Report

Consumer Control of Energy Data:

The Need for the Consent Management Mechanism in the Energy Sector of the Netherlands and Roadblocks Related to its Implementation

Lexo Zardiashvili and Francien Dechesne

July 2019
Leiden, Netherlands

SCALES project is a research project funded by the Netherlands Organization for Scientific Research programme on "Responsible Innovation", with several private and public partners participating. The overarching research question of SCALES is how to strike a balance between the occasional conflict stakes of individuals, public and private data-producers, data controllers and data-processors. The project aims to inform the regulatory and institutional landscape, allowing for optimal utilization of data analytics to serve the interests of governments, companies, and users, while optimally safeguarding individual rights and liberties. In achieving this objective, case studies have been conducted with the partners in the field of energy, law enforcement, and data analytics. This report has been produced by researchers at the eLaw Center for Law and Digital Technologies at Leiden University. In doing so, our understanding of practical aspects of the Dutch energy market is based on the information provided by Alliander as well as information available from public sources.

1. Introduction

In order for societies of the world to function or for countries to be able to power their economy, we need a stable energy supply. On the other hand, this energy supply has to increasingly come from renewable sources for our planet not to be depleted. [1] Following this reasoning, the United Nations prescribed *affordable and clean energy* as one of seventeen Sustainable Developments Goals. [2] This goal requires a focus on increasing energy efficiency and sharing of renewable energy sources in the global energy mix. Dealing with these two focal points requires encouraging energy market for investments, that implies expanding infrastructure and upgrading technology to supply modern energy services. [3]

The European Union designed a package of eight legislative acts, the "Clean Energy for all Europeans package", focusing the same focal points as UN to increase benefits for energy consumers (energy efficiency), for the environment (renewable energy) and economy (market encouragement). [4]

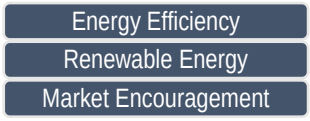

Figure 2. Goals of the Energy Reform

Among other things, technology in the form of *smart meters* is one of the factors influencing the energy market by creating possibilities for innovative business models, making it more profitable for businesses to provide clean and affordable energy. [5] Having this in mind, the EU legislative framework is promoting the introduction of such intelligent metering systems and setting 2020 as the target date to which 80% of energy consumers are equipped with smart meters. [6]

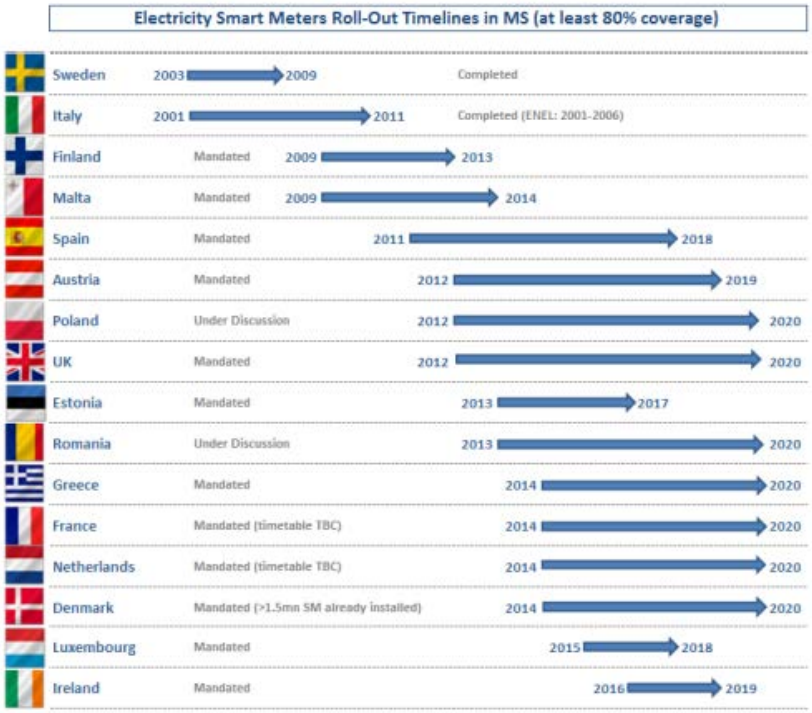

Figure 1. Roll-out plans: Implementation speed and penetration rate of at least 80% of all consumers by 2020 (Source: European Commission [41]).

