# Global Policy for Data Protection Organization within the SGB-SMIT Group

Version: 02 Jan 2020

# Summary

## § 1 Purpose of the Data Protection Policy

(1) This corporate policy is the binding basis for a legally compliant and sustainable protection of personal data on a corporate level. The SGB-SMIT Group commits itself within the scope of its corporate responsibility to comply with the Data Protection Legislation. This Data Protection Policy is applicable for the SGB-SMIT group worldwide and is based upon globally accepted basic principles on data protection.

(2) This corporate policy is intended to respect and protect the fundamental rights of data subjects, notably the right to protection of personal data. The Data Protection Policy creates one of the necessary contexts for data transmissions between the group companies worldwide. It ensures the appropriate data protection level for cross-border data flow required by the European General Data Protection Regulation (GDPR) and national legislations even to those countries where data protection level regulation do not exist.

## § 2 Scope of application

(1) This policy is applicable for all companies within the SGB-SMIT Group and thus for all companies where SGB-SMIT Beteiligungs GmbH or SGB-SMIT New Venture GmbH have indirect or direct participation or where they are responsible for the economic management of such companies

(2) It applies personally for all employees and supervisors of the SGB-SMIT Group

(3) The commandments and prohibitions of this corporate policy apply for any handling of personal data, no matter whether it is carried out electronically or paper-based. They equally include all types of data subjects (customers, employees, suppliers, etc.) in the scope of application.

(4) The managing directors of the local companies are bound to carry out amendments or modifications to this policy, unless the respective local legislation has stricter or different requirements with regard to data protection. These modifications or amendments must be added to this policy in form of a national annex.

## § 3 Definitions

(1) Personal data is any information related to an identified or identifiable natural person (data subject). In this context, customer data are part of personal data as well as staff data of employees. The name of an interlocutor, for instance, makes it possible to identify to a natural person in the same way that the email address does. It is enough if the respective information is linked to the name of the data subject or if, irrespective of this fact, it can be related from the context. Also, a person may be identifiable, if the information has to be combined with some additional knowledge first, this is e.g. the case with the license plate. How the information was received is irrelevant for the reference to a person. Even pictures, videos or sound recordings may represent personal data.

(2) There are special types of personal data which may reveal information about racial or ethnic origin, political opinions, religion or philosophical beliefs and potential trade union membership as well as genetic data, biometric data, data concerning health or data concerning sex life or sexual orientation of individuals.

(3) Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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.
(4) Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future;
(5) 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.
(6) Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
(7) Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
(8) Processor means the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
(9) Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
(10) Third party means a natural or legal person, 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.
(11) Consent of the data subject means an indication of data subject's wishes that is freely given, specific, informed and unambiguous by a statement or clear affirmative action that signifies agreement to the processing of his or her personal data.

## § 4 Data Protection Organization

(1) The company has appointed a data protection officer. The Data Protection Officer is also the responsible Group Data Protection Officer and is to be appointed - as far as legally necessary - as Data Protection Officer for every company of the group.
(2) You can reach the Data Protection Officer, Mr. Stefan Unger, via the following contact details: data-protection@sgb-smit.group or via telephone at: +49 (0)941 - 7841 – 6587.

(3) Every single company of the group will appoint a Data Protection Coordinator and communicate his or her details to the Data Protection Officer. The Data Protection Coordinators are the local interlocutors for data protection issues.

(4) The Data Protection Officer and the Data Protection Coordinators monitor the compliance with the GDPR as well as with other legal guidelines, including the guidelines of the present and other corporate data protection policies. The Data Protection Officer advises and reports to the corporate management regarding existing data protection obligations and is responsible for the communication with supervisory authorities. He checks selected processes randomly, risk oriented and in reasonable intervals for their conformity with data protection rules.

(5) The Data Protection Officer executes his or her missions using his or her expert knowledge and is not subject to instructions. He reports directly to the corporate management.

