1 Preamble

1.1 The Contractor supplies the Client with services supported by information technology and IT (information technology) or OT (operational technology) products that are specified in more detail in the contract.

1.2 These supplementary contractual terms additionally regulate information security requirements that must be met by the Contractor.

1.3 The information and applications covered by the contract are subject to a defined security requirement level (normal, high, very high) from which the specific form of the information security measures is derived. The security requirement itself as well as details regarding measures are described in the technical specifications.

1.4 Unless expressly agreed otherwise, any expenses incurred by the Contractor as a result of the implementation of the following requirements shall be covered by the agreed remuneration.

2 Information security requirements

2.1 Management of information security The Contractor has established in its company an appropriate information security management system (ISMS) or equivalent, suitable processes to guarantee information security within the scope of the provision of services and shall maintain this system throughout the entire term of the contract. The Contractor's ISMS shall, as a minimum, meet the information security requirements stipulated below and shall be based on DIN EN ISO/IEC 27001 or an equivalent requirement.

2.2 Roles and contact persons

a) Information security coordinator

When signing the contract, the Contractor must provide the Client with the name of a competent contact person for all aspects relating to information security (e.g. information security officer, IT security manager or chief information security officer (CISO)), who is able and authorized to provide the Client with information on all matters relating to the management of information security.

b) Contact person for regular communication

The Client may require the Contractor to designate further contact persons / role managers in all matters relevant to information security in the context of the commissioned service (e.g. functional, technical, or operational managers) and to clarify unambiguously the distribution of tasks and transfer of responsibility. The Contractor shall notify the Client of any changes without undue delay.

c) Contact person for emergency coordination

The Contractor shall designate a central contact person (SPOC / single point of contact) for emergency communications, who shall be available to the Client for the periods specified in the statement of work details (e.g. SLA). In an emergency, SPOC shall have access to all necessary product monitoring data of the supplier/service provider, the identity access management (IAM) system, and the software and hardware configuration data, and shall make these available to the Client and its emergency team on request and in a suitable format (readable and processable).

2.3 Security review

In the case of services requiring a high level of security, the Client reserves the right to demand
that the Contractor carry out a security review in accordance with the Manual of Industrial Security issued by the Federal Ministry of Economics and Technology ("Geheimschutzhandbuch") for employees or other persons deployed by the Contractor as part of its service provision who come into contact with information or systems categorized by the Client as particularly sensitive (see statement of work) or critical infrastructures within the meaning of the Ordinance on the Determination of Critical Infrastructures pursuant to the German Act on the Federal Office for Information Security (BSI-KritisV). The Contractor shall demonstrate to the Client in text form that the security review has been successfully carried out.

2.4 Status report
The Contractor shall provide the Client with a status report on the information security of the purchased service upon request. The report shall contain details such as: information on deviations from agreed information security requirements, historical statistics on security incidents and security patches, status of vulnerability management and audit results, availability of security controls, efforts to remedy incidents and invoicing if security measures have been agreed separately. The form, content and frequency of the report shall be mutually agreed between the Client and the Contractor within eight weeks of conclusion of the contract.

2.5 Commitment for subcontractors
The Contractor shall obtain an contractual obligation from any subcontractors or sub-suppliers that it uses in relation to this contractual relationship that they shall meet the requirements of this contract. The Contractor shall provide evidence of the subcontractors' obligation at the request of the Client.

2.6 Data processing
Should the Contractor process or store data belonging to the Client or its affiliated companies pursuant to Sections 15 et seq. of the German Stock Corporation Act (AktG), the Contractor undertakes to observe and comply with both regulatory and legal requirements as well as the requirements of the statement of work, specifically the provisions on backing up data.

2.7 Legal spheres - hosting
The Contractor undertakes to name all the countries in which the Client's data is hosted or application systems are operated at the time of the offer. The Contractor hereby gives its assurance that the data will not leave the named storage locations. Relocations within the EU are excepted from this but must be communicated to the Client in text form without undue delay. The Client shall be entitled to terminate the contract without notice if this provision is breached.

2.8 Guaranteed return of the data
In reference to any ordinary or extraordinary termination of the contract in future, the Contractor guarantees that the Client data stored by the Contractor and the structure of this data storage can be returned to the Client, i.e. that it is stored and processed by the Contractor in a format that can be processed by the Client. Proprietary formats or encryption technologies are not permitted.

