



|

Platone

PLATform for Operation of distribution NEtworks

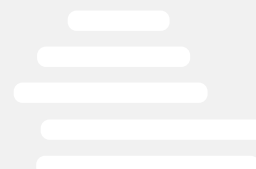
|

D10.2 v1.0

Privacy of Personal Data (POPD) – Requirement No. 2



The project PLATform for Operation of distribution NEtworks (Platone) receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no 864300.



Project Name	Platone
Contractual Delivery Date:	29.02.2020
Actual Delivery Date:	27.02.2020
Main responsible	Pádraic McKeever, RWTH Aachen
Workpackage:	WP10– Ethics requirements
Security:	CO
Nature:	Ethics
Version:	V1.0
Total number of pages:	28

Abstract

This deliverable reports on the current plans of Platone project to ensure the privacy, protection and ethical handling of personal data collected during operation of three Platone demos.

Keyword list

POPD, Ethics, Customers' Personal Data, GDPR

Disclaimer

All information provided reflects the status of the Platone project at the time of writing and may be subject to change. All information reflects only the authors' view and the Innovation and Networks Executive Agency (INEA) is not responsible for any use that may be made of the information contained in this deliverable.

Executive Summary

Deliverable D10.2 details how personal data is handled in Platone to ensure privacy and ethical handling of user data collected during the operation of the Platone demos.

In this deliverable a distinction between personal data and the technical data is made. We argue that technical data, such as grid measurements of quantities such as power or voltage level, cannot be used to identify the customers in any way and so is not personal data under the legal definitions. The handling of the technical data is the subject of D9.1.

This means that the legal privacy requirements on personal data will only be applied to this “customer personal” data (name, address etc.). The way that this data is handled is described in detail here in D10.2.

Authors and Reviewers

Main responsible		
Partner	Name	E-mail
RWTH Aachen		
	Pádraic McKeever Sara Khayyamim	pmckeever@eonerc.rwth-aachen.de
Author(s)/contributor(s)		
Partner	Name	
areti		
	Gabriele Fedele	
Acea Energia		
	Francesco Sorrentino	
Avacon		
	Benjamin Petters	
HEDNO		
	Dimitris Stratogiannis Eleni Daridou	
Reviewer(s)		
Partner	Name	
BAUM		
	Christoph Gieseke Manual Haas	
E.DSO		
	Kirsten Glennung	

Table of Contents

1	Introduction	6
1.1	Objectives of the Work Reported in this Deliverable	6
1.2	Outline of the Deliverable	6
1.3	How to Read this Document.....	7
2	Privacy of Personal Data in Demos.....	8
2.1	Italian Demo.....	8
2.1.1	Data minimisation.....	8
2.1.2	Safeguarding Customers' Rights	8
2.1.3	Security measures for confidentiality	9
2.1.4	Keeping the consent forms.....	9
2.1.5	Lawfulness, fairness and transparency	9
2.1.6	Data processing by third parties.....	10
2.2	Greek Demo	11
2.2.1	Data minimisation.....	11
2.2.2	Safeguarding Customers' Rights	11
2.2.3	Security measures for confidentiality	11
2.2.4	Keeping the consent forms.....	11
2.2.5	Lawfulness, fairness and transparency	11
2.2.6	Data processing by third parties.....	12
2.3	German Demo	13
2.3.1	Data minimisation.....	13
2.3.2	Safeguarding Customers' Rights	13
2.3.3	Security measures for confidentiality	14
2.3.4	Keeping the consent forms.....	14
2.3.5	Lawfulness, fairness and transparency	14
2.3.6	Data processing by third parties.....	14
3	List of References	15
Annex A	Supplementary Documents from Avacon.....	16
A.1	Avacon Technical and Organisational Measures	16
A.2	Avacon Data Protection People Guideline	26

1 Introduction

According to Art. 4(1) of GDPR (General Data Protection Regulation) [1], personal data means “any information relating to an identified or identifiable natural person ('data subject'), an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

D9.1 identifies five different types of Platone datasets, four of which are technical in nature (topology and asset description, measurements, market, prediction and planning) and one of which concerns customers' personal data. Only data from the technical datasets, from which it is not possible to identify the individual customers, will be processed by the Platone infrastructure.

This technical data is not personal data, as defined in Article 4(1) of the GDPR since it is not possible to identify the natural persons whom these data are referring to with a reasonable effort in terms of technology, time, money, etc. This distinction between technical data and personal data was already made in the H2020 SUCCESS project [2]. Similar to Platone, SUCCESS gathered technical data (such as power consumption) from equipment located at the customers' premises and processed the data in an IT infrastructure; these data were anonymised before leaving the customer premises (as they are in Platone). SUCCESS D3.3 [3] studied the legal position in detail in the course of performing a Data Protection Impact Assessment (DPIA) and concludes (in its Ch. 3.1, p14) that such technical data, which are gathered to ensure the correct functioning of the electricity network, are not personal data in the sense of Article 4(1) of the GDPR, for the reason that it is not possible with a reasonable effort to identify the natural persons to whom these data are referring.

