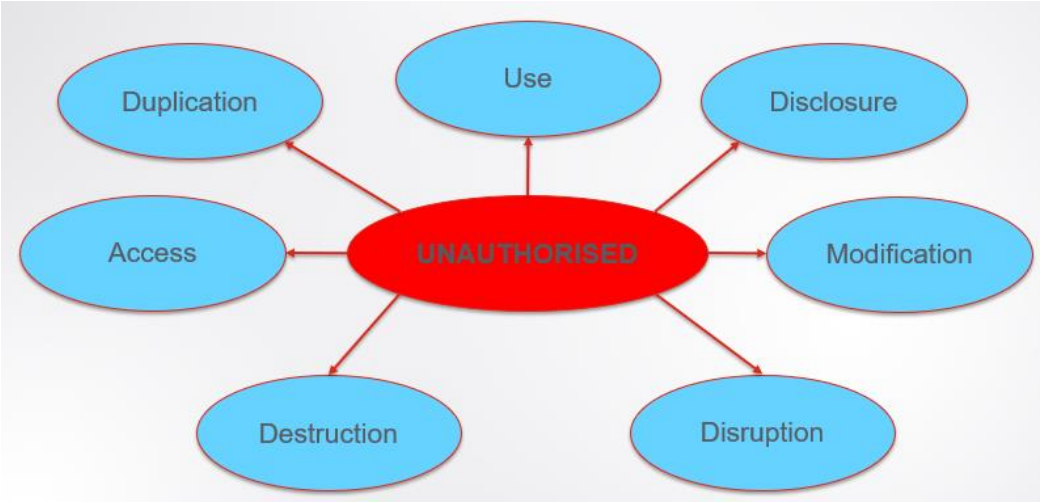

Figure 10 – Conditions Classified as Security Incidents in GDPR.

The breach notification is not definitive, meaning you don't need to have all the answers. A follow-on investigation can occur.

One of the challenging aspects for utilities with Article 33(1) has been the short 72-hour time window for notifying the supervisory authority given the number of sub-suppliers that often are involved in providing an energy service. As one example, we have seen contract language between a utility and a prepaid service provider that had as low as 24-hour breach notification from processor to controller. If one adds a second level of processor through, e.g., a cloud provider in this equation, the timelines start to become impossible to meet.

The European Commission Work Party 29 provided some relief on this aspect in its most recent revision of the Guidelines on Personal data breach notification under Regulation 2016/679 [23] that was adopted on February 6, 2018. It is now clarified that controllers are deemed to only be aware of a breach when it has been informed of it by the processor. Still this requirement has highlighted a weak point in utility business models that include a

string of processors underneath. Even if utilities have so far mostly been engaged in contracting updates to protect themselves on Article 33, it will longer-term be pertinent to consider flattening the supply-chain and potentially bring some parts of the offering in house to minimize the risks for false alarms and associated badwill given the short-time to notify on a personal information data breach.

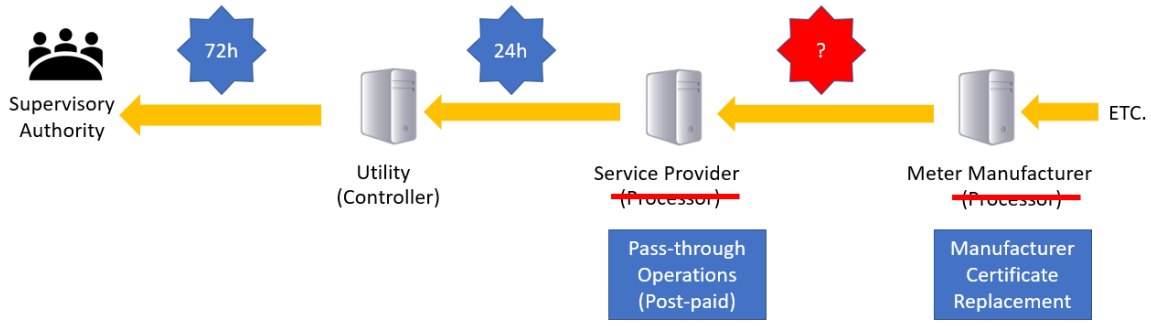

Figure 11 – Streamlining Roles in the Supply Chain for Simplified GDPR Compliance.

Furthermore, in case of meter vendors, the utility can demand to replace their certificates in the meter once deployed to avoid them as a processor. The IETF standard for Enrollment over Secure Transport (EST) [24] can be considered for this purpose in the long-term roadmap.

For utilities that outsource its metering reading operations, an alternative approach is to delineate responsibilities such that the service provider is not a processor. This can be achieved by having the service provider track meter serial number only with readings or by applying Homomorphic Encryption techniques as described in the next chapter on Article 32. The strategy is considered to work well for post-paid services (electric, gas and water), but not for pre-paid services in which case the service provider still has to hold customer name, address and credit information.

