

Appendix [Data Processing Procedures]

I. Additional Data Protection Requirements - Technical and Organisational Measures (AR/DM)

The technical and organisational measures described herein are agreed to be binding between _____ (Principal) and Hubject GmbH (Processor). They apply to the contractual relationship User Agreement.

The commissioned data processing is carried out on and with Principal-provided systems and hardware only:

yes* no

*May only be checked if no data are exported from the Principal's systems.

*If "yes", only questions with underlined question numbers need to be answered.

1. Physical access control

- 1.1 The buildings are secured with an alarm system:
 yes no
- 1.2 The building's entrance doors are equipped with the following locking system:
 manual locking system (Hubject GmbH) chip card access system (data centre)
- 1.3 Access authorisations for the aforementioned locking system are documented by name:
 yes no
- 1.4 Access to the building by third parties/guests/visitors is documented by name:
 yes (data centre) no no, access and presence is only possible when accompanied by company staff
- 1.5 Access to the building by cleaning and maintenance personnel is documented by name:
 yes no
- 1.6 The withdrawal of building access authorisations and access rights for computer systems from employees upon termination of their employment is regulated and documented:
 yes no
- 1.7 Access to server rooms is regulated by a special access concept and is documented by name (incl. cleaning personnel, security staff etc.):
 yes, in the data centre no no but all cleaning of server rooms is monitored

2. System access control

- 2.1 The company network is protected from the public Internet by an external firewall:
 yes, in the data centre no
 if yes:
 type: 2-tier, ASA5520 and ASA5550 plus Tipping Point 110 IPS
 updating procedure and frequency: 2x per week, automatically
- 2.2 For all IP addresses open to the Internet penetration tests are carried out on a regular basis:
 yes, in the data centre no
- 2.3 The Principal's data are separated within the company network by means of network technology:
 yes no
 if yes, by what measures: dedicated virtual unit (VM server) and VLAN
- 2.4 All employees are subject to the following password specifications:
 individual computer password for each employee which must be kept secret
 no collective passwords
 minimum length, if applicable: No. of characters/complexity: 8 characters (incl. special characters/capital letters)
 password time limit; if applicable, please indicate the respective interval for changes: 90 days
 automatic screen locking timeout: after 15 minutes
- 2.5 Virus scanning is performed on the following transition points interfacing the company network:
 email account
 FTP
 Web
- 2.6 Virus scanning is performed on all servers:
 yes no, Unix server only w/o direct data exchange with Windows
 if yes, updating procedure and frequency: data are checked before being imported, Linux server
- 2.7 Virus scanning is performed on all individual workstation computers:
 yes no
 if yes, updating procedure and frequency: hourly check for up-to-date signatures, automatic deployment,
- 2.8 Security-relevant software updates are loaded to the existing software regularly and automatically:
 yes no
- 2.9 Employees have local administrator rights:
 yes no
- 2.10 Employees are authorised to access the Internet:
 yes no
 if yes: browser's configuration is restrictive and cannot be changed by employees:
 yes no

3. Data access control

- 3.1 Authorisation concepts are in place and documented:
 yes no
- 3.2 The organisation of the granting of authorisations is documented by name (in particular who may grant what rights):
 yes no
- 3.3 The authorisations granted are updated and documented by name:
 yes no
- 3.4 Number of administrators authorised to copy/extract all or a large part of the Principal's data: 2, signed confidentiality undertakings pursuant to the German Federal Data Protection Act have been submitted
- 3.5 Number of employees (excluding administrators!) authorised to copy/extract all or a large part of the Principal's data: none
- 3.6 The following components of the workstation computers have been locked/deactivated to ensure that no data exported from the data centre may be saved externally:
 USB ports
 CD/DVD burners
 memory card slots
 other mobile data carriers, if yes, what type: _____
- 3.7 Remote maintenance/remote access paths are available for:
 external service providers
 employees
If remote maintenance/remote access paths are available, please complete the following information:
Method of authentication: user name and password
Protocols used (e.g.: SSH): SSL certificate-based and IP whitelisting