2.9 Deletion of data
After the successful return of the data has been confirmed by the Client, the Contractor guarantees that it shall delete and destroy all data relating to the contractual relationship at all primary and secondary locations of the Contractor and its subcontractors in a permanent and secure manner so that it cannot be restored. Exceptions shall only exist for data that the Contractor is legally obliged to store or where such storage has been contractually regulated. The Client shall provide evidence of this at the request of the Contractor.

2.10 Terminal devices
If the contractor uses its own terminal devices to provide the agreed service, the Contractor undertakes to comply with the following specifications of the Client. For the purposes of this provision, "terminal device" means any IT asset of the Contractor that is connected to the Client's IT applications or IT infrastructure (wired or wireless) or is used for processing the Client's data.

• Only devices that are actively managed by the Contractor may be used.
• The use of private terminal devices to connect to IT assets of the DB Group is prohibited unless expressly approved by the Client.
• Terminal devices must be secured in accordance with the current state of the art; this means setting up access protection (password or PIN), deactivating all transmission protocols that are not required, using encryption protocols for data transmission (e.g. WPA2 for Wi-Fi), and using encryption technologies for the terminal devices' stored data.

• The Contractor is responsible for the proper handling of the terminal devices and for protecting them against theft; if a terminal device is used outside the Client's locations, it must not remain unsecured or unattended.

• The Contractor undertakes to report the loss of a terminal device immediately to the responsible managers on the Client's side and to deactivate and block it immediately.

• The Contractor shall ensure that the terminal device is regularly (at least once a month) checked for security updates and updated in accordance with the current state of the art and shall provide proof of this on request. The requirements for data processing under section 2.6 apply to data backup.

• The operation of hacking tools, sniffers, etc. is prohibited unless expressly permitted.

• The Contractor is responsible for ensuring that the data networks of the Client and its affiliated companies are not coupled with other data networks.

• After the end of the usage period, the safe and professional disposal of the terminal device must be ensured by the Contractor; this includes the complete removal of all data and/or the removal of internal memory cards.

2.11 Encryption
The Contractor guarantees that data categorized as “DB Vertraulich” ("DB confidential") or “DB Streng vertraulich” ("DB strictly confidential") shall be encrypted for transmission and storage. The Client should be notified if the data is not stored at the Contractor's premises.

2.12 Cryptography
The Contractor guarantees that the cryptographic software used conform to the agreed state of the art. In coordination with the Client, the Contractor shall prepare a cryptographic concept using cryptographic software in accordance with the specifications of the Client in the statement of work.

2.13 Patchability
If the contract provides for the delivery of IT/OT systems or software, the Contractor guarantees that security gaps shall be closed during their lifecycle by means of patches. The Contractor shall deliver a patchable IT/OT system so that changes can be made subsequently without changing basic functionalities. The Contractor guarantees that any patches installed are tested according to the current state of the art, that they can be revoked in the event of production problems, and that changes are recorded and documented by the system.

2.14 Hardening
If the contract provides for the delivery of IT/OT systems, the Contractor guarantees that systems are hardened in conformity to the current state of the art (e.g. in line with the requirements of BSI and NIST). A corresponding protocol must be enclosed with the delivery of the product/service. Besides software and database systems, networks, possible backdoors and standard passwords should be considered. The installation principles resulting from the hardening must be documented and transmitted to the Client.

2.15 Standard passwords
Passwords embedded deep in the source code are not permitted. The Contractor shall provide the Client with a complete list of standard passwords. If the contract provides for the implementation of IT/OT systems, the Contractor undertakes to change standard passwords before going live.

2.16 Notification of security incidents
The Contractor undertakes to inform the Client of all security incidents or breaches of data protection pursuant to Art. 33 GDPR that occur in the environment of the Contractor or one of its subcontractors or that impact its direct or indirect provision of services. If the security incident is of relevance to the data and systems of the Client and its affiliated companies, the notification must be made without undue delay. For services with a security requirement level 'high' or above, security incidents that do
not affect the Client's data and systems shall be disclosed to the Client within the framework of sec-
urity incident reports, which must be prepared at least every six months and whose type and content
shall be mutually agreed within eight weeks of conclusion of the contract.

2.17 **Recovery of a safe state**
In the event of a security incident of relevance to the Client and its affiliated companies the Contractor
shall, in addition to informing the Client, immediately take all necessary measures to recover the
necessary security. If a concerted procedure with the Client is necessary for this, the Contractor shall
contact the Client with a detailed catalogue of measures and coordinate with the Client.