Hence, because the Platone technical datasets are, similarly to the SUCCESS case, technical data related to grid operation, the Platone technical datasets cannot be used to identify the customers in any way and so are not personal data. Deliverables D9.1 and D9.2 describe the handling of the technical datasets, including a data minimisation approach and how we made them available as open datasets.

In Platone, therefore, we define personal data as the data explicitly provided by customers when signing the contract such as: *name, phone number, address, bank account details*.

It can be categorically excluded here that any such personal data will be used in any way by the Platone project or its beneficiaries for collaboration and communication activities (e.g. on social media platforms like Twitter, LinkedIn, Skype etc.). The handling of the customers' personal data will be restricted, as detailed below in Ch. 2. No Platone event, dissemination activity or media communication will injure the rights of the demo participants in this regard as they will not contain customers' personal data in any way, shape or form.

All data will be treated according to the EU legislation governing the unbundling of DSOs and market operators (traders, aggregators, resellers, etc.). In order to comply with this unbundling legislation, initial contacts with customers to recruit them to participate in the Platone demos will not be made by the Platone partners running the demo infrastructures but by a third-party (the project partner BAUM).

1.1 Objectives of the Work Reported in this Deliverable

The objective of this deliverable is to describe how customers' personal data is handled in Platone to ensure privacy and ethical handling of the personal user data collected during the operation of the Platone demos. It describes how we protect the privacy and ethical handling of the personal data of the customers who are recruited to participate in the Platone demos.

1.2 Outline of the Deliverable

Ch.2 details the way in which the specific points below are handled for each of the three Platone demos in Italy, Greece and Germany:

1. Confirmation that all of the data they intend to process is relevant and limited to the purposes of the research project (in accordance with the '**data minimisation**' principle).

2. A description of the technical and organisational measures that will be implemented to **safeguard the rights and freedoms of the data** subjects/research participants.
3. A description of the **security measures** that will be implemented to prevent unauthorised access to personal data or the equipment used for processing.
4. Confirmation that detailed information on the **informed consent** procedures in regard to data processing will be **kept** on file
5. For further processing of previously collected personal data, an explicit confirmation that the beneficiary has **lawful basis for the data processing** and that the appropriate technical and organisational measures are in place to safeguard the rights of the data subjects.
6. Confirmation that any Data Processing Agreement/Addendum (or equivalent) with data processors - including relevant assessment of the controls of **third party** who store or process personal data - will be kept on file.

The above six points are handled in the respective six sub-chapters for each Platone demo in Ch. 2.x.1 through Ch. 2.x.6 below, where x has the range 1 to 3 and refers to the three Platone field trials.

1.3 How to Read this Document

D10.1: The reader can find in D10.1 the details on procedures and criteria used to identify/recruit participants (customers) in Platone demos. In D10.1 the content below is also available:

- Detailed information on the informed consent procedures including information about the management of informed consent forms.
- Templates of informed consent and information sheets.

D9.1 and D9.2: To find out that which datasets are identified in Platone, the reader can refer to D9.1. It is also described there that how these datasets will be processed and shared to support the H2020 Open Research Data Pilot during the project's development and after the project's conclusion. An updated version of this deliverable (D9.2) is planned for M20 of the project.

2 Privacy of Personal Data in Demos

2.1 Italian Demo

The partners in charge of ensuring the respect of privacy requirements for personal data protection involved in the Italian demo are areti S.p.A. and Acea Energia S.p.A.

Areti S.p.A. (areti) and Acea Energia S.p.A. (Acea Energia), within Acea S.p.A., have adapted their corporate organisations to GDPR provisions by identifying a Data Protection Officer and by designing a Privacy policy for the group.

In the Italian Demo, areti and Acea Energia, with respect to Article 32 of GDPR, will handle the following customer personal data:

- Personal data (name, last name, etc.);
- Identification data (social security number, vat number, etc.);
- Supply contract data (POD, type of activity, etc.);
- Bank account details;
- Contact details (mail, phone number, address).

2.1.1 Data minimisation

Customer personal data will be processed according to Data minimisation principles. No unnecessary copies of customer data will be created. Customer personal data collected during the implementation of Italian Demo will not be used for other purposes. In order to achieve this objective, only appointed personnel will be able to access the data collected.

Moreover, Acea Group has adopted a corporate Privacy Policy and specifically technical measures of data encryption to protect all the information that are on personnel's devices from unauthorised disclosure or editing or cancellation.

Any paper and digitalised consent forms and related spreadsheets list created during the course of the project will be deleted and disposed of at the end of the project in order to prevent and avoid the reuse of the data for other purposes, according to data minimisation principles of GDPR and Italian Law.

2.1.2 Safeguarding Customers' Rights

The rights of customers are protected by the Italian regulatory framework, which is influenced by European law. The entry into force of GDPR has affected the existing legislation on data protection. The D. Lgs. 196/2003, also known as the Privacy Code, has been amended by D.Lgs. 101/2018. This law formally transfers the GDPR into Italian law, by disposing that, since the entry into force of the present decree, the referral to the provisions of the Code on Personal Data (D.Lgs. 196/2003) must be considered as repealed. The Code must now refer to the provisions of EU Regulations.

