General Cybersecurity Terms and Conditions for Suppliers and Contractors

1. Definitions

In these Terms the following **expression** shall have the following meanings:

1.1. **'Purchaser' / 'Customer'** refers to the company PBS Turbo s.r.o. that commissions the Services under the relevant contract.

1.2. **'Supplier' / 'Contractor'** refers to the Purchaser's supplier or contractor.

1.3. **'Actively Exploited Vulnerability'** means a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without the system owner's consent.

1.4. **'Exploitable Vulnerability'** means a vulnerability that can be effectively exploited by an unauthorised third party under practical operating conditions.

1.5. **'CE Marking'** means a marking by which a manufacturer declares that a product containing digital elements and the procedures specified by the manufacturer comply with the essential cybersecurity requirements set out in Annex I to the Cyber Resilience Act and other applicable Union harmonisation legislation governing its affixing.

1.6. **'Cyber Resilience Act (CRA)'** refers to EU Regulation 2024/2847, as well as all delegated acts and national implementing provisions.

1.7. **'Services'** means information and communication services, as well as telecommunications and telecommunications-based services.

1.8. **'Manufacturer of a Product With Digital Elements'** means a natural or legal person who develops or manufactures products with digital elements, or who commissions the design, development or manufacture of products with digital elements and markets them under their own name or brand, whether for payment, for monetisation or free of charge.

1.9. **'Distributor'** means a Supplier who sells, leases and/or distributes a product with digital elements to the Purchaser without being the manufacturer of the product in question.

1.10. **'Terms'** refers to these 'General Terms and Conditions on Cybersecurity for Suppliers and Contractors'.

1.11. **'Network And Information Systems'** refer to all digital systems and networks used for the provision and use of information services. These include, for example, IT infrastructures, servers, communication networks and all associated hardware and software components.

1.12. **'Product With Digital Elements'** refers to a software or hardware product and its remote data processing solutions, including software or hardware components that are placed on the market separately. 'Remote data processing' in the aforementioned sense refers to data processing taking place remotely, for which software is designed and developed by the manufacturer itself or under its responsibility, and without which the product with digital elements would be unable to fulfil one of its functions.

1.13. **'Vulnerability'** means a weakness, susceptibility or malfunction in a product with digital elements, an ICT product or an ICT service that can be exploited by a cyber threat.

1.14. **'Security Incident'** means an event that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data, or of the services offered or accessible via Network And Information Systems.

1.15. **'Software Bill of Materials'** means a record of the details and supply chain relationships of the components contained in the software elements of a product with digital elements.

1.16. **‘Systems’** are IT systems, IT networks and IT facilities and/or data and telecommunications equipment, installations, networks, lines and transmission paths, including hardware and software.

1.17. **‘Support Period’** means the period, including a specific end date, during which the Manufacturer of a Product With Digital Elements must ensure that the Vulnerability of the Product With Digital Elements are addressed effectively and in accordance with the terms and conditions.

1.18. **‘Services’** means all services agreed under the contract to be performed and supplied by the Supplier.

2. Scope

2.1. These Terms apply to all Services provided by the Supplier and form an integral part of all orders placed by the Purchaser with the Supplier, as well as a binding part of the contractual terms and conditions underlying the order.

2.2. Contractual terms and conditions relating to cyber security issued by the Supplier or third parties shall not apply unless the parties have expressly agreed to their application in writing.

2.3. Insofar as the Supplier is subject to additional statutory obligations under the CRA and/or other legislation relating to information security which go beyond the requirements set out in these Terms, such obligations shall apply in addition to the requirements specified in these Terms.

3. Information security of Product With Digital Elements

3.1. Where the Services provided by the Supplier include Products With Digital Elements and the Supplier is the manufacturer of such products, the following shall apply:

i) The Supplier shall ensure that Product With Digital Elements provide an appropriate level of state-of-the-art cybersecurity, including the minimisation of any adverse impact on the availability of other products, connected devices or Services. In particular, the Product With Digital Elements must: a) be supplied without any known Exploitable Vulnerabilities; b) be supplied with a secure default configuration and offer the option to reset the products to their original state; c) ensure that Vulnerabilities can be remedied, where appropriate through automatic security updates, d) ensure the availability of essential and basic functions, even following a Security Incident, e) provide security-related information through the logging and/or monitoring of relevant internal processes, such as access to and changes to data, Services or functions, with the option to disable this function.

