

A code of conduct for smart grid management, using smart meter data

1. Introduction

As the energy transition unfolds, the challenges for the local grid are increasing. Decentralization of energy generation, based on intermittent resources as sun and wind, leading to reverse power flows, are increasing. Electrification of heat and transport are also contributing to significant load increase, and dynamic pricing in the market including demand/response mechanisms, this all creates a challenging task for DSO's to maintain and operate the low voltage (LV) grid in an affordable and reliable way.

Digitalization is supporting today the high voltage (HV) and medium voltage (MV) grid in its operations and maintenance, as these grids are already significantly digitalized, but the level of digitalization of the LV grid is low, due to the large size of LV grids, to which millions of customers are connected. Only the smart meter at the grid connection point is providing reliable data on the quality of the distribution service which the grid operator is providing to its customers. For distribution system operators it is therefore essential that they are able to use smart meter data for operating and maintaining the LV voltage grid to address the challenges as described above.

However smart meter data at the connection point is classified as personal data, to which European privacy regulation (the General Data Protection Regulation, GDPR) applies. As existing legacy energy legislation does not yet address the issue of using smart meter data for grid management purposes, the Dutch Distribution System Operators (hereinafter "**DSO's**") found themselves in need of legal certainty regarding the possible use of smart meter data for smart grid management. The Dutch DSO's therefore developed in good cooperation with the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) a Code of Conduct under the GDPR which provides for this legal certainty. This Code of Conduct prescribes a standardized (risk-based) approach how DSO's are able to assess per use case that use of smart meter data is in compliance with the GDPR (*General Data Protection Regulation*) (*in Dutch: Algemene Verordening Gegevensbescherming AVG*).

This paper describes this Code of Conduct, which is called by the DSO's the "Smart Grid Management Code of Conduct" (hereinafter the "**Code of Conduct**"), and the way how it is being implemented by the Dutch DSO's.

The Dutch Distribution and Transmission System Operators (DSO's & TSO's) recognize the potential of the digital transformation, but are also aware that privacy and security of data related to its customers and secure operation of the grid are crucial, when establishing a trustworthiness relation with their customers. They, as regulated system operators, expressed a clear ambition to become a trusted partner, on collecting, processing and distributing customer related data. In this respect the Code of Conduct should be regarded as a first milestone in a journey to achieve that ambition.

2. Starting points

The Code of Conduct has been developed from a governance framework, which is based on the following starting points:

- **Limited scope**

The Code of Conduct has a limited scope; the scope of the Code of Conduct is limited to the collection and processing of smart meter data which supports the operation and maintenance of the grid, which includes customer related processes and the processing of smart meter data. Distribution of (smart meter) data to third parties (such as energy suppliers) is explicitly out of scope of this Code of Conduct¹.

- **Code of Conduct applies to all Dutch System Operators (DSO's and TSO's)**

The Code of Conduct applies for all Dutch DSO's and TSO's and is adopted and approved of by all Dutch system operators (including the TSO's) via their cooperative association structure within their association "Netbeheer Nederland".

- **Agile governance**

Agile governance with appropriate checks and balances: In order to accomplish sufficient checks and balances within the responsibility domain of the Dutch System Operators, when processing (personal) data, we adopted and established the so-called "3 Angle model" regarding the governance aspects to the collecting and use and of smart meter data:

- (i) This 3Angle model is based on the well-known concept of the "Trias Politica", being the fundament of modern Western democracies. With this concept of horizontal separation of powers, the following 3 powers are clearly separated: The legislative power, the executive power, and the judicial power; each with separate and independent powers and areas of responsibility, so that the powers of one branch are not in conflict with the powers associated with the other branches. We used this concept of separated powers to create balance and human oversight when processing personal data and assessing the risk associated with that processing.
- (ii) These powers are well balanced: none is more powerful than the other, which ensures (as much as possible) that none of these powers may become too powerful to control. We distinguish:
 - the "legislative" role, which is the Code of Conduct owner (the association Netbeheer Nederland) who is entitled to adjust and amend the Code of Conduct from time to time;

¹ Ensuring privacy compliancy on data exchange to third parties will be addressed in the development of the Dutch Energy Data Exchange Framework, and will built upon this code of conduct (see also paragraph 5)

- the judicial (monitoring) role, which is headed by the Monitoring Body (as meant in art. 41 of the GDPR) established by the Dutch system operators and that holds responsibility for monitoring compliance with the Code of Conduct, in an independent way, without prejudice to the tasks and powers of the Dutch Data Protection Authority. Also the Data Protection Officers, in their independent role, form a part of this monitoring role and are able to report to this Monitoring Body.
- The executive (operational) role, which is formed by the operational side of the business, which creates the use cases and therewith defines the demand for the use of smart meter data, and which is responsible for taking care of the agreed mitigating risk measures.

