KION Group Data Protection Policy

Doc. no.:	Version:	Date:
POL-01	01	20.11.2019

Contents

Created	Checked	Approved
by: N. Moeren, KION Group Data Protection Officer	by: B. Engel, IT H. Frieges, HR J. P. Garcia Ugena, Dematic A. Giger, Procurement R. Lesli, Dematic US K. Meininger, LMH S. Rieck, IT Security H. Schichta, IT M. Daneshzadeh Tabrizi, Legal R. van Walsum, STILL J. Viebranz, Compliance	by: S. Schneeberger, Member of the Executive Board & Chief Digital Officer
Date:		Date:
Signature:		Signature:

1. Purpose

This policy shall strengthen our explicit commitment to protect the Personal Data of our employees, customers, vendors and other business partners in accordance with applicable data protection laws. Data protection is a key enabler for and crucial requirement of our company, currently evolving into digital services within our industry.

2. Scope

This policy applies to all of us working in legal entities of KION Group when processing Personal Data.

3. Terms and Definitions

The following definitions helps us to understand terms used in this policy:

Controller means the natural person or legal entity, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing Personal Data.

Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

Data Protection Impact Assessment is a risk assessment to evaluate and handle the risks to the rights and freedoms of the Data Subject caused by a specific processing of Personal Data.

Data Subject means the individual to whom the Personal Data relates.

Identifiable Natural Person is a natural person who can be identified, directly or indirectly.

KION Group Employee means an employee, including apprentices and individuals contracted as an employee or employed by a KION Group Legal Entity.

KION Group Legal Entity means a Legal Entity under the control of KION GROUP AG.

Personal Data means any information such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, economic, cultural or social identity of an Identifiable Natural Person (“Data Subject”).

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Processing means any operation which is performed on Personal Data, whether by automated means or not, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Secure Third Countries provide an adequate level of data protection as confirmed by the EU Commission.

Sensitive Data (Special Categories of Personal Data) is data about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership or the health (including genetic and biometric conditions) and sexual life. Under national law, further data categories can be considered sensitive, e.g. criminal offences.

Third Countries are all countries outside the European Union and the European Economic Area (EEA).

Third Party means a natural person or legal entity, public authority, agency or body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorized to process Personal Data.

Transfer of Personal Data is a disclosure of Personal Data by the Controller to a Third Party or to another Controller. A transfer takes place when granting access rights.

4. Roles and Responsibilities

We are all responsible for data protection. This means handling Personal Data according to KION Group standards and procedures. You shall conduct the available data protection trainings and report identified Personal Data Breaches (see chapter 13 and 11). The specific responsibility depends on our role within the KION Group.

4.1. KION Group Executive Board

With this policy the KION Group Executive Board sets the foundation for data protection. Adequate controls and an effective organization on KION Group level shall protect Personal Data.

4.2. Management Board of KION Group Legal Entities and Management Board of the Operating Units (OUs)

If you are a managing director of a KION Group Legal Entity, you shall ensure the implementation of an adequate data protection management system in your area of responsibility.

Therefore, you shall apply key controls as defined in our applicable standards and procedures, by:

- Appointing the mandatory internal data protection coordinator (DPC) or local data protection officer (local DPO) (where required, an external solution for the DPO or the appointment of one DPO for more than one Legal Entity are also possible),
- Informing the national data protection authority of the appointed local DPOs (if required),
- Allocating adequate resources for the local DPO / DPC,
- Implementing continuous monitoring of local legal changes (see also chapter 4.4),
- Implementing adequate documentation and control of data processing activities,
- Implementing adequate sourcing processes of data processing activities,
- Implementing adequate processes to deal with Data Subject requests and Personal Data breaches,
- Implementing adequate awareness of data protection within your organization.

4.3. Group Data Protection Officer (GDPO)

If you are appointed as a Group Data Protection Officer (GDPO), you shall design and operate the group-wide Data Protections Management System:

To this end, you shall apply risk-based key controls as defined in our applicable standards and procedures, by:

- Maintaining a risk-based control framework (data protection management system) to ensure group-wide compliance with data protection legislation,
- Conducting assessments to ensure the implementation of the data protection management system,

- Maintaining a local network of Data Protection Officers and Data Protection Coordinators, which will be supported by Data Protection Coordinators of Operating Units (OUs),
- Reporting the effectiveness of the data protection management system and related risks to the KION Executive Board,
- Acting as single point of contact for the authorities related to data protection topics.

