



Omniva Group

MINIMUM SUPPLIER INFORMATION SECURITY REQUIREMENTS

Version: 1

Year issued: 2026

These Minimum Supplier Information Security Requirements ("MSISR") set out the information security and data protection requirements applicable to any supplier, subcontractor, partner, or other third party ("Supplier") that, under any agreement with Omniva Group ("Omniva"), accesses, processes, transmits, or stores Omniva Data or connects to Omniva Systems (each as defined in Part 4).

The MSISR is incorporated by reference into, and forms an integral part of, each agreement between Omniva and the Supplier — whether a Professional Services Agreement, Software as a Service Agreement, Purchase Order, framework agreement, statement of work, Data Processing Agreement, or any other contract or arrangement (each, an "Agreement") — under which the Supplier provides goods or services to Omniva.

Table of Contents

1. Omniva Group: Introduction to Security Requirements	4
1.1. Purpose and Scope	4
1.2. Definitions.....	4
1.3. Order of Precedence	4
1.4. Personal Data and Cross-Border Processing.....	4
1.5. Minimum Security Requirements.....	4
1.6. Additional Controls for Specialised Services	5
1.7. Applicability	5
1.8. Supplier Group Entities	5
1.9. Right to Terminate.....	5
1.10. Governing Law.....	5
1.11. Updates.....	5
1.12. Excluded activities	5
2. Mandatory Minimum Security Requirements	6
Table A – Minimum Security Requirements	6
3. Additional Security Requirements for Specialised Engagement	20
Table B – Developing and Maintaining a Software	20
Table C – Access to Cardholder data.....	21
Table D – Hosting and Cloud Services	22
Table E – Maintaining Hardware.....	23
4. Definitions	25
Associated documents.....	28

1. Omniva Group: Introduction to Security Requirements

1.1. Purpose and Scope

Omniva Group uses, creates, and stores significant volumes of data in the course of its business operations and must ensure that the confidentiality, integrity, and availability of such data are protected at all times.

Under the Agreement between Omniva Group and the Supplier, the Supplier agrees to provide goods and/or services and to comply with the MSISR and associated Technical and Organisational Security Measures (“TOMs”). These Requirements are incorporated into and form part of the Agreement, including related agreements such as Data Processing Agreements. Therefore, by entering into, or continuing performance under, any Agreement, the Supplier agrees to comply with the version of the MSISR in effect as of the effective date of that Agreement, except as expressly modified in writing within the Agreement itself.

No separate signature or execution of the MSISR is required. The Supplier's agreement to be bound by the MSISR is evidenced by its entry into, or continued performance under, any Agreement.

MSISR are designed to vary depending on the level of risk the Supplier presents to Omniva, considering factors such as:

- the type of Omniva Data processed,
- network connectivity,
- products and services provided, and
- data availability and resiliency needs.

1.2. Definitions

Capitalised terms used in this MSISR have the meanings assigned to them in the Definitions section at Part 4, unless the context requires otherwise. If the MSISR forms part of an Agreement between the Supplier and a member of Omniva Group, the definitions in the MSISR prevail over conflicting definitions elsewhere in the Agreement, but only for interpretation of the MSISR.

1.3. Order of Precedence

In the event of any conflict or inconsistency between the MSISR and the body of an Agreement (or any Data Processing Agreement or other annex), the provision that affords the higher level of security or the greater legal protection to Omniva shall prevail, unless the Agreement expressly states otherwise with specific reference to the relevant MSISR provision.

1.4. Personal Data and Cross-Border Processing

Where the Supplier processes Personal Data on behalf of Omniva Group and/or processes Personal Data outside the European Economic Area (EEA), additional requirements in accordance with applicable Data Protection Legislation will be set out in the relevant Agreement. If such additional measures overlap or conflict with the MSISR, the more stringent requirement will apply.

1.5. Minimum Security Requirements

Part 2 of the MSISR sets out the mandatory minimum security requirements. If the Supplier cannot meet these requirements, it will be unable to enter into an Agreement with Omniva Group.

1.6. Additional Controls for Specialised Services

Part 3 of the MSISR sets out additional controls with which all Suppliers should seek to comply. However, any Supplier that meets one or more of the criteria described in Part 3 must comply with these Part 3 controls of the MSISR, in addition to the requirements outline in Part 2.

1.7. Applicability

This MSISR applies to all third-party Suppliers, subcontractors, and partners (“Suppliers”) providing goods or services to any member of Omniva Group that access, process, transmit, or store Omniva Data, or connect to Omniva Systems.

1.8. Supplier Group Entities

Where the Supplier is part of a corporate group, this MSISR binds only the specific group entity that is a party to the Agreement. If another group entity (not party to the Agreement) provides services to Omniva, directly or through the contracting Supplier, that entity will be deemed a Supplier under this Agreement and must comply with the MSISR herein.

1.9. Right to Terminate

Omniva may terminate the Agreement, in whole or in part, if the Supplier:

- Fails to comply with this MSISR,
- experiences a significant security incident or breach, or
- violates applicable data protection and/or Information Security requirements.

1.10. Governing Law

This Annex is governed by the laws of the Republic of Estonia, without prejudice to applicable EU regulations.

1.11. Updates

Omniva may update the MSISR from time to time to reflect changes in applicable law, regulatory guidance, the threat landscape, or industry standards. The current version is published at Omniva public web, together with a record of prior versions. Material changes will be communicated to the Supplier in writing (including by email to the Supplier's designated contact) and will take effect thirty (30) days after such notification, unless a shorter period is required by law, by a competent authority, or to address a material security or data protection risk. The Supplier's continued performance under any Agreement after the effective date of an updated MSISR constitutes acceptance of the updated requirements.

1.12. Excluded activities

Certain excluded activities (e.g., testing of services in alpha or beta phase) require a separate written agreement before being undertaken.

2. Mandatory Minimum Security Requirements

- 1) In addition to the below mandatory minimum security requirements, the Supplier shall manage information security in accordance with the practices described in ISO 27001 (not necessarily certified) or other equivalent international standards.
- 2) Where any part of the Services are not covered by the scope of the current ISO 27001 certification, the Supplier shall at all times and upon request be able to demonstrate it has implemented controls equivalent to industry standard controls such as, but not limited to, ISO/IEC 27002, in the current valid version. If ISO 27001 or equivalent certification exists, the Supplier shall provide proof of current certification and scope statement annually.
- 3) Omniva Group shall have the right to conduct information security audits relating to the supply of Services by the Supplier. Details regarding Omniva Group's right to audit are set out below. For-cause audits may be conducted without prior notice in the event of a suspected or confirmed material incident or material non-compliance with the Agreement or MSISR.