By a decision of the Dutch government the large-scale roll-out of smart meters has started in January 2015 with the aim that at the end of 2020, smart meters should have been offered to all Dutch households. [7] This is envisaged to provide access to data, enable novel business models in the energy market in which participating consumer is empowered, and therefore, the goals of Clean Energy Package are achieved [8]

However, the roll-out in the Netherlands has pre-history as the initial plans for the introduction of smart meters sparked fierce public debate in 2008 about *data privacy*. [5] One of the core functions of smart meters is data collection, that is directed towards more efficient grid management. [9] However, as research shows this data can also reveal information such as: when a consumer is at home, and when s/he is away, when s/he cooks dinner, watches TV, takes a shower, when laundry is done, kids are alone at home or which TV channel is being watched. [10] [11] [12] [13]

To deal with privacy issues, individual control over personal data has become an important subject in the ongoing large-scale roll-out since 2015 in the Netherlands. The General Data Protection Regulation (GDPR) also addresses the need for more individual control over personal data more explicitly, designing *consent* as the ultimate tool for exercising such control. [14]

The Smart Grids Task Force Expert Group 1 (hereafter EG1) set up to advise the European Commission related to smart grid deployment predicted in 2016 that the amount of data on energy consumption will increase tremendously. However, they argued that a consent management mechanism, allowing consumers to access and manage their data, is crucial to fully reap the potential benefits for the energy market and consumers in general. [15]

This report analyzes the challenges that the Dutch energy market faces during large-scale smart meter roll-out, in particular during implementing the customer consent management mechanism to on the one hand allow access to data (and enable modern energy services) and on the other to ensure that consumer is in charge of his/her data. This report does not address security issues related to smart meters (for an overview of security issues, please see P. v. Aubel and E. Poll, 2019 [5]).

In Chapter 1, we will elaborate on actors in the Dutch electricity market. In chapters 2 and 3, we will describe smart metering infrastructure in the Netherlands, and the data flows within such infrastructure. In Chapter 4 we will explain how do previous chapters raise an issue of data privacy, while in Chapter 5 we will elaborate what role a consent management mechanism has to play in dealing with this issue. Chapter 6 will list the roadblocks towards the implementation of such a consent management mechanism, and in Chapter 7, we will draw our conclusions.

2. Actors in the Dutch Energy Market

The Transmission System Operator (TSO) is in charge of operating the higher-voltage electricity grid and transmits electrical power from generation plants over the electrical grid[i] to the *Distribution System Operator (DSO)* that is responsible for the operation of the electrical grid at a regional level. [16]

The DSO is typically also responsible for operating lower voltage grid, the installation of smart meters, and for collecting meter readings. [5] There are seven DSOs in the Netherlands, with the three largest – Liander, Enexis, and Stedin – serving the majority of the country's population. [17] All seven Dutch DSOs united with TenneT – electricity TSO and Gasuine – gas TSO – form in a sector association called *Netbeheer Nederland* (Netherlands Grid Management) that establishes and publishes, among other things, codes of conduct for the processing of personal data involved in smart metering for different market parties. [18]

The Netherlands operates with a *supplier-centric model* since 2013 – meaning that energy is sold to the consumers by the *Energy Suppliers (ES)*, the commercial parties that use the infrastructure of the DSO to deliver electricity. [19] ESs are the parties that usually have direct contact with the consumer, billing them not only for their services but also for the network costs on behalf of DSOs. [15]

This supplier-centric model can only operate if DSOs that have direct access to meter readings, provide these data to ESs, who then will be able to provide billing and insights to the consumers based on their consumption. (see Figure 3) The *Energie Data Services Nederland (EDSN)* was set up by the Dutch DSOs to smoothen administrative processes involved in the provision of metering data. It acts as the data hub or *central access server (CAS)*, providing metering data to ESs irrespective of the DSO responsible for the region where a consumer is located. [5] [20]

The introduction of smart meters triggers the formation of a new category of parties: the *Independent Service Providers (ISPs)* (*Overige Diensten-Aanbieders* in Dutch). [5] While DSOs and ESs are typically gathering data to provide their legally mandated services (e.g., grid management, billing), ISPs can use data from smart meters to offer additional services, e.g., advising how to save energy via a smartphone app or a web tool. [21] See a more detailed list of purposes for

