
SIMON-KUCHER & PARTNERS

V.1.0

Binding Corporate Rules

RULES

TABLE OF CONTENTS

TABLE OF CONTENTS	2
1 INTRODUCTION	1
2 SCOPE	2
2.1 NATURE OF THE DATA TRANSFERRED.....	3
2.2 PURPOSES OF THE TRANSFER/PROCESSING.....	5
2.3 EMPLOYEE DATA	6
2.4 DATA IMPORTERS/EXPORTERS.....	6
2.4.1 <i>Data Exporters in the EU</i>	6
2.4.2 <i>Data Importers</i>	7
3 DEFINITIONS	8
4 PURPOSE LIMITATION	10
5 DATA QUALITY AND PROPORTIONNALITY	10
6 LEGAL BASIS FOR PROCESSING PERSONAL DATA	11
7 LEGAL BASIS FOR PROCESSING SENSITIVE DATA	12
8 TRANSPARENCY AND INFORMATION RIGHT	13
9 RIGHTS OF ACCESS, RECTIFICATION, ERASURE AND BLOCKING OF DATA	14
10 AUTOMATED INDIVIDUAL DECISIONS	15
11 SECURITY AND CONFIDENTIALITY	15
12 RELATIONSHIPS WITH PROCESSORS WHICH ARE MEMBERS OF THE GROUP	16
13 RESTRICTIONS ON TRANSFERS AND ONWARD TRANSFERS TO EXTERNAL CONTROLLERS AND PROCESSORS	17
14 TRAINING PROGRAM	18
15 AUDIT PROGRAM	18
16 COMPLIANCE AND SUPERVISION OF COMPLIANCE	19
17 ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING RESPECT OF BCRS	20
18 INTERNAL COMPLAINT MECHANISM	20
18.1 STEP 1: TRIGGER OF PROCESS.....	20
18.2 STEP 2: REFERRING THE DATA SUBJECT TO THE DPT/DPO	21
18.3 STEP 3: CLARIFICATION THROUGH THE DPT/DPO.....	21
18.4 STEP 4: RESPONSE TO PROJECT LEADER / CONTROLLING.....	22
18.5 STEP 5: INFORMATION FOR THE DATA SUBJECT.....	22
18.6 RESPITES	23
18.7 COMPLAINT FORM	23
19 THIRD PARTY BENEFICIARY RIGHTS	24
19.1 CONTENT OF THIRD PARTY BENEFICIARY CLAUSE	24
19.2 EASY ACCESS TO THE THIRD PARTY BENEFICIARY CLAUSE	25
20 LIABILITY	25
21 MUTUAL ASSISTANCE AND COOPERATION WITH DATA PROTECTION AUTHORITIES	26

S I M O N - K U C H E R & P A R T N E R S - B I N D I N G C O R P O R A T E

R U L E S

22	UPDATES OF THE RULES	26
23	RELATIONSHIP BETWEEN NATIONAL LAWS AND BCRS	27
24	FINAL PROVISIONS.....	27

1 INTRODUCTION

Simon-Kucher & Partners operates on four continents all over the world. Simon-Kucher & Partners know about the social, cultural and legal differences between all countries in which our offices can be found. Simon-Kucher & Partners serve customers from different countries and provide 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 the employees.

Simon-Kucher & Partners are committed to ensure an adequate level of privacy protection at all offices of Simon-Kucher & Partners without regard where on the world it might be. Social, cultural and legal differences between the countries must not affect the adequate level of privacy protection. Simon-Kucher & Partners want that customers, participants in research studies and of course the employees of Simon-Kucher & Partners can rely on the promise that Simon-Kucher & Partners treat personal data in all offices in an equally safe and responsible way and that Simon-Kucher & Partners follow the same privacy principles to ensure an adequate level of privacy protection throughout the group. Simon-Kucher & Partners aim to be a safe harbor for the employees' personal data as well as for personal data of customers and 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 bring the fundamental privacy protection principles to life. The Binding Corporate Rules will also ensure that Simon-Kucher & Partners can transfer personal data to the offices outside the EU in a legally compliant way. According to European Legislation a transfer of personal data may only occur if there is an adequate level of privacy protection at the office(s) which shall receive the data. Binding Corporate Rules ensure this adequate level of privacy protection as demanded by the EU Directives 95/46/EC and 2002/58/EC.