Table A – Minimum Security Requirements

The Supplier shall comply with the following mandatory minimum security requirements:

Controls	Description
General	
G.1 Confidentiality, integrity, and availability	Supplier is responsible for preserving the confidentiality, integrity, and availability of data within its possession, preventing corruption, loss, or unauthorized alteration or disclosure of such data. The Supplier shall ensure it has appropriate controls in place (including with its agents, contractors, and sub-contractors) to protect against unauthorized or unlawful access, use, disclosure, or other processing of the data and shall remediate any material security vulnerabilities within (30) days of identification, unless otherwise agreed in writing.
G.2 System security	The Supplier ensures that any system on which it holds any Omniva Data, including back-up data, is a secure system that complies with industry's best practices and only enables access to said data in electronic form to its Personnel to the extent necessary to provide the Services.

<p>G.3 Organisation and operational Information Security</p>	<p>The Supplier shall maintain an Information Security Management System (ISMS) aligned with applicable legal, regulatory, and contractual obligations, incorporating the following core components:</p> <ol style="list-style-type: none"> 1) Governance and Policy Framework - Implement and maintain documented information security, operational, and governance policies that are subject to regular review and approval, at intervals appropriate to regulatory and business requirements, but no less than annually. These policies shall establish controls, including but not limited to segregation of duties and clearly defined roles and responsibilities, to prevent unauthorized access, disclosure, modification, or misuse of information assets. Supplier ensures that these policies are communicated to relevant personnel and enforced. 2) Technical and Operational Safeguards - Supplier implements appropriate technical and organizational measures to manage and mitigate risks related to mobile computing, remote access, malware, and system vulnerabilities. These measures include secure development practices, synchronization of system time across all relevant infrastructure, and adherence to industry-recognized standards for vulnerability assessment, patch management, and remediation. 3) Monitoring, Logging, and Incident Response - Implement appropriate mechanisms for system and security event logging, monitoring, and auditability across critical information systems. Also establish, maintain, and periodically test an incident response plan designed to detect, report, respond to, and recover from information security incidents promptly and effectively. Testing frequency and scope shall be based on risk and operational needs. 4) Business Continuity and Disaster Recovery – The Supplier agrees to implement and maintain appropriate business continuity and disaster recovery procedures to ensure the availability and resilience of its critical services and systems. These procedures shall be documented, regularly reviewed, and tested at intervals appropriate to the risks, business impact, and operational context. 5) External Collaboration and Threat Intelligence - Where necessary or as required, the Supplier shall maintain and actively engage in appropriate relationships with relevant governmental authorities, regulatory bodies, industry-specific forums, and professional associations to ensure timely access to up-to-date threat intelligence and security best practices.
---	---

<p>G.4 NIS2 and Sectoral Cybersecurity Compliance</p>	<p>The Supplier acknowledges that Omniva Group operates in a sector subject to Directive (EU) 2022/2555 ("NIS2 Directive") and its national implementing legislation (including, in Estonia, the Cybersecurity Act (<i>Küberturvalisuse seadus</i>)), and that the Supplier forms part of Omniva Group's ICT supply chain for the purposes of those obligations.</p> <p>The Supplier shall:</p> <ol style="list-style-type: none"> 1) Status disclosure - Confirm to Omniva Group on request whether the Supplier is itself within the scope of the NIS2 Directive or any equivalent national implementing legislation (and, if so, whether classified as an essential or important entity), identify the competent authority supervising the Supplier, and notify Omniva Group without undue delay of any material change to that status during the term of the Agreement. 2) Reporting cadence support - Without prejudice to IR.1 and IR.2, where an incident affecting Omniva Group may trigger Omniva Group's reporting obligations under Article 23 of the NIS2 Directive, provide the information, logs, forensic data, and cooperation reasonably required to enable Omniva Group to meet the staged reporting timelines under that Article, including the 24-hour early warning, 72-hour incident notification, any intermediate status reports required by the competent authority, and the one-month final report, in each case sufficiently in advance of Omniva Group's regulatory deadline. 3) Coordinated supply chain risk assessments - Take into account, in its supply chain security measures under ICP.8, the results of any coordinated security risk assessments of critical supply chains carried out under Article 22 of the NIS2 Directive that are relevant to the goods or services provided to Omniva Group, and cooperate with Omniva Group in implementing mitigations identified by such assessments.
Controls	Description
Information and Cyber Security Protection	
<p>ICP.1 Protecting Information</p>	<p>The Supplier agrees to implement appropriate technical and organizational measures to safeguard all personal data and other Confidential Data entrusted to it, ensuring protection throughout the entire data lifecycle — including collection and processing to storage, transmission, and disposal. The Supplier shall maintain an up-to-date inventory of such data under its control or custody, documenting its classification, purpose of use, and applicable retention periods, in accordance with applicable data protection legislation and internal data governance policies.</p>

ICP.2 Information Security Testing	<p>Where the Supplier hosts or operates any internet-exposed system; including but not limited to websites, APIs, mobile applications, or cloud services - that stores, processes, transmits, or displays personal or Confidential Data, the following requirements shall apply. In the event the Supplier enters into agreements that overlap or conflict with the requirements below, the more stringent requirements shall prevail:</p> <ol style="list-style-type: none"> 1) Security testing, including penetration testing, shall be performed by appropriately qualified and independent personnel, such as testers holding CREST, OSCP, or equivalent industry-recognised certifications. 2) A regular security testing schedule shall be maintained, with testing occurring at least annually, after any material system change, and more frequently as risk dictates. 3) The Supplier shall provide Omniva Group, within 30 days of test completion, an executive summary of the latest penetration test results for the relevant system(s), including a summary of identified vulnerabilities and their severity ratings. 4) The Supplier shall remediate identified vulnerabilities in accordance with the following timelines unless otherwise agreed: Critical within 3 business days, High within 7 business days, Medium within 30 business, low within 60 business days. 5) The Supplier shall, upon request, provide Omniva Group with a status report on remediation progress until all High and Critical vulnerabilities are resolved.
ICP.3 Human Resource Security	<p>The Supplier agrees to establish and maintain appropriate measures to mitigate people-related security risks prior to, during, and after employment, based on role criticality, access to Confidential Data and applicable legal requirements. Where applicable, the Supplier shall:</p> <ol style="list-style-type: none"> 1) Carry out background checks and screening on relevant Personnel candidates, where legally permitted and appropriate to the role; 2) Incorporate information security responsibilities into Personnel contractual agreements and HR policies, as appropriate; 3) Deliver regular information security awareness education and training in accordance with its internal schedule; 4) Maintain formal disciplinary procedures for breaches of information security policies.
ICP.4 Access control	<p>The Supplier ensures the implementation of appropriate access control measures to protect information assets and resources, based on risk and operational requirements. These measures may include, but are not limited to:</p> <ol style="list-style-type: none"> 1) Establishing and implementing access control policies and procedures that address onboarding, offboarding, and internal role changes, as well as privileged access management; 2) Providing access based on the principle of least privilege and, where operationally feasible, segregation of duties; 3) Defining and communicating user responsibilities for the use of secret authentication information (e.g., passwords, PINs, MFA); 4) Reviewing user access rights at defined regular intervals in accordance with Omniva's Group access review procedures; 5) Enforcing multi-factor authentication (MFA) as a mandatory control for: (i) all administrative and privileged accounts; (ii) all remote access to systems processing or storing Omniva Data; (iii) all access to cloud management consoles; and (iv) any direct access to Omniva Systems. Password policies

