Binding Corporate Rules

v. 2.0 / 2020

IT Governance

Bonn Office
Willy-Brandt-Allee 13
53113 Bonn

Contents

1 Introduction

Simon-Kucher & Partners operates on all five continents with offices all over the world. Simon-Kucher & Partners is highly aware and very sensitive about the social, cultural and legal differences between all countries in which our offices can be found. Simon-Kucher & Partners serves customers from different countries and provides excellent advice in an international context. International projects demand transfer of personal data between the offices. This is true for research data as well as for personal data of our employees.

Simon-Kucher & Partners is committed to ensuring an adequate level of privacy protection in all offices of Simon-Kucher & Partners regardless where on the world it might be. Social, cultural and legal differences between the countries must not affect an adequate level of privacy protection. Simon-Kucher & Partners wants for their customers, participants in research studies and of course the employees of Simon-Kucher & Partners to be able to rely on the promise that Simon-Kucher & Partners treats personal data in all offices in an equally safe and responsible way and that Simon-Kucher & Partners follows the same privacy principles throughout the group to ensure an adequate level of privacy protection. Simon-Kucher & Partners consequently has established an effective framework for the processing of employee‘s personal data as well as for the processing of personal data of customers and research participants.

The objective of these Binding Corporate Rules (BCR) is to provide an adequate protection for the transfers and processing of personal data by offices of Simon-Kucher & Partners. They include but are not limited to a description of our high privacy protection standards and how Simon-Kucher & Partners brings the fundamental privacy protection principles to life. The Binding Corporate Rules also enable Simon-Kucher & Partners to transfer personal data to offices outside the EU in a legally compliant way. According to European Legislation, an export of personal data may only occur if there is an adequate level of privacy protection in importing locations. Binding Corporate Rules ensure this adequate level of privacy protection as required by the EU Regulation 2016/679 (General Data Protection Regulation – GDPR) and the EU Directive 2002/58.

Simon-Kucher & Partners can only achieve this goal of providing an adequate level of data protection if all members of the Group and every single employee accept these rules as binding. Therefore, it is the clear duty of all Simon-Kucher & Partners’ companies and employees to observe these Binding Corporate Rules at all times and to fulfill the BCR-requirements when processing personal data.

The board of management acknowledge that maintaining the adequate level of privacy protection demands continuous efforts of all groups of Simon-Kucher & Partners. Consequently, Simon-Kucher & Partners ensures compliance with the binding corporate rules. The audit

scheme, which is part of the Binding Corporate Rules, helps Simon-Kucher & Partners to monitor the privacy processes. Whenever Simon-Kucher & Partners finds that the Binding Corporate Rules are not being followed, the management will immediately take and support all necessary steps to restore compliance with the Binding Corporate Rules.

2 Definitions

Simon-Kucher & Partners is committed to ensuring that all relevant data protection definitions are compliant to the regulations of Regulation 2016/679 of the European Parliament.

Personal Data	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.
Sensitive Personal Data	Also referenced as special categories of data. Sensitive personal data reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
Data Subject / Individual	The data subject is the identified or identifiable natural person to whom the personal data refer.
Controller	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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
Third Party	Any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the

	processor and the persons who, under the direct authority of the controller or the processor, are authorized to process personal data.
Processing of Personal Data	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;
Data Subject's Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Data Protection Authority	A public authority in a Member State of the EU that is responsible for monitoring the application within its territory.
Headquarters	Shall mean the location of the Simon-Kucher & Partners Group in Bonn, Germany, where the majority of Simon-Kucher & Partners Group IT infrastructure is located.
Data Protection Officer (DPO)	The DPO is assigned for Simon-Kucher & Partners in Germany and takes care of data protection at the Headquarter of Simon-Kucher & Partners Group. He is in direct contact with the management board and supervises data protection processes. To fulfil this purpose he can contact the DPT to acquire necessary information or coordinate data protection tasks.

3 Scope

Our Binding Corporate Rules apply to all intra-group transfers and processing of personal data. They do not only apply to personal data processed in the EU and transferred outside the EU but to all personal data transferred between Simon-Kucher & Partners' offices. Third beneficiary rights apply only to data subjects in the EEA.

The Binding Corporate Rules apply to automated and manual processing of research data and employee data. These Binding Corporate Rules apply to data that has been defined to be "business confidential". The appendix "Data Protection Processes Handbook" is an essential

element of these Binding Corporate Rules. It defines processes for realization of privacy which are binding for all offices and employees in the same way as the Binding Corporate Rules.

The board of management, project leaders and persons which are responsible for Human Resources of offices that have signed the BCR Contract have to ensure that their employees follow the requirements defined in the Binding Corporate Rules along with the "Data Protection Processes Handbook".