In addition, you provide services to the KION Group:

- Support for training and raising awareness within the KION Group,
- Provision of tools and templates to ensure the implementation of the risk-based control framework, e.g. data processing inventory, Personal Data Breach process, Data Subject request handling,
- Advising Controllers and Processors (including advice on Data Protection Impact Assessments),
- Providing guidance and direction to KION Group Employees and managers in matters concerning the protection of Personal Data.

4.4. Data Protection Coordinator (DPC)

If you are appointed by the management of your Legal Entity (see chapter 4.2) as a Data Protection Coordinator (DPC) for an organizational unit, you shall support the implementation of the group-wide data protection management system, by:

- Functional reporting of the effectiveness of the local data protection management system and related risks to the management of the Legal Entity and to the GDPO,
- Coordinating the assessment, documentation and maintenance of the records of processing activities and the relevant controls (data processing inventory),
- Supporting assessments to ensure the implementation of the group-wide data protection management system within the area of your responsibility,
- Supporting the deployment of group-wide trainings and awareness measures,
- Identifying, together with the GDPO, local / national requirements in the area of data protection and relevant changes,
- Acting as a single point of contact for the GDPO or an external local DPO, as well as for the employees and managers of your area of responsibility,
- Ensuring the appropriate handling of Personal Data Breaches and Data Subject requests together with the GDPO and local DPO.

The role of the DPC can be taken on by an internal local DPO.

4.5. Local Data Protection Officer (local DPO)

If you are appointed as a local Data Protection Officer (local DPO), then you are taking over the official role as defined in the GDPR and / or as defined in local national law. In this case, the authorities must be notified of the local DPO by the responsible Legal Entity (if legally requested).

If you are appointed as a local DPO, you shall support the implementation of the group-wide data protection management system, by:

- Functional reporting of the effectiveness of the local data protection management system and related risks to the management of the Legal Entity and to the GDPO,
- Taking over the control function as defined in applicable data protection law, especially taking over the role as the single point of contact for local data protection authorities.
- Ensuring that local legal requirements in the area of data protection are followed,
- Providing guidance and direction to KION Group Employees and managers in matters concerning the protection of Personal Data,
- In case of an internal local DPO: Taking over the role as DPC (see chapter 4.4).

4.6. Chief Information Officer (CIO)

If you are a Chief Information Officer (CIO), then the rules for a manager (chapter 4.2) shall be applied in respect of leading the IT central function.

4.7. Chief Information Security Officer (CISO) and Information Security

If you are acting as a Chief Information Security Officer (CISO), you shall ensure the definition and implementation of adequate internal controls, by:

- Developing technical and organizational standards and procedures, in line with industry best practices, to protect information in accordance with their classification,
- In cooperation with the DPO, supporting and advising the Process Owners in defining the appropriate technical and organizational measure to protect their information processing system,
- Supporting the DPO in the development of risk-based security controls of technical and organization measures in accordance with applicable data protection law,
- Developing awareness programs on all levels of the organization on information security.

4.8. Legal

If you are acting as a lawyer in the legal department, you shall provide legal advice with respect to all data protection laws applicable throughout KION's activities all over the world by:

- Negotiating and concluding agreements relating to data protection laws, privacy statements and consent statements,
- Providing group-wide harmonized interpretations of legal data protection requirements to the GDPO and local DPO,
- Ongoing assessment of legal developments relating to data protection laws.

4.9. Internal Audit

If you are acting as an auditor of Group Internal Audit, you shall be responsible for conducting audits throughout the KION Group to identify risks and to align and follow-up on measures to mitigate those risks with management, by:

- Supporting the (Group) Data Protection Officer with regular audits and spot checks of compliance with data protection regulations within your regular audits.

4.10. Application Owner ("Administrator", "Asset Owner")

If you are operating an asset (e.g. an application) supporting Personal Data processing, you are acting as an administrator. In this case, you shall ensure the controls for secure and compliant operating, by:

- Ensuring that assets and IT systems are documented in the data processing inventory and updated in case of changes,
- Ensuring that required data processing contracts are in place and followed,
- Ensuring that the administration is carried out based on agreed-upon technical and organizational measures,
- Reporting identified Personal Data Breaches immediately (see chapter 11).

