

## **GENERAL TERMS AND CONDITIONS**

The following general terms and conditions are intended to govern contracts with suppliers of goods and services in the interest of DB Group s.p.a. all its group companies that refer to these general terms and conditions (hereinafter, simply, DB).

Article 1.	SCOPE OF THE GENERAL CONDITIONS.....	1
Article 2.	CONSIDERATIONS.....	1
Article 3.	INVOICING AND PAYMENTS.....	1
Article 4.	SERVICE PERFORMANCE.....	1
Article 5.	PROHIBITION OF SUBCONTRACTING AND CONTRACT ASSIGNMENT.....	1
Article 6.	IMPOSSIBILITY AND FORCE MAJEURE.....	2
Article 7.	APPLICABLE LAW AND JURISDICTION.....	2
Article 8.	AMENDMENTS.....	2
Article 9.	COMMUNICATIONS.....	2
Article 10.	CONFIDENTIALITY AND PRIVACY.....	2
Article 11.	LEGISLATIVE DECREE NO. 231/2001. ORGANISATIONAL MODEL AND CODE OF ETHICS.....	2
Article 12.	CYBERSECURITY.....	3
Article 13.	GENERAL PROVISIONS.....	3

### **Article 1. SCOPE OF THE GENERAL CONDITIONS.**

1. These general conditions of contract govern the relationship between the supplier and DB in connection with the provision of goods or services.
2. The general conditions, together with the order, if any, and all the contractual documentation constitute an integral part of the contract governing the relationship between the parties (hereinafter the "Contract").
3. In the event of conflict, the general conditions shall prevail over the contractual documentation prepared by the supplier.
4. The supplier waives the application of its own general conditions, which, if any, shall be deemed ineffective.

### **Article 2. CONSIDERATIONS**

1. Prices, rates and considerations for each good or service shall be communicated in advance.
2. Prices, rates and considerations include all expenses, charges and elements necessary for the precise performance of the Contract.
3. Prices, rates and considerations include charges for compliance with legal requirements for occupational health and safety, where applicable, which shall be expressly disclosed under the supplier's responsibility and at its expense and included in the contractual documentation.

### **Article 3. INVOICING AND PAYMENTS.**

1. The Recipient Code to be used for issuing the electronic invoice is SN4CSRI.
2. The invoice shall contain identifying elements of the goods or service to which the expense refers.
3. The PDF of the invoice shall be attached the XML file of the same as an integral part thereof.
4. The supplier shall issue individual and not cumulative invoices in the case of providing several services.
5. Payments shall be made only upon submission of a periodic statement of account from the supplier, to be transmitted by e-mail to [vendors@dbgroup.net](mailto:vendors@dbgroup.net) 10 (ten) days before the due date of the invoice.
6. Payment shall be made by bank transfer to the supplier's bank account within the agreed payment terms.
7. Payment terms due at the end of July and August shall be postponed to the end of September. Payment terms due at the end of November and December shall be postponed to the end of January.
8. The supplier shall be required to promptly notify DB of any changes in its corporate and tax data.

### **Article 4. SERVICE PERFORMANCE.**

1. The supplier undertakes to organise, manage and perform the Contract according to good practice, with full organisational and managerial autonomy and responsibility, as well as with its own personnel, materials and means.
2. In the performance of the Contract, the supplier undertakes to **(i)** comply with the provisions of the law and all regulations, legislation and provisions of the competent authorities applicable to the Contract; **(ii)** ensure precise fulfillment of its legal, tax and contractual obligations, including to its suppliers and subcontractors, if any.

### **Article 5. PROHIBITION OF SUBCONTRACTING AND CONTRACT ASSIGNMENT.**

1. The supplier is expressly prohibited from subcontracting the performance of the Contract to third parties.
2. The supplier is expressly prohibited from assigning the Contract to third parties, even in part.

**Article 6. IMPOSSIBILITY AND FORCE MAJEURE.**

1. The supplier shall not be considered to be in breach of contract if the total or partial performance of the assignments is impossible or prevented by fortuitous event (which presupposes the sudden inclusion in the agent's conduct of an unforeseeable factor that makes the occurrence of the event inevitable) or by an event of force majeure (and, therefore, resulting from nature or man, the action of which cannot be avoided).
2. Force majeure events shall not suspend the effective periods of the Contract, which they shall not affect.
3. DB shall be reimbursed for all expenses incurred due to the impossibility to provide the service, as well as its non-performance or suspension due to a fortuitous or force majeure event.