With this concept of the 3Angle model, the interests and fundamental rights and freedoms of natural persons (as meant in art. 35.1 GDPR) are protected in the best possible way. Besides that, this concept provides the necessary flexibility to assess and establish in a conjunctive way the best possible “data protection by design”, which is why we call it “agile governance”.

- **Limited code of conduct**

The Code of Conduct does not repeat (parts) of the GDPR, but further elaborates on the implementation of specific parts in the GDPR that are relevant and agreed by the system operators via their association structure. The core of the Code of Conduct consists of the following elements:

- (i) **Lawful basis**

The Code of Conduct sets forth a standard approach to assess whether data processing in a given use case is compliant. To avoid any doubt regarding the applicable lawful basis and to accomplish standardization in the sector, the lawful basis for processing of personal data by the DSO’s for smart grid management purposes (*netbeheerdoeleinden*) is set at “public interest” (art. 6.1.e GDPR).

Given the public task that System Operators have by law (Dutch Electricity Act 1998 and Gas Act (*Elektriciteitswet 1998 and Gaswet*)) “public interest” should be the lawful basis for processing personal data by the System Operators according to the Dutch Data Protection Authority. Given the public task of the DSO’s to manage and maintain the distribution grids, the lawful basis “legitimate interest” of the controller (the Dutch DSO’s qualify as controller), as meant in art. 6.1.f GDPR, was not felt appropriate, according to the Dutch DPA.

Although DSO’s being private companies, the Dutch DPA expressed the opinion that the existing Dutch Electricity and Gas regulations set forth an obligation for the DSO’s to manage and maintain the distribution grids, which cannot be qualified as specific legal obligations (art. 6.1.c GDPR) for processing smart meter data (as this is missing in the

current Dutch Electricity act. from 1998); as a result the obligations for the DSO's classify as necessary tasks to be performed "in public interest" (art. 6.1.e GDPR). This resulted in the approach regarding the risk assessments to be performed (see (ii)).

(ii) Necessity and Risk Assessment

A standardized approach to assess necessity and risk with 3 levels;

1. the necessity test to assess whether processing in the given use case is necessary to perform the public task (managing and maintaining the distribution grid) and associated risk (art. 6.1.e GDPR)
2. when risk remains high and therewith proportionality and subsidiarity demands are not met, the more in-depth Data Protection Impact Assessment (DPIA) follows for which a standardized DPIA template is to be used. When performing the DPIA, the monitoring role (privacy committee) and the operational role (use case working group) discuss with each other, making use of the guidance ethics approach by Professor Peter-Paul Verbeek (<https://begeleidingsethiek.nl/publicaties/guidance-ethics-approach/>) (art. 35 GDPR)
3. and ultimately a prior consultation to the Dutch Data Protection Authority when an assessed risk cannot be further mitigated with mitigating measures and/or procedures (art. 36 GDPR).

(iii) Information obligation and central point for complaints by data subjects

The Code of Conduct prescribes the provisioning of specific information regarding the processing activities by the DSO's for smart grid management to customers on this, including the possibility for formal objection by data subjects regarding. these processing activities by the DSO's.

(iv) Accountability

The Code of Conduct prescribes the provisioning (summary's) of TNA's (Task Necessity Assessments) and DPIA's on a joint public website of the DSO's and compliance reports in the annual accounts of the DSO's, which also have to be published on their websites.

3. Governance Framework

Agile governance

Based on the principles described in paragraph 2, a governance framework was defined, as shown in figure 1. This governance framework clearly expresses the separation of the 3 powers and roles, as well differentiate to the operational, managerial and executive levels within these pillars of the different powers. In this framework roles and responsibilities, related to the relevant requirements following from privacy regulation, have been defined, as well as the processes in which these actors work together.