3.1 Nature and Place of Storage of Data

Simon-Kucher & Partners is specialized in strategy, marketing, pricing and sales. Simon-Kucher & Partners is regarded as the world's leading pricing advisor. Pricing consulting is the core business of Simon-Kucher & Partners. Success is based on expert knowledge on how to determine the factors influencing pricing. This includes the knowledge on which sort of personal data may be required for pricing consultancy and research projects. Consequently, Simon-Kucher & Partners is the controller of such personal data necessary to fulfill their own business purposes. They advise their clients on the scope of personal data necessary for a research project and determine which information can be derived from such data concerning pricing for products and services.

Transferred data concerns anonymized research data in the first place. Personal data will only be transferred if it is absolutely necessary for a research project. The required data types depend on the purpose of each research project. It is ensured that sensitive personal data is identified at the time of project start and that the particular requirements for handling sensitive data is guaranteed (cf. part 5 and part 11 of the BCR).

Simon-Kucher & Partners transfers the following employee data as shown in depiction 1 for the purposes described in chapter 2.2:

- the complete name and birth name, date of birth and place of birth,
- native language,
- address and contact details,
- bank account information,
- electronically available documents such as CVs and similar documents,
- information on educational background,
- employee's level,
- division and/or location,
- probation period,

- vacation entitlement,
- working time model,
- salary information,
- work performance index,
- working objectives,
- Mentor/Mentee administration,
- whether the confidentiality obligation has been signed,
- Participation in our compliance trainings.

Personal data is stored on our secure servers in Bonn, Germany. Whenever a partner, office manager or project member accesses personal data in the project or employee database, this personal data is not duplicated on the accessing system and remains on the servers in the headquarters. Nevertheless, this infrastructure enables project members to access all necessary project data, no matter which office they are working at the time. Access is restricted. Project members have only access to personal data stored for the project they are working on.

Data Minimization

Simon-Kucher & Partners follows the concept of data minimization as laid out in Article 5 para. 1 lit. c GDPR, which includes that personal data has to be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed. Personal data is not necessary for the majority of research projects. Consequently, Simon-Kucher & Partners follows the concept of data avoidance, data minimization and use anonymization whenever possible. Simon-Kucher & Partners has set up a process for anonymization and pseudonymization which is documented in the "Data Protection Processes Handbook". Following this process ensures that Simon-Kucher & Partners does not not receive personal data from customers where it is not strictly necessary. In the event that personal data is provided unnecessarily or accidentally, this personal data will be destroyed as soon as possible, especially before any transfer of research data. Employees are obliged to follow this process and use anonymization wherever possible as described in the Data Protection Processes Handbook.

Certain projects may require processing of personal data to successfully conduct research. In those cases pseudonymization is used whenever and as soon as possible. Only absolutely necessary personal data will be used to conduct the research. Strict requirements apply if special categories of personal data are necessary for conducting the research.

3.2 Access to Employee Data

Simon-Kucher & Partners uses personal data stored in the employee database for administration purposes. Partners in all our offices have the ability to access (only read access) the history of level, division and locations as well as all information relevant to salary. Partners also have access to promotion, salary, bonuses and working objectives during the evaluation period.

In each country, at least one office manager is employed who is occupied with administrative tasks concerning the employment contract, such as payroll accounting and personnel bookkeeping. Those office managers are responsible for creating and maintaining the employment contracts and therefore have full access to employee personal data. The office manager has only full access to the data of employees of their country. For administrative purposes, such as project coordination, the office manager has read access to the basic data of all employees worldwide, including name, division, office and level..

Employee timesheets are stored on the same server as the employee database. Employee timesheets can be accessed by office managers for their respective employing country only. Office managers need the data to perform completeness checks. Employee timesheet data is used for the purpose of invoicing and compiling working hours for certain projects.

3.3 Data Importers/Exporters

Simon-Kucher & Partners would like to highlight that the centralized databases are located in Bonn, Germany and that while access to these databases during the project phase using a VPN connection grants a view on the data, the data is not transferred in a technical sense. At the end of the process, there is no copy of the data on the local device of the employee, as local copies of such data on the employee's computers are forbidden.

3.3.1 Data Exporters in the EU

As all our offices exchange data, all offices are potential importers and exporters. For these Binding Corporate Rules, Simon-Kucher & Partners only list the offices in Europe as data exporters.

The following offices export personal data outside the EU/EWR:

- Bonn, Germany
- Cologne, Germany
- Munich, Germany
- Frankfurt, Germany
- Paris, France
- Madrid, Spain

- Milan, Italy
- Copenhagen, Denmark
- Stockholm, Sweden
- Brussels, Belgium
- Luxembourg, Luxembourg
- Vienna, Austria
- Warsaw, Poland

3.3.2 Data Importers

The following offices may receive personal data from the exporters and are defined as importers:

- Tokyo, Japan
- Singapore, Republic of Singapore
- Dubai, United Arab Emirates
- Sydney, Australia
- Cairo, Egypt
- Istanbul, Turkey
- Atlanta, United States of America
- Boston, United States of America
- Chicago, United States of America
- Houston, United States of America
- New York, United States of America
- San Francisco, United States of America
- Silicon Valley, United States of America
- Mexico City, Mexico
- São Paulo, Brazil
- Santiago de Chile, Chile
- Beijing, China
- Hong Kong, China

- Shanghai, China
- London, United Kingdom

An updated list of Simon-Kucher & Partners' European and international Offices can be found here: https://www.simon-kucher.com/en/contact/offices

4 Purpose Limitation and Storage Limitation

According to Article 5 para. 1 lit. b GDPR personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Personal data will only be processed and transferred if it is necessary for the specific and legitimate purposes of research projects or employee administration as described above.