Simon-Kucher & Partners can only achieve this goal of providing an adequate level of data protection if all members of the Group and also every single employee accept these rules as binding. Therefore it is the clear duty for all Simon-Kucher & Partners' companies and employees to respect these Binding Corporate Rules at all times.

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-

S I M O N - K U C H E R & P A R T N E R S - B I N D I N G C O R P O R A T E

R U L E S

Kucher & Partners will ensure 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 find that the Binding Corporate Rules are not followed, the management will immediately take and support all necessary steps to restore compliance with the Binding Corporate Rules.

2 SCOPE

This 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 have been defined to be "business confidential". The appendix "Data Protection Processes Handbook" is an essential element of these Binding Corporate Rules. Therein defined processes for realization of privacy are binding for all offices and employees in the same way like the Binding Corporate Rules.

The board of management, Project Leader and persons which are responsible for Human Resources of offices which have signed the BCR-Contract have to ensure that their employees follow the requirements defined in the Binding Corporate Rules. Furthermore the attached "Data Protection Processes Handbook"" must be followed.

R U L E S

2.1 NATURE OF THE DATA TRANSFERRED

Simon-Kucher & Partners are specialized in strategy, marketing, pricing and sales. Simon-Kucher & Partners are regarded as the world's leading pricing advisor. Conducting pricing consultancy 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 about which sort or 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 (pricing consultancy). They advise their clients on the scope of personal data necessary for a research project (less as possible) and determine which information can be derived from such data concerning pricing for products and services.

Data transferred concerns anonymized research data in the first place. Only if it is absolutely necessary for a research project personal data will transferred. The data types which are required 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 this sensitive data is guaranteed (cf. part 5 and part 11 of the BCR).

Simon-Kucher & Partners transfer the following employee data like 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 tongue,
- 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,

R U L E S

- probation period,
- vacation entitlement,
- working time model,
- salary information,
- work performance index,
- working objectives,
- Mentor/Mentee administration,
- fact if 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 employees database, these personal data are not duplicated on the terminal equipment of the accessing entity. This means that personal data stays on the servers in Bonn and is not duplicated on the terminal equipment of the accessing employee. Nevertheless this infrastructure enables project members to access all necessary data of a project no matter at 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.

