Supplementary Terms and Conditions on Data Protection – Technical and Organisational Measures (ZB/MD)

The technical and organisational measures described herein shall be bindingly determined between _____ (client) and _____ (supplier). They shall apply to the contractual relationship (no. of the framework agreement, if available) _____.

The order data processing shall only take place on and with systems and hardware provided by the client:
☐ yes* ☐ no
- *May only be checked if no data are exported from the systems of the client.
- *If "yes", only questions with underlined figures need to be answered.

1. Access control

1.1 The buildings are secured with an alarm system:
☐ yes ☐ no

1.2 The entry doors of the building are equipped with the following locking system:
☐ manual locking system ☐ chip card access system

1.3 Access authorisations for the aforementioned locking system are documented by name:
☐ yes ☐ no

1.4 Access to the building by external parties/guests/visitors is documented by name:
☐ yes ☐ 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 There are regulations regarding the withdrawal of building access authorisations and access rights for computer systems incl. the documentation for employees in the event of termination of employment:
☐ yes ☐ no

1.7 There is a special access concept for server rooms inc. documentation indicating the names of the competent persons (inc. cleaning personnel, security staff etc.):
☐ yes ☐ no

2. Access control

2.1 The company network is protected from the public network with a hardware firewall:
☐ yes ☐ no
If yes:
type: _____
updating procedure and frequency: _____

2.2 Penetration tests of any IP addresses open to the Internet are carried out on a regular basis:
☐ yes ☐ no

2.3 There is a network separation of data of the client within the company network:
☐ yes ☐ no
if yes, by which measures: _____

2.4 Employees are bound to the following password specifications:
☐ individual computer password for each employee which must be kept secret
☐ no collective passwords
☐ minimum length, if applicable: number of characters/complexity: _____
☐ changing rhythm, if applicable, please indicate the respective time interval: _____
☐ automatic locking of the screen following time interval: _____

2.5 Virus scanners are used at the following transitions to the company network:
☐ e-mail account
☐ FTP
☐ Web

2.6 Use of a virus scanner on all servers:
☐ yes ☐ no
If yes, updating procedure and frequency: _____

2.7 Use of a virus scanner on all individual workstation computers:
☐ yes ☐ no
If yes, updating procedure and frequency: _____

2.8 Safety-relevant software updates are loaded to the existing software on a regular basis and automatically:
☐ yes ☐ no

2.9 Employees have local administration rights:
☐ yes ☐ no

2.10 Employees are authorised to access the Internet:
☐ yes ☐ no
If yes: restrictive browser configuration which cannot be changed by employees is installed:
☐ yes ☐ no

3. Access control

3.1 There are authorisation concepts and these are documented:
☐ yes ☐ no

3.2 The organisation of the granting of authorisations is documented by name (in particular who may grant which rights):
☐ yes ☐ no

3.3 The authorisations granted are documented by name:
☐ yes ☐ no

3.4 Number of administrators with the permission to copy/extract data of the client's inventories completely or to large extents: _____

3.5 Number of employees (no administrators!) with the permission to copy/extract data of the client's inventories completely or to large extents: _____

3.6 The following components of the workstation computers were locked/deactivated so that no data exports may be saved externally:
☐ USB ports
☐ CD/DVD burners
☐ memory card slots
☐ other mobile data carriers, if yes, which ones: _____

3.7 There are remote maintenance/remote access paths for:
☐ additional/external service providers
☐ employees
If there are remote maintenance/remote access paths, please complete the following information:
Type of authentication: _____
Protocols used (e.g.: SSH): _____

4. Circulation control

4.1 Type of encryption used for data exchange between client and contractor:
☐ SFTP
☐ S/Mime
☐ others, please explain the procedure: _____

4.2 The data sent by data carrier are encoded:
☐ yes ☐ no
If yes, please explain the procedure: _____

4.3 Explanation of the feedback procedure to the client upon receipt of a data carrier or assumed loss of a data carrier:
_____

4.4 Explanation of the disposal of the data carrier received by the client inc. documentation:
_____

4.5 Client data are saved encrypted, in addition:
☐ yes ☐ no
If yes, please explain the procedure:
_____

4.6 Backups are carried out:
☐ yes, encrypted ☐ yes, not encrypted ☐ no

4.7 Secured storage of backup media:
☐ yes ☐ no

4.8 How and when are the client's data deleted after the completion of an order (electronic data carriers/paper documents):
_____

4.9 Measures for the protection of the client's data (inc. temporary ones) on mobile workstation computers:
_____

4.10 Measures for the protection of the client's data (inc. temporary ones) on mobile data carriers:
_____

5. Entry control

5.1 For the replicability of the deletion/change of the client's data, log files are created for each employee by name:
☐ yes ☐ no

5.2 There is a restrictive access concept for the above mentioned log files:

☐ yes ☐ no

6. Order control

6.1 Employees are bound in writing to the data secret according to § 5 BDSG (Federal Data Protection Act [see Article16 RiLi 95/46/EG]):
☐ yes ☐ no

6.2 Employees are bound in writing to the telecommunications privacy according to § 88 TKG (Federal Telecommunications
Act [Article 5 RiLi 2002/58/EG]):
☐ yes ☐ no

6.3 The contractor obtains the following written additional declarations (in connection with data protection and data security) from its employees:

_____

6.4 Sub-contractors who have access to the client's data are/were commissioned:
☐ yes ☐ no

6.5 There are contracts with sub-contractors who process the client's data according to § 11 BDSG [Article 17 Para. 3 RiLi 95/46/EG and Article 17 Para. 1 RiLi 95/46/EG and, where applicable, operating security in accordance with Article 4 RiLi 2002/58/EG and RiLi 2009/136/EG]:
☐ yes ☐ no

6.6 There are sub-contractors outside the EU who have access to the client's data:
☐ yes ☐ no

6.7 Sub-contractors who get access to the client's data comply with the technical and organisational measures agreed in this checklist just as the contractor himself and have contractually warranted their compliance:
☐ yes ☐ no

6.8 There are training measures for employees with regard to the Federal Data Protection Act/data protection incl. documentation by name:
☐ yes ☐ no

6.9 There are currently the following certificates/data protection concepts for the company of the contractor which are submitted with this checklist (please indicate the respective titles and dates):

_____

7. Availability control

7.1 Frequency and number of generations of the data protection measures: _____

7.2 Storage location of backup data carriers:
☐ safe ☐ external storage at a distance of ≥3km (beeline)

7.3 Time of restart after complete destruction of the data centre in days: _____

7.4 There are maintenance agreements for the maintenance of IT systems by external parties:
☐ yes ☐ no

8. Separation control

8.1 The client's data are held available in an independent client which explicitly serves the order:
☐ yes ☐ no

8.2 There is an authorisation concept for the aforementioned client which excludes access to data by employees who do not work for the client/service recipient:
☐ yes ☐ no

8.3 Employees processing the client's data are seated in other rooms than employees working for other clients:
☐ yes ☐ no

8.4 Employees are bound in writing not to bring information from the client's data inventories into other projects/purposes:
☐ yes ☐ no

9. Signature

We warrant that the information rendered here corresponds to the current state of the technical and organisational measures for data protection implemented with us. Deviations from the information rendered here shall immediately be notified to the client/service recipient of the framework agreement according to sentence 1 of this checklist.

_____
Name and first name of the competent person who has completed the checklist (block letters)

_____ _____
Place, date Supplier-signature
and company seal