Supplementary Contract Terms and Conditions

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

- Version dated November 1st, 2026 -

1. Preamble

1.1 The Contractor supplies the Client with services supported by information technology and/or IT (information technology) or OT (operational technology) assets or products, as further specified in the contract.

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

1.3 Beginning December 11, 2027, the Contractor shall provide the contractual services, insofar as they constitute „products with digital elements“, in compliance with the applicable requirements of Regulation (EU) 2024/2847 (Cyber Resilience Act, CRA). Other legal requirements and any additional requirements under these Supplementary Contract Terms remain unaffected.

1.4 The information and IT/OT assets covered by the contract may be subject to a defined security requirement (normal, high, very high) and, where applicable, special legal requirements (e.g., legislation on critical infrastructures). The specific design of the information security measures shall be derived from these requirements. The security requirement itself and details of the measures, where applicable, are documented in the contract. If no security requirement is specified or no additional information security requirements are defined in the contract, the requirements for a "normal" security requirement shall be deemed agreed.

1.5 Insofar as an audit (pursuant to Item 3.2, Audits) 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.

1.6 Any expenses incurred by the Contractor in implementing the requirements of these Supplementary Contract Terms and any appendices are covered by the agreed remuneration. Any exceptions must be agreed by way of a contract amendment. The implementation of statutory requirements is excluded from this provision.

1.7 If the Contractor violates the obligations under Items 2.2.a), 2.4, 2.7, and 3.1 of these Supplementary Contract Terms, it shall pay the Client a contractual penalty for each violation amounting to 2% of the remuneration owed under the respective affected (individual) contract, unless the Contractor is not responsible for the violation. The Client's right to claim damages arising from the same breach of duty remains unaffected by the contractual penalty; however, any contractual penalty incurred shall be offset against such damages.

Any contractual penalties incurred on the basis of these Supplementary Contract Terms for Information Security shall amount to no more than 5% of the remuneration owed under the respective (individual) contract.

2. Information security requirements

2.1 Information security management

The Contractor has established suitable processes within its company to ensure information security. These processes cover the entire life cycle of the IT/OT assets, products, and services supplied that is relevant to contract fulfillment. The Contractor shall maintain these processes throughout the entire term of the contract, for example through an effective information security management system (ISMS). At a

minimum, the information security processes shall cover the information security requirements described in these Supplementary Contract Terms, including the appendices.

2.2 Information security contacts

a) Information security coordinator

When signing the contract, the Contractor must provide the Client with the name of a knowledgeable and responsible contact person for all aspects of information security (e.g., an information security officer, IT security manager, or Chief Information Security Officer) who is able and authorized to provide the Client with information.

b) Contact for contract-specific information security matters

The Contractor shall designate the responsible office or function for regular contractual and emergency communications, information security matters, and the reporting of identified vulnerabilities. This office shall be available to the Client within the time frames specified in the contract. In an emergency, the contact person shall have access to all necessary Contractor data (e.g., product monitoring, access, and configuration data) and shall act as the interface to the Client during emergency response.

The Contractor shall inform the Client without undue delay of any change in contact person.

2.3 Personnel security requirements

Special requirements regarding personal reliability and integrity apply to the Contractor's employees and other third parties engaged in service delivery, including subcontractors and their employees.

To ensure compliance with these requirements, the Client reserves the right to subject the employees concerned to additional screening and information-gathering procedures ("background checks"). The precise scope of these procedures shall be based on the applicable regulatory and normative personnel security requirements, in particular the requirements of the German Act on the Federal Office for Information Security (BSIG), the related specifications published by the German Federal Office for Information Security (BSI), and the requirements of the German Critical Infrastructure Umbrella Act (KRITIS-Dachgesetz). The Client reserves the right to permit employees to be deployed only after successful screening.

2.4 Qualified staff

The Contractor shall ensure that the personnel it deploys possess the qualifications and awareness of the necessary information security requirements to provide the services, that these are regularly updated, and, upon request, shall provide evidence thereof to the Client no more than once per year.

2.5 Obligations of subcontractors

The Contractor shall warrant that its subcontractors and their subcontractors used in providing the services comply with the requirements of this contract or with the requirements of a relevant information security framework or standard, such as DIN EN ISO/IEC 27001. Upon request by the Client, the Contractor shall provide appropriate evidence.

Suppliers of the Contractor that provide only physical products without digital elements shall not be considered subcontractors for the purposes of this requirement

2.6 Encryption

The Contractor shall ensure that Client information classified as "DB internal," "DB confidential," or "DB strictly confidential" is, as a general rule, protected during electronic transmission by suitable transport encryption and, when stored, by appropriate state-of-the-art technical and organizational measures. If cryptographic measures become insecure during the term of the contract, they shall be replaced following bilateral consultation. The Client and Contractor shall mutually agree on the allocation of the associated costs.

2.7 Jurisdictions for storage / processing

The Contractor shall identify all countries in which the Client's data is processed or stored. If the statement of work contains additional requirements for storage and processing locations, the Contractor shall confirm compliance with those requirements. If data is stored outside the Contractor's systems, the Contractor shall notify the Client separately.

The Contractor gives its assurance that the data shall not leave the named storage locations. Relocations within the EU are excepted, but must be communicated to the Client in writing without undue delay.