(6) It is the obligation of the respective managing directors or their employees to support the Data Protection Officer and the Data Protection Coordinators regarding the execution of their duties. Those technically responsible for the business processes must inform the Data Protection Coordinators in a timely manner about new personal data processing actions. In case of intended data processing which could result in particular risks for the personal rights of the data subjects, the Data Protection Officer must be consulted already before starting with the processing. This applies notably for personal data which merit specific protection. In many countries, abusive processing of personal data or other breaches against the Data Protection Law are prosecuted as per criminal law and could result in damage claims. Responsibility for violations of applicable Data Protection laws lies with individual employees and may lead to sanctions as provided by labor laws.

## § 5 Principles relating to processing of personal data

(1) Fairness and lawfulness

When processing personal data, the personal rights of the data subject must be respected. Personal data must be collected and processed in a lawful and fair manner.

(2) Purpose limitation

The processing of personal data must be limited to the initial purposes which were determined before the collection of the data. Subsequent amendment of the purposes is only possible in a restricted manner and requires a justification.

(3) Transparency

The data subject must be informed about the handling of his or her data. In principle, personal data shall be collected directly from the data subject. When collecting the data, the data subject must be able to identify the following or must receive according information about:

» The identity of the controller
» The purpose of the data processing
» Third parties or third-party categories, to which the data will be transmitted if necessary

(4) Avoiding and limiting data

Before processing personal data, it shall be verified if and to what extent the processing is necessary in relation to the purposes for which they are processed. If possible and if the effort is proportionate to the envisaged purposes, anonymized or statistical data shall be used. Personal data must not be retained for potential future purposes, except if it is specified or authorized by national law.

(5) Erasure
Personal data which, after expiry of legal or business process related retention periods, are no longer necessary must be erased. In singular cases, if there are indications for legitimate interests or for historic significance of the data, this data may remain stored until the legitimate interest has been legally clarified or until the group archives have been able to evaluate the data set with regard to the worthiness of archiving for historical purposes.
(6) Accuracy and timeliness of data
The personal data stored must be accurate, complete and, where necessary, kept up to date. Reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or obsolete is erased, rectified, amended or updated.
(7) Confidentiality and data security
Personal data is subject to secrecy of data. Personal data must be used in a confidential manner and must be secured against unauthorized access, unlawful processing or transmission and against accidental loss, alteration or destruction by appropriate organizational and technical measures.

## § 6 Using personal data – Admissible data processing

(1) In general, the processing of personal data is forbidden except if a legal standard explicitly authorizes using the data. According to the GDPR personal data may be processed in general:

- in case of an existing contractual relation with the data subject.
  Example: Storage and use of necessary personal data within the scope of an order or an existing employment contract. For the handling of employee and applicant data, please refer to the directive for the handling of personal data (Global directive for the handling of personal data).
- in the context of pre-contractual measures at the data subject’s request as well as when concluding a contract with the data subject.
  Example: Customer C requests information for one of our products and purchases it. The data necessary for sending the information material as well as for carrying out the transaction (delivery of the goods and payment of the purchase price) may be processed.
- If and to the extent that the data subject has given his or her consent.
  Example: The data subject subscribes to the newsletter.
- In case of a legal obligation to which the company is subjected.
  Example: Legal retention periods according to the Commercial Code and Fiscal Code.
- In case the company has legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Data processing on the grounds of a legitimate interest should, however, not be carried out without prior consultation by the Data Protection Officer.
  Example: Use of the postal address for sending promotional letters.

(2) The data subjects must not be subject to a decision based exclusively on automated processing – including profiling – which has legal effects on them or which otherwise affect them to a significant degree.

(3) Personal data shall be processed for a previously determined, explicit and legitimate purpose. Storage of data without purpose as, for instance, within the scope of data retention is forbidden.

(4) If possible, one should refrain from using personal data. Pseudonyms or anonymous data processing shall be preferred.

(5) Modification of the processing purposes for which the personal data were initially collected should be allowed only - in addition to the consent given by the data subject - where the processing is compatible with the purposes for which the personal data were initially collected. In this context the reasonable expectations of data subjects towards the company as to such a processing, the nature of the data used, the consequences for the data subject as well as the encryption or pseudonymization possibilities shall be taken into consideration.