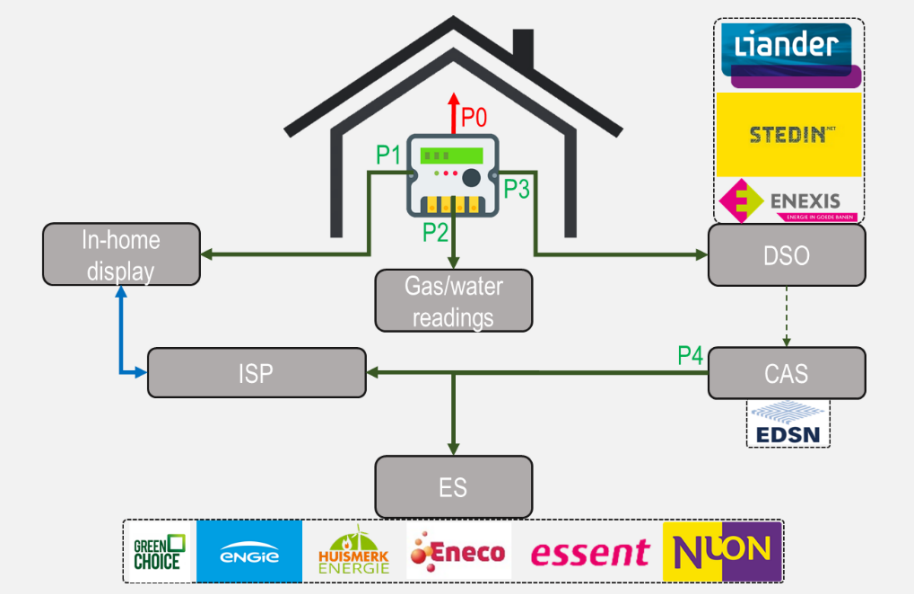

Figure 3. Standardized Smart Meter in the Netherlands (Source: DSMR [23], adapted from P. v. Aubel en E. Poll, "Smart Metering in the Netherlands: What, How and Why (draft)," vol. 109, pp. 719-725, July 2019. [5])

processing in Table 3. Purposes of processing smart meter data (Information from the Code [18])

ISPs that are operating energy price comparison websites, for example, can receive similar data as ESs via EDSN, while ISPs operating smart thermostats such as Google Nest [22], can get access to data by connecting directly to the smart meter at the location (See *Figure 3.* Standardized Smart Meter in the Netherlands (Source: DSMR [23], adapted from P. v. Aubel en E. Poll, "Smart Metering in the Netherlands: What, How and Why (draft)," vol. 109, pp. 719-725, July 2019. [5])

The next chapter provides a more detailed explanation of the categories of data that are being available by smart metering infrastructure.

3. Smart Metering Infrastructure

The last version of Dutch Smart Meter Requirements (DSMR) [23] published by *Netbeheer Nederland* prescribe specifications of smart meters. The smart meter itself has four communication ports (P0, P1, P2, P3), while the fifth communication port (P4) of the infrastructure is provided at the Central Access Server (at EDSN). (See *Figure 3.* Standardized Smart Meter in the Netherlands (Source: DSMR [23], adapted from P. v. Aubel en E. Poll, "Smart Metering in the Netherlands: What, How and Why (draft)," vol. 109, pp. 719-725, July 2019. [5]) Here are the specifications of each port:

P0 – This port is used for the local connection with external devices (such as hand-held terminals) during installation and maintenance work.

P1 – This port, also known as *consumer port,* allows for the local communication with third-party or auxiliary equipment, such as smart thermostats for instance. This port provides near-time information on energy consumption (see *Table 1.* Data via P1). It is a read-only interface and cannot be used to send data to CAS.

Table 1. Data via P1 (Source: DSMR [23])

Readings	Interval	Retention
Live electricity	1-10 seconds	-
Live gas	5 min	-
Tariff	Last available	-
Equip. status		-

P2 – This port connects to other local metering equipment, typically to enable connection with a smart natural gas or water meters.

P3 – This port communicates data from the smart meter to the Central Access System (CAS) of EDSN via head ends / systems of DSO's. Data that is being communicated includes meter readings (either the stored readings or the current meter readings), status checks, power quality and outage measurements, and remote updates (See *Table 2*. below)

Table 2. Data provided to DSO via P3 (Source: (Source: DSMR [23], adapted from P.v Aubel and E.Poll, 2019. [5])

Periodicity	Retention time
Monthly	13 months
Daily	40 days
Hourly (gas)	Ten days
15 min (electricity)	Ten days

P4 – This port is located at the CAS and communicates data to ESs and ISPs (data communicated to CAS from P3). Note that in some documents, P4 is used to describe communication from both P3 and P4 ports, as the same data is communicated via both ports.

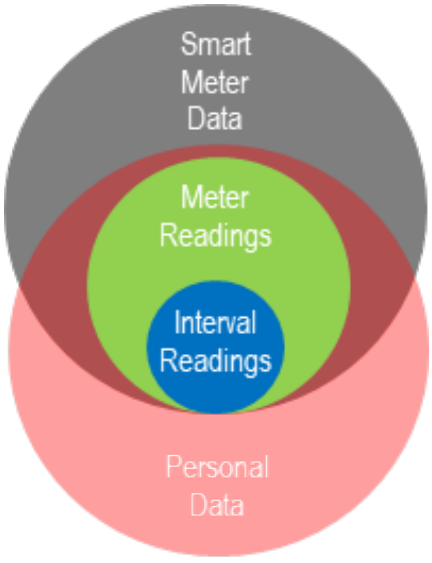

Figure 4. Relation of Smart Meter Data and Personal Data (Source: Code [18])

However, this should not be understood as EDSN pro-actively collecting metering data into a central database. [5] Metering data (*Table 2)* is stored in a meter. When ES or ISP requires metering data of a customer, it requests data from EDSN; EDSN forwards requests to the responsible DSO. DSO retrieves requested metering data via P3 port and sends it to EDSN, that caches data and awaits for final request from ES or ISP. Upon such request, EDSN communicates metering data via P4 port to ES or ISP.