**Article 7. APPLICABLE LAW AND JURISDICTION.**

1. Italian law shall apply to contracts.
2. Any dispute regarding the interpretation, performance or termination of the contracts, and/or any dispute connected or related thereto, shall be subjected exclusively to Italian jurisdiction and in particular to the Court of Treviso.

**Article 8. AMENDMENTS.**

1. All amendments, supplements and consensual termination of contracts shall be in writing.

**Article 9. COMMUNICATIONS.**

1. Any communications regarding contracts and the exercise of rights related thereto shall be in writing.
2. Any communications shall be made in a manner that allows for verification of receipt by the recipient (by certified e-mail or registered letter with return receipt) and be also sent in copy by e-mail.

**Article 10. CONFIDENTIALITY AND PRIVACY.**

1. The parties undertake to keep confidential any confidential information they become aware of during the performance of the Contract or by reason thereof, including in relation to the rates applied.
2. Confidential information means all information acquired by the parties and, in particular, but not limited to, personal, business commercial, accounting, technical and administrative data of the parties, suppliers, employees and professionals related to said parties, contracts, projects, technical drawings, documents, financial or commercial data, regardless of whether such information is indicated as confidential at the time of disclosure.
3. Confidential information may be acquired in any form and without limitation (oral, written, or graphic).
4. Under no circumstances may information be considered confidential if it is in the public domain or becomes so by an act or conduct not prohibited for the other party; was already known to the other party; was expressly classified as non-confidential; was acquired independently of the Contract; or is disclosed by a person who is not bound even indirectly by an obligation of secrecy.
5. Confidential information disclosed by subsidiaries, consultants, collaborators, agents, employees, or representatives of the parties is also governed by this provision.
6. In particular, the parties undertake **(i)** not to disclose and/or otherwise make confidential information known to third parties; **(ii)** to take the necessary precautions and security measures, according to the best standards, in order to keep information confidential, as well as in order to prevent its misappropriation and manipulation; **(iii)** to strictly comply with current privacy and data protection legislation.
7. The parties may not use, transfer, reproduce and copy confidential information.
8. The parties shall use the confidential information only for the agreed purposes and shall not disclose the same to third parties other than workers, directors, officers, employees, agents, collaborators, professional consultants, and contractors who require knowledge of the same for purposes other than the performance of the Contract.
9. No Contract provision shall be construed as granting any right under any patent, copyright, or other intellectual or industrial property right, nor as granting any right to confidential information, other than the limited right to use such information for the purposes of the Contract.
10. Upon expiry of the Contract and/or in the event of its termination the parties undertake to mutually return to each other the originals and copies of documents containing or referring to the confidential information.
11. The parties undertake to delete or destroy any transcripts and/or recordings made of the confidential information.
12. Confidentiality obligations shall be effective for an additional 3 (three) years from the termination of the same, for whatever reason.
13. The obligations shall apply in perpetuity with respect to information concerning intellectual and industrial property rights.

**Article 11. LEGISLATIVE DECREE NO. 231/2001. ORGANISATIONAL MODEL AND CODE OF ETHICS.**

1. The supplier declares to be aware that DB, pursuant to Legislative Decree No. 231 of 8 June 2001 (hereinafter the "Decree") has adopted an organisational, management and control model (hereinafter the "Organisational Model") and a code of ethics

(hereinafter the "Code of Ethics"), the latter of which is also available at DB's registered office and online at the following link [Corporate Social Responsibility | D.B. Group \(dbgroup.net\)](http://www.dbgroup.net/Corporate-Social-Responsibility-D.B.-Group). The supplier also declares to be aware of the provisions of Legislative Decree 231/2001, as well as the part of the Organisational Model that is relevant to the nature of the service covered by the Contract and the content of the Code of Ethics adopted by DB.

2. The Supplier undertakes, in the performance of all services regulated by these General Conditions, as well as in all relations with DB, to comply with and apply and ensure its employees and collaborators comply with the provisions of the Decree, the Organisational Model and the Code of Ethics, and not to engage in any commissive or omissive conduct likely to constitute unlawful conduct and, in particular, the crimes referred to in the Decree - regardless of the actual perpetration of the crime or its punishability - as well as to act in compliance with the rules and principles of the Decree itself.
3. The supplier undertakes, for itself and its employees and collaborators, to cooperate at all times with DB and the current members of its Supervisory Board, whether they act as individuals or as a collegiate body, responding to requests received from the same, aimed at preventing the commission of the crimes referred to in the Decree or violations of the Organisational Model and/or Code of Ethics.
4. Violation of even only one of the provisions of this Article 11 shall constitute a serious breach by the supplier of the obligations governing the relationship and shall entitle DB to terminate any existing contractual relationship with the supplier with immediate effect, pursuant to and for the purposes of Article 1456 of the Civil Code, without prejudice to DB's right to compensation for all damages that may have been incurred. The supplier declares to indemnify and hold DB harmless of any charges, expenses, costs, penalties, or damages that may be incurred by DB as a result of the supplier's violations.