Specifically allowed purposes are the invitation of participants to research and advisory projects and contact with participants of research and advisory projects.

If neither consent nor any other legal permission for the processing of data already collected for purposes other than the original purposes is given, changes to the purpose are only permitted if a "compatibility test" has been carried out which, among other things, includes a connection between the old and new purposes, the context of data collection, the purposes of further processing, the type of personal data in scope, the possible consequences for the data subjects and the security measures taken to safeguard the data.

According to Article 5 para. 1 lit. e GDPR, personal data shall be kept in a form which does not allow an identification of data subjects after the purposes for which the personal data are processed has been achieved. Employees are required to process personal data only as long as strictly necessary for achieving the purposes for which we have collected them.

5 Data Quality and Accuracy

According to Article 5 para. 1 lit. d GDPR, personal data shall be accurate and, where necessary, kept up to date. We are taking reasonable steps to ensure that inaccurate personal data is erased or corrected without undue delay.

The offices and employees of Simon-Kucher & Partners take reasonable steps to ensure that personal data is stored and transferred only for the specified purposes and are reliable for their intended use, accuracy, completeness and actuality. Simon-Kucher & Partners requires that their customers provide only accurate, complete and current data for the specified purposes.

If Simon-Kucher & Partners is notified by the data subject or in another way that any personal data stored at Simon-Kucher & Partners is inaccurate, incomplete or out of date, we will correct,

complete or update the respective data. If an update is not possible, the data must be deleted. Where needed, the employee must involve the Data Protection Team and the Data Protection Officer as well.

Project leaders and employees mustensure that personal data is adequate by classifying research data at the very beginning of a project. Simon-Kucher & Partners supports this classification by technical means. The data monitoring tool ensures that a classification of data necessary for a project must take place before the beginning of the project. Project members will receive an immediate response indicating which precautions have to be taken depending on the types of data involved.

6 Lawfulness, Fairness and Transparency, Principle of Proportionality

According to Article 5 para. 1 lit. a GDPR, personal data shall be processed lawfully and in a fair manner in relation to the data subject.

According to Article 6 para. 1 GDPR, personal data shall only be processed and transferred if any of the following requirements is fulfilled:

- The data subject has unambiguously given their consent (opt-in) for the processing of his or her personal data, or
- The processing is necessary for the performance of a contract which the data subject is party to or in order to implement pre-contractual measures requested by the data subject, or
- The processing is necessary for compliance with a legal obligation which the controller is subject to, or
- The processing is necessary in order to protect the vital interests of the data subject or another natural person, or
- The 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 or in a third party to which the data is disclosed, or
- The processing is necessary for the purposes of legitimate interests pursued by the controller, the third party or parties to which the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject, especially if the data subject is a child.

In the case of data processing under legitimate interests, a proportionality test shall be carried out to determine whether the measures are appropriate, necessary and proportionate. The

interests of Simon-Kucher & Partners must be carefully weighed against the possible counter-interests of the data subjects.

If any employee is in doubt about which of the alternatives or if one of the alternatives is applicable, he or she must immediately contact the DPO.

7 Legal Basis for Processing of Sensitive Data

According to Article 9 GDPR, processing of sensitive data is prohibited except if:

- the data subject has given their explicit consent to the processing of their sensitive data, except where applicable laws prohibit it, or
- The processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the context of employment legislation insofar as it is authorized by national law providing for adequate safeguards for the fundamental rights and freedoms of the data subject, or
- The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving their consent, or
- The processing relates to sensitive data which is explicitly made public by the data subject themselves, or
- The processing is necessary for the establishment, exercise or defense of legal claims, or
- The processing is necessary for reasons of substantial public interest on the basis of national law which shall be proportionate to the aim pursued, respecting the essence of the right to data protection and providing for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject, or
- The processing is necessary for the purposes of preventive or occupational health care, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of national law or pursuant to contract with a health care professionals when data is processed by or under the responsibility of a professional who is subject to the obligation of professional secrecy established by law or rules established by national competent bodies
- The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medical products or devices, on the

basis of national law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on national law which shall be proportionate to the aim pursued, respecting the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by national law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

If any employee should be in doubt about which of the alternatives or if any of the alternatives is applicable, he or she must immediately contact the DPO.

8 Transparency and Information Requirements

According to Article 5 para. 1 lit. a GDPR, personal data shall be processed in a transparent manner in relation to the data subject.

Simon-Kucher & Partners makes the Binding Corporate Rules readily available to every data subject in order to maintain transparency about the way Simon-Kucher & Partners processes personal data and inform them about their rights.