R U L E S

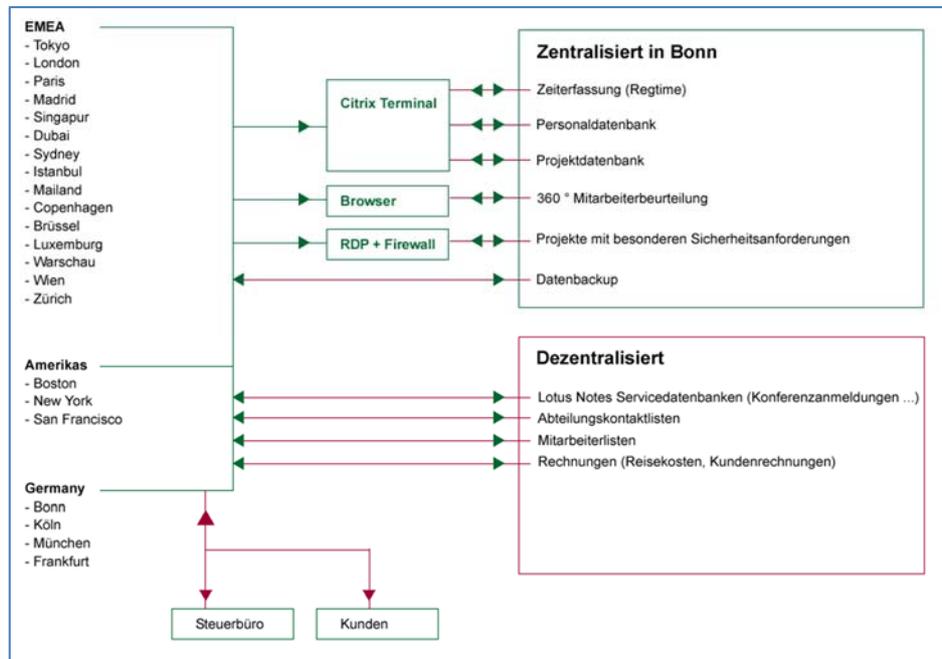


Figure 1: Data flow at Simon-Kucher & Partners

2.2 PURPOSES OF THE TRANSFER/PROCESSING

Simon-Kucher & Partners follow the concept that personal data is not necessary for the majority of research projects. Consequently Simon-Kucher & Partners follow the concept of data avoidance, data minimization and use anonymization whenever possible. Simon-Kucher & Partners 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 do not receive personal data from the customers where it is not strictly necessary and if the customer should provide unnecessary personal data, we have to destroy this personal data as soon as possible, especially before any transfer of the research data. Employees are obliged to follow this process and use anonymization wherever possible.

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

S I M O N - K U C H E R & P A R T N E R S - B I N D I N G C O R P O R A T E

R U L E S

2.3 EMPLOYEE DATA

Simon-Kucher & Partners use personal data stored in the employee database for administration purposes. Partners in all our offices have the possibility 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 exists who is occupied with administrative tasks concerning the employment contract such as payroll accounting and personnel bookkeeping. Those office managers are responsible to create and maintain the employment contracts and therefore have full access to personal data of the employees. The office manager has only full access concerning employees of his country. For administrative purposes the office manager has read access to the basic data of all employees worldwide including name, division, office and level for administrative purposes such as project coordination.

Personal data recorded by the time recording system "Regtime" are stored on the same server as the employee database. Personal data recorded by Regtime can be accessed by office managers only for their country. Office managers need the data to perform a check of completeness. The personal data recorded by Regtime is used for the purpose of invoicing and compiling working hours for certain projects.

2.4 DATA IMPORTERS/EXPORTERS

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

.

2.4.1 DATA EXPORTERS IN THE EU

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

R U L E S

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

- Bonn, Germany
- Cologne, Germany
- Munich, Germany
- Frankfurt, Germany
- London, United Kingdom
- Paris, France
- Madrid, Spain
- Milano, Italy
- Copenhagen, Denmark
- Brussels, Belgium
- Luxembourg, Luxembourg
- Vienna, Austria

2.4.2 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
- Istanbul, Turkey

R U L E S

- Warsaw, Poland
- Boston, United States of America
- New York, United States of America
- San Francisco, United States of America
- Beijing, China

3 D E F I N I T I O N S

Simon-Kucher & Partners are committed to ensure that all relevant data protection definitions are compliant to the regulations of the Directive 95/46/EC of the European Parliament

Personal Data

any information relating to an identified or identifiable natural person (individual); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

Sensitive Personal Data

are also referenced as special categories of data. Sensitive personal data reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, personal data concerning health or sex life.

Data Subject / Individual

the data subject is the identified or identifiable natural person to whom the personal data refer.

Controller

shall mean any person or body which collects processes or uses personal data on his, her or its

R U L E S

own behalf or which commissions others to do the same.

Processor

shall mean any person or body which collects processes or uses personal data on behalf of a controller.

Third Party

shall mean 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 the data as long as the processor is located in one of the Member States of the European Union or another state party to the Agreement on the European Economic Area.

Processing of personal data

shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

Data Subject's consent / Opt-in

shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed for particular purposes.

Data Protection Authority

is the public authority in a Member State of the EU that is responsible for monitoring the application within its territory.

R U L E S

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 fulfill this purpose he can contact the DPT to acquire necessary information or coordinate data protection tasks.

4 PURPOSE LIMITATION

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. If personal data shall be processed for different purposes than the original purposes, the employees are committed to follow the process "Choice" in chapter 6 of "Data Protection Processes Handbook".