Note that such process for the retrieval of meter readings might take up to 24 hours, the difference between P4 and P1 is not just that P4 data is less fine-grained (15-min data instead of 10-sec), but also data is not available in real-time if it is communicated via P4. [5]

4. Processing of Personal Data

Data generated in the smart meters can reveal personal information about the consumers. [10] Having this in mind, *Netbeheer Nederland* issued the "Code of Conduct for the Processing of Personal Data by DSOs in the Context of Installation and Management of Smart Meters with Private Customers" (hereafter "Code") that is legally binding for all DSOs since 2012.

The code [18] categorizes data into three types of data: (1) smart meter data – covers all the data received by CAS, such as status (up/down), the settings of the clock and firmware. (2) meter readings (in Dutch: *"meetgegevens"* or *"meterstanden"*) refer to the data that relates to the energy consumption of the customer. (3) Interval readings are meter readings based on a specified time interval (e.g., 10-second, 15-min data for electricity). *(See Figure 4.)*

The code explains that while meter readings (and therefore interval readings) are personal data, not all smart meter data can always be considered personal data. For example, anonymous technical data such as information on *time synching*, *voltage quality, or battery status* fall outside of the scope of personal data. [18] The Code was approved to be in compliance with *Wet bescherming persoonsgegevens (Wbp)* or the Dutch Personal Data Protection Act by *College Bescherming Persoonsgegevens (CBP)* that was the name of the Dutch Data Protection Authority at that time. [24] Nevertheless,

Processor	Purpose		Controller	Caterogry of data	Personal / non-pesonal data	Ground for processing	Limitations
DSO	A. Grid Management	A1. Technical control of the grid	DSO	Smart meter data	Non-personal data	N/A	Not if remotely turned-off
					Personal Data	Statutory obligation	
		A2. Meter management		Smart meter data	Non-personal data	N/A	No limitations
					Personal Data	Statutory obligation	
		A3. Analytics and statistics		Smart meter data	Non-personal data (including anonymised personal data)	Statutory obligation	Not if remotely turned-off
	B. Market Facilitation	B1. Billing	ES	Meter readings (excl. interval readings)	Personal data	Statutory obligation	Contract between ES and a customer
		B2. Energy saving		Meter readings (excl. interval readings)	Personal data	Statutory obligation	Not if remotely turned-off
		B3. Other services	ES / ISP	Interval Readings	Personal data	Consent	Not if remotely turned-off
				Smart meter data	Non-personal data	N/A	Not if remotely turned-off
					Personal data	Consent	

Table 3. Purposes of processing smart meter data (Information from the Code [18])

the Code fails to draw a complete picture to what exactly constitutes processing of personal data (in particular, smart meter data other than meter readings), an issue that we will also touch upon in chapter 4.

Following the reasoning in the Code, meter readings communicated from the smart meter to DSOs (and afterward to CAS) via P3 port are personal data. The Code also clarifies *purposes* for which DSOs can process the mentioned data (see *Table 3*.):

A. Grid management – amended Electricity Act of 1998 [25], Electricity and Gas Information Code (hereafter "Information Code") [26] and the Code [18] prescribe legal mandate of DSOs to provide grid management as their primary task. Such management might include locating and solving voltage interruptions, reducing grid loss, executing control orders, or other related tasks (see in *Table 3*. - A1. Technical control of the grid). Grid management also refers to tasks related to meter management (see in *Table 3*. – A2), and includes synchronizing clock in the smart meter, checking battery status and other related tasks. Finally, grid management activities can involve the processing of data for experimentation and innovation (see in *Table 3*. – A3).

Note that, because of the public debate on privacy issues regarding smart meter data (discussed in more detail in *chapter 4*), the Code prescribes a right of the energy consumer to "turn off" remote readability of smart meters. [18] If such right is exercised, DSOs are not allowed to continue processing data for technical control of the grid (A1) or data for analytics and statistics (A3).

However, DSOs can process smart metering data, including any personal data even when the customer has turned off remote readability, but the processing is necessary for meeting with the statutory obligation of managing the smart meters (see in *Table 3*. – A2).

B. Market facilitation – The second core function of DSOs is market facilitation. This might involve several types of processing. First of all, in the words of Electricity Act of 1998 [25] and the Data Management Regulation and the Payment of Electricity and Gas [27] the role of a DSO in the *"administrative process"* is to provide consumption data of a customer to ES for billing (See *Table 3*. – B1). Note that, while it is a statutory obligation for the DSO to provide consumption data to ES, for the latter processing of such data comes from the necessity of a performance of a contract. Therefore what kind of data has to flow to an ES is dependent on the agreement between the ES and a customer. [18] Currently, data necessary for the ES to bill the customer can be an annual (maximum monthly [28]) meter readings and excludes interval readings (15-min data). [5] If an ES wants to acquire interval readings for purposes other than billing, they have to ground such processing on consumer consent. (See *Table 3*. – B)

As mentioned earlier in chapter 1, other services that smart meter data can be used for include smart thermostats aimed to stimulate energy savings (See *Table 3*. – B2), or other services (e.g., price comparison service) (See *Table 3*. – B3). The ground for processing data mentioned in the previous paragraph is the consent of a customer. Note that, interval data can only be provided to ESs and ISPs if they have the explicit consent of a customer and, also, if they provide energy-saving services.