ii) For the purposes of complying with clause 3.1(i), the Supplier shall carry out an assessment of the cybersecurity risks posed by products with digital elements and shall take the results of this assessment into account during the planning, design, development, manufacture, supply and maintenance phases of the products with digital elements, in order to minimise the cybersecurity risks, prevent Security Incident and minimise the impact of such Security Incident as far as possible. The Supplier shall make the results of this assessment available to the Purchaser in documented form upon request.

iii) During the Support Period (see clause 3.1 iv) in this regard) (including, but not limited to, development, manufacture, delivery and maintenance), the Supplier shall, free of charge, implement and maintain appropriate standards, processes, methods and other measures required by the CRA to prevent, identify, assess and remedy any Vulnerabilities in the Product With Digital Elements. The Supplier shall immediately notify the Purchaser of any Vulnerabilities of which the Supplier is aware or ought to be aware prior to delivery of the Product With Digital Elements, or of which the Supplier becomes aware during the Support Period, including feasible mitigation measures (e.g. configuration options, patches). This applies in particular to Product With Digital Elements or components thereof that are intended for incorporation into the Purchaser’s products.

iv) Prior to the conclusion of the contract, the Supplier shall specify the Support Period during which it will fulfil its obligations to address Vulnerabilities in accordance with clause 3.1 iii). The duration of the Support Period shall correspond at least to the usual Service life of comparable products, unless expressly agreed otherwise in writing.

v) The Supplier shall provide the Purchaser, free of charge, with a complete Software Bill of Materials in a standard, machine-readable format. The Software Bill of Materials must uniquely identify all software components contained in the Product With Digital Elements provided, including those from third parties, and specify the respective version designation. It shall be provided no later than upon handover of the products with digital elements and, subsequently, in the event of any significant changes or updates that affect the Software Bill of Materials.

vi) Upon request, the Supplier shall immediately provide the Purchaser with all documents and information necessary to enable the Purchaser to demonstrate the conformity of the Product With Digital Elements, as components of the Purchaser's own products, with statutory requirements. Furthermore, clause 4.5 shall apply mutatis mutandis. Insofar as the Supplier, as a manufacturer, is subject to the CRA, the Supplier shall, at the Purchaser's request, make the technical documentation within the meaning of Article 31 of the CRA available to the Purchaser free of charge.

3.2. Where the Services provided by the Supplier comprise Product With Digital Elements and the Supplier is a distributor of such Product With Digital Elements, the following shall apply:

i) The following provisions in accordance with Clause 3.2 replace the preceding provisions in accordance with Clause 3.1.

ii) The Supplier shall ensure that its contracts with its subcontractors guarantee compliance with the requirements set out in Clause 3.1 for Manufacturers of Product With Digital Elements within its supply chain.

iii) The Supplier shall verify, on the basis of the information available to it, that

(a) the Product With Digital Elements which it supplies to the Purchaser comply with the requirements of clause 3.1(i) and

(b) the procedures laid down by the Manufacturer of the Product With Digital Elements meet the requirements of clause 3.1(iii) in each case.

iv) The Supplier shall ensure that the Product With Digital Elements supplied to the Purchaser bear the CE Marking and have not been subjected to any modification that would compromise their conformity with the CRA.

v) If the Supplier is of the opinion or has reason to believe that a Product With Digital Elements or the procedures specified by the manufacturer do not meet the requirements of clauses 3.1(i) and/or 3.1(iii), the Supplier shall not make the product available to the Purchaser until such time as the conformity of that product and the procedures specified by the manufacturer with the aforementioned requirements has been established. If the Product With Digital Elements poses a significant cybersecurity risk, the Supplier shall immediately inform the Purchaser and the manufacturer thereof. Furthermore, the Supplier shall ensure that the necessary corrective measures are taken without delay to bring the product into conformity with the aforementioned requirements or, where appropriate, to withdraw the product from the market or recall it. In the event of corrective measures or a recall, the Supplier shall cooperate fully and free of charge with the Purchaser and the competent authorities, including the replacement of non-compliant Product With Digital Elements.

vi) Upon request, the Distributor shall immediately provide the Purchaser with all documents and information received from his subcontractors that are necessary to enable the Purchaser to demonstrate the conformity of the Product With Digital Elements, as

components of the Purchaser's own products, with statutory requirements. Furthermore, clause 4.5 shall apply mutatis mutandis.