The data subject can access the parts of the Binding Corporate Rules relevant to them on the Simon-Kucher & Partners' websites as part of the privacy notice. At data subject's requests, employees will direct the data subject to the appropriate privacy policy on the homepage. If the data subject has no internet access, Simon-Kucher & Partners will make the Binding Corporate Rules available to the data subject in text form.

Before any processing or transferring personal data, the data subject must be informed according to our "transparency and notice" process which is part of our "Data Protection Processes Handbook". Employees are required to check the process and must decide on how to inform and notify the data subject. If we collect personal data directly from the data subject, we may only not inform the data subject when they already have knowledge of the necessary information.

Simon-Kucher & Partners must inform data subjects

a) when Simon-Kucher & Partners first asks them to provide personal information or

b) in any event before Simon-Kucher & Partners uses any personal data for a purpose other than that for which it was originally collected or processed

c) within a reasonable period of time after obtaining the personal data, but at the latest within one month, taking into account the specific circumstances in which the personal data is processed

d) if the personal data is to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

e) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed

Simon-Kucher & Partners will provide the following information:

- the identity and the contact details of the controller (responsible Simon-Kucher & Partners entity) and, where applicable, of the controller's representative;
- the contact details of the data protection officer;
- the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
- where the processing is based on legitimate interests of Simon-Kucher & Partners or those of a third party, the legitimate interests pursued by Simon-Kucher & Partners or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, intended transfers of personal data to a third country or international organization and the existence or absence of safeguards such as our BCR, EU Standard Contractual Clauses, adequacy decisions of the EU commission or similar safeguards;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request access to and rectification or erasure of personal data, or to restrict or object to processing as well as the right to data portability;
- where the processing is based on the consent of the data subject, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the possibility to contact the Data Protection Team or the Data Protection Officer directly (contact details must be provided)
- the right to lodge a complaint with a supervisory authority;

- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide personal data and of the possible consequences of failure to provide such data;
- 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.

If we collect data from other sources than directly from the data subject, we have to inform the data subject additionally about:

- The categories of personal data involved
- the source of the personal data,, and if applicable, whether it originated from publicly accessible sources.

The only exceptions to the requirement to inform the data subject are:

- If the data subject already has all the necessary information or
- if the data has not been obtained from the data subject and the provision of such information proves impossible, would involve a disproportionate effort or if recording or disclosure is expressly stipulated by law.

If any employee considers choosing one of the aforementioned exceptions, they must contact the DPO.

9 Data Subject's Rights

All Simon-Kucher & Partners entities that have signed the BCR contract are obliged to fulfill the requirements concerning the data subject's rights.

9.1 Right to Access

Simon-Kucher & Partners grant data subjects access to their personal data. This includes the right to obtain a copy of all data relating to them without constraint within one month from the data subject's request. We may only extend this deadline by further two months in rare cases and only if we notify the data subject about the extension within the first month. The notice shall include the reasons for the delay. The copy has to be provided free of charge.

Employees have to follow the process "Right of Access" of the "Data Protection Processes Handbook".

9.2 Correction, Restriction, Erasure

Data subjects have the right to demand that Simon-Kucher & Partners correct, amend or delete incorrect personal data. Data subjects are free to contact the Data Protection Team to exercise their right of access. The Data Protection Team's email address is: dpt@simon-kucher.com.

We are obliged to notify all third parties that we have transferred the relevant data to about any correction, restriction or erasure of personal data. This would not apply if the execution was impossible or caused disproportionate efforts. Additionally, on the request of the data subject, we have to provide them with the details of the recipients of their data.

9.3 Data Portability

We are obliged to provide the data subject with their personal data in a structured, commonly used and machine-readable format where automated processing is based on the data subject's consent (Opt-In) or on a contract which the data subject is a party of.

9.4 Right to object

Every data subject has the right to object, at any time on compelling legitimate grounds relating to their particular situation, to the processing of their personal data, unless that processing is required by law. The DPT will evaluate if the objection is justified. The data subject can directly contact the DPT at: dpt@simon-kucher.com. Where the objection is justified, the processing must cease. Stored data has to be erased in most of the cases. The DPT will advise on this topic on a case to case basis.

Every data subject has the right to object, on request and free of charge, to the processing of personal data relating to him for the purposes of direct marketing and we are going to stop processing of personal data for such purposes immediately.

10 Automated Individual Decisions including Profiling

A commitment of the Simon-Kucher & Partners group is that no evaluation of, or decision about the data subject which significantly effects them legally or factually will be based solely on automated processing of their data including profiling unless the decision:

- is necessary for entering into, or performance of, a contract between the data subject and us, or is authorized by national law to which we are subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or.
- Is based on the data subject's explicit consent

- suitable measures are implemented to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on our part, to express their point of view and to contest the decision.