(6) When collecting personal data, the data subject must be informed extensively about the handling of his or her data. Information must include processing purpose, identity of the controller, recipients of his or her personal data as well as all other information as defined by Art. 13 GDPR, in order to guarantee a fair and transparent processing. Information must be written in an easily accessible and easy to understand form, and in a clear and plain language.

(7) In case personal data are not collected with the data subject but are, for instance, provided by another company, the data subject must be informed, in accordance with Art. 14 GDPR, after the fact and extensively about the handling of his or her data. This applies equally in case of a modification of the processing purposes.

(8) Personal data shall be accurate and, if necessary, up to date. The data processing scope should be considered necessary and relevant with regard to its determined purposes. The respective department must ensure the implementation by establishing suitable processes. Furthermore, existing data must be verified on a regular basis as to their accuracy, necessity and current.

## § 7 Special categories of personal data

As a basic principle, special categories of personal data must only be collected, processed or used with the consent of the data subject or, in exceptional cases, with an explicit legal authorization. Furthermore, additional technical and organizational measures (e.g. encryption during transport, minimum rights granting) shall be taken to protect the special personal data.

## § 8 Data transmission

(1) Transmission of personal data to third parties is only allowed if permitted by law or with the consent of the data subject.

(2) Should the recipient of personal data be situated outside of the European Union or of the European Economic Area, special measures need to be taken in order to preserve the rights and interests of data subjects.

### § 9 External service providers

(1) In each case where external service providers shall be granted access to personal data, the Data Protection Officer must be informed in advance.

(2) Service providers with possible access to personal data must be selected carefully before providing them with or giving them access to personal data. The selection process must be documented and should consider particularly the following aspects:

- Technical ability of the service provider for data handling
- Technical and organizational safety measures
- Experience of the supplier in the domain
- Other aspects which suggest the reliability of the supplier (data protection documents, preparedness to cooperate, response times etc.)

(3) Where a service provider is appointed to collect, process or use personal data, an order processing contract must be concluded.  The contract must govern the aspects regarding data protection and IT security.

(4) The technical and organizational measures contractually agreed with the service provider must be verified on a regular basis. The result of such verification must be documented.

### § 10 Data minimization, Privacy by Design/Privacy by Default

(1) The handling of personal data must be in line with the aim of collecting, processing or using as little data as possible of a data subject (“data minimization”). Notably, personal data must be anonymized or pseudonymized to the extent possible with regard to its purposes. For instance, knowing and using the full name of a data subject will not be necessary when carrying out a statistical analysis of data. This information may rather be replaced by a random value allowing also for a differentiation of the subsequent information.

(2) This applies accordingly when selecting and designing data processing systems. Data protection has to be integrated from the beginning in the specifications and structure of data processing systems so as to facilitate the compliance with the basic principles of privacy and data protection, notably the basic principle of data minimization.

### § 11 Rights of data subjects

(1) Data subjects have the right of access to personal data which are stored in the company concerning him or her.

(2) When processing requests, the identity of the data subject must be clearly determinable. Where there are reasonable doubts concerning the identity, the provision of additional information may be requested. The access to information is given in written form except if the data subject has filed his or her request in electronic format. Where personal data has been transmitted to third parties, the identity of the recipient or the categories of recipients must be equally disclosed.

(3) Data subjects have the right to rectification of their personal data if they turn out to be inaccurate. Also, they have the right to request completion of incomplete personal data.
(4) The data subject has the right to object to the processing of his or her personal data for advertising or market research and opinion polls. The data must be blocked for these purposes.
(5) The data subject has the right to request the erasure of his or her data if the legal basis for the processing of the data is missing or has ceased to exist. The same applies when the purpose of the data processing has become void over time or due to other reasons. Existing storage obligations and legitimate interests which are opposing to the erasure have to be taken into consideration.
(6) The data subject has a fundamental right to object the processing of his or her data. This right must be taken into consideration if the legitimate interest due to a particular personal situation overrides the processing interest. This does not apply if a mandatory legal provision for the execution of the processing exists.
(7) The data subject must be informed within one month about all measures taken upon his or her request.
(8) The Data Protection Officer will offer his or her advice in order to preserve the rights of the data subjects.