4. Disclosure control

- 4.1 Method of encryption used for data exchange between Principal and Processor:
 SFTP
 S/Mime: exchange of documents takes place through BSI via the sharepoint which enables controlling of access to these documents through credentials
 others, please explain procedure: SSL certificate-based and IP whitelisting
- 4.2 All data sent by data carrier are encrypted:
 yes no
if yes, please explain the procedure: no data sent by data carrier
- 4.3 Please explain the feedback procedure used to notify the Principal of the receipt of a data carrier or the assumed loss of a data carrier:
no data sent by data carrier
- 4.4 Please explain how the data carrier received by the Principal is disposed of and how this is documented:
no data sent by data carrier
- 4.5 In addition, the Principal's data are stored in encrypted form:
 yes no
if yes, please explain the procedure: FIPS 140-2 Level 1FSS
- 4.6 Backups are carried out:
 yes, encrypted yes, unencrypted no
- 4.7 Secured storage of backup media:
 yes no
- 4.8 Upon expiry of the commission, how and when are the Principal's data deleted (electronic data carriers/paper documents):
Upon expiry of the contract all client data stored are made available to the client in a machine-readable format if so requested by the client, and, upon a readability confirmation or upon expiry of a reasonable time limit, all administrator and user accounts and all applications and data will be deleted by Colt
- 4.9 Measures for the protection of the Principal's data (incl. temporary data) on mobile workstation computers:
not applicable
- 4.10 Measures for the protection of the Principal's data (incl. temporary data) on mobile data carriers:
not applicable

5. Input control

- 5.1 In order to ensure the transparency of all actions deleting/changing the Principal's data, log files are created for each employee by name:
 yes no
- 5.2 Access to the above-mentioned log files is governed by a restrictive access concept:
 yes no

6. Compliance control

- 6.1 All employees must undertake in writing to maintain the confidentiality of all personal data pursuant to Section 5 of the German Federal Data Protection Act [see Article 16 Directive 95/46/EC]
 yes no
- 6.2 All employees must undertake in writing to maintain the confidentiality of all telecommunications data pursuant to Section 88 of the German Telecommunications Act [Article 5 Directive 2002/58/EC]
 yes no
- 6.3 The Processor obtains the following additional written declarations (in connection with data protection and data security) from its employees:

- 6.4 Subcontractors who have access to the Principal's data are/have been commissioned:
 yes no
- 6.5 All subcontractors processing the Principal's data are bound by agreements governing the commissioned data processing in accordance with Section 11 of the German Federal Data Protection Act [Article 17 Para. 3 Directive 95/46/EC and, if applicable, governing security pursuant to Article 4 Directive 2002/58/EC in conjunction with Directive 2009/136/EC]:
 yes no
- 6.6 There are subcontractors outside the EU who have access to the Principal's data:
 yes no
- 6.7 All subcontractors who are granted access to the Principal's data comply with the technical and organisational measures agreed in this checklist just as the Processor himself and have contractually warranted their compliance:
 yes no
- 6.8 All employees must attend training sessions relating to data protection, which are documented by name:
 yes no
- 6.9 Currently, the following certificates/data protection concepts are in place for the Processor's business, which may upon request be reviewed at the office of the Principal:
Hubject: data protection concept of 2/3 May 2013

7. Availability control

- 7.1 Frequency and number of generations of the data protection measures: Full backup weekly, incremental backups daily
- 7.2 Storage location of backup data carriers:
 safe external storage at an (air-line) distance of \geq 3km
- 7.3 Restart time (in days) after complete destruction of the data centre: ---
- 7.4 IT system maintenance agreements have been entered into with third parties:
 yes no

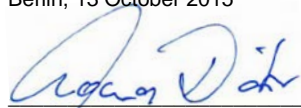
8. Separation control

- 8.1 The Principal's data are held available in an independent, dedicated client used for the commission:
 yes no
- 8.2 Access to the aforementioned client is governed by an authorisation concept which excludes access to the data by employees who do not work for the Principal:
 yes no
- 8.3 Employees processing the Principal's data are seated in other rooms than employees working for other principals:
 yes no
- 8.4 Employees must undertake in writing not to use information from the Principal's data in other projects / for other purposes:
 yes no

9. Signature

We warrant that the information provided herein reflect the current state and level of the technical and organisational measures taken by us to safeguard data protection and data security. Any deviation from the information provided herein must be notified directly to the Principal being a party to the User Agreement pursuant to sentence 1 of this Part I Additional Data Protection Requirements - Technical and Organisational Measures (AR/DM) .