All employees know and must respect that sensitive data is provided with additional safeguards as described in our "Data Protection Processes Handbook" to comply with the special requirements to the process "Opt-In" (chapter 6.5.3).

5 DATA QUALITY AND PROPORTIONNALITY

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

S I M O N - K U C H E R & P A R T N E R S - B I N D I N G C O R P O R A T E

R U L E S

When Simon-Kucher & Partners are notified by the data subject or in another way, that any personal data stored at Simon-Kucher & Partners, , are inaccurate, incomplete or not current we will correct, complete or update the respective data. If an update is not possible the data must be deleted. Where needed, the employee will involve the Data Protection Team and the Data Protection Officer as well.

Project-Leader and employees will be ensuring that personal data is adequate by classifying research data at the very beginning of a project. Simon-Kucher & Partners support 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.

Offices and employees will ensure that personal data is only processed as long as it is necessary for the purpose for which they have been obtained.

6 LEGAL BASIS FOR PROCESSING PERSONAL DATA

Personal data must only be processed and transferred if any of the following requirements is fulfilled:

- The data subject has unambiguously given his consent (opt-in), or
- The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or
- The processing is necessary for compliance with a legal obligation to which the controller is subject, or
- The processing is necessary in order to protect the vital interests of the data subject, 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 whom the data are disclosed, or

R U L E S

- The processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

If any employee should be in doubt which of the alternatives or if one of the alternatives is applicable, he has to immediately contact the DPO.

7 LEGAL BASIS FOR PROCESSING SENSITIVE DATA

Processing of sensitive data is prohibited except if:

- the data subject has given his explicit consent to the processing of those sensitive data, except where the 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 field of employment law in so far as it is authorized by national law providing for adequate safeguards, 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 his consent, or
- The processing relates to sensitive data which are manifestly made public by the data subject, or
- The processing of sensitive data is necessary for the establishment, exercise or defense of legal claims, or
- The processing of the sensitive data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those sensitive data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

R U L E S

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

8 TRANSPARENCY AND INFORMATION RIGHT

Simon-Kucher & Partners will make the Binding Corporate Rules readily available to every data subject to maintain transparency about the way Simon-Kucher & Partners treat personal data and inform him or her about his or her rights.

The data subject can view the parts of the Binding Corporate Rules which are published in the Internet privacy policy of the Simon-Kucher & Partner offices at every time. At data subject's requests employees will direct the data subject to the appropriate privacy policy on the homepage. If the data subject has got no Internet access Simon-Kucher & Partners will make the Binding Corporate Rules available to the data subject in text form.

Before processing or transferring personal data the data subject must be informed according to our "notice" process which is part of our "Data Protection Processes Handbook" (chapter 5). The employees are committed, to check the process and must decide how to inform and notify the data subject.

Simon-Kucher & Partners must inform data subjects

- a) when Simon-Kucher & Partners first ask him or her to provide personal information or
- b) as soon thereafter as is practicable
- c) in any event before Simon-Kucher & Partners use such personal data for a purpose other than for which it was originally collected or processed
- d) At the time Simon-Kucher & Partners stores personal data that has not been collected from the individual directly.

Simon-Kucher & Partners will provide the following information:

- information concerning the controller's identity

R U L E S

- types of personal data which will be collected, processed or used
- the purposes for which Simon-Kucher & Partners collect and use his or her personal data
- that he or she can contact the Data Protection Team or the Data Protection Officer directly (contact details must be provided)
- the types of parties to which Simon-Kucher & Partners disclose his or her personal data
- information about our objection process which enables the data subject to limit or completely terminate the use of his or her personal data.

The only exception to inform the data subject is if the data have not been obtained from the data subject and if the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. If any employee should consider choosing one of the exceptions mentioned before he has to immediately contact the DPO.

9 RIGHTS OF ACCESS, RECTIFICATION, ERASURE AND BLOCKING OF DATA

Simon-Kucher & Partners grant data subjects access to personal data about them. This includes the right to obtain without constraint at a reasonable interval and any time in case of well-grounded reasons, and without excessive delay or expense a copy of all data relating to them.