**§ 12 Third party information requests about data subjects**

Where a body requests information about data subjects, for instance customers or corporate employees, the transmission of information is only permitted if

- the body requesting information can present a legitimate interest for it, and
- a legal standard makes the information mandatory, as well as
- the identity of the requesting party or body has been clearly and undoubtedly determined.

**§ 13 Records of processing activities**

(1) The company shall keep records of all data processing activities. Every department shall have responsible person who documents all necessary information regarding the procedures of the respective departments in conformity with the legal requirements set forth in Art. 30 GDPR. The Data Protection Officer may be consulted with regard to the information required by law.
(2) The company will make the records available to the supervisory authorities upon their request. By mutual agreement with the corporate management, the Data Protection Officer is responsible for this.

**§ 14 Security of processing**

Personal data must be protected at all times against unauthorized access, unlawful processing or transmission as well as against loss, adulteration or destruction. The availability, confidentiality and integrity of the data must be ensured. This applies irrespective of the fact whether the data processing is carried out electronically or paper-based. Technical and organizational measures for the protection of personal data must be determined and implemented before introducing any new data processing procedures, notably new IT systems. These measures must be in line with the state-of-the-art, with the risks arising from processing and with the need for protection of the data. The responsible department may consult notably with the IT department and the Data Protection Officer. The technical and organizational measures must be continuously adapted to the technical developments and to any organizational changes. Please refer to the corporate IT security policy.

### § 15 Training

Employees who have regular or constant access to personal data, who collect such data or who develop systems for the processing of such data, shall be trained appropriately about the legal provisions regarding data protection. The Data Protection Officer decides about the form and periodicity of the corresponding training sessions.

### § 16 Secrecy of data

(1) It is forbidden for employees to collect, process or use personal data without proper authorization. Before carrying out their respective tasks, they have to commit to a confidential use of personal data. The commitment is made through the corporate management using the form provided for such effect.
(2) Additionally, employees with special non-disclosure agreements (e.g. secrecy of telecommunications according to § 88 of the German law on telecommunications) are bound to this commitment in writing by the corporate management.

### § 17 Complaints

(1) Every data subject has the right to lodge complaints regarding the processing of his or her data if he or she deems it to be a violation of his or her rights. Likewise, employees may report breaches of this policy anytime.
(2) The competent body for aforementioned complaints is the Data Protection Officer as internal, independent instance who is not subject to instructions.
(3) Independently, every data subject has the right to lodge a complaint with the competent data protection supervisory authority.

### § 18 Control of data protection

Compliance with the data protection policies and with the Data Protection Laws in force will be controlled regularly by means of data protection audits and other controls. The responsibility for carrying out these audits rests with the group data protection officer, the data protection coordinators and other corporate departments with audit rights or, where appropriate, external auditors.

### § 19 Internal investigations

(1) Measures for fact finding and for avoiding or discovering criminal acts or major breaches of obligations in the context of employment must be carried out in strict observation of the relevant, legal data protection provisions. The accompanying collection and use of data which is necessary for investigation purposes must notably be appropriate and proportionate to the legitimate interests of the data subject.
(2) The data subject must be informed as soon as possible about the measures carried out with regard to his person.
(3) With all forms of internal investigations, the Data Protection Officer must be consulted regarding the selection and form of the measures in advance.

### § 20 Data protection impact assessment

(1) Every department must carry out Data Protection Impact Assessments for procedures carried out under their responsibility whenever an elevated risk to the rights and freedoms of the data subjects can be expected due to the processing of data. The Data Protection Impact Assessment includes all legally required descriptions of Art. 35, item 7 GDPR.

(2) The Data Protection Officer advises the departments during the execution of the Data Protection Impact Assessment as well as with regard to the question about high risks for data subjects due to processing.

### § 21 Personal data breach ("data leak")

(1) In case of unlawful disclosure of corporate and personal data to third parties, the respective superior and/or Data Protection Officer have/has to be informed immediately.