It is important to note that instead of obtaining the 15-min interval data via P3 (via the DSOs), an ISP can also obtain data via the P1 port. They then have to provide a consumer with a device to attach to P1 to send back data, e.g., via that customer's internet connection. Such information flow will circumvent the DSOs and CAS. [5]

Finally, it is not clear to what extent some smart meter data outside of the category of meter readings might fall under the definition of personal data. The question arises if the combination of different data (e.g., clock sync, voltage quality, meter status) can ever be combined in a manner to reveal privacy-sensitive information of a customer.

5. Data Privacy and Access to Data

The first phase of smart meter roll-out in the Netherland was initiated in 2007, having in mind the same goal of energy efficiency as today. [10] This initiative that tried to force smart meter infrastructure to

Dutch citizens did not consider consumer privacy beyond the *Wbp* which was in force at the time and failed to comply with the requirements of Article 8 of European Convention of Human Rights. [5] Following this reasoning the Senate of the Netherlands blocked this initiative and passed the laws only after several amendments. Detailed accounts of this phase of a roll-out provided by Cuijpers and Koops [10] reveal that by putting pressure on unwilling consumers to accept smart meters, initiators jeopardized public perception of the legitimacy of the roll-out.

In order to calm the public debate surrounding the privacy issues of the first phase of roll-out, the final package passed by the parliament not only removed the obligation to accept new smart meters, but introduced a possibility to "*administratively turn off*" remote readability of a smart meter if a smart meter had already been installed. (See *Chapter 3* in particular *Table 3*. – Limitations) These amendments also introduced the necessity of consumer consent for ESs and ISPs to process 15-min interval data, instead of this being the default metering regime. [5]

Statistics published by the central government in 2017, illustrated that around 10% of consumers refused installation of smart meters, and 2% had turned off remote readability. [29]

Under the current framework, it is not clear whether DSOs are able to process personal data beyond necessary tasks to maintain the functioning of the grid. (see in *Table 3*.) For instance, it is questionable if it is possible for the DSOs to collect consent to process personal data for improving the grid. (However, in one recent case, one of the DSOs, did ask for the consent from the consumers of energy to collect interval data. [30]) Note that these measures go beyond requirements of *Wbp* or the current *AVG* (Algemene Verordening Gegevensbescherming, the Dutch translation of the GDPR) to arguably decrease the pressure created by the public perception of the roll-out.

This approach allowed the Dutch government to pass a new roll-out law. However, another pressure that the market experiences is the forced move towards data access and exchange caused by "Clean energy package." EG1 refers to the Energy Efficiency Directive to state in their latest report ("*Towards Interoperability for Electricity and Gas Data Access & Exchange within the EU*") that consumers must be able to receive their meter reading data to allow access to it to the ESs or ISPs of their choice. [6] Moreover, EG1 suggests for the states to develop a standardized national arrangement to ensure that data access and exchange happens via a trusted mechanism, in a transparent and non-discriminatory manner. [19]

Currently, such a trusted mechanism is under development in the Netherlands (See [15]; [19]) and aims to provide a golden mean between two pressing needs described above – on the one hand, to enable the possibility of data exchange and, on the other, to maintain strong protection of privacy. Chapter 6 below, tries to describe such a mechanism in consideration and the challenges the market faces during its implementation.

6. Consent Management Mechanism

In March 2019, Netherlands Authority for Consumers and Markets (*Autoriteit Consument en Markt, ACM*) published a vision document on data governance with regard to energy (hereafter "ACM vision") [31] Aiming to complement "Clean energy package", this document designates the necessity of developing the system of data management in the Netherlands.

The ACM vision suggests that such a system should be reliable, affordable, and safe. Most importantly, this system must ensure consumer control over his/her data. The document refers to the right to data portability (hereafter Rt2DP) prescribed in the Article 20 of AVG [32] to describe desirable framework of the consumer