Acea Energia and areti, within Acea group, are deeply committed to guarantee the rights of customers, in particular the following ones as provided by art. 15-22 of GDPR:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object to processing;
- the rights in relation to automated decision making and profiling.

To support and guarantee the above mentioned rights, areti and Acea Energia have established dedicated internal Policies. Customers have the right to request from the Controller (whose role is

defined in Article 4 of GDPR [1]) access to, rectification or erasure of personal data. They can also demand a restriction of processing of their data. Customers can communicate to the Data Protection Officer (DPO) of the Acea Group using the dedicated mail privacy@aceaspa.it and/or to the Controller by a registered letter sent to P.le Ostiense n.2 – 00154 Roma (Italia). The DPO is responsible to supervise and evaluate the compliance to European and Italian Law of personal data management within the company.

In order to support these rights, in case of a possible violation of his/her rights, customers can send a compliant to the Data Processing Supervisor (*“Garante per la protezione dei dati personali”*), the Independent Administrative Body established by Italian Law in 1996 for ensuring the protection of personal data of Italian citizens. The compliant can be delivered by hand or sent by registered letter to the Data Processing Supervisor office in Piazza Venezia 11 - 00187 Roma or by using certified mail to protocollo@pec.gpdp.it

2.1.3 Security measures for confidentiality

Data collected and the equipment used for processing them will be preserved according to the internal policy of Acea S.p.A. in order to avoid unauthorised access to personal data. Data will be stored in the customer management software of the company (Document Management System).

The Acea group has been implementing technical measures for managing and attributing the access to guarantee that only appointed users can access data, services and information.

Access to systems and services will be possible with unique credentials for the authentication, composed of username and password, paired with an authorisation profile predefined on the role and on the responsibility of each user.

In case of data breach, Acea S.p.A., and its subsidiaries companies, will notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, any personal data breach to the Data Processing Supervisor, according to GDPR provisions. Any personal data breaches will be documented.

2.1.4 Keeping the consent forms

Customer data will be processed and stored, only with the consent of the customers. The consent forms will be kept on file in paper for a period that will not be longer than necessitated for the purposes for which the personal data are processed. Consent forms will be accessible by Mr. Francesco Sorrentino, as responsible person in charge of keeping the forms physically secure in archives and in digital format in the Document Management System, in order to avoid unauthorised and / or non-compliant access, and by Mr. Gianluca Nori and Mr. Simone Minniti, as creators of the spreadsheet lists and as data processors.

2.1.5 Lawfulness, fairness and transparency

The Consent Form filled in by each customer is the legal basis upon which data processing will be possible in accordance with GDPR and Italian Law provisions. Only consenting customers' data will be processed by the selected Processors. The spreadsheet list containing customer data will be encrypted on the local system and it will be accessible only by the selected data processors.

Besides that, every member of Acea Group staff has received and accepted the Privacy policy of the Acea Group, in compliance with GDPR provisions, for processing data in accordance with confidentiality principles.

2.1.6 Data processing by third parties

Acea Energia and areti confirm that it is not planned to employ third parties for processing personal data.

2.2 Greek Demo

The DSO partner involved in the Greek demo is HEDNO.

The personal data expected to be handled is that which will be given by the customers recruited during the Greek customer workshops. This is expected to be Name, Address, and phone number.

2.2.1 Data minimisation

It is confirmed that all the data intended for processing is relevant and limited to the purposes of Platone (in accordance with the 'data minimisation' principle).

A spreadsheet list will be made and sent to the department in the company authorised to handle customer data and then the spreadsheet list will be deleted, so that no unnecessary copies of the personal data continue to exist. Afterwards only anonymised technical data will be handled within the demo.

The physical copies of the personal data paper forms will be locked and secured in a locker in HEDNO's headquarters PERRAIVOU 20 KALLIRROIS ODO 5, ATHINA 11743, Greece.

2.2.2 Safeguarding Customers' Rights

HEDNO's policy is GDPR compliant to support below rights of customer:

- *the right to be informed*
- *the right of access*
- *the right to rectification*
- *the right to erasure*
- *the right to restrict processing*
- *the right to data portability*
- *the right to object to processing*
- *the rights in relation to automated decision making and profiling*

We provide customers with the contact details in order to enable them to claim their rights. All the provisions of the GDPR regulation applies on supporting customers' rights

2.2.3 Security measures for confidentiality

The paper consent forms filled in by the customers during the workshops will be locked and secured in a locker in HEDNO's headquarters to ensure that nobody can have access to personal data.

Digital data: securely stored on customer management system (all necessary security measures are deployed).

2.2.4 Keeping the consent forms

Consent forms will be securely stored in HEDNO's premises, they will be processed once in order to create the spreadsheet list and they will be destroyed when the project is completed.