Employees have to follow the process "Rights to information" (Auskunftsrecht) in chapter 10 of the "Data Protection Processes Handbook"

Data subjects have the right to demand from Simon-Kucher & Partners to correct, amend or delete the personal data where they are inaccurate. 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

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

R U L E S

by law. The DPO will evaluate if the objection is justified. The data subject can directly contact the DPO at: simon-kucher@2b-advice.com. Where the objection is justified, the processing must cease.

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.

10 AUTOMATED INDIVIDUAL DECISIONS

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

- the decision is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract and the request of the data subject has been fulfilled
- there are suitable measures to safeguard the data subject's legitimate interests and the controller informs the data subject that a decision within the meaning of subsection 1 has been taken. In particular, arrangements allowing data subjects to assert their point of view shall constitute suitable measures. The controller shall be obligated to review its decision. The decision is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

11 SECURITY AND CONFIDENTIALITY

Simon-Kucher & Partners take reasonable precautions to protect personal data from loss, misuse and unauthorized access, disclosure, alteration, and destruction. Simon-Kucher & Partners have implemented technical and organizational measures which comprise physical access control, system access control, logical access control, disclosure control, input control, job control, availability control and separation control which are described in detail in chapter 8.4.3.1 of the "Data Protection Processes Handbook".

R U L E S

Having regard to the state of the art and the cost of their implementation, such measures ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Sensitive data is subject to high protection level and is processed by the Simon-Kucher & Partners Group with enhanced security measures.

These technical and organizational measures are subject to frequently conducted audits by the Simon-Kucher & Partners Group. The realizations of these audits are yearly planned by the Data Protection Team. The audit or a part of the audit can 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 necessary information for the audit.

12 RELATIONSHIPS WITH PROCESSORS WHICH ARE MEMBERS OF THE GROUP

The Simon-Kucher & Partners GmbH provides IT services for the other offices of the Simon-Kucher & Partners Group. Most of the central computer capacities for access of the other offices are located in Bonn, Germany by the Simon-Kucher & Partners GmbH. The central SAP infrastructure is also hosted by the IT in Bonn, Germany.

Between the contracting authority in the company group and Simon-Kucher & Partners GmbH the relevant rules of data processing according to the legal requirements will be complied. The parties agree on binding rules in accordance with article 17, no. 3 of Directive 95/46/EC between controller and processor and specify the scope of the directive right of the controller.. 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 controllers. The responsible body for the processing on the system is the controller.

The technical and organizational measures for adherence of data protection inside the group are based on the central data storage through 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 TRANSFERS AND ONWARD TRANSFERS TO EXTERNAL CONTROLLERS AND PROCESSORS

Offices of the Simon-Kucher & Partners group may only disclose personal data to processors if it is necessary to achieve the specific purpose. Procedures which provide a transfer of personal data to processors or to external providers must be reported to the DPO before transfer will be 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 instructions from the controller and shall be responsible for the implementation of the adequate security and confidentiality measures.

Offices of the Simon-Kucher & Partners Group are obliged to conclude an agreement in written form with external data processors inside the EU or in a country with an adequate level of data protection that they can only act by instructions from the controller and are responsible of appropriate measures to ensure of the security and confidentiality of data processing.

All transfers of data to external controllers located out of the EU must respect the European rules on transborder data flows. (Articles 25-26 of Directive 95/46/EC; 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 the articles 25 and 26 by the EU directive).

All transfers of data to external processors located out of the EU must follow the rules relating to the processors concerning confidentiality of processing and security of processing (Articles 16-17 Directive 95/45/EC) in addition to the rules on transborder data flows (Articles 25-26 of Directive 95/46/EC). The requirements of Article 25 and 26 Directive 95/46/EC 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 required transfer of personal data outside the group and outside the EU and employees are not certain about the data protection implication they must contact the Data Protection Officer.