Berlin, 13 October 2015


(Thomas Daiber)


(Christian Hahn)

II. Additional Data Protection Requirements - Commissioned Data Processing (AR/D)

All collection, processing and/or use of personal data is carried out as a commissioned data processing as defined by Section 11 of the German Federal Data Protection Act (*Bundesdatenschutzgesetz, BDSG*). If the commissioned data processing is carried out at a location outside of the Federal Republic of Germany but within a member state of the European Union or within any other state that is a signatory of the Agreement on the European Economic Area the corresponding EU legislation applies [Article 17 Para. 3 Directive 95/46/EC], which is indicated in brackets in each case below. Any transfer to a third country requires the prior consent of the Principal, and may only be carried out if and when the special requirements of Sections 4b, 4c of the German Federal Data Protection Act [Articles 25 and 26 Directive 95/46/EC] are met.

1. Object, scope and duration of the commission

- 1.1. Object and scope of the commission
The commission's object is governed by the User Agreement to which these Additional Requirements is enclosed as Appendix and to which reference is made herein (hereinafter referred to as the Agreement).
- 1.2. Duration of the commission
The duration of this commission (term) corresponds to the term of the Agreement.
It may be terminated prematurely and with immediate effect in case of a violation of statutory or contractual data protection provisions. The same applies if the Processor does not want to or cannot execute an instruction legitimately issued by the Principal.

2. Substantiation of the commission's content

- 2.1. Scope, type and purpose of the planned collection, processing or use of data
The scope, type and purpose of the collection, processing and/or use of personal data by the Processor on behalf of the Principal are concretely described in section 8 in conjunction with section 15 (Contractual Terms User Agreement EMP) and in section 10 in conjunction with section 17 (Contractual Terms User Agreement CPO) of the Agreement.

2.2. Types of data

The following types/categories of personal data are collected, processed and/or used:

- name, title, academic degree
- occupation, industry or business designation
- address
- date/year/day of birth
- communication data (e.g. telephone, email)
- telecommunications data (transaction, location and usage details within the meaning of the German Telecommunications Act (*Telekommunikationsgesetz, TKG*), [Article 3 Directive 2002/58/EC])
- contract master data (contractual relation, product and/or contract interest)
- customer history
- contract settlement and payment data
- sensitive data (information on racial and ethnic background, political opinions, religious or philosophical beliefs, membership in trade unions, health or sexual life)
- personal data subject to a professional confidentiality requirement
- data related to criminal acts or regulatory offences or suspected criminal acts or regulatory offences
- bank and credit card account details
- planning and control data
- inquiry information (obtained by third parties, e.g. credit agencies or public registries)
- contract ID, charge detail records (see Appendix Interface Description)

2.3. Data subjects

The data subjects whose data are used within the scope of this commission are:

- employees
- relatives of employees
- pensioners/survivors
- applicants
- customers of Hsubject's contract partners (EM Users)
- employees of external companies
- interested parties
- lessees/lessors
- suppliers
- contact persons

3. Technical and organisational measures pursuant to Section 9 of the German Federal Data Protection Act [Article 17 Para. 1 Directive 95/46/EC]

The Processor shall document the implementation of the technical and organisational measures pursuant to Section 9 of the German Federal Data Protection Act [Article 17 Para. 1 Directive 95/46/EC and, if applicable, of security measures pursuant to Article 4 Directive 2002/58/EC in conjunction with Directive 2009/136/EC] before commissioning and prior to the start of processing, and shall submit said document to the Principal for review. If the Principal accepts the documented measures they are to be the basis of the commission. If, upon review by the Principal, adjustments are required they must be carried out by mutual agreement. The Processor must comply with the basic principles of proper data processing.

The Processor undertakes to comply with the following technical and organisational measures pursuant to Section 9 of the German Federal Data Protection Act and its appendix [Article 17 Para. 1 Directive 95/46/EC and, if applicable, the security measures in accordance with Article 4 Directive 2002/58/EC in conjunction with Directive 2009/136/EC]:

- The Additional Data Protection Requirements - Technical and Organisational Measures (AR/DM), which are attached as an annexe, are agreed to be binding on the Processor.
- In exceptional cases and if agreed on by the Principal, instead of using the AR/DM, the Processor may prepare a commission-specific documentation of the technical and organisational measures taken.

The technical and organisational measures are subject to technical progress and further development. To this extent, the Processor may implement alternative appropriate measures. In so doing, the Processor must maintain a security level in line with the measures agreed. Essential changes must be agreed upon in writing. If required to do so by the Principal the Processor shall

provide the Principal with the information pursuant to Section 4g Subsection 2 Sentence 1 of the German Federal Data Protection Act [Article 18 Directive 95/46/EC].