All Simon-Kucher & Partners' entities adhering to the BCRs commit themselves to not make an automated decision based on sensitive data, unless one of the following conditions is true:

- The data subject has provided us with their valid consent to use such data for one or more clearly defined purposes, or
- Processing is necessary for reasons of substantial public interest, on the basis of national law which shall be proportionate to the aim pursued, respecting the essence of the right to data protection and providing for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

11 Security and Confidentiality

All Simon-Kucher & Partners entities that have committed to the BCR are required to take reasonable precautions to protect personal data from unauthorized or unlawful processing and against accidental loss, destruction or damage. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, all Simon-Kucher & Partners entities submitting to the BCR shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Measures that comprise physical access control, system access control, logical access control, disclosure control, input control, job control, availability control and separation control are described in the "Data Protection Processes Handbook".

Sensitive data is subject to a high protection level and has to be processed with elevated security measures taken by all Simon-Kucher & Partners entities submitting to the BCR.

These technical and organizational measures are subject to frequently conducted audits by the Simon-Kucher & Partners Group. The audits are planned yearly by the Data Protection Team. The audit or a part of the audit may also be conducted by an independent third party. Offices of the Simon-Kucher & Partners Group are committed to allow and support the planned audits. This includes supporting the auditor with all information necessary for the audit.

Technical and organizational measures have to be designed and implemented in a way that helps all involved parties to follow the requirements of the BCR easily (privacy by default, privacy by design).

12 Processors which are Members of the Group

Simon-Kucher & Partners GmbH provides IT services for the other offices of the Simon-Kucher & Partners Group. Most of the central computing facilities that may be accessed by the other offices are located in Bonn, Germany, on the premises of the Simon-Kucher & Partners GmbH. The central SAP infrastructure is also hosted by Simon-Kucher & Partners IT in Bonn, Germany.

The contracting authority in the company group and Simon-Kucher & Partners GmbH will comply with the relevant rules of data processing according to the legal requirements. The parties agree on binding rules in accordance with Article 28 GDPR between controller and processor and specify the scope of the right of the controller to issue instructions for the processing of personal data. The activity of the processor is limited first and foremost to providing the technical infrastructure in accordance with the technical guidelines and specifications of Simon-Kucher & Partners Group and to technically enable data processing triggered by the controller. The responsible body for data processing on the systems is the controller.

The technical and organizational measures for data protection within the group that are based on the central data storage are established by the Simon-Kucher & Partners GmbH in Bonn and aligned group-wide. They are the basis for data processing by Simon-Kucher & Partners. Controllers and processors within the Simon-Kucher & Partners group will follow the defined processes for security and confidentiality (chapter 11 of BCR).

13 Restrictions on (onward) Transfers to external Controllers and Processors

Offices of the Simon-Kucher & Partners group subject to the BCRs may only disclose personal data to processors if it is necessary to achieve the specified purpose. Procedures which provide a transfer of personal data to processors or to external providers must be reported to the DPO before any intended transfer is performed.

External processors located inside the EU or in a country recognized by the EU Commission as ensuring an adequate level of protection must be bound by a written agreement stipulating that the processor shall act only on controller's explicit instructions and shall be responsible for the implementation of adequate security and confidentiality measures.

Offices of the Simon-Kucher & Partners Group are obliged to conclude an agreement with external data processors inside the EU or in a country with an adequate level of data protection in written form, including electronic format, which fulfills the requirements of Article 28 GDPR and especially states that the processor may only act on instructions from the controller and is

responsible for appropriate measures to ensure the security and confidentiality of data processing.

All transfers of data to external controllers located outside of the EU must respect the European rules on trans-border data flows. (Articles 44 ff. GDPR; e.g. by reference to the approved European Commission standard contract clauses 2001/497/EC or 2004/915/EC or other appropriate arrangements in accordance with Article 46 GDPR).

All transfers of data to external processors located outside of the EU must follow the rules relating to the processors concerning confidentiality of processing and security of processing (Articles 28 GDPR) in addition to the rules on trans-border data flows (Article 44 GDPR). The requirements of Article 44 ff. GDPR can be especially fulfilled by using the EU-Standard-Contractual Clauses 2010/87/EU.

We have defined processes to ensure this in our "Data Protection Processes Handbook". If a project requires transfer of personal data outside the group and outside the EU and employees are not certain about the data protection implications, they must contact the Data Protection Officer or the Data Protection Team.

14 Data Protection Impact Assessment

All Simon-Kucher & Partners entities subject to the BCR are required to perform a Data Protection Impact Assessment if processing activities provide a prospected high risk for the data subjects. If the result of such a Data Protection Impact Assessment comprises a high risk for the individual and no measures to mitigate those risks are met, Simon-Kucher & Partners' headquarters must contact the lead supervisory authority for prior consultation.

15 Accountability

Each Simon-Kucher & Partners entity subject to the BCRs acting as a controller is responsible to comply with the requirements and principles included in our Binding Corporate Rules and must be able to demonstrate compliance with those principles and rules.

In order to demonstrate compliance with the BCR, all Simon-Kucher & Partners entities subject to the BCRs or the GDPR must create and maintain records of processing activities which they perform either as a controller or a processor. The documentation shall follow the requirements of Article 30 GDPR. The records of processing activities are maintained in the centralized Simon-Kucher & Partners electronic data protection management system. If the data protection supervisory in charge requests the records of processing activities, Simon-Kucher & Partners' headquarters will provide access to records of processing activities for entities outside the EU.