14 TRAINING PROGRAM

Simon-Kucher & Partners will perform frequent and special trainings to ensure it, that all the employees have a sound 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. The offices of the Simon-Kucher & Partners group are obliged to letting the 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 enable 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 enable their employees for participation.

15 AUDIT PROGRAM

To ensure compliance with our Binding Corporate Rules Simon-Kucher & Partners will conduct audits on a regular basis and comprise internal and external audits. The internal audits will be conducted once a year by an DPT-Auditor. 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 DPT-Auditors. 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 DPT-Auditors will evaluate all aspects of BCR compliance, including the tasks and work of the other DPT-Members and the DPO required by the BCRs. When conducting these BCR audits and

R U L E S

writing the reports the DPT-Auditors are free of instructions from the DPO and other Members of the DPT.

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

The audit plan also allows the Data Protection Authorities to have 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 the 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.

16 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 are employees in each country and office of Simon-Kucher & Partners. Members of the Data Protection Team must not be subject for 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 DPT-Auditors 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 with the DPT-Auditors audits, trains the employees in accordance to Data Protection and Binding Corporate Rules. He reports the compliance of Data Protection and Binding Corporate Rules yearly to the board of management. The DPO is also available for requests of employees about data protection

The Data Protection Team can handle certain local complains and issues from data subjects (e.g. data subject's request to access his data) and are responsible to report major privacy issues to the DPO. The members of the Data Protection Team are available for the DPO for questions and will

R U L E S

provide the DPO with necessary local information. They are also involved in internal audits and ensure compliance on a local level.

17 ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING RESPECT OF BCRS

Where a member of the Simon-Kucher & Partners group has reasons to believe that the legislation applicable to him prevents the company from fulfilling its obligations under our Binding Corporate Rules and has substantial effect on the guarantees provided by the rules, he will promptly inform the responsible body (EU headquarters) and the DPO of Simon-Kucher & Partners. The only exemption to this rule is where 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 take a responsible decision on what action to take after a statement by the DPO. The DPO is committed to consult the competent Data Protection Authorities in case of doubt. Before he gets in contact with Data Protection Authority he must inform the board of management.

18 INTERNAL COMPLAINT MECHANISM

18.1 STEP 1: TRIGGER OF PROCESS

The process will be triggered if Simon-Kucher & Partners receives a complaint message from a data subject how they process with his personal data. The internal complaint mechanism will be explained in the privacy policy. Data subjects can trigger the compliant mechanism when they file a complaint by 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 can contact the DPO also directly at

Simon-Kucher & Partners Strategy & Marketing Consultants GmbH
– Datenschutzbeauftragter / Data Protection Officer –
Joseph-Schumpeter-Allee 25

R U L E S

53227 Bonn

- Germany –

E-Mail: dpt@simon-kucher.com

It is also possible that the data subject can contact project members or other employees to complain about the ways Simon-Kucher & Partners handle his or her personal data. The employee who has been confronted with the data subject's complaint has to 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 will also define on the complaint form.

The complaint can also take place in an anonymized form. But the data subject cannot expect to receive a response. It is possible that necessary questions for clarification of the issue cannot be asked to the data subject. But nevertheless, anonymized complaints also trigger the internal complaint mechanism like non-anonymized complaints.

18.2 STEP 2: REFERRING THE DATA SUBJECT TO THE DPT/DPO

The employees of Simon-Kucher & Partners must immediately forward the 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 form must immediately be forwarded to the DPT. This will be technically ensured. If any data subject will directly contact the legal entities of Simon-Kucher & Partners in Germany, they must forward this complaint form immediately to the DPO. This will be also technically ensured. After receiving the complaint form the DPT/DPO will send an acknowledgement of receipt within two weeks to the data subject. The confirmation may include further questions necessary for the clarification of the issue.

18.3 STEP 3: CLARIFICATION THROUGH THE DPT/DPO

For reacting to the complaint of the data subject the DPT/DPO will clarify all circumstances. The members of the DPT and the DPO are obliged to maintain confidentiality about the identity of the data subject. In some countries these confidentiality obligation is a legal requirement. The

R U L E S

DPT/DPO mustn't reveal the identity of the data subject without the release of the confidentiality obligation.