4.11. Process Owner

If you are responsible for a data processing service, which means that you are defining the purpose, the processed data and the data processing tools being, you are operating as a Process Owner. In this case, you shall ensure, that the controls for compliant data processing are considered, by:

- Ensuring and monitoring the implementation of the data protection requirements for the relevant business area, e.g. by documenting and maintaining the record of processing register (as a representative for a Controller or as a representative for a Processor) and by fulfilling the informing requirements for the Data Subject,
- Ensuring that required data processing contracts are in place and followed (including relevant documentation and evidence for data protection compliance),
- Ensuring that the required privacy impact assessment is carried out, if applicable,
- Ensuring that the administration is carried out based on agreed-upon technical and organizational measures,
- Reporting of identified Personal Data Breaches immediately (see chapter 11).

5. Principles of Processing

When you process Personal Data, you shall apply the following principles:

1. **Lawfulness, fairness and transparency**: Personal data shall be processed in a fair and lawful manner and required processing information shall be provided to the Data Subject.

   You are only allowed to process Personal Data when at least one option applies:
   a) the Data Subject consented to the processing of Personal Data for the intended purpose;
   b) processing is allowed based on rules provided by national law (e.g. collective agreements)
   c) processing is necessary for the preparation or performance of a contract to which the Data Subject is party;
   d) processing is necessary for compliance with a legal obligation of the Controller;
   e) processing is necessary to protect the vital interests of the Data Subject or of another natural person;
   f) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
   g) processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data.

2. **Purpose limitation**: Personal data shall be collected for specified, explicit and legitimate purposes and not processed further in a manner that is incompatible with those purposes.

3. **Data minimization**: When processing Personal Data, this data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. **Accuracy**: When processing Personal Data, the data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or corrected without delay.

5. **Storage limitation**: When processing Personal Data, the data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed.

6. **Integrity and confidentiality**: Personal data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful

processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

6. Processing Sensitive Data ("Special Categories of Personal Data")

The processing of sensitive data carries higher risks for Data Subjects if misused or processed incorrectly and shall only be done based on the applicable legal restrictions.

If you as a Process Owner are responsible for the introduction or modification of data processing activities concerning sensitive data, you shall follow applicable controls or get in contact with your Data Protection Coordinator or Data Protection Officer.

7. Transparency of Data Processing

7.1. Privacy Information on Web Pages

Each KION Group Legal Entity shall take appropriate measures to provide the required information to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the Data Subject, the information may be provided orally, if the identity of the Data Subject is proven by other means.

Each KION Group Legal Entity provide a data privacy statement on its internet web page, which provides the relevant information related to the processing of Personal Data of it stakeholders.

In general, the KION Group processes and transfers Personal Data, including sensitive Personal Data relating to the following Data Subject groups:

- Applicants of KION Group legal entities (including rejected applicants);
- Employees of (potential) customers;
- Employees of external business partners (including dealers, contractors, suppliers, etc.);
- Employees of KION Group (including former employees and relatives);
- Other Data Subjects (including visitors, journalists, employees of an authority, etc.).

7.2. Direct Notification of the Data Subject

You as a Process Owner shall inform the Data Subject directly, when you are

- collecting information from the Data Subject for the first time (e.g. hiring of new employees, new customers), or
- processing data of the Data Subject for the first time (e.g. cold calling), where Personal Data has not been obtained from the Data Subject directly.

The implementation shall be based on applicable solutions standardizing the implementation within KION Group (see chapter 13).

7.3. Mandatory Content of Data Processing Information

You as a Process Owner shall inform the Data Subject directly when processing data of a Data Subject for the first time about the following, legally required information, e.g.:

- the identity and the contact details of the Controller and, where applicable, of the Controller's representative;
- the contact details of the Data Protection Officer, where applicable;
- the purposes of the processing for which the Personal Data is intended, as well as the legal basis for the processing;

- the categories of Personal Data concerned;
- the recipients or categories of recipients of the Personal Data, if any;
- where applicable, that the Controller intends to transfer Personal Data to a recipient in a Third Country, with reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.
- the period for which the Personal Data will be stored, or, if that is not possible, the criteria used to determine that period;
- where the processing is justified as a legitimate interest, the legitimate interests pursued by the Controller or by a Third Party;
- the existence of the right to request access to and rectification or erasure of Personal Data or restriction of processing concerning the Data Subject from the Controller and to object to processing as well as the right to data portability;
- where processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- from which source the Personal Data originates, and, if applicable, whether it came from publicly accessible sources;
- the existence of automated decision-making, including Profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

This information shall be given when collecting the Personal Data or when obtaining the data from other sources within a reasonable period after obtaining the Personal Data, but at the latest within one month after starting the processing of the Personal Data.