16 Training Program

Simon-Kucher & Partners performs frequent and special trainings to ensure all employees have a profound understanding of the requirements of the Binding Corporate Rules and all relevant data protection principles and necessary processes. The training program is designed to fit the requirements of the employees. Employees will be specifically trained to their needs and roles. The offices of the Simon-Kucher & Partners group are obliged to let employees participate in the trainings. The Data Protection Team and the Data Privacy Officer will monitor the execution of the trainings.

Besides these frequent data protection trainings, special trainings will be conducted if necessary. Simon-Kucher & Partners will train all employees to use new software or hardware in a way that complies with our high data protection standards. Should circumstances for a special training of employees or an individual employee be present, the offices of Simon-Kucher & Partner group are obliged to conduct these trainings and to facilitate the participation of their employees.

17 Audit Program

To ensure compliance with our Binding Corporate Rules, Simon-Kucher & Partners conducts audits on a regular basis, which comprise internal and external audits. The internal audits are conducted once a year by an auditor from the Data Protection Team. External audits by a third party will be conducted on the basis of surprise controls. Although the Office for the surprise control will be picked randomly, it will be ensured that all Offices will be externally audited within three years.

The audit program covers all aspects of the BCRs, including methods of ensuring that corrective actions and measures will be implemented to achieve compliance with the Binding Corporate Rules.

The audit catalog and the content are defined during the yearly audit planning by the DPO in cooperation with the Data Protection Team. The results of the audits – no matter if they were conducted internally or externally – must be communicated to the DPO and to the board of management. The auditor of the DPT will evaluate all aspects of BCR compliance, including the tasks and work of other DPT members and the DPO required by the BCRs. When conducting these BCR audits and writing the reports, the auditors of the DPT are free from instructions issued by the DPO and other Members of the DPT.

The DPO stores audit reports for three years. Simon-Kucher & Partners ensures that the Data Protection Authorities may receive a copy of such audit reports upon request.

The audit plan also grants the Data Protection Authorities the power to carry out a data protection audit if required. Consequently, each member of Simon-Kucher & Partners accepts that they could be audited by Data Protection Authorities and that they will abide by the advice of the Data Protection Authorities on any issue related to our Binding Corporate Rules.

18 Compliance and Supervision of Compliance

Simon-Kucher & Partners have appointed appropriate staff with management support to oversee and ensure compliance with the Binding Corporate Rules. The Data Protection Officer advises the board of management, deals with Data Protection Authorities' investigations and requests, compiles annual reports on compliance and ensures compliance on a global level. Members of the DPT may be employees in any country and office of Simon-Kucher & Partners. Members of the Data Protection Team must not be subject to a conflict of interest.

An actual overview of the members of the Data Protection Teams must be provided at any time to the Data Protection Officer.

The Data Protection Officer is supported by the Members of the DPT which are not auditors of the DPT in keeping BCR compliance.

The DPO of Simon-Kucher & Partners advises the board of management and is the contact for the Data Protection Authorities in case of investigations. The DPO plans audits with the auditors of the DPT and trains employees in accordance with the Data Protection and Binding Corporate Rules. He reports compliance with Data Protection and Binding Corporate Rules to the board of management on a yearly basis. The DPO is also available for any inquiries of employees about data protection.

The Data Protection Team can handle certain local complaints and issues from data subjects (e.g. a data subject's request to access their data) and is responsible to report major privacy issues to the DPO. The members of the Data Protection Team are available to the DPO for questions and will provide the DPO with necessary local information. They are also involved in internal audits and ensure compliance on a local level.

19 Actions in Case of National Legislation Preventing Respect of BCRs

Where a member of the Simon-Kucher & Partners group has reason to believe that the legislation applicable to them prevents the company from fulfilling its obligations under our Binding Corporate Rules and has substantial effect on the guarantees provided by the rules, they will promptly inform the responsible body (EU headquarters) and the DPO of Simon-Kucher & Partners. The only exemption to this rule is where the provision of such information is

prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

Where there is conflict between national law and the commitments in the BCR, the board of management in the headquarters will make a responsible decision on what action to take following a statement by the DPO. The DPO is required to consult the responsible Data Protection Authorities in case of doubt. Before they contact the Data Protection Authority, they must inform the board of management.

This includes any legally binding request for disclosure of personal data by a law enforcement authority or state security body. In such a case, the DPO shall inform the competent supervisory authority about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

If in specific cases the suspension and/or notification are prohibited, the contacted Simon-Kucher & Partners' entity subject to the BCR will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

If in the above cases, despite having used its best efforts, the contacted Simon-Kucher & Partners' entity is not in a position to notify the competent supervisory authorities, it hereby commits to annually providing general information on the requests it received to the competent supervisory authorities (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).