2.2.5 Lawfulness, fairness and transparency

The role of the DSO imposes the use of personal data since customers are served by the DSO. Personal data sharing is necessary in order to fulfil the operational requirement of the DSO. Consequently, there is a legitimate interest on collecting personal data for the scope of operation.

HEDNO will make a spreadsheet list and we will send it to the department in our company that has the authorisation to handle customer data and then it will be deleted. Afterwards only anonymised technical data will be handled within the demo.

Consent forms will be securely stored in HEDNO's premises, they will be processed once in order to create the spreadsheet and they will be destroyed when the project is completed.

2.2.6 Data processing by third parties

HEDNO confirms that we don't use third party for data processing.

2.3 German Demo

In German demo, Avacon, will handle the following personal data:

- Name (mandatory)
- Phone number (mandatory)
- Address (mandatory)
- Bank account details – If agreements with customers are made on compensation or pro rata reimbursement
- ID of customers electricity meter - If agreements with customers are made on compensation of switched off/on energy
- ID assignment for processing in the field test

2.3.1 Data minimisation

Avacon confirms that all personal data collected from customers will be limited to the purpose of the project. The principle of "data minimisation" will be applied to ensure that no unnecessary copies of customer data will be created.

2.3.2 Safeguarding Customers' Rights

Technical organisational measures which serve to protect personal data and minimise risks against the threats of data processing are implemented on all Avacon's systems (see Annex A.1).

The customer has following rights:

- *the right to be informed*
- *the right of access*
- *the right to rectification*
- *the right to erasure*
- *the right to restrict processing*
- *the right to data portability*
- *the right to object to processing*
- *the rights in relation to automated decision making and profiling*

All employees of Avacon, including the project team of Avacon Netz, is obliged to protect the above rights of the customers. Through their employment contracts, employees are contractually obliged to safeguard the confidentiality of personal data (see Annex A.2).

The regulations below are applied in Germany to support above rights of the customer:

- General Data Protection Regulation – „Datenschutzgrundverordnung“ - DSGVO
- Federal Data Protection Act - as a supplement to the GDPR; "Bundesdatenschutzgesetz"
- Group Policy - People Guideline PG04 - Data Protection
- Company Policy 054 – Privacy.

The procedures which are planned to support customers' rights are:

- Informational letters about customer rights will be made available to the customer, including detailed information towards the contact persons and mailbox for questions concerning personal data.
- The rights of data subjects are safeguarded using the internal process for data subject inquiries.
- The project leader, Benjamin Petters (Avacon Netz), must implement and ensure all rights concerned, including customer rights for deletion, transfer and use.

2.3.3 Security measures for confidentiality

Customer data will be provided by Avacon's customers' management system via encrypted mails and, if necessary, via a paper consent form filled in by the customer and returned via letter. Customers will have to sign an agreement for project membership, which also will be sent by letter. A spreadsheet list will be created to collect all data provided by the customers. The spread sheet will be stored encrypted on local systems and only be accessible for authorised members of Avacon's project team.

2.3.4 Keeping the consent forms

Paper consent forms as well as confirmations for participations for the project membership will be kept in locked cupboards located in the office of Avacon at Joachim-Campe-Straße 14, 38226 Salzgitter. Consent form will be accessible for the project leader, Benjamin Petters. The spreadsheet list and paper consent forms will be deleted/disposed at the end of the project, in accordance with DIN 66399 data protection law. In Avacon's customer management systems a notification of customers' participation in the project will be stored.

2.3.5 Lawfulness, fairness and transparency

Collected customer data will only be used in the frame of the Platone project to contact customers to inform them about the project content, or to make appointments for installation and dismantling of equipment. Bank account data will collected in case agreements about compensations or comparable agreements leading to cash flows being made to customers.

Data will be used in compliance with the applicable data protection regulations and only with the customer's consent. Data will only be used for the purpose described. The principles of the GDPR are preserved.

An authorisation concept for data processing is in place. It includes a separate data storage, data encryption, storage and mechanisms that ensures that only authorised project members to have access to data.

2.3.6 Data processing by third parties


It is not planned to employ any third parties to process any personal data.

3 List of References

- [1] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, "REGULATION (EU) 2016/679 on 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 Data Protection Regulation)," 2016. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [2] "SUCCESS- Securing Critical Energy Infrastructure," Project Number 700416, 2018. [Online]. Available: <https://success-energy.eu/>.
- [3] "D3.3 Privacy-Preserving Information Security Architecture," SUCCESS EU Horizon 2020 Project, 2018.