2.18 **Notification of vulnerabilities**
If products provided by the Contractor or IT/OT systems operated by the Contractor are affected by
vulnerabilities, the Contractor shall be obliged to report these to the Client securely and without un-
due delay. Where possible, the results of an initial analysis should be classified according to the
Common Vulnerability Scoring System or on the basis of assessments by the Federal Office for
Information Security.
The notification should contain the following elements:

- Precise description of the product (if applicable, details regarding the design, subsystem, compo-
nent, manufacturer's name, release, product and/or batch number of the software, firmware, driver, 
BIOS and hardware provided)
- Detailed description of the vulnerability including its exploitability
- Initial evaluation from the Contractor's point of view and recommendation of specific countermeas-
ures for dealing with the vulnerabilities, taking into account any relevant requirements for security-
related approval and release
- Number and documented installation locations (stating the technical system including room and 
cabinet location) of the affected products, provided that the Contractor has this information.

2.19 **Identity management**
If the Contractor operates IT/OT systems on behalf of the Client, the Contractor shall guarantee the
management of identities and access to data and interfaces in conformity to the current state of the
art, unless otherwise agreed in the contract. All natural persons and technical users are provided
with a separate user account. The Contractor shall provide the Client with intelligence from its identity
and access management (IAM) system upon request.

2.20 **Access**
Direct or covert access to the information systems (operational systems, networks, programs, da-
tasets) of the Client and its affiliated companies is only permitted to the Contractor if it has received
express access authorization in text form from the Client; such access authorization is restricted to
the expressly approved and deployed employees of the Contractor or its subcontractors. Transfer of
access authorizations to third parties is forbidden. Any access authorization granted may only be
used in the context of the contractually assumed services.

2.21 **Operational safety**
The Client reserves the right to carry out blocks or monitoring as a result of government agency
orders or in line with the conditions of use. Also, it must be possible to suspend network access at
any time if the devices of the Contractor that are connected to the network affect in any way the
operating security or the operating behavior of the network or of other devices or software connected
to the network. The above applies subject to differing provisions on the handling of personal data in
the contractual relationship.

3 **Assessment of the level of information security maturity at the Contractor's premises**

3.1 **Security organization information**
The Contractor shall disclose to the Client information about its security organization, on the basis of
which the Client can perform an evaluation of the level of maturity of information security. This infor-
mation may include, for example, a management summary of the security organization in the scope
of application of the service, reports from an existing information security management system, a
DIN EN ISO/IEC 27001 certificate including the Statement of Applicability (SoA) or equivalent evidence, and current audit results in the scope of application of the service.

3.2 Audit
The Contractor agrees that the Client or another third party commissioned by the Client may audit the Contractor during the term of the contract with regard to its information security and compliance with data protection regulations. The basis of the information security audit is ISO27001 as well as the current state of the art; the subject of the audit is the appropriate implementation of the agreed information security requirements relating to the order (service, product) and the structure and effectiveness of the Contractor’s information security organization. The data protection audits are based on the GDPR and the German Federal Data Protection Act (BDSG).

In principle, at least two years should elapse between routine audits. They shall be conducted during normal business hours, and the duration of the on-site part of the audit shall be limited to one to two working days if possible. The Client shall provide at least six weeks’ notice of routine audits that are not related to a specific cause or event. Ad hoc audits can take place at short notice, depending on the severity of the cause or its urgency.

The Contractor shall provide the necessary documents such as management reports, operational documents (configuration and authorization data), reports from the ISMS, etc. in a timely manner (generally three weeks or more before the date of the audit), shall grant the necessary reading rights, and shall comply with its duties to cooperate for the purposes of the audit, e.g. granting the necessary access rights, providing documentation and access. The Client shall provide the Contractor with the results of the audit in the form of a report.

The Contractor undertakes to adapt the audit results marked as critical in improvement projects and to report on its progress in regular communications. The Client and the Contractor shall mutually agree on the scope of and schedule for these improvement projects. The Client reserves the right to check the progress of the improvement measures on site. The time frame mentioned above for routine audits shall apply to the preparation of these checks.

The costs incurred by the Client for a routine audit that is not related to a specific cause or event shall be borne by the Client. The costs incurred by the Client for an ad hoc audit that is initiated as a result of a security incident, for example, shall be borne by the Contractor.