2.8 Reporting information security incidents

The Contractor shall inform the Client of all information security incidents and personal data breaches pursuant to Art. 33 GDPR that occur within the environment of the Contractor or one of its subcontractors and affect the direct or indirect provision of services to the Client. If an information security incident directly affects data and/or assets of the Client or its Affiliated Companies, the initial notification must be made without undue delay, but no later than 24 hours after the Contractor becomes aware of the security incident, and a detailed notification, including an impact analysis, must be made no later than 72 hours after such awareness.

At a minimum, the notification must include the following:

- Time at which the incident occurred and when it was detected
- Affected systems and data
- Measures taken
- An initial assessment of the severity/criticality/legal relevance.

Contract-specific notification content shall be mutually agreed in writing within eight weeks after signing the contract, but no later than before the start of service provision or delivery of the product.

Notifications shall be sent to security-issues@deutschebahn.com as well as to the contacts specified in the contract.

If subcontractors and/or service providers are used, the Contractor shall ensure that it can nevertheless comply with the reporting deadlines specified.

2.9 Handling information security incidents

In the event of an information security incident relevant to the Client (see Item 2.8 of these Supplementary Contract Terms), the Contractor shall, in addition to informing the Client, take all necessary measures without undue delay to restore the required level of security. If a coordinated approach with the Client is necessary, the Contractor shall submit a detailed catalog of measures to the Client and coordinate with the Client. If support from the Client, its Affiliated Companies, and/or engaged third parties is necessary to implement the measures, the Contractor shall, subject to an appropriate confidentiality agreement, grant them access to all necessary information, systems, and business premises.

2.10 Access control

Direct or covert access to the information systems (including operational systems, networks, applications, and data inventories) of the Client and its Affiliated Companies shall be permitted to the Contractor only if the Contractor has received explicit, documented access authorization from the Client. Such authorization shall be restricted to the deployed and explicitly approved employees of the Contractor or its subcontractors. Transfer of access authorization to third parties is prohibited. Any access authorization granted may be used solely in connection with the contractually agreed services. If access authorization is no longer required (e.g., upon termination of an employee's employment), the Contractor shall inform the Client without undue delay.

3. Information security assessment of the contractor

3.1 Assessment of the security organization

Upon request, the Contractor shall disclose information about its information security organization to the Client and provide suitable evidence relating to the specific service, on the basis of which the Client can assess information security. This may include, for example, an ISMS status report (a template can be provided upon request), a management summary of the security organization within the scope of the service, reports from an existing information security management system, a DIN EN ISO/IEC 27001 certificate including a detailed description of the scope, the Statement of Applicability (SoA), and the DIN EN ISO/IEC 27001 audit report, a VdS 10000 certificate, or equivalent evidence such as current audit results within the scope of the service.

3.2 Audits

The Contractor agrees that the Client or a 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. Information security audits are based on DIN EN ISO/IEC 27001 and the current state of the art. The audits examine the appropriate implementation of the agreed information security requirements and the effectiveness of the information security organization in relation to the contract.

Data protection audits are based on the GDPR and the German Federal Data Protection Act (BDSG). Details regarding audit performance, required effort, and any follow-up measures are described below.

a) Routine audits

The Client shall provide at least six weeks' notice of a routine audit. The Contractor shall provide the necessary documents in a timely manner (generally no later than three weeks before the audit date), such as management reports, ISMS reports, and operational documents including configuration and authorization data, and shall fulfill its duties to cooperate with the audit, including providing access and granting the necessary access rights. Audits shall be conducted during normal business hours. The Client shall provide the Contractor with the audit results in the form of a report. Audit reports submitted by the Contractor from independent third parties, such as ISO 27001 or TISAX certification, an ISAE 3402 report, or a SOC 2 report, in each case covering the service to be provided, may, at the Client's discretion, expedite the audit or eliminate the need to conduct it.

b) Issue-based audits

The Client shall have the right to conduct an issue-based audit in the event of a serious information security incident or repeated violations of these Supplementary Contract Terms, provided that the Client is affected by the incident. Depending on the severity of the circumstances, audits may be conducted at short notice.

c) Measures to remedy nonconformities

If an audit identifies vulnerabilities, nonconformities, or personal data breaches on the part of the Contractor, the Contractor shall remedy them in a timely manner. The Client and the Contractor shall mutually agree upon the scope and schedule for the implementation of these measures. The Client shall be informed of the status of the measures as part of regular reporting.

The Client reserves the right to verify on site the progress and effectiveness of the improvement measures through an issue-based audit. The time frame specified above for preparing audits shall apply to these reviews.

d) Estimated effort and costs

The Client shall conduct routine audits based on the criticality of the service provided, no more than once every two years, using a standardized approach and predominantly as remote audits. Here, the average required time for preparation and execution of the audit is roughly two days on the Contractor’s side. The Client will require an average of five days of the Contractor’s time for on-site audits. This amount does not include the time required for the provision of the documentation to be examined. The effort required for issue-based audits cannot be estimated on a general basis.

Audits in the context of critical facilities shall generally be conducted on-site. If the services are not performed solely by the Contractor, the audit may extend to the entire supply chain. The Contractor shall ensure that its contracts include the necessary provisions to facilitate such audits. The effort required for these audits may be higher, as their scope and content are determined by applicable statutory and regulatory requirements.

Each contracting party shall bear its own costs incurred in connection with audits.