#### **Article 12. CYBERSECURITY.**

1. The supplier shall comply with the cybersecurity policy adopted by DB which is based on the (i) ISO/IEC 27001:2013 and (ii) ISO/IEC 27002:2013 standards, (iii) EU Regulation 2016/679, (iv) Legislative Decree 81/2008 and (v) Legislative Decree 231/2001, as well as on the principles of (a) protection of the locations where the IT resources are allocated (contingency, authorisation, tracking and monitoring and accesses, as well as provision of adequate environmental conditions and protection from power outages or electrical anomalies), (b) security in the use of IT resources (training, awareness regarding related threats and provision of penalties for violations and misuse) (c) asset management (identification, census, inventory of assets, as well as provision for a process of safe decommissioning and/or destruction), (d) information security (capacity management and monitoring of the use of ICT resources, definition of Key Performance Indicators, execution of a process of continuous performance monitoring of ICT resources, optimisation of utilisation and strengthening of security controls, malware protection, backup, network security, logging, monitoring, vulnerability management, and definition of remediation or mitigation actions), (e) security of logical access (based on the principles of need-to-know, least privilege, and segregation-of-duties), (f) security in cryptographic controls, (g) security in ICT system acquisition activities, (h) security in the maintenance of ICT systems, (o) secure decommissioning of ICT systems, (i) security of Cloud Computing services, (l) information security incident management (detection/reporting, classification and triage, analysis, containment, eradication, follow-up, and lesson learned), (m) third-party reliability assessment, (n) security in the management of Business Continuity aspects, and (o) compliance.
2. In this regard, the supplier undertakes:
  - to ensure processing of information according to the level of classification in terms of confidentiality;
  - not to infringe on the proprietary rights of DB's or third parties' data, software, technical documentation, and ICT resources;
  - to perform backup activities (databases, transactions, application and system logs), allowing DB to have access to backups performed where they relate to data pertinent to supplier performance;
  - to internally allocate tasks and responsibilities pertaining to security safeguards (referring to key internal and external threats) for the protection of data, applications and systems;
  - to put in place appropriate tracking measures to ensure accountability and reconstructability of operations performed, at least with respect to critical operations and access to confidential data;
  - to communicate, if requested, the location of data centers and the number of persons with access to confidential data;
  - to periodically carry out appropriate vulnerability assessments and/or penetration tests, communicating to DB the outcome of such activities and sharing with the same the corresponding recovery plan (in terms of procedures, timing and monitoring);
  - to allow DB, directly or through a third party, to verify compliance with contractual security agreements and/or to complete the verification questionnaire, transmitting a copy within 10 (ten) days of the request;
  - to communicate any information security and business continuity incidents of the managed services, in order to allow the activation of management or emergency procedures, recognising that, otherwise, the severity of its breach may result in express termination pursuant to Article 1456 of the Civil Code, in addition to compensation for consequential damages;
  - having concluded all relationships with DB, to eliminate confidential data in its systems or media, providing evidence and documentation attesting to such elimination.

#### **Article 13. GENERAL PROVISIONS.**

1. The overall understanding between the parties shall consist of the contents of the Contract, the respective attachments, any additional orders, and these general conditions.

2. The parties undertake to retain all documents related to the Contract and its performance for **5 (five) years** and to make them available to the other party within **10 (ten) days** of the request.
3. Each party may not use the other party's trade name, trademark, logo and any other distinctive sign for commercial and/or advertising purposes without written permission.
4. The Contract does not create any employment, corporate or, in general, partnership relationship between the parties.
5. The parties do not exercise any managerial or hierarchical power over the other party's employees and/or contractors.
6. Each Contract cancels and supersedes any previous verbal and/or written agreement between the parties.
7. The invalidity and/or ineffectiveness of one or more clauses of the Contract shall not imply the invalidity or ineffectiveness of the entire contract.
8. Failure to exercise a right or faculty arising from the law or from the Contract concluded between the parties shall not be construed as a waiver of the exercise thereof.

Pursuant to the provisions of Articles 1341 and 1342 of the Civil Code, the following provisions are specifically approved: Art. 6 (impossibility and force majeure), Art. 7 applicable law and waiver of territorial jurisdiction, Art. 10 (confidentiality obligation), Art. 11 (compliance with the 231 model, code of ethics and express termination clause) and Art 13 (right of audit).