20 Internal Complaint Mechanism

20.1 Step 1: Initializing

The process is triggered in case Simon-Kucher & Partners receives a complaint message from a data subject about the processing of their personal data. The internal complaint mechanism is explained in the privacy policy. Data subjects can trigger the compliant mechanism by filing a complaint using the form on the website. Data subjects in Germany can also directly contact the DPO of Simon-Kucher & Partners at any given time by using the complaint form.

Data subjects may also contact the DPO also directly at

2B Advice GmbH
- DPO for Simon-Kucher & Partners -
Jospeph-Schumpeter-Allee 25
53227 Bonn
- *Germany* –

E-Mail: simon-kucher@2b-advice.com

It is also possible for the data subject to contact project members or other employees to complain about the ways Simon-Kucher & Partners handles their personal data. The employee who has received the data subject's complaint must inform the data subject about the possibilities and contact details to file a complaint.

The references for the internal complaint mechanism also contain legal redress according to chapter 19 of the BCR. These are also be defined on the complaint form.

The complaint may also be filed anonymously, but the data subject cannot expect to receive a response in that case. It is possible that we will not be able to ask the necessary questions for clarification of the issue. Nevertheless, anonymized complaints also trigger the internal complaint mechanism like non-anonymized complaints.

20.2 Step 2: Referring the Data Subject to the DPT/DPO

Employees of Simon-Kucher & Partners must immediately forward a received complaint from a data subject to the Data Protection Team or to the Data Protection Officer. The data subject must be informed about the internal complaint mechanism responsibility of the DPO/DPT.

The process is time critical. The complaint must immediately be forwarded to the DPT. If a data subject directly contacts the legal entity of Simon-Kucher & Partners in Germany, they must forward this complaint form immediately to the DPO. After receiving the complaint form, the DPT/DPO will send an acknowledgement of receipt to the data subject within two weeks. The confirmation may include further questions necessary for the clarification of the issue.

20.3 Step 3: Clarification by the DPT/DPO

In the response to the complaint of the data subject, the DPT/DPO will clarify all relevant details of the relevant circumstances. The members of the DPT and the DPO are obliged to maintain confidentiality about the identity of the data subject. In some countries, this confidentiality obligation is a legal requirement. The DPT/DPO must not reveal the identity of the data subject without the release of the confidentiality obligation.

When the DPT/DPO has collected all required facts, the DPT/DPO will evaluate if the usage of personal data was incompliant with the data principles laid down in the BCRs.

20.4 Step 4: Response to Project Leader / Controlling

When the investigation has been finished, the DPT/DPO must report the result to the responsible Project Leader. The DPT/DPO will keep the identity of the data subject secret but will provide all necessary information to the controller to terminate any possible incompliant usage of personal data.

The DPT/DPO ensures that all required measures have been taken to resolve the request.

The DPT/DPO will also report to the involved project leader if the result of the investigation is that the complaint of the data subject was not justified and using personal data was permissible in the given case.

20.5 Step 5: Information for the Data Subject

The DPT/DPO will inform the data subject after it has been ensured that any potential incompliant usage of personal data has been terminated. The information must contain all necessary details for the data subject about the removal of a breach if applicable.

If the DPT/DPO determines that no breach has occurred, they will also inform the data subject with a short explanation. This explanation must contain the reasons why the data processing procedure is legal.

The notification of the data subject must take place within one (1) month. In difficult or complex cases the deadline can be extended to two additional months. Simon-Kucher & Partners must inform the data subject about the extension and the reasons for the extension. Consequently, conducting the internal complaint procedure may not take longer than 3 months.

The notification of the data subject contains references to the judicial remedies procedure.

20.6 Deadlines

The following deadlines apply for the procedure:

- Forwarding of the complaint form: **immediately**
- Acknowledgement of receipt: **within 2 weeks**
- Conclusion of the complaint process: **within 1 month**
- Conclusion of a complex complaint process: **within 3 months (max.)**

20.7 Complaint form

The complaint form is based on the content of the former European Data Protection Panel complaint form and contains the following information:

- **The data subject:** first name, last name, address, E-Mail address, country of residence
- **Confidentiality:** reference to the agreement of the data subject to the disclosure of their identity if it is necessary for the complaint mechanism
- **SKP Unit:** a detailed description about the data exporter who is responsible for the data breach; notice of the website if applicable
- **Complaint:** specification of data types (checkboxes for sensitive data if applicable), indication of a violation of BCR rules without a direct personal concern (e.g. missing or incomplete privacy statement on the homepage), detailed description of the complaint,

documents or evidences for a breach if applicable, declaration of suffered disadvantages through the asserted breach

- **Steps already taken:** indication of no available results of the internal complaint mechanism, indication of the possibility or duty to notify the data protection authority, indication of whether a judicial proceeding has been initiated
- **Judicial remedies:** Indication of legal redress under section 19.

21 Third Party Beneficiary Rights

21.1 Content of third party beneficiary clause

The data subject has the right of access to stored personal information about them. They also have the right to correction, erasure or blocking of their personal data.