	<p>shall align with current NIST SP 800-63B guidance, including minimum length, breach-corpus checks, and prohibition of forced periodic rotation absent indicators of compromise.</p>
<p>ICP.5 Secure Information Transfer</p>	<p>The Supplier shall ensure that all transfers, transmissions, disclosures, or sharing of Omniva Group Data are performed only through secure information transfer methods and communication channels approved by Omniva Group and appropriate to the sensitivity and classification of the information.</p> <p>The Supplier shall:</p> <ol style="list-style-type: none"> 1) Use strong encryption and secure transfer protocols consistent with recognised industry standards for confidential or sensitive information in transit. 2) Use only transfer methods approved by Omniva Group, such as encrypted email, secure file transfer solutions, secure transfer protocols (e.g., SFTP, HTTPS, TLS-protected APIs), approved collaboration platforms, or secure cloud-sharing services with appropriate access controls. 3) Prohibit insecure or unauthorised transfer methods, including unencrypted email, public file-sharing services not approved by Omniva Group, insecure protocols (e.g., FTP), personal email, messaging, file-sharing, or storage accounts, and unsecured removable media. 4) Restrict access to transferred information to authorised personnel on a need-to-know basis. 5) Protect transferred information against unauthorised access, disclosure, alteration, destruction, loss, or corruption during transmission. 6) Ensure that cross-border transfers of personal data comply with applicable data protection legislation and the requirements set out in DP.8.
<p>ICP.6 Cryptography</p>	<p>The Supplier must implement cryptographic controls in alignment with industry-accepted standards and based on the sensitivity and risk profile of the information processed. In particular:</p> <ol style="list-style-type: none"> 1) Define and implement a policy outlining required encryption measures aligned with the Supplier’s information classification scheme and the associated risk levels; such encryption shall meet or exceed AES-256 for data at rest and TLS 1.2 (or higher) for data in transit, and deprecated algorithms or protocols shall be disabled. 2) Define and implement a policy governing the use, protection, and lifecycle management of cryptographic keys, in accordance with applicable standards and operational needs and ensure that keys are stored and managed in a secure hardware security module (HSM) or equivalent secure environment.
<p>ICP.7 Physical and Environmental Security</p>	<p>The Supplier shall implement appropriate measures to maintain physical security across its sites and premises (e.g., offices, data centers), based on the risk level, criticality of assets, and local operational requirements. These measures may include, but are not limited to:</p> <ol style="list-style-type: none"> 1) Securing physical perimeters and controlling points of entry, as appropriate to the facility type; 2) Applying security controls to offices, rooms, secure areas, and loading zones based on their access sensitivity; 3) Protecting critical equipment (e.g., operational technology, utilities, and power systems) where relevant and within the Suppliers control; 4) Establishing and maintaining procedures for working in or accessing secure areas.

<p>ICP.8 Supplier Relationships</p>	<p>The Supplier agrees to implement appropriate measures to manage the risks associated with its third-party Suppliers that access, process, or store Omniva's Group information assets on its behalf. These measures should be aligned with industry best practices. In particular, the Supplier shall ensure that:</p> <ol style="list-style-type: none"> 1) A documented third-party risk management programme is in place to define information security requirements and mitigation strategies, based on the criticality of the Supplier; 2) Information security requirements are established and formally agreed in contracts with third-party Suppliers handling sensitive information or systems; 3) Monitoring, review, and, where feasible and risk-justified, auditing of third-party service delivery is performed 4) Changes in third-party service provision are managed through maintenance and adjustment of relevant information security policies, procedures, and controls. 5) The Supplier shall ensure that all contractual agreements with sub-processors or sub-contractors impose obligations at least equivalent to, or stricter than, those set out in this Annex, including security, privacy, and audit rights and shall be contractually flowed down to all such third-party suppliers. 6) The Supplier shall maintain a current list of sub-processors and sub-contractors that access, process, store, or transmit personal or Confidential Data, and shall provide such list to Omniva Group on request. The Supplier shall obtain Omniva Group's prior written authorisation (which may be in the form of a general authorisation referencing the list) before engaging any new sub-processor in respect of such data, and shall give Omniva Group at least thirty (30) days' written notice of any intended addition or replacement of a sub-processor, during which Omniva Group may object on reasonable grounds (including security, regulatory, or data-transfer grounds). If Omniva Group reasonably objects and the parties cannot agree on a remediation, Omniva Group may terminate the affected Agreement, in whole or in part, without penalty.
<p>ICP.9 System Development and Maintenance</p>	<p>The Supplier shall implement appropriate information security controls across its information systems and throughout the software development lifecycle, based on system criticality and risk. These measures shall include, but are not limited to:</p> <ol style="list-style-type: none"> 1) Establishing and enforcing documented rules and procedures for the secure development of software and systems, applied consistently across development activities in a manner proportionate to risk and project scope. 2) Implementing formal change and deployment management processes to ensure that material changes are reviewed, tested, and approved prior to deployment, including secure code review conducted by appropriately qualified personnel. The Supplier agrees to take all reasonable steps to minimise any adverse impact on business-critical systems and services resulting from such deployments. 3) The Supplier agrees to Segregate development, testing, and operational environments. 4) Where the Supplier provides development services for Omniva Group, the Supplier shall provide Omniva upon request: <ol style="list-style-type: none"> a. The SBOM in a common format currently defined as SPDX, CPE or CycloneDX format, including identification of the provided product and any third-party software components and is not limited

	<p>to Open Source components. The SBOM shall include at least the following:</p> <ol style="list-style-type: none"> i. The name and version of the software components ii. Third-party licence terms and conditions (if any) iii. The original Vendor's CPE uniquely identifies the components iv. The Supplier of the components v. the download location of the component in case it is publicly available <p>b. The Supplier also agree to not share any code created under the Agreement, regardless of the stage of development, in any shared or non-private environment, such as an open access code repository, regardless of password protection.</p> <p>The Supplier shall remediate all vulnerabilities identified in development or production environments shall be remediated within the following maximum timeframes, unless otherwise agreed: Critical (CVSS 9.0–10.0) within 3 business days, High (CVSS 7.0–8.9) within 7 business days, Medium (CVSS 4.0–6.9) within 30 business days, and Low (CVSS 0.1–3.9) within 60 business days.</p>
<p>ICP.10 Business Continuity Management</p>	<p>The Supplier shall include appropriate information security continuity and resilience measures within its business continuity management system, based on the criticality of systems and the risks to business operations. These measures may include:</p> <ol style="list-style-type: none"> 1) Developing policies, processes, and plans to support the continuity of information security and its management during adverse events; 2) Conducting and documenting the results of business continuity plan tests at pre-defined intervals to assess the effectiveness of information security continuity controls 3) Implementing redundancy measures, where necessary and feasible, to maintain the availability of critical information processing facilities. 4) Following any business continuity or disaster Recovery test, the Supplier shall provide Omniva Group with a summary of results, identified gaps, and remediation actions within thirty (30) days.
<p>ICP.11 Cyber Insurance</p>	<p>Insurance Requirement</p> <p>The Supplier shall maintain valid cyber liability insurance where its annual global turnover exceeds fifty million euros (€50,000,000). The Supplier shall notify Omniva Group without undue delay upon becoming aware that its annual global turnover has reached or exceeded fifty million euros (€50,000,000) if it happens during the Agreement period and shall put the required cyber liability insurance in place within a reasonable period thereafter. In such cases, the Supplier must hold cyber insurance coverage appropriate to the scale and risk of its operations, and in any event not less than one million euros (€1,000,000) per incident, unless otherwise agreed in writing by Omniva Group</p> <ul style="list-style-type: none"> • The insurance shall cover, at a minimum, regulatory fines (where insurable), forensic investigation costs, breach notification expenses, and third-party claims arising from any Cyber Incident or Data Breach.

