



Data Protection Policy

Document ID 18001

Powerlines

Version 1.0, 2018-05-25

Document History

Document name		
Document ID 18001 Data Protection Policy(29928834_2).DOCX		
Version	Date	Comments, Amendments
0.1	2018-02-23	Initial draft
1.0	2018-05-25	Finalisation, approval
	Role	Person
Drafting	Data Protection Coordinator	Gerd Brunner
Approval	CEO	

Contents

1	Data Protection Policy.....	4
1.1	Management Commitment	4
1.2	Scope	4
1.3	Data Protection Objectives	4
1.4	Organisation of Data Protection and Information Security	6
1.5	Measures	6
1.6	Organisational Roles in Data protection and Information Security.....	6
1.7	Data Protection Awareness through Targeted Training	7
1.8	Engagement of Partners and Service Providers.....	7
1.9	Resources	7
1.10	Communication of Data Protection Incidents – Data Protection Breaches	7
1.11	Penalties.....	7
1.12	Review and Revision	8
1.13	Final Clause.....	8

1 Data Protection Policy

1.1 Management Commitment

Protection of the personal data of individuals (or 'data subjects') is enforced within the United Kingdom under the EU General Data Protection Regulation 'GDPR' and Data Protection Act 2018. In order to increase the confidence of our stakeholders, customers, partners and employees that, Powerlines Group GmbH (Powerlines) and its subsidiaries complies with this stipulated obligation. as a data controller. We consider it our duty to ensure the appropriate security measures and adequate protection of the personal data is provided.

This management commitment constitutes the clear remit of the Powerlines Group GmbH management to implement an efficient data protection management system ('DPMS') that complies with statutory framework conditions. This applies to Powerlines Group GmbH and all subsidiaries.

Data protection mandate

With this mandate, the management of Powerlines Group GmbH reinforces its commitment to data protection

To protect personal data as well as possible, clearly defined rules and regulations are required. This policy and its associated regulations establish how information and systems are protected within the organisation and how this should be coordinated. With the adoption of the data protection policy the data protection objectives that are established become a part of the company model and must be observed by all employees.

With the data protection manual and the basic data protection specifications, a data protection management system is implemented and operates in accordance with current laws and directives.

1.2 Scope

This data protection policy applies to Powerlines Group GmbH and all its subsidiaries. This data protection policy and associated guidelines obligates all employees to comply with the obligations set forth herein.

1.3 Data Protection Objectives

Powerlines must operate a consistent and continuous data protection management system in order to systematically plan, organise, manage and monitor statutory data protection requirements. The objective here is to (i) ensure the rights and freedoms of data subjects and (ii) to recognise company risks in the data protection realm promptly, and be able to manage them. Furthermore, evidence of accuracy and compliance with due diligence in handling and processing the personal data of data subjects should be provided and documented for both shareholders and managers. For this purpose, when planning and introducing processes, and in the course of their execution, the company will take into account the following **data protection objectives**:

Data protection objective 1: Ensuring the availability of personal data:

- Ensuring that there is no unintentional or unlawful destruction of data
- Ensuring that data is available for further processing where, and to the extent, that this is legally or contractually prescribed

Data protection objective 2: Ensuring the confidentiality of personal data:

- Extensive encryption of data
- Ensuring that there is no unauthorised disclosure of data
- Ensuring that there is no unauthorised access to or other processing of data
- Ensuring that data processing does not lead unintentionally or unlawfully to discrimination against, or cause harm or distress data subjects
- Ensuring that data processing does not lead to identity theft or identity fraud
- Ensuring that there is no loss of confidentiality of personal data that is subject to professional confidentiality

Data protection objective 3: Ensuring the integrity of personal data:

Personal data processing is designed in such a way that there can be no unauthorised alteration of data and the data is correctly represented.

- Ensuring that there is no unintentional or unlawful alteration of data
- Ensuring that data processing does not lead to financial loss
- Ensuring that there is no unauthorised cancellation of pseudonymisation

Data protection objective 4: Transparency of data processing:

- Personal data processing should be capable of being tracked, checked and assessed without expending unreasonable effort.

Data protection objective 5: Strict purposeful data processing:

Personal data processing must be organised in such a way that data cannot (or only by expending disproportionately high effort) be collected, processed and used for a purpose other than that identified.

- No collection of unnecessary data
- Deletion of data immediately after the purpose is achieved
- Conclusion of agreements with data processors (for example, suppliers and external service providers)

Data protection objective 6: Continuous safeguarding of the rights of data subjects:

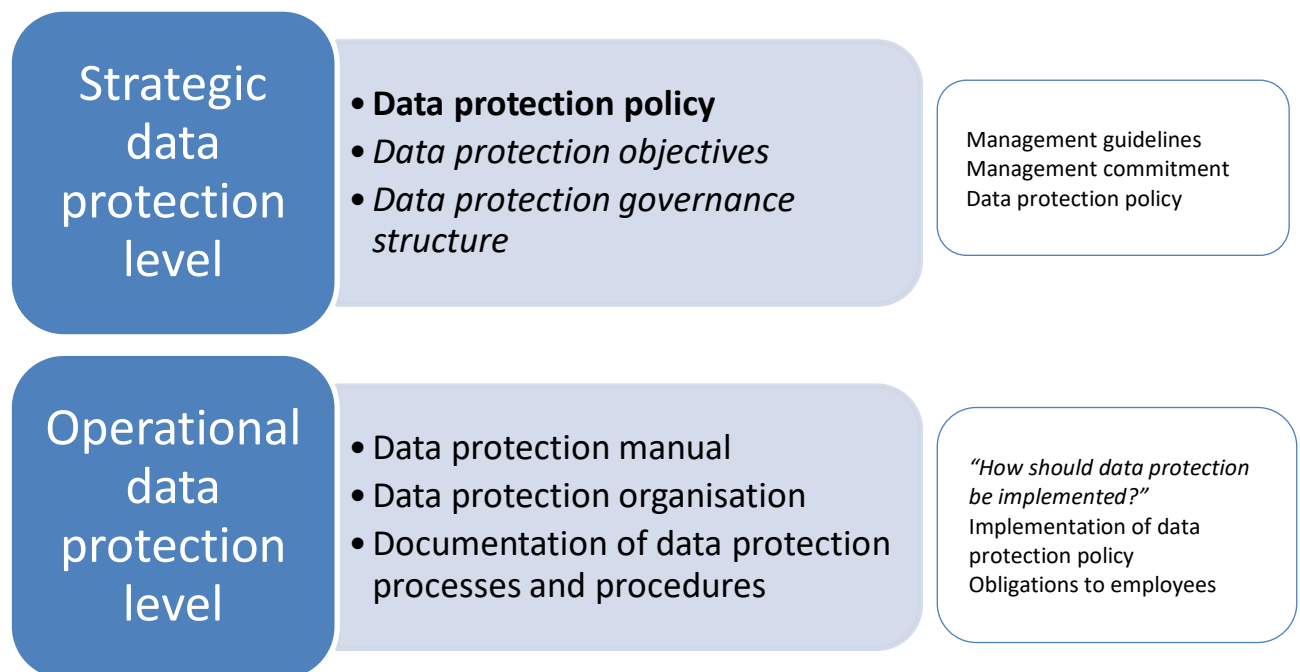
Personal data processing must be designed in such a way that data subjects can exercise their rights effectively.

- Ensuring that data subjects are consistently able to obtain or find the data protection information to which they are entitled
- Ensuring that data subjects are not hindered in exercising or upholding their data protection rights

When practically implementing the objectives, the protective measures in question must take into account 'the state of the art' in terms of technology and must be in reasonable proportion economically to the protection requirement of the processed data and information.

1.4 Organisation of Data Protection and Information Security

This data protection policy specifies the strategic framework for how data protection should be implemented. Operational additions to the data protection policy are specified using a data protection manual, data protection organisation guidelines and defined data protection processes and procedures.



Data protection manual

The data protection manual and its corresponding specifications and processes outline the formal implementation of this data protection policy. ***"How should data protection be implemented in Powerlines?"*** is the central question in our data protection manual. It gives guidelines for practical implementation.

1.5 Measures

Measures for implementing data protection can be in the form of technical and organisational measures. These also include guidelines, company regulations or operational instructions.

1.6 Organisational Roles in Data protection and Information Security

The **Management of Powerlines Group GmbH** assumes overall responsibility for **data protection** in the company and manages data protection at a strategic level. In the subsidiaries this task and

responsibility belongs to the respective local management. At an operational level, data protection is implemented by local data protection coordinators. With the help of the Powerlines Group GmbH data protection coordinator and data protection core team, the local data protection coordinators give full advice to everyone involved in the data protection process and operate a sustainable data protection management system.

Responsibilities, roles, duties and competences are described in the aforementioned accompanying documents.

1.7 Data Protection Awareness through Targeted Training

Data protection can only be adequately implemented across the whole group if all employees are informed of and trained in current strategies, guidelines and procedures. In Powerlines Group GmbH therefore, measures such as regular training are also implemented for creating awareness, as an important tool for increasing information security and data protection.

1.8 Engagement of Partners and Service Providers

Suppliers and external service providers (data processors) must be bound by separate agreements that meet the requirements of GDPR and company policy if they process personal data under contract or have the opportunity to gain knowledge of the company's personal data or other information not classified as publicly available.

Service providers are involved in the data protection management process if this is necessary as a legal and organisational requirement.

1.9 Resources

Data protection is operated by people for people. So that a secure IT service, information security and data protection at the level required for Powerlines Group GmbH can be operated, management ensures the personal and financial resources required are in place. It should be ensured at the same time that these resources are used responsibly and in accordance with company policy.

1.10 Communication of Data Protection Incidents – Data Protection Breaches

All employees of Powerlines Group GmbH are obliged to report data security incidents immediately to their supervisor or the relevant competent data protection coordinator to ensure the fastest possible elimination, or restoration of the target state. The urgency or severity of an incident may only be assessed by the relevant competent data protection coordinator.

1.11 Penalties

A breach of this data protection policy can constitute a violation of the employment contract and be penalised accordingly.

1.12 Review and Revision

This data protection policy, the data protection manual and the associated guidelines are subject to an annual cycle of review and revision to guarantee that the specifications described herein are up to date.

1.13 Final Clause

This data protection policy is subject to a constant process of improvement and adaptation to the relevant current data protection provisions.