Annex A Supplementary Documents from Avacon

A.1 Avacon Technical and Organisational Measures

 E.ON-Company abbreviations – Contractor abbreviations: Annex 1 – Technical and Organizational Measures

Annex 1

Technical and Organizational Protective Measures for security requirements: medium

Seite 1 von 10

e-on E.ON-Company abbreviations – Contractor abbreviations: Annex 1 – Technical and Organizational Measures

Contents

1.	Physical access control	3
1.1.	Physical access control	3
1.2.	Organizational access controls	3
1.3.	Server rooms ("Closed shop" operation).....	3
2.	Logical access control	3
2.1.	Logical access control measures.....	3
2.2.	Network access protection	3
2.3.	Maintenance access protection	4
3.	Data access controls	4
3.1.	Data access protection measures.....	4
3.2.	Secure disposal or subsequent use of data media/secure deletion of documents	4
4.	Transfer control	4
4.1.	Employee requirement for data secrecy.....	4
4.2.	Guidelines and procedures for the classification of data	5
4.3.	Physical data transfer	5
4.4.	Electronic data transfer	5
4.5.	Anonymization / pseudonymization	5
5.	Input control	5
5.1.	Logs.....	5
6.	Order control.....	5
6.1.	Data protection officer (Article 37 to 39 GDPR & national law)	6
6.2.	Contractual requirement.....	6
6.3.	Selection of contractors	6
6.4.	Instructions	6
6.5.	Data protection management system	6
7.	Availability checks.....	8
7.1.	Backup concept	8
7.2.	Storage of business documents.....	9
7.3.	Other security measures.....	9
8.	Segregation control	9
8.1.	Multi-client capability.....	9
8.2.	Segregation of office, development, testing and production environments	10

Seite 2 von 10

e-on E.ON-Company abbreviations – Contractor abbreviations: Annex 1 – Technical and Organizational Measures

1. Physical access control

1.1. Physical access control

- There are reasonable, non-mechanical access control measures for the building.

1.2. Organizational access controls

- Employees of the Data Protection (DP) division visibly display their official or company identification.
- Identification is mandatory for external individuals by means of a visibly displayed visitor's pass.
- Code or ID cards that are issued to external individuals have a strictly limited period of validity determined on the basis of the purpose of the visit.
- Visitor and company identifications are allocated in a revisable manner.
- Visitor identification is revoked daily.
- Personal details of company visitors are recorded in a visitor log/visitor list.

1.3. Server rooms ("Closed shop" operation)

- There is definition and documentation of individuals with access to the server rooms.
- In the event that external individuals require access to the server rooms, there are specific regulations or established procedures (as for access for maintenance work by external personnel).
- Maintenance and cleaning personnel shall undergo applicable access control tests for the server rooms.
- Maintenance and cleaning personnel can only move within previously defined areas.

2. Logical access control

2.1. Logical access control measures

- All information systems and services have a formal user registration and de-registration process for granting and withdrawing access authorizations.
- The complexity of passwords and PINs is subject to minimum requirements that meet the current state of the art.
- The procedure with passwords (e.g., prohibition of disclosure, storage) is regulated in written form.

2.2. Network access protection

- External access to the network is provided over a secure connection (e.g., VPN, certificate).
- It is ensured that only authorized persons have logical access to network components.
- There is a formal approval procedure that systems and applications involving personal data must follow before obtaining network access.
- It is ensured that only authorized devices obtain logical access to the organization's network.
- WLAN is sufficiently secured against unauthorized access.

e-on E.ON-Company abbreviations – Contractor abbreviations: Annex 1 – Technical and Organizational Measures

2.3. Maintenance access protection

- There are implemented appropriate measures for the identification and authentication of external maintenance personnel, such as secure password protection.
- The user password for external maintenance personnel is changed immediately after the completion of maintenance.
- Software modifications by external personnel as part of (remote) service calls are approved by the responsible area and subsequently monitored.

3. Data access controls

3.1. Data access protection measures

- An authorization concept regulates the granting and withdrawal of rights.
- There is a validation process for the authorization process and the authorizations granted, and the respective documentation is available.
- The status of authorization management is regularly reported as part of a data protection report.
- Authorization processes ensure at all times that only specifically authorized persons hold admittance, access and entry authorizations to relevant installations for the provision of services (buildings, rooms, systems, network, applications) (need-to-know principle).
- All modifications to the authorizations are documented revisable to allow tracking of which authorizations were granted at which time to which persons.
- Affiliation of employees or partners in the area outsourced by E.ON is monitored at least quarterly, and their commercial need at least annually.
- The users ensure that their DP equipment is appropriately protected when it is unattended.
- The “clean desk” and “clear screen” principles are actively implemented.
- Special security software of an external manufacturer is installed for guaranteeing data and access protection.
- Digital signature techniques are implemented to detect manipulations.

3.2. Secure disposal or subsequent use of data media/secure deletion of documents

- There are clear instructions for handling data mediums that are no longer required. This includes paper that has been written on or printed documents.
- There is a clear instruction for the disposal or subsequent use of devices equipped with storage mediums.
- Documents and data mediums whose legal, contractual or regulatory storage period has expired are being destroyed.

4. Transfer control

4.1. Employee requirement for data secrecy

Seite 4 von 10

e-on E.ON-Company abbreviations – Contractor abbreviations: Annex 1 – Technical and Organizational Measures

- All personnel that process personal data by means of an automated process are obligated to comply with data secrecy regulations.
- New employees receive data protection information for the handling of personal data.
- All parties involved are aware of data security and data protection issues.
- Individuals processing personal data are trained on data protection behavior in the workplace through data protection trainings.
- There are specific rules for the treatment of departing, especially dismissed, employees.