	<ul style="list-style-type: none"> The Supplier shall provide proof of such insurance upon request and shall notify Omniva Group without undue delay of any cancellation, lapse, material modification, or non-renewal of the policy. <p>For Suppliers with annual turnover below fifty million euros (€50,000,000), Omniva Group reserves the right to require cyber liability insurance, where justified by the nature, scope, or risk level of the services provided.</p> <p>Where the scope of services is low-risk, Omniva Group may accept lower coverage levels, provided the Supplier demonstrates that the insurance maintained is adequate and proportionate to the risks of the engagement.</p> <p>Proof and Notification</p> <p>The Supplier shall provide Omniva Group, upon request, with a valid certificate of insurance evidencing the required coverage. The Supplier shall notify Omniva Group without undue delay of any cancellation, material modification, or non-renewal of such insurance.</p> <p>The requirement for cyber liability insurance does not limit or exclude the Supplier's liabilities under this Agreement.</p>
<p>ICP.12 Artificial Intelligence and Generative AI</p>	<p>Where the Supplier uses, integrates, develops, or makes available any artificial intelligence or machine learning system ("AI System"), including generative AI, large language models, agentic systems, or AI-enabled features within other products, in connection with the goods or services provided to Omniva Group, or where the Supplier's personnel use AI Systems in the course of performing the Supplier's obligations, the following requirements apply.</p> <ol style="list-style-type: none"> Use of Omniva Data with AI Systems - The Supplier shall not, and shall ensure that its personnel and sub-suppliers do not, submit, upload, input, or otherwise expose Omniva Data (including Personal Data, Confidential Data, source code, configuration, credentials, or operational data) to any AI System unless: <ol style="list-style-type: none"> the AI System is operated by the Supplier in an environment compliant with this MSISR and any applicable Data Processing Agreement; the AI System is a third-party service that has been approved in writing by Omniva Group for the relevant use case; or the input is fully and irreversibly anonymized such that it no longer relates to Omniva Group, its customers, personnel, or operations. Public or consumer-tier generative AI services (including web-based chat interfaces, free-tier or trial offerings, and AI-enabled browser features) shall not be used with Omniva Data without prior written authorisation from Omniva Group. Training and improvement - Omniva Data shall not be used to train, fine-tune, adapt, evaluate, or otherwise improve any AI System, whether the Supplier's own or a third party's, except with Omniva Group's prior written consent specifying the permitted scope, purpose, retention, and deletion of the data and any derived model artefacts. Where consent is given, the Supplier shall ensure that model weights, embeddings, and other derived artefacts incorporating Omniva Data are subject to the same protection requirements as the underlying data.

	<ol style="list-style-type: none">4) Vendor terms and data handling - Before using any third-party AI System with Omniva Data, the Supplier shall verify that the provider's terms (i) prohibit use of inputs and outputs for training or improvement of provider models, (ii) commit to deletion of inputs and outputs within a defined retention period, (iii) provide adequate confidentiality and security commitments, and (iv) where Personal Data is involved, support the transfer mechanisms and processor obligations required under the applicable Data Processing Agreement.5) Output handling and human oversight - The Supplier shall not permit AI Systems to take consequential actions affecting Omniva Group (including code deployment to production, changes to access rights, financial transactions, communications sent on Omniva Group's behalf, or decisions producing legal or similarly significant effects on individuals) without appropriate human review or other mitigating controls. AI-generated outputs incorporated into deliverables to Omniva Group shall be reviewed for accuracy, intellectual property compliance, and inclusion of confidential or personal information before delivery.6) EU AI Act compliance - Where the Supplier acts as a provider, deployer, importer, or distributor under Regulation (EU) 2024/1689 ("EU AI Act") in respect of any AI System used in delivery to Omniva Group, the Supplier shall comply with the obligations applicable to its role. In particular, where the AI System is classified as high-risk under the EU AI Act, the Supplier shall (i) ensure conformity assessment, risk management, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness, and cybersecurity measures consistent with Chapter III of the EU AI Act; (ii) provide Omniva Group with the information required to enable Omniva Group to meet its own obligations as a deployer; and (iii) cooperate with competent authorities as required. Prohibited AI practices under Article 5 of the EU AI Act shall not be performed in connection with the goods or services provided to Omniva Group.7) Transparency and disclosure - The Supplier shall disclose to Omniva Group, on request and in advance of deployment for material use cases: the AI Systems used in delivery, the provider and hosting location of any third-party AI System, the categories of Omniva Data processed, the purposes of use, and any known material limitations, biases, or risks. Where AI Systems interact directly with natural persons on Omniva Group's behalf, the Supplier shall ensure that those persons are informed that they are interacting with an AI System, consistent with Article 50 of the EU AI Act.8) Generative AI in code and content - Where Supplier use generative AI tools to produce code, documentation, configurations, or other deliverables for Omniva Group, the Supplier remains fully responsible for the security, quality, licensing position, and originality of those deliverables, and shall ensure that no proprietary or open-source code is incorporated in breach of applicable licence terms.
--	---