When the DPT/DPO has collected all facts, the DPT/DPO will evaluate if the usage of personal data was non-compliant to the data principles laid down in the BCRs.

18.4 STEP 4: RESPONSE TO PROJECT LEADER / CONTROLLING

When the investigation has been finished, the DPT/DPO must report the result to the concerned 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 non-compliant usage of personal data.

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

The DPT/DPO will also report it 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 case.

18.5 STEP 5: INFORMATION FOR THE DATA SUBJECT

The DPT/DPO will inform the data subject after it has been ensured that the non-compliant usage of personal data has been terminated. The information must contain all necessary details for the data subject about the removal of an eventually breach.

If the DPT/DPO ensures that a breach has not been existing it/he will also inform the data subject with a short explanation. This explanation must contain the reasons why the data processing procedure is legal.

The information to the data subject must take place within 6 months. The data subject must be informed about the estimated time for the complaint-process if the complaint mechanism is likely to take a longer time period. Conducting the internal complaint mechanism must not take longer than 12 months.

The information to the data subject contains references to the judicial remedies procedure in section 19.

R U L E S

18.6 RESPITES

The following respites apply for the procedure:

Forwarding of the compliant form	immediately
Acknowledgement of receipt	within 2 weeks
Finishing of the complaint mechanism	within 6 months
Finishing of a complex complaint mechanism	within 12 months (max.)

18.7 COMPLAINT FORM

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

The data subject	first name, last name, address, E-Mail address, country
Confidentially	allusion about the agreement of the data subject for the announcement of his 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; eventually notice of the website
Complaint	allusion to data types (checkboxes for sensitive data in place), allusion about a violation of BCR-rules without directly concernment (e.g. missing or incomplete privacy statement on the homepage), detailed description of the complaint, possibly documents or evidences for the

R U L E S

	breach, declaration of suffered disadvantages through the asserted breach
Steps, already taken	allusion about no available results of the internal complaint mechanism, allusion about the informing to the data protection authority, allusion to a judicial proceeding have been initiated
judicial remedies	allusion about the legal redress under section 19.

19 THIRD PARTY BENEFICIARY RIGHTS

19.1 CONTENT OF THIRD PARTY BENEFICIARY CLAUSE

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

Data subjects have got 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 got the right to submit a complaint about a breach of located Simon-Kucher & Partners offices against the Binding Corporate Rules to the data protection authority of the concerned country or the data protection authority in the country of Simon-Kucher & Partners' European Headquarters.

Data subjects have also the right to make legal claims for breach of the Binding Corporate Rules against the Simon-Kucher & Partners Group. In a judicial altercation the onus lies with the claimed company of the Simon-Kucher & Partners group that they did not break the Binding Corporate Rules. The data subject can claim 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 before the appropriate Data Protection Authorities and before the courts

R U L E S

- a) either in the jurisdiction of the member that is at the origin of the transfer, or
- b) in the jurisdiction of the European Headquarters

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

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

20 LIABILITY

The 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 the members of the group.

The burden of proof stays with the Simon-Kucher & Partners Strategy & Marketing Consultants GmbH to demonstrate that the 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 data protection authority. He or she can also submit judicial proceedings to the committed court of the data exporter located in the EU or to the committed court of the EU headquarter from 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.

R U L E S

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

21 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 the request of the Data Protection Authority or of a data subject with necessary information in an adequate time 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 the necessary information in an adequate time.

22 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 and keeps track of and record any updates to the rules and provides the necessary information to the data subjects or Data Protection Authorities upon request. Simon-Kucher & Partners are 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 transfer must be made to a new member until the new member is effectively bound by the Binding Corporate Rules and can prove compliance.

R U L E S

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.

23 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 on 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 Community 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.

24 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.

S I M O N - K U C H E R & P A R T N E R S - B I N D I N G C O R P O R A T E

R U L E S

A member is incorporated in the list of the Binding Corporate Rules members not until then it fulfills 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.