3.3. The Supplier hereby declares that the Product With Digital Elements included in the Services provided by the Supplier:

i) has successfully undergone respective conformity assessment according to the statutory requirements;

ii) has no records in the European Vulnerability database or other publicly accessible Vulnerability databases.

For the purposes of demonstrating compliance with the clause 3.3. i), the Supplier shall upon handover of the Product With Digital Elements provide the Purchaser with respective declaration of conformity and any subsequent updates thereto, no later than immediately upon their issue.

3.4. The Supplier shall provide the Purchaser, free of charge, with the information and instructions set out in Annex II of the CRA no later than upon handover of the Product With Digital Elements in connection with the Services provided.

3.5. With regard to claims and demands asserted by third parties on account of a breach by the Supplier of the obligations set out in this section of these Terms (Clause 3), Clause 4.6 shall apply mutatis mutandis.

3.6. Clause 4.8 shall apply mutatis mutandis to any notifications from the Supplier relating to obligations or matters governed by this section of these Terms.

3.7. With regard to the Purchaser's monitoring of the Supplier's compliance with contractual and/or statutory information security obligations, Clause 4.9 shall apply mutatis mutandis. Furthermore, the Purchaser is entitled at any time to test the Product With Digital Elements, either itself or through third parties – for example, by means of penetration tests – for Exploitable Vulnerabilities, in which case the Supplier shall provide the Purchaser with appropriate support.

3.8. If the Supplier breaches a material obligation under these Terms, or if the Supplier – in so far as this applies to the Supplier or to the Products With Digital Elements supplied by the Supplier – fails to meet the CRA's requirements, the Purchaser shall be entitled to terminate the relevant contract immediately and without notice, or to withdraw from the contract. Any further statutory and contractual rights of the Purchaser remain unaffected.

4. Information security of data and Network And Information Systems

4.1. The Supplier shall take appropriate and proportionate technical and organisational measures in accordance with the state of the art to protect the Purchaser's data and its Network And Information Systems, which are processed in connection with the Services provided, against unauthorised access, and to prevent or minimise the impact of Security Incident on the Purchaser. The Supplier undertakes to strictly comply with the Purchaser's information security policies communicated to the Supplier, or to apply its own policies approved in advance by the Purchaser. Where the Services include software or system development, customization, or maintenance, the Supplier shall adhere to secure software development lifecycle principles (Secure SDLC, Security by Design and Security by Default) and perform verification against known Vulnerabilities.

4.2. Upon request, the Supplier shall provide the Purchaser, in writing, with all information required by the Purchaser to carry out and document an assessment of the information security risks associated with the Services provided. This includes, in particular, information on the technical and organisational security measures implemented, a list of the ICT products, services and processes provided to Purchaser, certifications, risk assessments, details of relevant subcontractors, access arrangements and known Vulnerabilities. The Supplier shall inform the Purchaser immediately in writing of any significant changes that affect or may affect the assessment of information security risks in connection with the Services provided.

4.3. The Supplier shall notify the Purchaser without delay, and in any event within twelve (12) hours of the Supplier becoming aware of the matter, and free of charge, of all Security Incidents that have occurred or are suspected to have occurred, as well as of all Vulnerabilities discovered and/or actively exploited in the Supplier's operations or in relation to its Services and products, insofar as the Purchaser is actually affected by them or could be affected in the future. This notification shall include, to the extent known to the Supplier at that time or ascertainable with reasonable effort, at least:

i) the date and time at which the security incident or vulnerability came to the Supplier's attention;

ii) a brief description of the security incident or vulnerability, including the services, products, systems, data and locations affected or potentially affected;

iii) an assessment (1) of the actual or potential impact on the Purchaser, as well as the effects on the availability, authenticity, integrity or confidentiality of the Purchaser's data, services or network and information systems; (2) of the severity and consequences; (3) of relevant indicators of compromise; (4) of causes known to date;

iv) information on whether the security incident or vulnerability could be attributable to unlawful or malicious acts;

v) the containment and remedial measures already taken and those planned.

The Supplier shall inform the Purchaser, without being asked and on an ongoing basis, of the measures taken to investigate and remedy the Security Incident that has occurred or is suspected, or the Vulnerability that has been discovered and/or is being actively exploited. This includes all information necessary to assess the impact of the Security Incident that has occurred or is suspected, or of the Vulnerability that has been discovered and/or is being actively exploited, and to enable the Purchaser to fulfil its legal obligations, in particular in the field of information security law, at the very least, the information set out in (i) to (v).