Controls	Description
Information Security Incident Management	
IR.1 Response Plan	<p>The Supplier must maintain a documented Information Security Incident Response Plan, reviewed and updated periodically in accordance with Good Industry Practice. The Supplier shall respond to Information Security Incidents promptly and proportionately, based on the nature, severity, and potential impact of the incident, in alignment with its documented incident response procedures.</p> <p>The Incident Response practices shall include, at a minimum, the following</p> <ol style="list-style-type: none"> 1) Clearly documented roles and responsibilities for incident management, including escalation paths, key dependencies, and designated points of contact, appropriate to the scale and complexity of the incident; 2) Established and communicated channels for reporting actual or suspected Information Security Incidents, events, vulnerabilities, or weaknesses, regardless of their origin; 3) A structured methodology for triage, categorisation, and prioritisation of incidents, based on severity, urgency, and potential impact; 4) Post-incident review processes (e.g., lessons-learned or root cause analysis) following material or significant incidents, to support continuous improvement of the response capability; 5) Procedures for the secure documentation, handling, and preservation of incident-related evidence, where applicable, and in accordance with legal, regulatory, or forensic requirements. 6) The Supplier shall, upon request, make all relevant logs, forensic reports, and technical details necessary for Omniva Group to fulfil its regulatory obligations within 48 hours, subject to applicable confidentiality restrictions.
IR.2 Notification Requirements	<ol style="list-style-type: none"> 1. Cybersecurity Incidents <p>The Supplier shall notify Omniva Group without undue delay, and no later than 24 hours of becoming aware of any actual or suspected information incident that may affect the confidentiality, integrity, or availability of Omniva Data, Omniva Systems, or services, or the Supplier’s ability to perform under this Agreement. "Becoming aware" means the point at which the Supplier has a reasonable degree of certainty that a security incident has occurred, irrespective of whether full technical analysis is complete. Where the Supplier reasonably believes the incident may constitute a significant incident under Article 23 of the NIS2 Directive, or a personal data breach, the Supplier shall flag this in the initial notification. Updates shall be provided at intervals agreed with Omniva Group until the incident is contained, remediated, and closed.</p> 2. Personal Data Breaches <p>Where an incident involves personal data, the Supplier shall comply with General Data Protection Regulation (EU) 2016/679 ("GDPR") and, where relevant, with any Data Protection Addendum or other contractual commitments in place between the parties. Omniva Group shall be notified in parallel, to enable coordination and assessment of any mutual obligations.</p> 3. Minimum Information to be Provided <p>Initial notifications shall, to the extent available, include:</p>

	<ul style="list-style-type: none"> a. date and time of discovery and of the incident; b. circumstances and nature of the incident; c. when and how the Supplier became aware; d. actual or likely consequences of the incident; e. measures taken to address the incident, mitigate adverse effects, and prevent recurrence; f. any known or potential cross-border impact. <p>4. Regulatory or Third-Party Requests</p> <p>If the Supplier receives any request or communication from a supervisory authority, data subject, or other third party relating to an incident,</p> <ul style="list-style-type: none"> • Personal Data Matters (e.g. personal data breaches, data subject requests, or communications from data protection authorities) shall be notified to: privacy@omnivagroup.com • Cybersecurity or Other Security Matters (e.g., NIS2-related incidents, regulatory or law enforcement inquiries) shall be notified to: security@omniva.ee. <p>Where legally permissible and without prejudice to the Supplier’s own statutory obligations, the Supplier shall consult and coordinate with Omniva Group before responding.</p>
<p>IR.3 Cooperation with Customers’ Investigations</p>	<p>The Supplier shall provide reasonable cooperation to Omniva Group, in the event of an Information Security Incident. Such cooperation shall be provided to the extent reasonably necessary to support incident analysis, containment, remediation, and any required regulatory or legal reporting.</p> <p>All cooperation shall be subject to and conducted in accordance with:</p> <ol style="list-style-type: none"> 1) The Supplier’s obligations under applicable data protection legislation, including but not limited to the General Data Protection Regulation (EU) 2016/679 ("GDPR"). 2) The Supplier’s confidentiality obligations to Omniva Group; and 3) Any applicable laws, regulations, or legally binding directives. <p>Nothing in this clause shall be construed as requiring the Supplier to disclose confidential information, proprietary methods, or data belonging to other customers or unrelated third parties without a proper legal basis or prior written consent.</p>
Controls	Description
Data Protection	
<p>DP.1 Legal compliance</p>	<p>The Supplier has embedded data protection practices into their operations at all levels to ensure continued compliance with the GDPR as well as other local regulations.</p>
<p>DP.2 Purpose limitation and data minimisation</p>	<p>The Supplier declares and agrees that they collect and process Personal data only for specific, explicit and legitimate purposes, ensuring that only minimum amount of data necessary is processed and retained for those purposes (for Data retention see DP.6).</p>
<p>DP.3 Lawful basis and transparency</p>	<p>The Supplier agrees that it processes personal data on a lawful basis and provides clear, transparent information to data subjects and partners about how their data is collected, used, and shared through publicly available privacy notices.</p>

DP.4 Data breach response	The Supplier maintains a structured incident management process (see IR.1). In the event of a personal data breach, the impact is assessed without undue delay and where required notifications are made to Omniva Group, the relevant supervisory authority and affected individuals (if they have such obligation) in accordance with IR.2 and IR.3 .
DP.5 Respect for data subjects rights	The Supplier shall uphold the rights of individuals under GDPR, including: <ol style="list-style-type: none"> 1) Right to data access: The Supplier's customers have the right to access their personal data stored by the Supplier. 2) Right to data correction: The Supplier's Customers have the right to have inaccurate personal data corrected. 3) Right to Data Deletion: The Supplier's customers have the right to request the deletion of personal data held by the Supplier, subject to certain legal requirements. 4) Right to Data Portability: The Supplier's customers have the right to receive their personal data in a transferable format.
DP.6 Data retention	The Supplier agrees to retain personal data only for as long as necessary to fulfil the purpose for which it was collected, including meeting legal, regulatory or contractual requirements. Upon expiry of the retention period or termination of the Agreement, the Supplier shall securely delete, return or anonymize such personal data and provide Omniva Group with a written certificate of destruction upon request.
DP.7 Third- Party processors	When working with third-party processors: <ol style="list-style-type: none"> 1) The Supplier works only with vendors who meet GDPR compliance standards and provide sufficient guarantees regarding data protection. 2) All third-party processors of the Supplier that processes Omniva Group data are carefully selected to ensure they meet security standards that are equal to those laid out in this document or stricter (see ICP.8)
DP.8 International data transfers	Where the Supplier transfers personal data to a country outside the European Economic Area (EEA), such transfers shall be conducted in compliance with Chapter five (5) of the General Data Protection Regulation (EU) 2016/679 ("GDPR"). Specifically: <ol style="list-style-type: none"> 1) The Supplier shall implement appropriate safeguards, including but not limited to the use of Standard Contractual Clauses (SCCs) as adopted or approved by the European Commission, or other lawful transfer mechanisms as permitted under the GDPR. 2) Where applicable, the Supplier should ensure that such transfers are made to jurisdictions that are subject to a valid adequacy decision issued by the European Commission under Article 45 of the GDPR. 3) The Supplier shall conduct and document Transfer Impact Assessment (TIAs) for all transfers outside the EEA and make such documentation available to Omniva Group Upon request. 4) The supplier shall notify Omniva Group in advance of implementing any new international transfer mechanism or change to an existing mechanism that affects Omniva Group's data.