4. Correction, blocking and deletion of data

Except as provided in Section 11 herein, the Processor must not correct, delete or block any of the data that are processed under this commission unless instructed to do so by the Principal. If a data subject directly contacts the Processor in order to have their data corrected or deleted, the Processor shall pass on such request to the Principal without undue delay. If the Processor's participation is required to ensure a preservation of the data subject's rights on the part of the Principal, the Processor shall take the appropriate measures according to the Principal's instructions.

5. Controls and other obligations of the Processor

In addition to its duty to comply with the provisions set out herein the Processor has the following obligations pursuant to Section 11 Subsection 4 of the German Federal Data Protection Act [Article 17 Para. 3 Directive 95/46/EC]:

- Maintaining the confidentiality of all personal data pursuant to Section 5 of the German Federal Data Protection Act [Article 16 Directive 95/46/EC] and/or maintaining the confidentiality of all telecommunications data pursuant to Section 88 of the German Telecommunications Act [Article 5 Directive 2002/58/EC in conjunction with Directive 2009/136/EC]. The Processor shall ensure that any person who can access personal data of the Principal in accordance with this commission undertakes to maintain the confidentiality of such data and that they are informed of the special data protection obligations arising from this commission and that the data processing must be carried out according to the instructions received and only for the intended purposes. The resultant confidentiality requirement applies beyond the end of the contract for an indefinite period of time regardless of any other confidentiality requirements that may have been agreed. The same applies to any telecommunications data that must be kept confidential.
- Implementation of and compliance with the technical and organisational measures pursuant to Section 9 of the German Federal Data Protection Act and its appendix [Article 17 Para. 1 Directive 95/46/EC and, if applicable, security measures in accordance with Article 4 Directive 2002/58/EC in conjunction with Directive 2009/136/EC] required for this commission.
- Notification of the Principal without undue delay regarding any inspections and other measures taken by the supervisory authority pursuant to Section 38 of the German Federal Data Protection Act [Article 28 Directive 95/46/EC]. This also applies if any other competent authority carries out an investigation involving the Processor pursuant to Sections 43, 44 of the German Federal Data Protection Act [Articles 22 ff Directive 95/46/EC].
- Controlling compliance by means of regular examinations of the execution and/or performance of the contract, in particular regarding the adherence to the provisions and measures agreed for performance of the commission and any adjustments that may be required thereto.
- Providing proof of the technical and organisational measures to the Principal.

6. Subcontractors

To the extent that subcontractors are to be involved in the processing or use of personal data of the Principal, such arrangements will be authorised if the following conditions are fulfilled:

- As a general rule, the involvement of subcontractors is not allowed unless the Principal has given its prior written consent. Currently, the Processor commissioned the subcontractors listed below with the processing of personal data. The Principal agrees to their commissioning:

Operation of the platform including IT services

- Bosch Software Innovations GmbH; Stuttgarter Str. 130; 71332 Waiblingen (Germany)
 - Colt Technology Services GmbH, Herriotstraße 4, 60528 Frankfurt (Germany)
 - Destruction of data
 - External storage of data carriers
- The Processor shall ensure that the contents of the contractual arrangements entered into with the subcontractor(s) correspond to the data protection provisions agreed between the Principal and the Processor.
 - When commissioning subcontractors the Processor must ensure that the subcontractor grants to the Principal inspection and audit rights in accordance with the provisions set out herein and Section 11 of the German Federal Data Protection Act in conjunction with No. 6 of the appendix to the Act for Section 9 of the Act [Article 17 Para. 3 Directive 95/46/EC in conjunction with Para. 1 thereof, and, if applicable regarding security measures pursuant to Article 4 Directive 2002/58/EC in conjunction with Directive 2009/136/EC]. This also includes the Principal's right to obtain, upon a written request to this effect, information on the contract's contents as to data protection provisions and on the implementation of data protection obligations in the subcontractual relationship, if necessary by means of inspecting the relevant contract documents.

7. Competent persons

For the Processor:

The Processor will provide to the Principal the name of the data protection officer responsible, or – if no such data protection officer needs be appointed – a contact person for data protection matters.

The Processor's appointed data protection officer is:

Mr Stefan Drost, [mailto: datenschutz@hsubject.com](mailto:datenschutz@hsubject.com)

The Principal must be notified without undue delay of any changes in the person of the data protection officer.