Where you as a Process Owner intend to further process the Personal Data for a purpose other than the one for which the Personal Data was collected, you shall consult your Data Protection Coordinator to provide the Data Subject with information on that other purpose and with any relevant further information prior to that further processing.

The implementation shall be based on applicable solutions standardizing the implementation within the KION Group (see chapter 13).

8. Data Subject Rights

If your Personal Data is being processed by a KION Group Legal Entity (Controller), you are a Data Subject and you have the following rights. Restrictions of this rights might be done, if legally allowed:

- Right of access: The right to obtain confirmation from the Controller whether or not your Personal Data is being processed, and, where that is the case, access and information to the Personal Data.
- Right to rectification: The right to obtain the rectification of inaccurate Personal Data without undue delay the rectification of inaccurate Personal Data.
- Right to erasure (‘right to be forgotten’): Right to obtain from the Controller the erasure of Personal Data without undue delay. The Controller shall have the obligation to erase Personal Data without undue delay if no overriding legitimate grounds for the processing exist.
- Right to restriction of processing: The right to obtain a restriction of processing from the Controller, meaning the marking of stored Personal Data with the aim of limiting its processing in the future.
- Right to data portability: The right to receive your Personal Data, that you have provided to the Controller, in a structured, commonly used and machine-readable format and have the right to transmit that data to another Controller without hindrance from the Controller to which the Personal Data has been provided.
- Right to object: The right to object to the processing of your Personal Data, including Profiling, at any time. The Controller shall no longer process the Personal Data unless the Controller

demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defense of legal claims.

The exercise of the Data Subject's rights may be restricted due to applicable laws. The local Data Protection Officer of the KION Group legal entities shall respond to the Data Subject requests as a Controller, considering applicable laws without undue delay, in any case within one month.

The implementation shall be based on applicable KION standards (see chapter 13).

9. Transfer of Personal Data

Personal data is being transferred when granting another party (such as service providers or vendors) or other KION Group legal entities access to Personal Data. The data recipient shall be instructed in writing to use the data only for the defined business purposes.

In the normal course and scope of business, KION Group legal entities share Personal Data with Third Parties or other KION Group legal entities worldwide to facilitate the services, business operations, prevent fraud, provide joint content as described in the data processing agreement.

KION Group legal entities may only transfer Personal Data on the instructions of the Controller (except where required by the relevant applicable law or local competent authorities) when there is a legitimate business need and appropriate technical and organizational security measures.

If data is transmitted to a recipient based in a Third Country, this country must agree to maintain a data protection level equivalent to this policy. This does not apply, if the Personal Data transfer is based on a legal obligation.

If Personal Data is transmitted by a Third Party to a KION Group Legal Entity, it must be ensured that the data can be used for the intended business purpose, e.g. by signing a data processing agreement.

In the case of Personal Data being transmitted from a KION Group Legal Entity located in the European Economic Area (EEA) to a KION Group Legal Entity located in a Third Country, the Controller transmitting the data shall be held liable for any violations of this policy committed by the Legal Entity located in a Third Country with regard to the Data Subject whose data was collected in the EEA, as if the violation had been committed by the Controller transmitting the data.

Any Transfer of Personal Data to a recipient based in a Third Country must be safeguarded by EU standard clauses issued by the European Commission. Even in the case of an existing adequacy decision for the respective country by the EU Commission, the signing of EU standard clauses between the KION Group Legal Entity and the recipient in the respective country is mandatory. This obligation also applies to any intercompany Transfer of Personal Data, from a KION Group Legal Entity based in the EEA to a KION Group Legal Entity based in a Third Country.

The implementation shall be based on applicable KION standards (see chapter 13).

10. Security and Privacy Impact Assessment of Processing

You shall protect Personal Data against unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form.

Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he / she has not been authorized to carry out as part of his / her legitimate duties is unauthorized.

The “need to know” principle applies. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation of roles and responsibilities.

When you introduce new methods of Personal Data processing, particularly new IT systems, then you shall define and implement technical and organizational measures to protect Personal Data. These measures must be based on the state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification). The technical and organizational measures for protecting Personal Data are part of the corporate information security management and must be adjusted continuously to the technical developments and organizational changes.