<p>DP.9 Accountability, Governance and dispute resolution</p>	<ol style="list-style-type: none"> 1) The Supplier has appointed a dedicated Data Protection Officer (DPO) in accordance with Article 37 of the General Data Protection Regulation (EU) 2016/679 (“GDPR”). The DPO is responsible for overseeing the Supplier’s data protection compliance. The Supplier shall make available to Omniva Group, the contact details of their DPO. 2) The Supplier agrees to a transparent and fair resolution of any disputes concerning the processing of personal data. In the event of a privacy-related complaint or dispute concerning the processing of personal data, the Supplier and Omniva Group seek to resolve the matter promptly and cooperatively. Where necessary, disputes may be escalated to the competent State Data Protection Authority or resolved through appropriate legal channels.
<p>Controls</p>	<p>Description</p>
<p>Audit Rights</p>	
<p>A.1 Audit Access</p>	<p>The Services and IT systems provided by the Supplier shall be subject to audit by Omniva Group (or any external auditors as Omniva Group may appoint) within reasonable written notice. Audit activities may include supplier self-assessment questionnaires, documentation review, interviews, evidence collection, process document analysis, and physical or remote audits, provided that these activities do not require access to production/Confidential Data of the Supplier and/or its customers unless explicitly authorised in writing. The Supplier shall remediate any critical or high-risk findings identified during an audit within thirty (30) days, or within an agreed timeframe, and provide Omniva Group with written confirmation of remediation completion.</p>
<p>A.2 Access limitations and</p>	<p>No Access to Production or Supplier’s confidential data - Omniva Group shall not access live production data of the Supplier’s other customers as part of a routine audit, and the Supplier may apply reasonable confidentiality and operational safeguards (including supervised access, redaction of third-party data, and execution of NDAs by auditors). However, this limitation shall not apply to: (i) access to Omniva Data wherever held, including in production environments; (ii) for-cause audits following a confirmed or reasonably suspected Information Security Incident affecting Omniva Data or Omniva Systems; (iii) audits, inspections, or information requests by a competent regulator, supervisory authority, or court; and (iv) audits required to verify remediation of previously identified Critical or High findings. The Supplier shall not unreasonably withhold, delay, or condition authorisation for such audits.</p>
<p>A.3 Audit Findings</p>	<p>The Supplier shall review and assess any audit findings or observations in accordance with its internal risk management framework. Remediation efforts shall be prioritized and implemented based on the assessed level of risk, taking into account the potential impact to Omniva’s Group, services, and the Supplier’s data protection obligations.</p>
<p>A.4 Conflict Resolution and Precedence</p>	<p>In the event of a conflict between this audit provision and any broader audit clause in the main agreement, the provisions of this section shall prevail in respect of information security audit and assurance activities, unless expressly stated otherwise.</p>

<p>A.5 Enforcement and Remedies</p>	<p>Termination for Cause – Omniva Group may terminate the Agreement immediately upon written notice if the Supplier a) materially breaches these security requirements and fails to cure such breach within 30 calendar days of written notice; or b) commits a material breach that is not reasonably capable of cure (including a confirmed data breach involving Omniva Data, repeated incidents, refusal to cooperate with an investigation under IR.3, or failure to remediate a Critical vulnerability within the IR.2/ICP.2 timelines); or c) if Omniva Group reasonably determines that continuing the relationship presents an unacceptable security risk.</p>
--	---

3. Additional Security Requirements for Specialised Engagement

Compliance with the provisions of this Part 3 is mandatory for the entire duration of any engagement in which the Supplier provides Omniva Group with one or more of the specialised services described in Tables B to E (“Specialised Services”).

For the avoidance of doubt:

- The requirements in this Part 3 are in addition to those set out in the preceding sections of this document. Where the Supplier ceases to provide Specialised Services but continues to provide other goods or services within the scope of this MSISR, Parts 1, 2, and 4 of the MSISR continue to apply for the remainder of the engagement.
- Only the provisions applicable to the specific Specialised Services performed by the Supplier shall apply.
- If the Supplier does not perform any of the Specialised Services set out in Tables B to E, these additional requirements shall not apply.

In the event of any inconsistency or conflict between the provisions in this Part 3 and those in the mandatory sections, the provision that offers the **higher level of security and/or greater legal protection to Omniva Group** shall prevail.

The Supplier shall notify Omniva Group without undue delay upon becoming aware of any non-compliance with the requirements of this Part 3. Such notification shall include details of the non-compliance, its impact, and corrective actions taken or planned. Failure to comply with this Part 3 may constitute a material breach of the Agreement and may result in suspension or termination of the engagement, without prejudice to any other remedies available to Omniva Group under the agreement or applicable law.

Table B – Developing and Maintaining a Software

Compliance with the requirements in Table B is mandatory for the full duration of any engagement in which the Supplier develops and/or maintains software for Omniva Group. In such cases, the Supplier shall, and shall ensure that Supplier:

Controls	Description
B.1 Policies and Procedures	Maintain information security policies and procedures that comply with all applicable laws, regulations, and industry standards. Ensure that all Supplier personnel follow such policies and procedures at all times.
B.2 Development Principles	Operate a documented Secure Software Development Life Cycle (SDLC) process including, at a minimum: (i) evidence of secure code reviews; (ii) periodic application penetration testing conducted by an independent specialist third party; (iii) documented remediation procedures ensuring timely resolution of all discovered high and medium risk vulnerabilities (classified using the CVSS); and (iv) a mandatory security checkpoint in the change management process.

B.3 Change Management	Implement all necessary modifications to IT systems and processes in response to changes in security requirements, ensuring that such changes do not reduce the security level below that previously in place.
B.4 Training for Development Teams	(1) Ensure that all members of the development team have received training in secure coding techniques; (2) Provide security awareness training to all Supplier personnel, including development team members working on Omniva Group projects.
B.5 Infrastructure Security	Maintain infrastructure security controls including, at a minimum: (1) timely patch management; (2) anti-malware protection; (3) system hardening; (4) strong password policies, including enforced multi-factor authentication (MFA); (5) prompt identification and remediation of security weaknesses; and (6) provision to Omniva Group, upon request (either annually or in the event of an incident), of evidence of periodic application penetration testing and remediation of discovered vulnerabilities.

If the Supplier cannot meet any of the above requirements at any time, it must inform Omniva Group without undue delay, providing a remediation plan and timeline.

Table C – Access to Cardholder data

Where the Supplier performs any services involving the storage, transmission, or processing of payment card transactions, and/or has access to Cardholder Data, whether such data is collected, transmitted, processed, or stored in the Supplier’s environment or in an Omniva-controlled environment, the Supplier shall, for the full duration of the engagement, comply with the following requirements in addition to those set out elsewhere in this document:

Controls	Description
C.1 Attestation	The Supplier shall maintain a valid PCI DSS Attestation of Compliance ("AoC") for the full duration of this Agreement. The Supplier shall provide Omniva Group with a copy of its current AoC annually upon issuance or renewal, and without undue delay upon Omniva Group’s request.
C.2 Compliance	<p>The Supplier shall remain compliant with the most current version of the PCI DSS for the full scope of systems handling PCI-applicable data and shall maintain such compliance throughout the duration of this Agreement.</p> <p>Where any subcontractor or third party engaged by the Supplier processes, accesses, stores, or manages Cardholder Data on behalf of the Supplier, the Supplier shall:</p> <ol style="list-style-type: none"> 1) obtain a valid PCI DSS AoC from such subcontractor or third party; and 2) make such AoC available to Omniva Group upon request. <p>If the Supplier becomes, or is reasonably likely to become, non-compliant with PCI DSS for any portion of the relevant systems, the Supplier shall:</p> <ol style="list-style-type: none"> 1) immediately notify Omniva Group in writing; 2) take prompt remedial action without undue delay; and

	3) provide Omniva Group with regular written status updates until compliance is restored.
C.3 Access Limitation	The Supplier shall ensure that access to Omniva Group's PCI Cardholder Data is strictly limited to authorised Supplier personnel who require such access for the performance of their contractual obligations.
C.4 Supplier Responsibility	The Supplier acknowledges and agrees that it is solely responsible for the security of PCI Cardholder Data and the PCI Cardholder Data Environment relevant to its obligations under this Agreement. The Supplier shall implement and maintain appropriate technical and organisational security measures, in accordance with PCI DSS requirements and recognised best practices, to protect such data and environment.
C.5 Indemnity	The Supplier shall indemnify, defend, and hold harmless Omniva Group from and against any and all losses, damages, liabilities, costs, fines, levies, or penalties (including regulatory penalties) arising from or related to any non-compliance with PCI DSS by the Supplier, its subcontractors, sub-processors, or personnel.