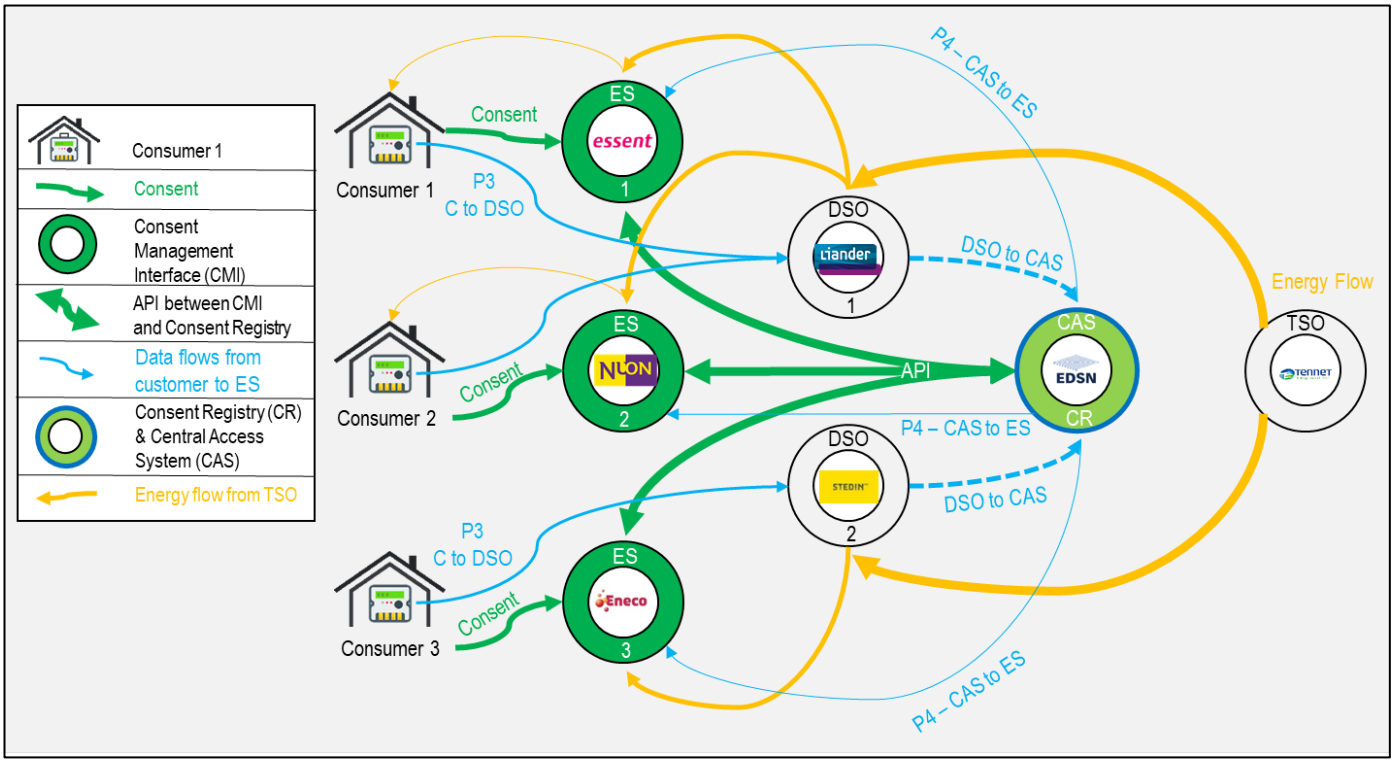

Figure 5. Flows in Central Access System and Consent Register.

control, suggesting that every consumer must have her own *"measurement data page"* on the internet, on which she is able to grant or withdraw access to the data to various market parties via *consent*.

In order to achieve such consumer-control, ACM highlights the importance of developing a comprehensive authorization model, so that it is technically impossible for unauthorized parties to have access to the data [31].

Although discussions on such trusted consent management (and authorization) mechanism for data governance has been ongoing for the last few years ([15]; [19]), it has escalated following the publication of the ACM Vision. The currently discussed platform-independent system aims to designate EDSN/DSO's as the party operating centralized consent registry (CR) for data kept by DSOs from DSOs' sources (e.g. metering data). This enables to register consent at the data source. Consent for other data sources should be given to the owner of- and resgistered at the data sourceThis CR will contain, among other information, a list of processing activities on the data of a consumer, history of consents, categories of data being processed, purposes, and grounds of processing.

ESs and ISPs that are in a contractual relationship with a consumer will connect to the CR with Application Programming Interface (API). They will have the option to display the information available through CR to the consumer in their independent online consent management interface (CMI) (See Figure 5).

Nevertheless, a genuinely successful implementation of such a system will need to take into consideration existent roadblocks discussed in the next chapter.

7. Roadblocks for Implementing CMM

There are particular roadblocks that Dutch energy market faces while working towards implementing the consent management mechanism for enabling access to the data for facilitating market and reaching the goals of "Clean Energy Package" as well as UN sustainable development goals:

I. General legal ambiguity - the First roadblock for successful implementation of CMM is ambiguity related to data governance in the Dutch energy market. [31] Primary (e.g., Electricity Act) and secondary (e.g., Information Code) legislation in the Netherlands not only pre-dates AVG but also scatters relevant provisions about processing of personal data, creating much ambiguity for the market parties about concretely what data constitutes personal data and what are their roles (who is a controller, processor).