Article 34(1) – Communication of a personal data breach to the data subject

> "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

In case of a large-scale personal data breach, the controller does not only need to report this to the Supervisory Authority, but also to the affected users. A breach can concern confidentiality, integrity or availability of personal data. A security incident resulting in personal data being made unavailable for a period of time is also a type of breach, as the

lack of access to the data can have a significant impact on the rights and freedoms of natural persons. The controller should at least provide the following information:

- a description of the nature of the breach;
- the name and contact details of the data protection officer or other contact point;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

In principle, the relevant breach should be communicated to the affected data subjects directly, unless doing so would involve a disproportionate effort. In such a case, there shall instead be made through a public communication whereby the data subjects are informed in an equally effective manner. Both approaches can be considered for utilities.

Utilities have millions of users - many of which only hear from their utility once of month through the utility bill. Based on this large user base and infrequent communications pattern, we have seen service providers in the UK working to handshake with the Supervisory Authority to make breach notifications on their behalf to the public. This practice has the benefit of not risking to use a contact channel that is compromised by the breach (and as such could be used by attackers for impersonation). The approach does, however, not take the opportunity to proactively establish a better communication pattern with the users and switch from selling a pure commodity to selling energy as a service as is desired within the industry. SMS and email are two communication forms that the EC Working Party 29's lists as recommended direct messaging mechanisms. For more forth-coming utilities there is also the opportunity to integrate breach notifications with smartphone apps and wall-mounted energy monitors such as those made popular by Quby [25] in the Netherlands.

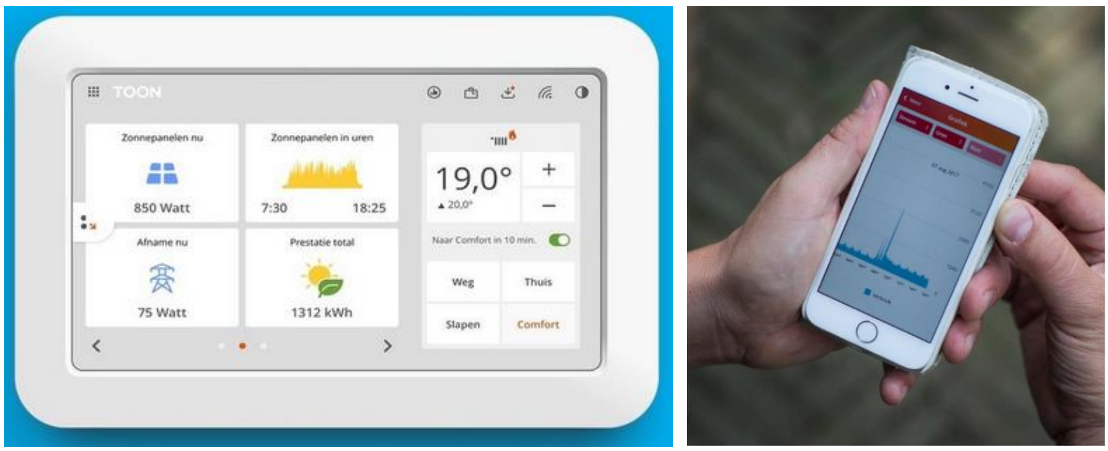

Figure 12 – The Toon Wall-mounted Energy Monitor and Smartphone App; Quby [25].

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES
Article 44(1) – General principles for transfers

> "Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."

Article 44 requires the controller to guarantee the location of data inside the European Economic Area (EAA) and it has been one of the most difficult requirements in GDPR for utilities to fulfil given their often multi-national organization and frequent use of outsourcing / cloud storage. The status today is that Russia and China do not have legislation that can be referenced for compliance, while US operations are covered by the EU-US Adequate Privacy Shield Agreement and Certification. Operations in, e.g., India can be made compliant but, in that case, only through an explicit ISO27001 [21] certification.

A bit surprisingly, cloud service providers have been some of the most difficult processors to deal with as per interviews we have made for this report. They are large and intimidating and like to dictate the terms of contracts tipping the ownership of compliance back to the utility (e.g. the ownership to track where the personal data is stored). In this case, the best way is to stay firm and to ensure that Article 28.3, describing the requirements on a processor, is verbatim included in sub-supplier contracts. Few B2B companies should be able to argue with such an ask if they want to stay in business.

Conclusions

Utilities have millions of unattended devices, a low overall rating as an industry in terms of cyber-security preparedness [17], many legacy systems that are not easily replaced and a business model that includes extensive outsourcing. This is not an easy starting point to answer up to the new GDPR regulation with its expanded PII definition and subjects access rights that applies to both controllers and processors. A lot of thorough work is currently underway within utilities to document Data Protection Impact Assessments (DPIAs) for the May 25, 2018 deadline when GDPR starts to be enforced. However, as the ICO [5] has realized, this is just the starting point. The next step for utilities is to create a

long-term GDPR roadmap with the target to not only achieve full compliance but also to strengthen competitiveness and customer relationships.

We have found that a fair number of activities are ongoing in the European Commission Smart Grids Task Force that will be beneficial for utilities to piggy-back on. In particular, the Working Group on Electricity and Gas Data Format and Procedures [15] is expected to release a final report by end 2018 with recommendations on standard protocols and formats for both "Download My Data Service" and "Share My Data Service". Aligning to those initiatives is seen as a safe way to achieve a strong GDPR roadmap.