	"Legislative"		"Monitoring (judicial)"		"Monitoring (judicial)"		"Operational"		"Operational"		"Operational"	
	Framing data usage for smart grid management		Monitoring assessment data usage for smart grid management		Monitoring information provisioning and complaint handling data usage smart grid management		Determination of data needs for smart grid management		Information provisioning & complaint handling usage data for smart grid management		Operational data collection & processing for smart grid management	
Executive board level (decisionmaking)	End responsible & owner of the code of conduct, mandated by all distribution system operators	NBNL	Endresponsible for correct execution of the assessment methodology, sanctioning and decisionmaking on assessment framework	MB	Endresponsible for correct assessment on information provisioning	MB	Decisionmaking sector use cases	DR S&I	Endresponsible for consistent information provisioning and complaint handling with respect to data usage for smart grid management	DR K&M	Endresponsible for compliancy of implemented use cases and mitigating measures	Dir AM
	Decision on code of conduct & updates, resubmitting to Privacy Regulator	NBNL	Decisionmaking on the assessment criteria in the assessment template (DPIA model)	MB	Endresponsible for correct assessment on complaint handling	MB						
Managerial level (processes & procedures)	Evaluation use code of conduct (periodically)	NBNL	Drafting independent advice on the result of the privacy assessment	FG	Assessing & advising on information provisioning and complaint handling with respect to data usage for smart grid management	FG	Decisionmaking on template sector use cases	DR S&I	Managing consistent information provisioning and complaint handling with respect to data usage for smart grid management	KT Klant	Operational monitoring of compliancy of implemented use cases and mitigating measures	Lid KT SM
	Consultation relevant external stakeholders	NBNL	Evaluating & updating assessment criteria in the assessment template (DPIA model)	FG	Escalation level on complaint handling & advise on individual complaints with respect to data usage for smart grid management	FG						
Operational staff level (execution)	Monitoring consistence with other legislation	TR	Executing privacy impact assessments	PO	Monitoring quality of information provisioning & complaint handling with respect to data for smartgrid management	PO	Drafting sector use cases	wg AM	Establishing centralized website & content management, incl. traffic monitoring	NBNL	Correct operational implementation of assessed use cases and mitigating measures	product owner AM
					Monitoring accessibility of the central website (incl. URL routing via websites DSO's)	PO			Enabling & routing questions & complaints from customers	NBNL		
									Intake and first tier response questions & complaints with respect to data usage for smart grid management	DSO's: PO		

Legend		
NBNL: association Dutch System Operators	DR S&I: sector board on system management & infrastructure	Lid KT SM: each DSO Member of sector working group on smart meters
TR: sector working group on regulation	Wg AM: working group on use cases	Product owner AM: business responsible person department for IT developments at each DSO Asset management
MB: Monitoring Body	DR K&M: sector board on customers & markets	
FG: Independent Data Protection Officer	KT Klant: sector management team on customers	
PO: Business Privacy Officer	Dir AM: director Asset management of each DSO	

Figure 1: The governance framework

Legislative

The General Meeting of the Dutch system operators, being the members of Netbeheer Nederland (*ledenraad*) acts on the decisive and executive level and holds responsibility over the (substance and content of the) Code of Conduct. Therewith the highest level of the association, the General Meeting of members, represents the legislative power in this governance framework.

Judicial (monitoring)

The Monitoring Body, as meant in art. 41 GDPR monitors compliance with the Code of Conduct and as such holds responsibility over the independent risk assessing in which the provisioning of information to the public and data subjects, forms an essential part. The actual necessity and risk assessing takes place on the managerial level in this pillar and is performed by an independent expert committee with a prominent advisory role for the independent Data Protection Officers (as meant in art. 37 GDPR) appointed by the DSO's, and a significant role for the cooperating privacy officers, who support the business owners of the Dutch System

Operators in the operational pillar. The Monitoring Body is in contact with the Dutch DPA and, without prejudice to the tasks and powers of the DPA, the Monitoring Body shall take appropriate action in cases of infringement of the code by a DSO, which eventually may lead to suspension or exclusion of the DSO from the association. The articles of association of Netbeheer Nederland provide for such mechanism.

Executive (operational)

The executive (operational) power, appointed to the cooperation of the System Operators within the *Domeinraad System & Infra* (which is defined in the articles of association as an association body), holds responsibility over the establishment of use cases defining the need for processing smart meter data, and over the correct execution of the risk mitigating measures and procedures laid down in the sector's Data Protection Policy (as meant in art. 24 GDPR) that forms part of the Code of Conduct as an annex.

The initiative to assess an use case, and explanation and description of the need of processing smart meter data, always starts within the business and therewith within this operational pillar.

3Angle model vs 3 Lines of Defence

The 3Angle model provides the necessary flexibility to assess any real risk regarding the interests and freedom of natural persons when processing data and also provides for the needed agility to establish in a conjunctive way mitigating measures to protect the interests and freedom of natural persons. To ensure this, the discussion method and guidance ethics approach is used by the privacy committee (monitoring role) and the use case working group (operational role).