4.4. In the event of security breaches or Vulnerabilities reported to the Supplier or which have become publicly known, the Supplier shall immediately and free of charge provide a security update or take all other measures necessary to remedy the security breaches and Vulnerabilities.

4.5. The Supplier shall, upon first request, cooperate with the supervisory authorities responsible for the Purchaser, facilitate on-site inspections by the authorities and provide the Purchaser with appropriate support in connection with official inspection measures.

4.6. The Supplier shall, upon first request, indemnify the Purchaser against all claims and demands and defend the Purchaser against all claims asserted by third parties arising from a breach of the Supplier's obligations set out in this section of these Terms (Clause 4). The Supplier shall reimburse the Purchaser for all reasonable defence costs and other damages incurred.

4.7. The Supplier shall ensure that its contracts with subcontractors impose on them essentially the same information security requirements as those applicable to the Supplier under this Section 4, and that these requirements are appropriately passed on throughout the supply chain. The Supplier shall not engage any subcontractor for the provision of Services without the prior written consent of the Purchaser. The Supplier remains fully responsible for the performance and compliance of its subcontractors.

4.8. All communications from the Supplier relating to obligations or matters governed by this section of these Terms shall be addressed to the Purchaser's contact point as follows:

a) **Security Incidents** and/or discovered and/or actively exploited **Vulnerabilities** have to be reported to Purchaser in accordance with Clause 4.3 by using the following functional E-Mail address:

b) Any other communication which **is not** the reporting of a Security Incident and/or of discovered and/or actively exploited Vulnerability in accordance with Clause 4.3 shall be addressed to the responsible purchase team member of the Purchaser with whom the Supplier is in contact for the concerned supply.

c) For its part, the Supplier must provide the Purchaser with a central point of contact, including an email address, and inform the Purchaser immediately of any changes.

4.9. The Purchaser is entitled to verify the Supplier's compliance with its contractual and/or statutory information security obligations by obtaining information and requesting evidence from the Supplier, for example in the form of industry-standard certifications and/or self-declarations from the Supplier. The Purchaser is also entitled to verify the Supplier's compliance with its contractual and/or statutory cybersecurity obligations by means of an audit or to have such an audit carried out with the assistance of a qualified third party who is bound by a duty of confidentiality towards the Purchaser regarding the Supplier's business and trade secrets. If the audit reveals a significant breach of the Supplier's information security obligations, the Supplier shall bear the costs of the audit.

4.10. Upon termination of the relevant contract, the Supplier shall immediately deactivate, remove or arrange for the deactivation or removal of all access, remote maintenance, administration, support and other access authorisations to the Purchaser's systems, Network And Information Systems, applications, interfaces or data belonging to the Purchaser without delay, or to arrange for their deactivation or removal. This includes, in particular, user and privileged accounts, service accounts, passwords, access data, certificates, tokens, as well as VPN, remote access and support access points and other technical connection artefacts. The Supplier shall, upon request, immediately confirm in writing to the Purchaser that these measures have been fully implemented and ensure that the above obligations are also fulfilled by its subcontractors and other third parties engaged. Furthermore, upon termination of the contract or upon the Purchaser's request, the Supplier shall promptly deliver to the Purchaser all data, documentation, and work results in a standard interoperable format, and subsequently permanently and securely delete or destroy all copies of the Purchaser's data, including backups, and provide a written certificate of destruction.

4.11. All data and information provided by the Purchaser or processed on its behalf remains the exclusive property of the Purchaser. The Supplier is granted only a limited, non-exclusive right to use such data strictly to the extent necessary to perform the Services. The Supplier and its personnel shall maintain strict confidentiality regarding all data, confidential information, security architecture, and the existence and terms of the contractual relationship itself. The Supplier shall not use the Purchaser as a commercial reference without prior written approval.

4.12. Any material changes to the systems, infrastructure, configurations, or procedures used in the provision of the Services must be notified to and approved by the Purchaser in advance under a formal change management procedure. The Supplier shall maintain and regularly test business continuity and disaster recovery plans (BCP/DRP) ensuring the continuous availability of the Services and the resilience of Network And Information Systems.

4.13. Insofar as the Supplier creates, adapts, or provides bespoke software code or documentation under the Services, the Purchaser acquires exclusive, unrestricted exploitation and licensing rights to such code and works (including source code and documentation), unless expressly stipulated otherwise in the specific contract.