Furthermore, in order to maintain control over Personal Identifiable Information (PII) we recommend to keep an organizational separation between the AMI and DA departments also in the future. Anonymization and aggregation are techniques to apply in the interface between the two as the need for high-frequency metering data increases within DA in order to manage the influx of more and more Distributed Energy Resources (DER) on the feeder lines. As can be supported by the vendor community, it is also proposed to look into a new decentralized privacy solution that avoids bringing back all the high frequency data from the smart meters to the back-office and instead communicating these directly to the power grid equipment on the same feeder line.

As for legacy systems, we propose to contain these using what we call an onion strategy, i.e. using layers of security related to where the application is hosted, how it is connected and who is managing it.

The GDPR also includes requirements on very quick breach notifications, a minimization per design of PII exposure and the prohibition of fully automated PII processing. These requirements would be easier to fulfill if having a flattened supply chain. This is, however, not always feasible from a cost, personnel and business model viewpoint. As such, we have identified several Privacy-Enhancing Techniques (PETs) that can preferably be used in the interface to 3rd parties including pseudonymization, meter vendor certificate replacement, pass-through post-paid meter reading, User Managed Access (UMA) cross-party consent and Explainable AI (XAI).

As Marlon Brando once said: "Privacy is not something that I'm merely entitled to, it's an absolute prerequisite". Similarly, GDPR is not something to merely be minimally adhered to, it's an opportunity to excel in. The journey has just begun.

Works Cited

[1] European Commission, "The EU General Data Protection Regulation," European Union, 2018. [Online]. Available: https://www.eugdpr.org/. [Accessed 5 2 2018].

[2] The European Parlament, "Regulation (EU) 2016/679 - General Data Protection Regulation," 27 4 2016. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. [Accessed 2018 12 4].

[3] European Commission, "Data Protection Directive 95/46/EC," 24 10 1995. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

[4] E. Iannopollo, "The State Of GDPR Readiness," Forrester Research, 2018.

[5] ICO, "GDPR is not Y2K," 22 12 2017. [Online]. Available: https://iconewsblog.org.uk/2017/12/22/gdpr-is-not-y2k/.

[6] ICO, "Information Commissioner's Office," 12 4 2018. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

[7] Proteus-Cyber, 12 4 2018. [Online]. Available: https://proteuscyber.com/.

[8] European Commission, 12 4 2018. [Online]. Available: https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force.

[9] European Commission, 24 1 2018. [Online]. Available: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615239.

[10] Kantara, 12 4 2018. [Online]. Available: https://kantarainitiative.org/confluence/display/uma/Home.

[11] Oauth, "Oath 2.0," 12 4 2018. [Online]. Available: https://oauth.net/.

[12] ICO, 14 9 2017. [Online]. Available: https://ico.org.uk/for-organisations/data-protection-bill/.

[13] BDSG, "Hogan Lovells," 24 8 2017. [Online]. Available: https://www.hldataprotection.com/2017/08/articles/international-eu-privacy/germany-publishes-english-version-of-its-national-gdpr-implementation-act/.

[14] European Commission, "My Energy Data," European Smart Grids Task Force _ Expert Group 1, Brussels, 2016.

[15] Europesan Commission, "Terms of Reference for Working Group on Electricity and Gas Data Format and Procedures," 17 02 2017. [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/tor_eg1_wg_on_data_format_procedures.pdf.

[16] Defense Advanced Research Projects Agency (DARPA), 12 4 2018. [Online]. Available: https://www.darpa.mil/program/explainable-artificial-intelligence.

[17] Bitsight Technologies, "Fourth Annual BitSight Insights Industry Index Report," 8 12 2016. [Online]. Available: https://www.bitsighttech.com/press-releases/new-report-highlights-criticality-cybersecurity-legal-sector. [Accessed 14 4 2018].

[18] European Commission, "Art 25 GDPR - Data protection by design and by default," 12 4 2018. [Online]. Available: https://gdpr-info.eu/art-25-gdpr/.

[19] European Commission, "Best Available Technique Reference Document," 2016.

[20] D. Eckhoff and I. Wagner, "Privacy in trhe Smart City - Applications, Technologies, Challenges and Solutions," 5 9 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8025782/.

[21] ISO/IEC, "ISO 27001, The International Information Security Standard," 2013. [Online]. Available: https://www.itgovernance.co.uk/iso27001.

[22] European Commission, "Charter of Fundamental Rights of the European Union," 26 10 2012. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

[23] European Commission, "Guidelines on Personal data breach notification under Regulation 2016/679 (WP250rev.01)," 6 2 2018. [Online]. Available: ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827.

[24] M. Pritikin, "RFC 7030 Enrollment over Secure Transport (EST)," 10 2013. [Online]. Available: https://tools.ietf.org/html/rfc7030.

[25] Quby, "Quby - we create Toon," [Online]. Available: https://www.quby.com/. [Accessed 12 4 2018].