Table D – Hosting and Cloud Services

This section applies where the Supplier:

- Provides facilities hosting Omniva Group infrastructure (e.g., data centres).
- Provides infrastructure for the management and storage of Omniva Group data.
- Hosts Omniva Group's IT solutions.
- Provides professional services supporting deployment and ongoing management of externally hosted information resources (outside Omniva Group facilities).

Where any of the above services are provided, the Supplier shall comply with the following:

Controls	Description
D.1 Technical and Organisational Measures	Maintain appropriate and proportionate technical and organisational measures to protect the confidentiality, integrity, and availability of Omniva Group Data and to prevent a Data Breach. Such measures shall meet, at minimum, the standards set out in Article 32 of the GDPR . Upon request, Supplier shall provide documented evidence of the measures implemented and maintained.
D.2 Framework Compliance	Demonstrate compliance with the SOC 2 control framework (or an equivalent framework offering an equal or higher security standard). Where full certification is not in place, the Supplier shall provide a written statement identifying non-compliance areas and a remediation plan with timelines.

D.3 Compliance Review	Provide Omniva Group, at least annually, with an unqualified SOC 2 Type 2 examination report issued in accordance with applicable AICPA standards (or equivalent) by an independent, qualified auditor engaged and compensated by the Supplier.
D.4 Third-party provider audit	Where third-party systems are used to deliver services, such third parties must hold current certification against an internationally recognised standard (e.g., ISO/IEC 27001, SOC 2 Type 2).
D.5 Audit Rights	Permit Omniva Group, at no additional cost and on reasonable prior written notice, to conduct security assessments and/or audits of the Supplier’s technical and organisational security measures. The Supplier shall respond to all written requests, questionnaires, and documentation requests within agreed timelines, and facilitate access to facilities, systems, processes, and procedures as required for the audit. Valid, current SOC 2 Type 2 reports and penetration testing reports may serve as evidence of annual audit compliance.
D.6 Logging	Maintain integration-ready logging, monitoring, and remediation capabilities compatible with Omniva Group’s logging requirements.
D.7 Provider configuration	For any Omniva Group Data stored in cloud environments (including third-party IaaS, SaaS, and PaaS), implement and maintain cloud security posture management solutions to detect and automatically remediate threats, misconfigurations, misuse, and compliance violations.
D.8 Federated Authentication	Support industry-standard identity federation protocols (e.g., SAML, OpenID Connect, OAuth 2.0) to enforce authentication and access controls across SaaS and API integrations.

Table E – Maintaining Hardware

This section applies where the Supplier provides or maintains hardware products for Omniva Group. The Supplier shall implement the following measures:

Controls	Description
E.1 General Requirements	Maintain a documented Information Security Management System (ISMS) based on a recognised standard (ISO/IEC 27001 or equivalent). Have a formal risk management process, up-to-date security policies, and be responsible for subcontractor compliance with equivalent security requirements. Subcontractors must be approved by Omniva Group.
E2. Supply Chain and Development Security	Develop hardware and embedded software in accordance with secure development lifecycle (SDLC) best practices. Secure development environments with appropriate controls (firewalls, IDS/IPS, anti-malware). Maintain hardware integrity controls (e.g., tamper-evident seals, signed firmware). Provide a Software Bill of Materials (SBOM) upon request.

E3. Secure Configuration and Hardening	Deliver all hardware with secure baseline configurations; disable unnecessary services, accounts, and ports. Enforce strong authentication, prohibit hard-coded passwords, apply least privilege, meet recognised cryptography standards (NIST SP 800-131A or equivalent), and secure wireless technology in compliance with applicable standards.
E4. Vulnerability Management	Implement timely patch management for hardware, firmware, and software. Conduct and share summaries of penetration tests upon request.
E5. Remote Management and Monitoring	Ensure secure remote maintenance access, with session limits, timeouts, and audit logging. Protect and retain logs for at least 180 days; allow forwarding to Omniva Group SIEM or syslog.
E6. Personnel Security	Conduct lawful background checks, provide security training, and ensure confidentiality agreements for all personnel with access to Omniva Group assets.
E7. Physical Security and Device Handling	Maintain secure storage and servicing facilities, enforce documented chain of custody, and track assets using a formal system.
E8. Data Sanitization and Destruction	Perform sanitisation to NIST SP 800-88 (or equivalent) standards before repurposing or return. Destroy hardware securely before disposal. Provide certificates of sanitisation or destruction.
E9. Incident Response and Reporting	Maintain an incident response plan. Notify Omniva Group within 24 hours of becoming aware of a suspected or confirmed Data Breach. Fully cooperate with investigations.
E10. End-of-Life Management	Maintain a documented hardware end-of-life and obsolescence strategy, including support and secure transition plans.
E11. Auditing and Compliance	Permit Omniva Group to audit compliance. Provide annual compliance reports.
E12. Legal and Regulatory Compliance	Comply with all applicable data protection and cybersecurity laws, including but not limited to: GDPR, NIS2 Directive, and the Estonian Cybersecurity Act. Supplier is responsible for tracking legislative changes and maintaining ongoing compliance.

4. Definitions

The definitions in this Part 4 apply to the MSISR.