Therewith this 3Angle model regarding risk assessment (and in the end risk management model) is to our opinion preferred above the 3Lines of Defence model more traditionally known in risk management. Risk associated with the processing of (personal) data needs a risk management model that is more flexible and agile then the 3 Lines of Defence model that can be perceived as a more traditional waterfall method. In order to achieve 'compliance by design' or 'data protection by design', a model such as the 3Angle model is needed. Especially the constructive discussion between the different roles (and therewith actors) in this model is needed to achieve an appropriate level of 'data protection by design' and risk assessing and managing.

4. Code of Conduct

Based on the principles and the governance framework described above, a Code of Conduct for smart grid management, using smart meter data, was developed, in close cooperation with the stakeholders within the DSO's, accountable for the responsibilities shown in the governance framework. This led to a Code of Conduct containing the following sections:

1. Scope

The scope of the Code of Conduct is defined to the processing (which includes collection and use) of personal data in the Netherlands by a distribution system operator (DSO) when processing customer metering data necessary for its lawful task, as referred to in The Dutch Electricity Act and Gas Act (*Elektriciteitswet 1998 and Gaswet*).

Granting of access to metering data concerning customers to a supplier or a third party, including the provision of information about the consumption of energy, billing, moving house and changing suppliers, are excluded from this Code of Conduct.

2. Purpose

In the context of Smart Grid Management, a grid operator shall only process meter data (which may contain personal data) insofar as such processing is necessary for the tasks of grid management as entrusted to it by law and is therefore in the legitimate interest of a grid operator; which are called '(grid management purposes' (*netbeheerdoeleinden*).

In accordance with the Dutch Electricity Act 1998 and Gas Act, a DSO does not carry out any processing activities other than those that are necessary for the proper performance of the tasks assigned to it by or pursuant to these Acts.

3. Information provisioning

The Code of Conduct requires DSO's to jointly inform customers in a comprehensible, unambiguous and uniform manner about grid management objectives related to their legal task. Customers are informed about the independent role and function of the DSO in the energy system, an explanation of metering data processed for grid management purposes and the way in which the DSO has safeguarded the interests of those involved.

The Code of Conduct requires DSO's to provide jointly, and in the same manner, clear information to customers about their right to complain regarding the processing of personal data for system operation purposes as is covered by the Code of Conduct; this without prejudice to the other provisions of the GDPR concerning the provision of information as applicable to each DSO as a data controller.

4. Risk assessment: 3 levels

The Code of Conduct defines a clear template in which the needs for collecting and processing of smart meter data is specified and unambiguously related to the purpose of grid management. To guarantee a uniform assessment of these use cases, the DSO's jointly adopted a data protection impact assessment model (DPIA model) that contains the relevant elements to be assessed (also described in the appendix to the Code of Conduct). The model consists of 3 different levels to assess; starting with the Network Task Assessment (NTA), and if from this assessment, the risk is qualified as "high", then a more in-depth Data Protection Impact Assessment (DPIA) is initiated.

In order to ensure a uniform assessment framework for the evaluation of an use case with the assessment model, the DSO's jointly adopted a Data Protection Policy in which they have specified the applicable mitigating measures and appropriate safeguards with regard to Smart Grid Management (this policy is annexed to the Code of Conduct and may be

updated from time to time with over time other mitigating measures and appropriate safeguards that have been established following the assessment procedures).

For each use case, the DSO assesses, using the assessment model, whether the intended processing of metering data should be regarded as the processing of personal data. In case of processing of personal data for grid management purposes, an assessment is carried out as to whether that processing is necessary for the fulfilment of its public task as referred to in Article 6(1)(e) of the General Data Protection Act by using the TNA template in the assessment model.

If it follows from this TNA assessment within the assessment model that, in the implementation of a use case, the processing is necessary to perform the public task of the DSO, and such safeguards are in place that the processing of personal data for grid management purposes is likely to present a low risk to the rights and freedoms of natural persons (in assessing the proportionality and subsidiarity in the necessity assessment), then following adoption and recording of this assessment the processing may take place in compliance with the other provisions regarding the processing of personal data in the GDPR and in the specific legislation and regulations for energy.

If it follows from an TNA assessment within the assessment model that a processing of personal data for grid management purposes is likely to lead to a high risk for the rights and freedoms of natural persons and/or if the processing, in view of its nature, size, context and purposes, is likely to lead to a high risk for the rights and freedoms of natural persons, then a more in-depth Data Protection Impact assessment (as meant in art. 35 GDPR) is carried out by using the DPIA template in the assessment model.

If it follows from the DPIA assessment within the assessment model that such (additional) measures and guarantees have been put in place that the processing of personal data for grid management purposes is likely to involve a low risk to the rights and freedoms of natural persons, then, after this assessment has been established and recorded, the processing may take place in compliance with the other provisions regarding the processing of personal data in the GDPR and in the specific legislation and regulations for energy.