Data subjects have the right to submit a complaint about a breach against the Binding Corporate Rules to a company of the Simon-Kucher & Partners group. The data subject can address the complaint to the Data Protection Officer of Simon-Kucher & Partners.

Data subjects have the right to submit their complaint to the data protection authority of the relevant group member's country of residence (or of the country of Simon-Kucher & Partners' European headquarters) that, in their opinion, has committed a breach against the Binding Corporate Rules.

Data subjects also have the right to make legal claims for a breach against the Binding Corporate Rules of the Simon-Kucher & Partners Group. In a judicial dispute, the onus to prove that they did not break the Binding Corporate Rules lies with the claimed company of the Simon-Kucher & Partners group. The data subject can file a claim either against the company which has exported the personal data out of the EU or the Simon-Kucher & Partners Strategy & Marketing Consultants GmbH. The data subject is entitled to take action against the Simon-Kucher & Partners' group with the appropriate Data Protection Authorities and the courts

a) either in the jurisdiction of the member that is the origin of the transfer, or

b) in the jurisdiction of the European Headquarters

The company against whom action is taken is obliged to pay the adjudicated indemnity to the data subject.

21.2 Easy Access to the third party beneficiary clause

Simon-Kucher & Partners is obliged to grant easy access to the third party beneficiary clause in the global intranet for the employees of the Simon-Kucher & Partners group.

Simon-Kucher & Partners is also obliged to grant easy access to the third party beneficiary clause in the privacy statement of the website for data subjects outside of the Simon-Kucher & Partners Group.

22 Liability

Simon-Kucher & Partners Strategy & Marketing Consultants GmbH accepts responsibility for and agree to take the necessary action to remedy the acts of other members of the Simon-Kucher & Partners group outside of the EU and to pay compensation for any damages resulting from the violation of the BCRs by any members of the group.

The burden of proof lies with the Simon-Kucher & Partners Strategy & Marketing Consultants GmbH to demonstrate that the group member outside the EU is not liable for the violation resulting in the damages claimed by the data subject.

In case of a violation of the Binding Corporate Rules, any person who has been damaged can submit a complaint to the relevant data protection authority. They can also submit judicial proceedings to the court with jurisdiction over the data exporter located in the EU or to the court with jurisdiction over the EU headquarters of the Simon-Kucher & Partners Strategy & Marketing Consultants GmbH which is located in Bonn, Germany.

If the Simon-Kucher & Partners Strategy & Marketing Consultants GmbH can prove that the member outside the EU is not liable for the violation, it may discharge itself from any responsibility.

Simon-Kucher & Partners Strategy & Marketing Consultants GmbH is responsible for ensuring a complete insurance protection so that damage claims of data subjects can be remedied.

23 Mutual Assistance and Cooperation with Data Protection Authorities

All members of the Simon-Kucher & Partners Group must cooperate and assist each other to handle a request or complaint from an individual or an investigation or inquiry by Data Protection Authorities.

They are especially obligated to provide necessary information in an adequate time on request of the Data Protection Authority or of a data subject and to cooperate with the Data Protection Authority.

All members of the Simon-Kucher & Partners Group will abide by the advice of the Data Protection Authorities on any issues regarding the interpretation of the Binding Corporate Rules. They also provide all necessary information in an adequate time.

24 Updates of the Rules

Simon-Kucher & Partners will report any significant changes to the Binding Corporate Rules or to the list of members to all our group members and to the Data Protection Authorities to take into account modifications of the regulatory environment and the company structure.

The DPO keeps a fully updated list of the members of the BCRs, keeps track of and records any updates to the rules and provides the necessary information to the data subjects or Data Protection Authorities upon request. Simon-Kucher & Partners is obliged to report any update to the Binding Corporate Rules and a list of members immediately to the DPO.

The DPO is obliged to provide the necessary information to the Data Protection Authorities and data subjects if requested.

No data transfer may be made to a new member until the new member is effectively bound by the Binding Corporate Rules and can prove compliance with them.

Any changes to the BCRs or to the list of members will be reported once a year to the Data Protection Authorities granting the authorizations with a brief explanation of the reasons justifying the update.

The DPO will report substantial modifications to the Binding Corporate Rules to the data subjects.

25 Relationship between National Laws and BCRs

Where the local legislation, for instance EU legislation, requires a higher level of protection for personal data, it will take precedence over these Binding Corporate Rules.

In any case, the exporter will apply the local legislation for collecting, processing and using personal data:

a) if the processing is carried out in the context of the activities of an establishment of the controller in the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

b) if the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

c) if the controller is not established on EU territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory

of the said Member State, unless such equipment is used only for purposes of transit through the territory of the community.

26 Final Provisions

Binding Corporate Rules become effective for the respective member of the Simon-Kucher & Partners group as soon as the member has signed the BCR subsequent contract.

A member is incorporated in the list of the Binding Corporate Rules members only once it has fulfilled the obligations contained in the Binding Corporate Rules and an audit has revealed that the required technical and organizational measures are in place and employees are trained.