“Affiliate”	(i) in relation to OMNIVA Group, a legal entity which, presently or in the future, directly or indirectly, is Controlled by AS Eesti Post or under common Control with AS Eesti Post; and (ii) in relation to the Supplier, a legal entity which, presently or in the future, directly or indirectly, is Controlled by the Supplier or under common Control with the Supplier;
“Confidential Data”	<p>means any Omniva Group Data and any other information, in any form or medium (whether oral, written, electronic, visual, or otherwise), that is disclosed by or on behalf of Omniva Group to the Supplier, or to which the Supplier or Supplier Personnel obtain access in connection with the Agreement, and that either (i) is marked or otherwise identified as "confidential," "restricted," "proprietary," or with a similar designation, or (ii) by its nature, content, or the circumstances of its disclosure would reasonably be understood to be confidential. Confidential Data includes, without limitation: Personal Data; Cardholder Data; business, financial, commercial, operational, technical, and personnel information; information security, system architecture, network, configuration, and vulnerability information; credentials, cryptographic keys, certificates, and access tokens; pricing, contract, customer, partner, and sub-supplier information; trade secrets and know-how; and any back-up, derived, aggregated, or transmitted copies of any of the foregoing, throughout the entire data lifecycle from collection through destruction.</p> <p>Confidential Data does not include information that the Supplier can demonstrate by contemporaneous written records: (a) was lawfully in the Supplier's possession on a non-confidential basis prior to disclosure by Omniva Group; (b) is or becomes publicly available other than as a result of any act or omission of the Supplier or Supplier Personnel in breach of this MSISR or any other obligation of confidentiality; (c) is lawfully obtained from a third party without any obligation of confidentiality; or (d) is independently developed by the Supplier without use of, or reference to, Omniva Group's Confidential Data. For the avoidance of doubt, the foregoing exclusions do not apply to Personal Data or Cardholder Data, which remain protected at all times in accordance with applicable Data Protection Legislation and PCI DSS.</p>
“Control” or “Controlled”	the controlling entity possessing, directly or indirectly, or jointly with a third party or parties, the power to direct management and policies of the controlled entity;
“Data Protection Legislation”	means all applicable laws and regulations relating to the processing of personal data and privacy, including but not limited to the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the ePrivacy Directive 2002/58/EC (as amended), and any applicable national implementing legislation, regulations, and secondary legislation, including any amendments or replacements thereto, as well as any guidance, codes of practice, or decisions issued by a Supervisory Authority or other competent authority.
“OMNIVA Data”	all data or records of whatever nature and in whatever form relating to the business, employees, customers, Suppliers or otherwise relating to the business of OMNIVA Group, including all information, records, and digital assets — of whatever nature, format, or classification — that are owned by, relate to, or are processed on behalf of Omniva Group, including but not limited to business and operational records, Personal Data (as defined under GDPR), Cardholder Data (as defined under PCI DSS), and any

	back-up, derived, or transmitted copies thereof, across the entire data lifecycle from collection through destruction.
“OMNIVA Group”	AS Eesti Post (commercial registry code: 10328799). Omniva Group consists of AS Eesti Post as the parent company, Omniva LT, UAB and Omniva LT Sorting, UAB in Lithuania, Omniva SIA in Latvia, and Picapac OÜ in Estonia as subsidiaries. References to AS Eesti Post or any Affiliate of AS Eesti Post from time to time and a reference to Omniva Group in the MSISR shall be construed as a reference to all and any of them. It includes the relevant member of the Omniva Group that is a party to any agreement with the Supplier to which the MSISR forms part of such agreement.
“OMNIVA Group Systems”	the information technology and communication systems, including networks, hardware, software, middleware, virtual platforms, embedded technology (see definition below) and interfaces owned by or licensed to OMNIVA Group or any of its or their agents, customers or contractors;
"Embedded Technology"	embedded Technology Devices are physical objects used for monitoring and / or affecting the physical environment with sensors, data storage and / or processing ability, internal software, and / or the ability to exchange data with other devices and systems over an IT network.
“GDPR”	Regulation (EU) 2016/679 (the General Data Protection Regulation), including any amendments and updates in force from time to time;
“Good Industry Practice”	in respect of any activity, performing that activity effectively, reliably and professionally using the degree of skill, care, diligence, prudence, foresight and judgement which would reasonably be expected from a skilled and experienced operator of similar standing engaged in the provision of similar services;
“IaaS”	means Infrastructure as a Service;
"Information Security"	means the protection and the preservation of the confidentiality, integrity and availability of Omniva Group Data and Information Systems, compliance with all applicable data protection regulations with respect to the storage, transmission and processing of information and information systems.
“Information Security Incident”	<ol style="list-style-type: none"> 1) any actual compromise of the confidentiality, integrity or availability of OMNIVA Group Data; 2) any actual compromise of, or unauthorized access to, any system that Processes OMNIVA Group Data that presents a risk to the confidentiality, integrity or availability of OMNIVA Group Data; or 3) receipt of a complaint, report, or other information regarding the potential compromise or exposure of OMNIVA Group Data Processed by Supplier;
“Internet”	the global network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols;
“ISO 27000 series”	means a collection of international standards of the International Organization for Standardization (ISO) that define security measures for the protection of IT ;
"Log(s)"	means the record of security events.

"MFA"	means Multi Factor Authentication
"MSISR"	Omniva Groups Minimum Information Security Requirements for Suppliers;
"NIST"	means National Institute of Standards and Technology.
"Partner"	Suppliers, including subcontractors, i.e. all companies who do business with any company or division of OMNIVA Group;
"PaaS"	means Platform as a Service.
„PCI“	means Payment Card Industry
„PCI-DSS“	Refers to the current version of the Payment card industry (PCI) Data Security Standard (DSS), its supporting documentation and any subsequent version(s) of said standard published by the PCI Security Standards Council or its successor(s).
“Process” or “Processing” or “Processes”	any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
“Personal Data”	any personal data (as such term is defined in Data Protection Legislation) which is subject to the applicable Data Protection Legislation;
"SaaS"	means Software as a Service
"SBOM"	means Software Bill of Materials.
“Secure Software Development Life Cycle (Secure SDLC)”	A documented software development process that integrates security practices and activities at each stage of the development lifecycle, including but not limited to: requirements analysis, design, development, testing, deployment, and maintenance, with the objective of preventing, detecting, and remediating security vulnerabilities.
“Services”	any or all of the services provided by the Supplier;
"SIEM"	means Security Information and Event Management.
"SOC 2"	is a security framework that specifies how organisations should protect customer data from unauthorised access, security incidents, and other vulnerabilities.
"Specialised Services"	The specific categories of services described in Part 3 of this document, which may include, but are not limited to, software development, software maintenance, system integration, or other technology-related services requiring additional security requirements beyond the general mandatory controls.

“Supervisory Authority” or “Competent Supervisory Authority”	means an independent public authority which is established by a Member State pursuant to Article 51 of the General Data Protection Regulation (EU) 2016/679 (“GDPR”) and is responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. The term includes any applicable data protection authority with jurisdiction over the Parties’ processing of Personal Data under the Agreement.
“Supplier”	the counterparty to any agreement with OMNIVA Group to which the MSISR forms part of such agreement;
“Supplier Personnel”	the employees, contractors and other individuals who are engaged by the Supplier, its Affiliates or their subcontractors from time to time to meet the Supplier’s obligations;
“Web based applications”	A web-based application is a computer program that utilizes web browsers and / or web technologies (HTML, API and others) to perform tasks over a computer network.

Associated documents

- Code of Conduct: <https://www.omnivagroup.com/policies/>
- Data Processing Addendum
- Principles for Processing of Customer data: AS Eesti Post (Estonia), Omniva SIA (Latvia), Omniva LT UAB (Lithuania): <https://www.omnivagroup.com/policies>
- Procurement Plan: <https://www.omnivagroup.com/procurement/>