If it follows from a DPIA assessment that an intended processing for grid management purposes is or can be subject to insufficient mitigating measures and suitable guarantees, as a result of which a too high risk to the rights and freedoms of those involved remains, then the DSO's can decide not to carry out the intended processing or to consult the Dutch Data Protection Authority (a 'prior consultation' as meant in art. 36 GDPR). The Data Protection Authority will then provide a binding advise to the DSO's regarding the intended processing.

These 3 levels of risk assessment, as described above is shown in figure 2

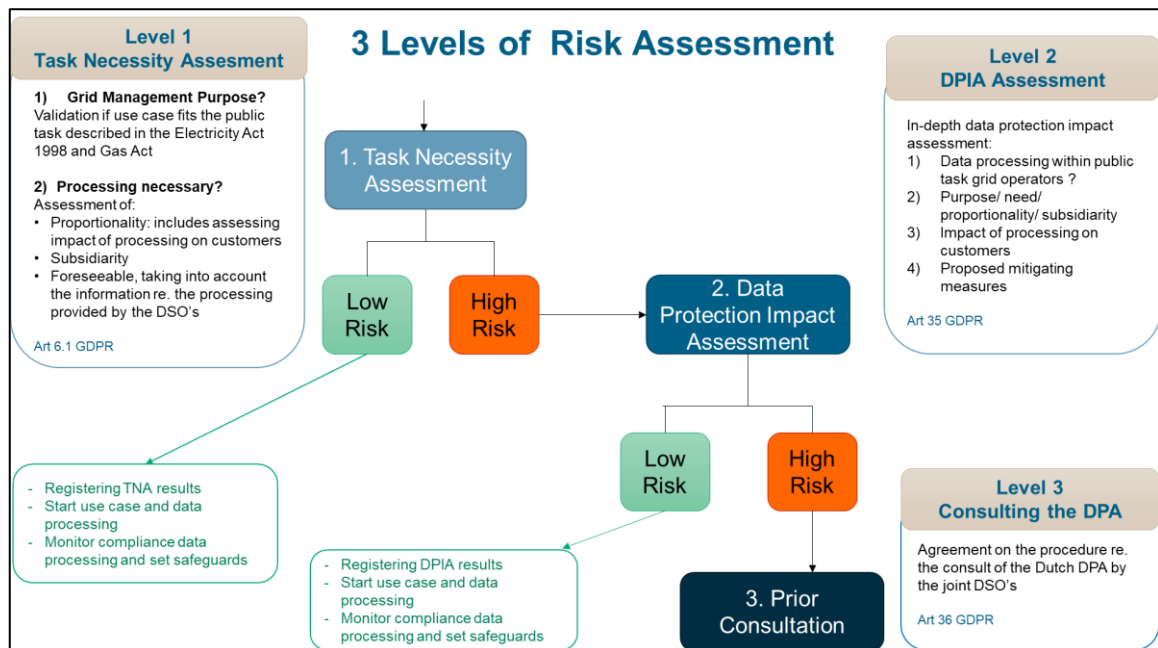


Figure 2: the 3 Levels of Risk Assessment

Future use regarding impact assessments

With this framework of 3 levels of risk assessment and the accompanying procedures regarding reassessment and timely evaluation of assessed risks, the DSO's have provided for a structure that safeguards human oversight. Moreover, this structure can also be applied for other cases where risk impact assessments are relevant, for instance when applying algorithms and use of artificial intelligence is requested in an use case.

5. Control & accountability

When executing an impact assessment (either it being a TNA or DPIA), the DSO's shall determine a validity period for the review of the assessed intended processing. A use case will be re-assessed when there is a change in the risk posed by the processing operations being assessed or if the validity period of the assessment of the processing has expired. When carrying out a re-assessment, a review of the initial implementation is conducted, including the mitigating measures and appropriate safeguards and a review of the information provided to customers.

The DSO's keep a joint register of use cases and assessments carried out using the assessment model. This includes the assessed degree of risk to data subjects and the time limit for re-assessment of the intended processing. A summary of the main results of the impact assessments (either it being a TNA or DPIA) is published in clear language and made

available upon request by a customer or other interested parties via the joint website of the DSO's.

The DSO's annually account for their compliance with this Code of Conduct by means of a statement of accountant in their annual reports, which include information on grid management purposes, the provision of information to customers, assessments carried out and impact assessments adopted, and handling of complaints from those concerned. In addition, a justification is published on the public websites of the DSO's.