4.2. Guidelines and procedures for the classification of data

- There is a company-wide concept for the classification of data.
- Company-wide procedures for handling classified information are implemented in practice.

4.3. Physical data transfer

- The company is aware of all processes for which transfer control is required.
- The company ensures that data are transmitted only to the correct addressee indicated by the client or based on the intended purposes.

4.4. Electronic data transfer

- The company maintains a summary/list of places at which transfers can be performed under program control.
- Documentation for the programs installed for automated transfers is available.

4.5. Anonymization / pseudonymization

- The company makes use of the capability for anonymization and pseudonymization in terms of transferring personal data.
- When making use of pseudonymization of documentation data it is ensured that the pseudonym cannot be sent to the recipient together with the real name.

5. Input control

5.1. Logs

- There is a logging concept that determines the type, content and extent of the logging and describes the incident parameters within the logs.
- Logs indicate at the user level which applications or services a specific user has used within a defined period.
- Log data for input control are protected against unauthorized viewing or manipulation.
- The data for input control are subject to a strict purpose limitation and used solely for the purpose of data protection control. No behavior and performance monitoring of employees is conducted through evaluation of the log files without a specific reason.
- A company guideline/policy that contains processes for the evaluation of log files when there is suspicion of a security breach or after a security breach is available.

6. Order control

Seite 5 von 10

e-on E.ON-Company abbreviations – Contractor abbreviations: Annex 1 – Technical and Organizational Measures

6.1. Data protection officer (Article 37 to 39 GDPR & national law)

- A data protection officer is designated.
- Data protection officers shall have no conflict of interests.
- The data protection officer possesses the qualifications and reliability required for the specific company.
- The data protection officer has been designated in writing.
- The management supports the data protection officer.
- The data protection officer is directly subordinated to the management and reports directly to it.
- The data protection officer is informed and involved in the planning of new processes or the modification of existing processes on a timely basis.
- The data protection officer actively participates in process design.

6.2. Contractual requirement

- All contractors in terms of processors of personal data are contractually bound by the data controller.
- The written order complies with the listing of requirements under Article 28, section 3 of the GDPR.

6.3. Selection of contractors

- The client was provided with significant information on data protection and the technical and organizational measures of the contractor prior to assigning the contract.
- The decision and the reasons for the selection of the contractor were documented by the company.
- The company checks the compliance of the contractor with data protection regulations for those areas that are not confirmed by certification before the start of the processing, and monitors the contractor on a regular basis thereafter.

6.4. Instructions

- The client appoints persons authorized to issue instructions to the contractor.

6.5. Data protection management system

- A company-wide data protection and risk management system has been set up that complies with the requirements of the GDPR. Outsourced IT infrastructure services are fully integrated into this risk management system.
- With regard to the processing of personal data, risk analysis is conducted based on established and transparent criteria, and information security and data protection risks are identified, evaluated and properly handled in a compulsorily established and continuous process based on these criteria, and the effectiveness of the measures is reviewed by regular internal audits.
- A data protection report is issued quarterly regarding the current status of the effectiveness of the data protection management system and any failures or data protection/security relevant events, and is made available upon request.

e-on E.ON-Company abbreviations – Contractor abbreviations: Annex 1 – Technical and Organizational Measures

- There are data protection and data security plans in place specifically for the physical security of company-operated data centers and platform-specific characteristics. These can be made available on request.
- All documents that are to be made available are issued in a way as to make it possible for informed third parties to review the respective information security implemented and the data security measures executed. The documentation is kept up to date. Documentation with modified contents is made available on request.
- The management is fully informed and integrated in an information security and data protection organization and the respective communication, escalation and decision processes and ensures that the tasks and responsibilities can be executed to the extent required and with satisfactory quality.
- Sufficient resources are made available for establishing, implementing, executing, monitoring, reviewing, maintaining and improving the data management system and proof of the availability exists.
- It is guaranteed that only personnel that have sufficient skills to comprehend the assigned tasks are involved in operating the data protection management system. This is ensured by instruction and other training measures.
- Internal audits regarding data protection status' are conducted on a regular – at least annual – basis, independent of IT security and risk evaluations. This makes it possible to recognize variations between the contractually established data protection level (all of the agreed technical and organizational measures, TOMs) and the actual data protection status, which then can be evaluated with regard to the resultant risk and provided on request.
- A plan of action is established after data protection management audits that clearly states with which steps and within what appropriate time frame the established deltas are removed. This can be made available on request.
- Continuous improvement of Data Protection Management System is based on the Plan-Do-Check-Act Cycle, under which the client becomes aware on request of the Plan phase and is involved in the execution (Act) if dedicated and multi-client resources are involved in the personal data of the client.
- The technical data protection requirements and measures are based on relevant standards such as ISO 27002 or additional BSI basic IT protection. The Data Protection Management System is tested for effectiveness by internal and external (inspection) testing.
- Data protection measures are based on defined protection requirements for IT applications, IT systems and networks (as defined by the responsible area).
- The respective contact persons are designated and specific contacts and procedures for the exchange of information are established in coordinating data protection measures with the client.
- Suitable procedures exist for monitoring (prompt detection of errors, identification of data protection and security breaches and events related to data protection, confirmation that incidents have in fact been resolved) data protection that are documented in mandatory procedure descriptions and operating instructions and can be presented on request, at least once a year.