II. Data confidentiality and access - even if legislation is organized and clarified it is questionable under the current substantive norms whether provision of data by DSOs to third parties for additional services (See Table 3 – B2, B3) is even allowed due to the confidentiality requirements in Article 79 of the Electricity Act [25]. To elaborate on this issue, right to access (hereafter RtA) prescribed in Article 15 of the AVG [32] does require DSOs to provide access to the consumers themselves, but not to ESs or ISPs. Such direct access (to ESs or ISPs) could be granted, for instance, if consumers exercised their right to data portability (rather than RtA) under Article 20 of AVG. [32] However, the Rt2DP can only be exercised if DSOs were processing the data on the grounds of the *consent* or *performance of a contract*. [33] While DSOs in all situations process data on the grounds of the statutory obligation (see Table 3) they are not always involved in the processing as the data controller. In cases where data is being processed for billing purpose (see Table 3 – B1), DSOs process personal data to support ESs that are supposedly data controllers, in this case, require data for the performance of the contract. Therefore it can be argued that in case of these data, the Rt2DP can apply to dissolve this roadblock. However, to say this with certainty, the first roadblock has to be dissolved, providing legal clarity on the roles of market parties with regards to the processing of personal data. Note that we refer to the confidentiality of the personal data regarding a consumer here. If DSOs are required to maintain the confidentiality of the data due to state or professional secrecy regulations, this cannot be overruled by Rt2DP nor by RtA.

III. Authentication - one of the most discussed roadblocks to the successful implementation of CMM is the challenge of authenticating the consumer, giving the consent to the access/exchange of data. If not dealt properly, this might cause the data breach. [34] Any individual can contact an ISP, claiming to live at some address to then obtain meter readings of that household. In 2015, a journalist demonstrated that some ISPs in the Netherlands do not perform any identity check whatsoever. [35] Moreover, there has been data leaks where an ISP or ES accidentally or deliberately abused their access to data kept by EDSN. [36] Currently, to counter this issue, DSOs are conducting additional access control checks, requiring ESs or ISPs to supply some customer-specific information as proof that customers have permitted to access their data. [37] Note that as the roles of the parties are not clearly defined (See *Roadblock I*) and often change from one party to another, it is not easy to define the final responsible party for authorization (and therefore responsible for any possible data breach). As DSOs are the first node to the data collection, it is sometimes expected from them to take on this responsibility. However, in cases where processing is related to market facilitation (see Table 3 – B), such an assumption might be flawed. Regardless of the clarity on this issue, currently thought consent management mechanisms assume shared responsibility of the parties that are working together to agree on the sufficient mechanism for the authentication. While *DigID* [38] is a government solution for online authorization and cannot yet allow private companies such as parties at electricity market to use their services, similar mechanisms provided by private parties are being discussed. Currently discussed possible solutions include iDin [39] that is the authentication solution similar to the popular identification tool in the banking sector of the Netherlands (iDeal) and IRMA [40], a privacy-friendly solution designed by the researchers at Radboud University. Moreover, authentication can also be ensured and enhanced with other verification means. Identity of a consumer can be checked for instance, by sending a letter by mail with some access code required to get access

to consent management mechanism online. While this is a costly and slow process, smart meter infrastructure itself allows a cheap and effective way to authenticate customers: Meters display a message send by the DSO via P3 port. So to check the identity of a consumer (or the link of the identity to the specific address), the smart meter could display a message that the consumer reports back to the consent management mechanism. Note, that this functionality is used in other countries to authenticate consumers, but not (yet) in the Netherlands. [5]

IV. Pressures – last but not the least significant roadblock to the proper implementation of the consent management mechanism are the pressures discussed in chapter 4. Fearful perception of the roll-out and the data exchange in public, might lead to posing excessive limitations on data processing within the Dutch energy market, hindering market parties to reap the full potential of smart metering, facilitate energy market by empowering the consumer and reach the goals of increased energy efficiency and renewable energy.

8. Conclusions

We have provided an overview of the situation in the Dutch energy market, in particular, elaborated the driving forces that are in place, pressuring market parties towards directions of increased privacy and at the same time more interoperability and open access to data. We highlighted roadblocks present while moving towards this direction and, by doing so, we hope to provide absolute clarity on the steps necessary to implement system ensuring energy consumer is in control of her data. The first step towards this direction can be an update of the legislation and dissolving legal ambiguity.

References

[1] United Nations, "Affordable and Clean Energy: Why It Matters".

[2] United Nations, "Sustainalbe Development Goals," United Nations Development Program, 2015.

[3] United Nations, "Ensure Access to Affordable, Reliable, Sustainable and Modern Energy," United Nations Development Program.

[4] European Commission, "Clean Energy For All Europeans," 2016.

[5] P. v. Aubel and E. Poll, "Smart Metering in the Netherlands: What, How and Why (draft)," vol. 109, pp. 719-725, July 2019.

[6] "Directve 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Dirrective 2003/54/EC," *Off J Eur Union,* vol. 211, pp. 55-93, 2009.

[7] The Minister of Economic Affairs, "Letter on Decree on large-scale rollout of smart meters - Security of energy supply and supply," 2014.