Complaints on smart grid management

The Code of Conduct requires that the DSO's provide a joint transparent, simple and inexpensive procedure for dealing with queries and complaints from data subjects relating to the use of metering data for the purposes of smart grid management and thereby a single point of contact where customers can obtain all necessary information on their rights.

This procedure provides for safeguards that the complaint is not handled by a person who has been involved in the processing to which the complaint relates, that the complainant is informed in writing on finding and conclusions. The complaint is handled as soon as possible, in principle within eight weeks (which is in line with existing specific electricity regulations); all this without prejudice to the other provisions of the data protection regulation concerning the rights of data subjects and the provision of information thereon by a DSO as the data controller, as well other regulations to protect the data subjects in their role as consumer.

Monitoring

The Code of Conduct, defines an independent supervisory committee of this Code of Conduct: the Monitoring Body (as meant in art. 41 GDPR). The Monitoring Body is (to be) accredited by the Dutch Data Protection Authority in accordance with its accreditation criteria as approved by the European Data Protection Board (EDPB). This Monitoring Body, which is setup at executive board level, is fully accountable towards the Dutch Data Protection Authority on the monitoring of compliance with the Code of Conduct by all DSO's, including the provision of information to stakeholders, a correct functioning complaints procedure, and the process of assessing risks to stakeholders, and a correct execution of risk assessments with the assessment model (NTA's and DPIA's).

Operations & code review

The Code of Conduct is evaluated regularly by the DSO's, at least once every five years. Stakeholders' findings are included in the evaluation of the Code of Conduct. Any changes or amendments will be resubmitted by the DSO's (by Netbeheer Nederland) to the Dutch Data Protection Authority for approval.

4. Implementation

Developing the Code of Conduct and implementation in the organisations of the Dutch DSO's took place in the period of July 2020 – December 2021. The objectives were twofold:

- Developing a Code of Conduct for the users of smart meter data for grid management purposes, which is approved by the Dutch Data Protection Authority;
- Harmonization of existing procedures, which today differ between the Dutch DSO's, into one and for the customer, transparent process and means of communication.

After the governance framework was defined, it became possible to identify which departments and which functions in the organisations of the DSO's were responsible for acting on the identified roles & responsibilities. Via a significant number of internal stakeholder meetings those employees were involved in the development of the correct text of the Code of Conduct. Also the management and executives of the Dutch 'DSO's confirmed the governance, following from the governance framework and the need for harmonization.

During the development of the Code of Conduct also external stakeholder management was addressed. During the whole period a good and informal working relation with the Data Protection Authority was maintained, and the conversations with the Data Protection Authority contributed to the quality of the Code of Conduct. Also meetings with 2 consumer associations were held to inform them on the development of the Code of Conduct, the reasons and the approach the DSO's envisaged; their feedback, especially on customer communications aspects, were used in the process. With the Ministry of Economic Affairs two meetings took place to ensure consistency between the Code of Conduct and the upcoming new Dutch Energy Act.

Based on the Code of Conduct and the governance framework, the main processes, that substantiate correct usage of the Code of Conduct, have been developed and implemented in 2021. These processes are shown in figure 3.

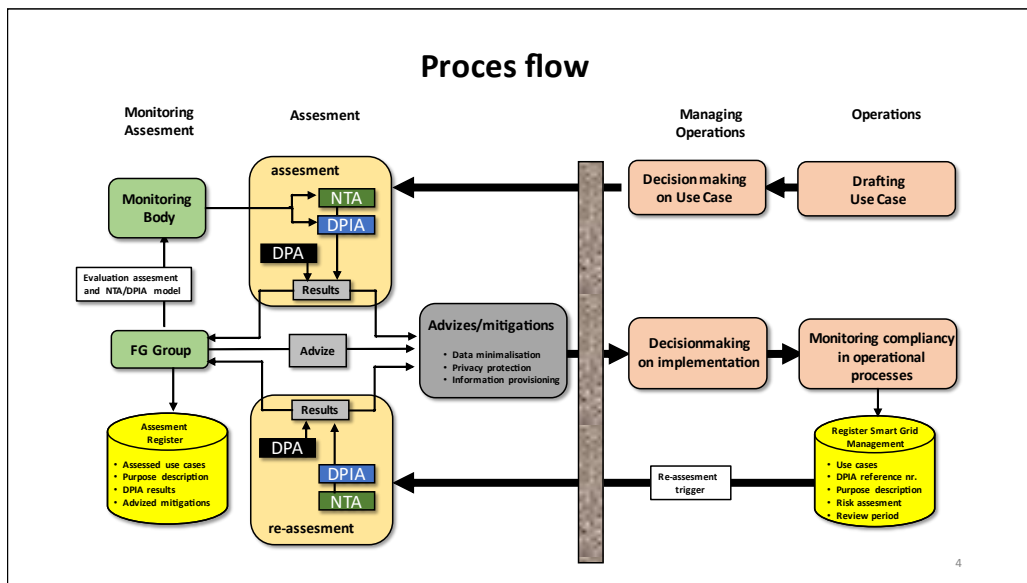


Figure 3 Process Flow

The following teams, populated with employees from all Dutch DSO's were established and kick off sessions organized:

- The working group “AM use cases”, responsible for drafting the sector use cases (e.g. on power quality, outage management, grid capacity planning), using the agreed sector use case template

The “expert group privacy GEMS”, in which privacy officers of the DSO's jointly work together, responsible for the actual assessment of the sector use case, resulting in an assessment report. The actual assessment is thereby based on a dialogue with members of the working group “AM use case” , which contribute to a good understanding of the assessment criteria and contributing to the quality of the use case before finalisation and its final assessment by the privacy officers from the expert group privacy. For this discussion, use is made of the Guidance ethics approach (a translation of the Dutch publication Aanpak begeleidingsethiek by ECP.nl: <https://ecp.nl/publicatie/guidance-ethics-approach/>) .

- The “FG group” (the group of Data Protection Officers (DPO's)), responsible for advice and monitoring compliancy to the GDPR. This DPO group will provide an independent advice on data protection impact assessment to the management responsible for system & infrastructure, on the sector use cases; their advice will be incorporated in the assessment report.
- The “customer communications group” staffed by employees from the customer communications departments of the Dutch DSO's. For harmonization and efficiency reasons it was decided to launch a centralized national website, specific addressing the topic of data privacy and the Code of Conduct which the DSO's adopted to guarantee data protection at the level the consumer expects. This website is integrated in the

portals of all DSO's (see figure 4). Traffic to this website will be monitored, as well as the number of triggered questions and complaints, as this will provide valuable feedback information for improvements, as well as it will support the expert group privacy in getting a common understanding and consistent subsequent actions on these questions and complaints triggered, necessary for their monitoring role within the 3Angle model. Each individual DSO will remain responsible for the correct and timely handling of questions and complaints.

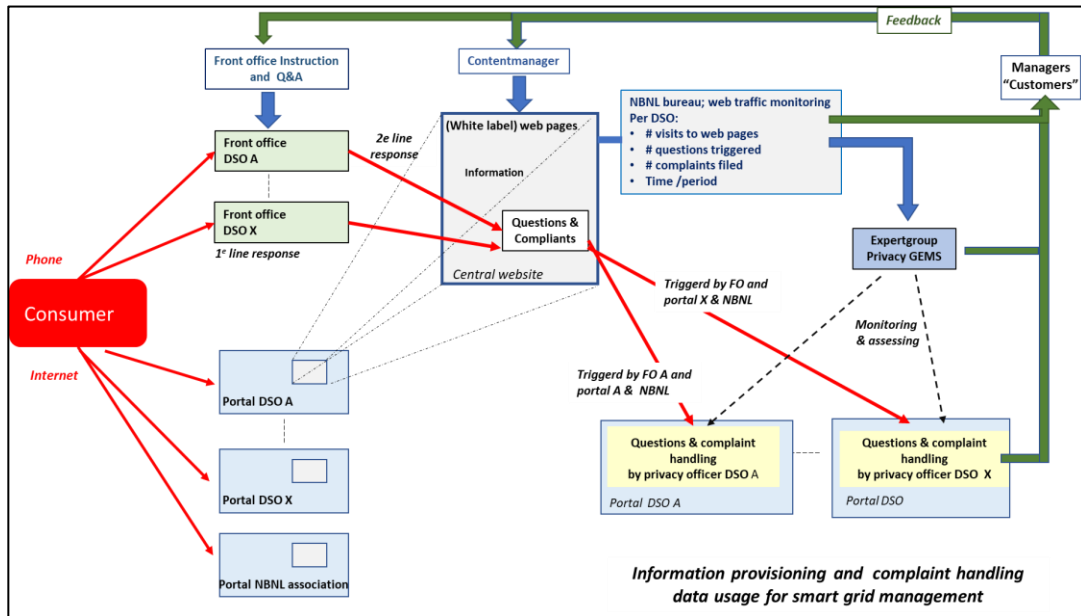


Figure 4. Information provisioning and complaint handling data usage for smart grid management