Where a type of processing - taking into account the nature, scope, context and purposes of the processing - is likely to result in a high risk to the rights and freedoms of a Data Subject, the Process Owner shall carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data (Data Protection Impact Assessment) prior to the processing. This is particularly required in case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including Profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing on a large scale of special categories of data, or of Personal Data, relating to criminal convictions and offences; or
(c) a systematic monitoring of a publicly accessible area on a large scale.

In conducting those Data Protection Impact Assessments, the Data Protection Officer needs to be consulted. Furthermore, the Data Protection Officer needs to evaluate the assessment.

Details on secure and confidential data processing can be found in the corresponding standards (see chapter 13).

11. Personal Data Breach

If you, as an employee of an KION Group Legal Entity or a contracted Third Party, are aware of a Personal Data Breach, you shall communicate it immediately through the appropriate communication channels specified, e.g., on the KION Social Intranet https://kion.sharepoint.com/sites/kion_group/SitePages/Tools/Data_Protection_and_Security/Data-Protection-and-Security.aspx.

Possible cases of Personal Data breach include:

- improper Transfer of Personal Data to Third Parties,
- improper access by Third Parties to Personal Data, or
- loss of Personal Data.

The reporting and handling of Personal Data breaches shall take place based on applicable standards and need to be followed in order to fulfil legal obligations with respect to reporting, documentation and mitigation of Personal Data Breaches.

12. Cooperation with Data Protection Authorities

The KION Group and its respective legal entities shall respond to all requests from data protection authorities.

If you receive such a request from a data protection authority, you shall immediately inform the local Data Protection Officer or legal and the Group Data Protection Officer. Regarding Transfers of

Personal Data between KION Group Legal Entities, the importing and exporting entities will cooperate with inquiries and accept audits from the data protection authority responsible for the entity exporting the data.

In addition, each data protection authority may audit KION Group's Legal Entities and advise on matters related to the KION Group Data Protection Policy.

13. Policy Implementation and Enforcement

The implementation and enforcement of this policy is supported by data protection standards, procedures, guidelines and templates. Data protection standards are a set of mandatory rules and actions. Procedures are detailed step-by-step descriptions of mandatory tasks performed to achieve a certain goal. Guidelines are documents describing recommended actions or operating instructions to support the operational implementation of the policy, standards and procedures.

For each Legal Entity, an appointed Data Protection Coordinator and, where legally required, a local Data Protection Officer monitor the implementation of this policy (see chapter 4.4 and 4.5).

Employees shall comply with this policy and applicable data protection laws. Therefore, appropriate training shall be carried out. Employees shall be instructed at the start of their employment about their obligation to protect Personal Data. This obligation should also remain after the termination of their employment.

A copy of this policy and other relevant data protection and security-related standards and procedures are available to employees at any time on the data protection site of the intranet https://kion.sharepoint.com/sites/kion_group/SitePages/Tools/Data_Protection_and_Security/Data-Protection-and-Security.aspx.

The implementation of this policy shall be monitored by risk-based audits and assessments carried out by the Group Data Protection Officer, Local Data Protection Officers and supported by Internal Audit.

The Group Data Protection Officer will perform a management review at least once per year together with the responsible member of the KION Executive Board.

14. Liability Statement

We have not foreseen a transfer of liability. Therefore, each Legal Entity is responsible for compliance with applicable data protection legislation. The liability therefore remains with each responsible Legal Entity. Contradicting instructions, which cannot be solved by the involved parties, shall be escalated to the Group Data Protection Officer.

15. Handling of Exceptions and Conflict of Rules with Local Legislation

This Policy defines the mandatory baseline requirements, even if the applicable law sets a lower legal standard. Where applicable law contains a higher level of protection than this policy, the concerned KION Group Legal Entities shall collect and process Personal Data in accordance with the applicable law.

If a KION Group Legal Entity identifies a conflict between applicable laws and this policy, the Group Data Protection Officer shall be notified to obtain a risk-based exception.

16. Policy Update

The KION GROUP AG reserves the right to update this policy. This might be required to comply with legislative changes, interpretations of the data protection authorities, or to reflect organizational changes within the KION Group. Changes of this policy shall be applied by the effective date.

17. Contact of Group Data Protection Officer

Group Data Protection Officer
KION Group AG
Thea-Rasche-Straße 8
60549 Frankfurt
dataprotection@kiongroup.com

18. Change History

VERSION	DATE	NAME	CHANGES / COMMENTS
V.01	20.11.2019	Group Data Protection Policy	Initial version
V.01.1	14.04.2021	Group Data Protection Policy	Change of URL