[8] M. Winters, "Roles and Responsibilities of Network Operators," Allen & Overy LLP, Brussels, 2018.

[9] N. Uribe-Pérez, L. Hernández, D. De la Vega and A. Itziar, "State of the Art and Trends Review of Smart Metering in Electricity Grids," *Applied Sciences (Accessed on ResearchGate),* 22 January 2016.

[10] C. Cuijpers and E. Koops, "Smart Metering and Privacy in Europe: Lessons from the Dutch case," *European Data Protection,* pp. 269-293, 2012.

[11] E. Quinn, "Smart Metering and Privacy: Existing Laws and Competing Policies," *A Report for the Colorado Public Utilities Commision,* 2009.

[12] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet and D. Irwin, "Private Memoirs of a Smart Meter," in *BuildSys '10 Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, Zurich, Switzerland, 2010.

[13] U. Greveler, B. Justus and D. Loehr, "Multimedia Content Identification Trhough Smart Power Usage Profiles," in *Computers, Privacy and Data Protection (CPDP 2012)*, 22012.

[14] I. van Ooijen and H. U. Vrabec, "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective," *Journal of Consumer Policy,* vol. 42, no. 1, pp. 91-107, 2019.

[15] European Smart Grids Task Force Expert Group 1 - Standards and Interoperability, "My Energy Data," 2016.

[16] ENTSO-E, CEDEC, GEODE, EURELECTRIC and EDSO, "TSO - DSO Data Management Report," 2016.

[17] Alliander, "Presentation Results 2016," 2017.

[18] Netbeheer Nederland, "Code of Conduct for the Processing of Personal Data by Grid Operators in the Context of Installation and Management of Smart Meters with Private Consumers," 2012.

[19] European Smart Grid Task Force Expert Group 1, "Towards Interoperability for Electricity and Gas Data Access & Exchange within the EU," 2019.

[20] Energie Data Services Nederland (EDSN), "Our Story," EDSN, [Online]. Available: https://www.edsn.nl/ons-verhaal/. [Accessed 1 July 2019].

[21] INNAX, "Onze dienstverlening," INNAX, [Online]. Available: https://www.innax.nl/diensten/energiemeetdiensten/oda-diensten/. [Accessed 1 July 2019].

[22] Google Nest, "Nest Learning Thermostat," [Online]. Available: https://store.google.com/product/nest_learning_thermostat_3rd_gen. [Accessed 2 July 2019].

[23] Netbeheer NL, "Dutch Smart Meter Requirements 4.0.7," 2014.

[24] College Bescherming persoonsgegevens (The Dutch Data Protection Authority), "Besluit Gedragscode Slimme meters," Staatscourant van het Koninkrijk der Nederlanden, Den Haag, 2012.

[25] "Elektriciteitswet 1998," Staatscourant van het Koninkrijk der Nederlanden, Den Haag, 1998.

[26] De Autoriteit Consument en Markt, "Informatiecode elektriciteit en gas," Den Haag, 2016.

[27] "Regeling gegevensbeheer en afdracht elektriciteit en gas," Economische Zaken, Landbouw en Innovatie, Den Haag, 2011.

[28] De Rijksoverheid voor Nederland, "Convenant energiebesparing gebouwde omgeving," Den Haag, 2019.

[29] Netherlands Enterprise Agency (RVO), "Marktbarometer aanbieding slimme meters.," 2018.

[30] J. Jansen, "Stedin wil slimme meters van zonnepanelenbezitters uitlezen voor info stroomnet," *Tweekers,* 27 May 2019.

[31] Autoriteit Consument & Markt, "Visie datagovernance energie," 2019.

[32] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da,* Brussels: Official Hournal of the European Union L 119/1, 2016.

[33] H. U. Vrabec:, Uncontrollable: Data Subject Rights and the Data-driven economy, Leiden: (PhD Thesis) , 2019.

[34] B. te Paske, C. Cuijpers, M. van Eekelen, E. Poll and B. van Schoonhoven , "Risicoanalyse Slimme Meter Keten," TNO, Delft, Netherlands, 2012.

[35] M. J., "Slimme meter makkelijk af te lezen voor iedereen," 2015.

[36] K. J., "Gegevens over energieverbruik twee miljoen huishoudens gestolen," Nu.nl, 2016.

[37] NEDU, "Impressie actieplan dataveiligheid," 2017.

[38] DigID, "DigID," [Online]. Available: https://www.digid.nl/.

[39] IDIN, "About IDIN," [Online]. Available: https://www.idin.nl/en/about-idin/. [Accessed 1 July 2019].

[40] Privacy By Design, "About IRMA," [Online]. Available: https://privacybydesign.foundation/irma-en/. [Accessed 1 July 2019].

[41] European Commission, "Cost-benefit Analyses and State of Play of Smart Metering Deployment in the EU-27," European Commission, 2014.

[i] Large industrial electricity consumers are often directly connected to the transmission grid.