e-on E.ON-Company abbreviations – Contractor abbreviations: Annex 1 – Technical and Organizational Measures

- Security indicators that threaten the processing of personal data are monitored so that incidents (e.g., virus or malware incidents, abuse of root rights, hacker attacks, etc.) can be reacted against quickly.
- Processes have been established that ensure the implementation of rights of affected individuals as per Art. 15–21 of the GDPR. These include:
 - Information regarding personal data processed and provision of a copy of those data
 - Rectification and completion of personal data
 - Erasure of personal data on request
 - Restriction of personal data
 - Data portability/transfer
 - Right to object
 - Data protection by design and default (Privacy by Design and Default)
- If forensic analysis is required, the relevant information for subsequent analysis of the incident is provided in agreement with the client. If criminal activity is suspected, this is done in such a way that forensic analyses can be conducted (no modification of data attributes, safeguarding against subsequent modification). Evidence is preserved in a legally tenable manner on request.
- Hardware and software products are obtained from acknowledged and responsible sources. There is reliable technical support and a traceable supply chain.
- Software developed in-house or externally acquired that is used in the processing of personal data has been checked against the weaknesses indicated in the OWASP TOP Ten and SANS Top 25 Most Dangerous Software Errors.
- Information regarding technical weaknesses of data systems in use is obtained on a timely basis, the vulnerability of the organization to exploitation of such weaknesses is evaluated and appropriate measures for dealing with the resultant risk are implemented. The patch roll-out is agreed upon with the client.
- It is ensured that resource use is monitored and agreed upon with the client to ensure the contractually agreed adequate systems performance. Agreed capacities may not be directed to other lessees without agreement of the client.
- Personal data on hardware that is to be discarded is irretrievably deleted to the highest possible state of the art, or the hardware is completely destroyed securely.
- Assets of the organization that are associated with information and facilities for processing of data are regularly identified and inventoried. Furthermore, security controls and servicing of these facilities are provided.
- Subcontractors are required to comply at least with the requirements agreed upon with the client. Implementation and monitoring of reasonable measures are ensured by the subcontractors.

7. Availability checks

7.1. Backup concept

- Accurate documentation exists for the backup concept requirements.
- Backup media are adequately protected against theft and destruction.

e-on E.ON-Company abbreviations – Contractor abbreviations: Annex 1 – Technical and Organizational Measures

- The company has approved procedures for data protection available and they are documented in operating instructions.
- The individuals competent and responsible for data protection are designated by name. Their responsibilities are documented.
- Capacity planning for data protection is available.
- The restoration and integrity of available backups is tested regularly.

7.2. Storage of business documents

- The company has its own archive room that is designated for the receipt of data mediums and documents that are required to be stored.
- Only the most necessary personnel have access to the archive areas. Access authorizations are documented in the archive regulations.
- An archivist is appointed for the archive.
- Data mediums and documents are issued and stored only by authorized archive personnel.
- Revisable documentation for the entry and issue of data mediums and documents is maintained.
- Inventory of data mediums and documents in the archive are regularly controlled by means of a target/actual comparison.
- Documents and electronically maintained data that exceed their legal, statutory or contractual retention deadline are deleted/destroyed under a deletion plan in accordance with data protection laws.
- A follow-up system exists for deletion after expiry of the retention period.

7.3. Other security measures

- Only server centers that present the qualified certification are used for the outsourcing of data processing (the computer centers of providers are certified as corresponding to TSI level 3 at minimum). Furthermore, it is ensured that CC locations are not exposed to any correlated hazards, and this is confirmed by risk analysis.
- Written service instructions for all security measures are available.
- Whether employees are observing the security measures that apply to them is checked on a regular basis.
- Employees are regularly trained in the handling of security devices and compliance with security instructions.
- Faults and measures for correcting them are documented in a tamper-proof manner.

8. Segregation control

8.1. Multi-client capability

- Clients are adequately segregated when using a multi-client system. This ensures that the data of several clients are not mutually visible or modifiable. It is also not possible to infer information about the respective clients. The client is informed about the use and operating principles of multi-client systems.

e-on E.ON-Company abbreviations – Contractor abbreviations: Annex 1 – Technical and Organizational Measures

- The availability, confidentiality and integrity of personal data is guaranteed without reservation in the event of an investigation (the police, tax authorities, etc.).
- The procedural documentation contains transparent information for thorough multi-client capability.
- System and security recording is (at least logically) carried out separately by client and archived separately.
- Security incidents in multi-client systems (of any sort) affecting the outsourced areas of the client are brought to the latter's attention immediately.

