Supplementary Contractual Terms and Conditions

of Deutsche Bahn AG (DB AG) and its Affiliated Companies on Information Security Requirements (Supplementary Contractual Terms for Information Security)

- Edition January 01, 2021 –

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 (normal, high, very high) on which the specific form of the information security measures is based. The protection category itself, as well as details regarding measures, are described in the statement of work or, alternatively, in the contract.

1.4 Insofar as an audit cannot be demonstrably carried out as planned by the Client for reasons relating to professional law, the Contractor shall inform the Client of these reasons in a timely manner. The parties shall then agree on a modified audit plan. Both the professional law applicable to the Contractor and the interests of the Client shall be taken into account in the process.

1.5 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 Information security management

The Contractor has established suitable processes in its company to guarantee information security within the scope of the provision of services and shall maintain this system throughout the entire term of the contract. For example, this shall be done in the form of an appropriate information security management system (ISMS) or equivalent, suitable processes for guaranteeing information security in the context of service provision. The Contractor's information security processes 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 or 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 contract. In case of an emergency, the SPOC has access to all necessary data of the Contractor (e.g. product monitoring, identity access management (IAM) and configuration data) and provides it to the Client and its emergency team on request and in a suitable format (readable and processable).

2.3 **Security review**

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 ("Industrial Security Manual") 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 service description) 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 **Expert staff**

The Contractor shall ensure that the personnel it employs has the necessary qualifications and awareness of the requirements for information security and shall prove this to the Client on request.

2.6 **Obligation of subcontractors**

The Contractor shall warrant that its subcontractors and their subcontractors employed in relation to this contractual relationship shall comply with the requirements of this contract, with ISO27001 or with those of a comparable standard. The Contractor shall provide appropriate evidence if the Client requests this.

2.7 **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.

2.8 **Encryption**

The Contractor guarantees that data categorized as "DB confidential" or "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.

2.9 **Legal sphere - 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 shall 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.

2.10 **Deletion of data**

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 immediately upon termination of the contract so that this data cannot be restored. Exceptions shall exist only for data that the Contractor is legally obliged to store or where such storage has been contractually regulated. The Contractor shall provide evidence of this at the request of the Client.

2.11 **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 terminal devices must be secured according to the current state of the art.
- The Contractor undertakes to report the loss or compromising of a terminal device immediately to the responsible managers on the Client's side and to deactivate and block it immediately.
- 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.

2.12 **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. The type and content of the notification shall be agreed by mutual consent within eight weeks after conclusion of the contract. Security incidents that do not affect the Client's data and systems shall be disclosed to the Client as part of the regular status report.

2.13 **Restoring a secure 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 restore the necessary security. If a concerted procedure with the Client is necessary for this, the Contractor shall contact the Client with a detailed catalog of measures and coordinate with the Client. Where the assistance of third parties is necessary for processing measures, the Contractor shall grant them access to all necessary information, systems and business premises.

2.14 **Access**

Direct or covert access to the information systems (operational systems, networks, programs, datasets) of the Client and its affiliated companies shall be permitted to the Contractor only if it has received express access authorization from the Client and this authorization has been documented; such access authorization shall be restricted to the expressly approved and deployed employees of the Contractor or its subcontractors. Transfer of access authorization to third parties is forbidden. Any access authorization granted may be used only in the context of the contractually assumed services.

2.15 **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 site

3.1 Security organization information

The Contractor shall disclose to the Client intelligence from its security organization, on the basis of which the Client can perform an evaluation of the level of maturity of information security. This information 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 on behalf of the Client may audit the Contractor during the contract period with regard to the Contractor's information security and compliance with privacy regulations. The information security audits are based on ISO27001 and the current state of the art. The audits check the appropriate implementation of the agreed information security requirements in relation to the order (service, product) and the structure and effectiveness of the Contractor's information security organization. The privacy 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) 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.

❑