- A Monitoring Body has been set up at executive level, responsible for the correct functioning of the assessment methodology and processes. The Monitoring Body will develop a monitoring plan for its activities, and initiated activities to meet the accrediting criteria for Monitoring Bodies, published in 2021 by the Dutch Data Protection Authority. Formal filing for this accreditation of the monitoring body is expected in 2022.
In order to achieve high independency of the Monitoring Body, a chairman of the Monitoring Body was appointed, not being a board member of any Dutch DSO, but the CEO of the Dutch Gas TSO.
- The initial version of the Code of Conduct, was submitted for approval to the Dutch Data Protection Authority in the beginning of 2021. During 2021, and upon request of the Dutch DPA, additional clarification on a number of topics were given and meetings were held to discuss and agree on these.
- The final version of the Code of Conduct, as described in this paper, has been submitted for approval January 2021. On 14 February 2022 the Code of Conduct was initially approved by the Dutch DPA (“ontwerp besluit”). With its official publication, a 6-8 weeks formal notification/consultation procedure started. Final approval by the Dutch

DPA followed on 19 April 2022 and this decision was published on 3 May 2022. Approval has been granted subject to the accreditation of the Monitoring Body, which must be accredited by the Dutch DPA within 2 years after the approval date of 19 April 2022.

5. Future/ Next steps

With the Code of Conduct in place and well-functioning, an important fundament has been laid for further development on data privacy issues which go beyond the existing scope of data usage for grid management purposes solely.

Both in Europe as in the Netherlands, significant work is underway to build data exchange ecosystems (data spaces), both sectoral (Energy) as cross sectoral (e.g. Building, Automotive, Industrial, Financial, etc). The European Commission issued in its communication on data strategies in 2020, their ambition to define a horizontal data exchange framework which would enable different sectors to develop their sectoral data exchange frameworks in a way that, through federation, an European wide cross sectoral data exchange could take place, and which supports further developments of one European Market and the realization of the Green Deal objectives; all enabled by an European wide federated data exchange ecosystem.

As also in data exchange data protection will be an important topic to handle, we foresee that also independent monitoring and data protection impact assessments will play an important role on those data exchanges. For those challenges we will consider the reuse of elements (methodology, processes etc.), as developed in this approved Code of Conduct.

Also upcoming regulation on the use of AI algorithms providing full transparency, and avoiding ethnic profiling and discrimination, will require additional monitoring and assessment procedures. The created system, with a risk based approach regarding the use of data, will, via enhancements of the Code of Conduct, also stand the challenge of the new proposed EU AI Regulation, in which also a risk based approach regarding the use of Artificial Intelligence and therewith needed data is introduced.

To conclude, the system with the Code of Conduct and the governance framework based on the 3Angle model and a powerful Monitoring Body, will provide for a solid fundament and the flexibility needed in a world of data sharing and data processing and will fall within the boundaries proposed in the new proposed EU Data Governance Act.

Seen from this perspective, this Code of Conduct should be regarded as a solid first step in our journey towards how to establish a secure and privacy ensured future in the digital world of tomorrow.

6. Learnings & Conclusions

This paper has the intention to share the insights and experiences we learned during the process of developing and implementing this Code of Conduct, thereby supporting those who plan to undertake similar initiatives.

We learned:

- It is a lot about change management and content; This requires a strong integrated approach on running a change management project with strong legal expertise on (upcoming) data and data protection regulation.
- Significant time needs to be spend on internal stakeholder management. The topic of data processing is often new, crosses multiple departmental and sectoral lines, and everybody needed to be brought on board to become part of the success, instead of developing resistance to the change.
- External stakeholder management turned out be essential as data protection issues around smart meters should be regarded in a wider context. Consumer organisations should be contacted and informed during the process, as well as the energy regulator and the ministry of economic affairs; this to ensure consistency with existing and upcoming codes and energy regulation
- A good informal working relation with the Data Protection Authority proved to be crucial for success: this provided good feedback which contributed to the quality of the Code of Conduct, while at the same time the Data Protection Authority did not commit itself in any formal way during the process to approval.
- We had to pay specific attention to customer communication aspect of the Code of Conduct, as this new, and legally complex to understand, topic initially had not the attention and priority of the customer communications departments within the DSO's, who basically focussed more on their core tasks related to grid connections and billing issues.
- In the working groups we learned that technicians on the one hand and data protection and legal officers and councils on the other hand, come from different worlds. It is essential to spent time together and discuss in a structured manner, such as by using the Guidance ethics approach, to get mutually educated; this to come to an integrated and well understood approach on using smart meter data for grid management purposes, ensuring compliance and "data protection by design"
- Executive sponsorship proved also in the project to be key: understanding the strategic relevance of the project and supporting by decision making and accelerating the speed of change.

Authors: Peter Hermans, Juliette van Balen

Date: May 2022