8.2. Segregation of office, development, testing and production environments

- Office, development, testing and production systems are operated (at least logically) in clearly separated grid segments.
- Exclusively test data are used for testing and development purposes.
- Test data based on actual data are anonymized.
- There is a concept for the creation and implementation of test data.

A.2 Avacon Data Protection People Guideline



PG-04: Data Protection

People Guideline

This People Guideline applies to you if you process personal data within E.ON

What is data protection? What is meant by personal data?

Data protection has to protect personal data against unauthorized or unlawful acts of processing. Data is 'personal' if it concerns an individual (the "data subject") and provides information as to this individual's personal or material circumstances. Personal data comprises, but is not limited to, a person's name, date of birth, address, bank details, e-mail address and IP address as well as logs of user activities, user data in cookies, personal profiles of individuals, smart meter data and charging data at e-mobility charging points.

E.ON is legally obligated to maintain an adequate level of data protection. E.ON has also a vital interest in protecting all personal data against unauthorized or unlawful processing. This includes the protection of associated resources such as IT resources but also includes printouts, paper contracts etc.

What are my tasks with regard to data protection?

As a matter of principle, all employees of E.ON are required to protect personal data in their daily work.

The following is a list of the most important requirements when dealing with personal data:

- (1) Collect and process personal data only if the data subject has given his or her consent or if another legal ground exists (e.g. use name and address for a delivery which is needed to fulfill a contract).
- (2) Ensure that processing of personal data is appropriate; i.e. in particular, exercise caution so that the intended purposes of the data processing are achieved with the lowest possible impact on the privacy of the data subjects (e.g. anonymizing data, where possible).
- (3) Process personal data solely for the intended purposes (i.e. the purpose(s) of each data processing must be defined and documented). In the event of any change of purpose or a new purpose, consult the responsible Data Protection Officer.
- (4) If possible, collect personal data directly from the data subjects. Make clear which data is mandatory and which data is voluntary.

PG-04: Data Protection
Valid as of: 01.01.2018

Author: Legal & Compliance
Board approval: 05.12.2017

- (5) Consider the rights of the data subjects, in particular:
- (a) Inform the data subject regarding the processing of their data at the time when the data is collected. This information has to be easily understandable, transparent and precise. Furthermore, it must include specific items such as the intended purpose for which the data is processed, the legal grounds for doing so, data retention principles and potential recipients.
 - (b) Provide data subjects with their data upon request, unless a legal exception exists.
 - (c) Correct data as soon as you are aware of incorrect data.
 - (d) Securely delete personal data (in particular when the data is no longer needed for the intended purpose or when the data subject withdraws his or her consent). If the data cannot be deleted (e.g. for the defense of legal claims such as, for example, in the event of outstanding payments after a contract has ended), exercise caution and ensure that the usage of the data is limited (e.g. archive the data and limit the processing thereof).
 - (e) Limit the processing of personal data when this is legitimately requested by a data subject (e.g. when data accuracy is contested by the data subject).
 - (f) Inform third parties to whom the personal data has been disclosed (e.g. another E.ON Unit or an external company) of any deletions, rectifications or restrictions on processing, unless a legal exception exists.
 - (g) Respect the objections of data subjects (e.g. when the data is used for direct marketing or building customer profiles).
 - (h) Take action (such as deleting or disclosing data) following a request from a data subject only after the identity and entitlement of the person requesting the action has been unambiguously verified.
- (6) Contribute to the integrity, confidentiality and availability of personal data by following E.ON-wide and local information security standards (e.g. clean desk principle, password policy), which are applicable to the remit of your position.
- (7) Transfer personal data to a third party (i.e. another E.ON Unit or an external company/person) only when the relevant legal requirements have been met. This means that an agreement for data processing on behalf of E.ON must have been concluded or another reason must have been provided permitting the transfer (e.g. the defense of legal claims). With regard to the transfer of data to countries outside the European Union/EEA, additional legal requirements apply. In case of doubt, contact the responsible Data Protection Officer.
- (8) Report any actual or potential breaches of data (e.g. unlawful disclosure or misuse of personal data) immediately to your manager and Data Protection Officer.
- (9) Involve your Data Protection Officer as early as possible (preferably, during the planning phase) and provide all requested information in the event of:
- (a) any planned, new internal or external processing of personal data, and

PG-04: Data Protection
Valid as of: 01.01.2018

Author: Legal & Compliance
Board approval: 05.12.2017

(b) any subsequent changes thereto.

This is required in order to ensure that legal and internal data protection requirements are taken into account in good time (Privacy by design).

(10) Attend any relevant training sessions pertaining to data protection.

Contacts and further information

Further information on Data Protection is provided in the following documents:

- FP-12: Legal, Incident and Crisis Management & Data Protection, Appendix B on Data Protection
- Local Data Protection Policy and documents
- [Information Security page on Connect](#)

In addition, your Data Protection Officer is happy to assist you regarding any questions you may have concerning data protection. Contact details for the [German Data Protection Officers can be found here](#) on Connect, the [non-German Data Protection officers can be found here](#).