(2) The report shall include all relevant information for the fact-finding, notably the receiving body, the data subjects as well as nature and extent of the data transmitted.

(3) The compliance with a possible information obligation towards supervisory authorities is exclusively ensured by the Data Protection Officer. Where necessary, the data subjects will be informed by the corporate management in coordination with the Data Protection Officer.

### § 22 Accountability

Compliance with the provisions of this policy must be provable at any time. In this context special care has to be given to the traceability and transparency of measures which have been taken, for instance with associated documents.

### § 23 Update of the policy; traceability

(1) This policy shall be reviewed on a regular basis as to whether it is necessary to adapt or amend it within the context of the evolution of data protection laws or technological or organizational changes.

(2) Amendments of this policy shall be valid without adhering to a specific form. The employees and supervisors must be informed immediately and in an appropriate manner about the amended provisions.

| | |
|---|---|
| Apr 6, 2020 | H. Uekermann<br>H. Uekermann (Apr 6, 2020) |
| Date | MANAGEMENT<br>SGB-SMIT GMBH |
| Apr 6, 2020 | H. Ketterer<br>H. Ketterer (Apr 6, 2020) |
| Date | MANAGEMENT<br>SGB-SMIT GMBH |

# Globale Richtlinie Datenschutzorganisation von Hr. Unger

Final Audit Report 2020-04-06

| | |
|---|---|
| Created: | 2020-03-26 |
| By: | Sandra Schwimmer (sandra.schwimmer@sgb-smit.group) |
| Status: | Signed |
| Transaction ID: | CBJCHBCAABAALrVOdW7IVRNjqTHt8vTG1US-oxgyPckQ |

## "Globale Richtlinie Datenschutzorganisation von Hr. Unger" History

Document created by Sandra Schwimmer (sandra.schwimmer@sgb-smit.group)

2020-03-26 - 9:31:23 AM GMT- IP address: 87.180.182.239

Document emailed to H. Uekermann (heinrich.uekermann@sgb-smit.group) for signature

2020-03-26 - 9:32:17 AM GMT

Email viewed by H. Uekermann (heinrich.uekermann@sgb-smit.group)

2020-03-27 - 1:28:51 PM GMT- IP address: 93.240.151.42

Document e-signed by H. Uekermann (heinrich.uekermann@sgb-smit.group)

Signature Date: 2020-04-06 - 7:57:26 AM GMT - Time Source: server- IP address: 217.230.45.177

Signed document emailed to Sandra Schwimmer (sandra.schwimmer@sgb-smit.group) and H. Uekermann (heinrich.uekermann@sgb-smit.group)

2020-04-06 - 7:57:26 AM GMT

# Globale Richtlinie Datenschutzorganisation von Hr. Unger - signed

Final Audit Report 2020-04-06

| | |
|---|---|
| Created: | 2020-04-06 |
| By: | Sandra Schwimmer (bianca.samhuber@sgb-trafo.de) |
| Status: | Signed |
| Transaction ID: | CBJCHBCAABAAGGahYHXJpL6pPRo9Tj0jOZ9V7FmCQj2V |

## "Globale Richtlinie Datenschutzorganisation von Hr. Unger - signed" History

Document created by Sandra Schwimmer (bianca.samhuber@sgb-trafo.de)

2020-04-06 - 8:09:00 AM GMT- IP address: 93.240.151.42

Document emailed to H. Ketterer (holger.ketterer@sgb-smit.group) for signature

2020-04-06 - 8:09:32 AM GMT

Email viewed by H. Ketterer (holger.ketterer@sgb-smit.group)

2020-04-06 - 8:37:23 AM GMT- IP address: 93.240.151.42

Document e-signed by H. Ketterer (holger.ketterer@sgb-smit.group)

Signature Date: 2020-04-06 - 9:38:13 AM GMT - Time Source: server- IP address: 93.240.151.42

✓ Signed document emailed to Sandra Schwimmer (bianca.samhuber@sgb-trafo.de) and H. Ketterer (holger.ketterer@sgb-smit.group)

2020-04-06 - 9:38:13 AM GMT