For the Principal:

If the Processor processes sensitive data on behalf of the Principal the Principal appoints the following persons who are authorised to issue instructions to the Processor:

Surname, name, telephone

8. Principal's inspection rights

The Principal is entitled to carry out compliance checks in coordination with the Processor or to have them carried out by examiners to be appointed on a case-by-case basis. The Principal has the right to verify compliance of the provisions agreed herein by means of sample checks of the Processor's business operations during random visits, which generally must be announced in due time. The Processor undertakes to submit to the Principal any information that is required for performance of its compliance control obligation and to make available the required evidence if requested to do so by the Principal.

With regard to the Principal's monitoring obligations pursuant to Section 11 Subsection 2 Sentence 4 of the German Federal Data Protection Act [Article 17 Para. 2 Directive 95/46/EC] or according to the applicable national legislation, the Processor submits to the Principal evidence documenting the implementation of the technical and organisational measures pursuant to Section 9 of the German Federal Data Protection Act and its appendix [Article 17 Para. 1 Directive 95/46/EC and, if applicable, of security measures according to Article 4 Directive 2002/58/EC in conjunction with Directive 2009/136/EC] prior to the start of data processing and, if requested to do so by the Principal, throughout the duration of the commission.

As evidence of the technical and organisational measures taken the Processor may submit to the Principal up-to-date audit statements, reports or extracts of reports prepared by independent entities (e.g. public accountants, internal audit, IT security department, data protection auditors, quality auditors) or appropriate IT security or data protection audit certificates (e.g. according to the *BSI Grundschrift* standard published by the German Federal Office for Information Security).

9. Reporting of violations by the Processor

If the Processor or any person employed by the Processor violates any provision governing the protection of the Principal's personal data or any provision agreed in the commission the Processor shall notify the Principal thereof without undue delay.

It is understood that the parties may be subject to reporting requirements pursuant to Section 42a of the German Federal Data Protection Act, Section 93 Subsection 3 of the German Telecommunications Act and Section 15a of the German Telemedia Act [Article 4 Directive 2002/58/EC] in case of a loss or an unlawful transmission or knowledge of personal data. Therefore, the Principal must be notified of such incidents without undue delay regardless of their cause. This also applies in case of serious disruptions to business processes (e.g. lost data, destroyed or deleted files, computer virus infections, failure of essential hardware components, software-related disruptions caused by programming errors or wrong configuration), in case of any other suspected violations of provisions for the protection of personal data, or in case of any other irregularities in the handling of the Principal's personal data. If the Principal is subject to a reporting requirement pursuant to Section 42a of the German Federal Data Protection Act the Processor shall support the Principal in meeting said requirements.

10. Principal's authority to issue instructions

All data must and may only be handled in compliance with the agreed provisions and in line with the instructions issued by the Principal (see Section 11 Subsection 3 Sentence 1 of the German Federal Data Protection Act [Article 17 Para. 3 Directive 95/46/EC]). Within the scope of the commission's description set out in this agreement, the Principal reserves a comprehensive right to issue instructions as to the type, scope and procedure of data processing, which it may substantiate by means of individual instructions. Any modification of the object of processing and of the procedure used must be agreed between the Principal and the Processor and must be documented. Except as expressly stated in the service description, the Processor must not disclose any information to third parties or data subjects unless the Principal has given its prior written consent.

The Processor must not use the data for any other purposes and, in particular, is not entitled to pass them on to third parties. Copies or duplicates must not be prepared unless the Principal has given its consent. This does not apply to backup copies insofar as they are required to ensure proper data processing, and to any data that are required for compliance with any statutory duty to retain records. If the Processor is of the opinion that an instruction is issued in violation of data protection provisions it shall notify the Principal thereof without undue delay in accordance with Section 11 Subsection 3 Sentence 2 of the German Federal Data Protection Act [Article 17 Para. 3 Directive 95/46/EC]. The Processor is entitled to suspend the implementation of the respective instruction until it is confirmed or changed by the responsible person appointed by the Principal.

11. Deletion of data and return of data carriers

After completion of the contractual services, or earlier if requested by the Principal – but upon expiry of the agreement at the latest – the Processor shall submit to the Principal any documents received, any results or output produced in connection with any processing or use, and any sets of data which are related to the commission, or destroy them in accordance with data protection rules if the Principal has given its prior consent to their being destroyed. The same applies to test and rejected materials. The report/log documenting deletion/destruction must be submitted to the Principal.

The Processor shall retain, even after expiry of this commission, any documentation needed to provide proof of the fact that the data are processed in due compliance with the commission or any other applicable data processing rules, for a period corresponding to the applicable period of retention.