Version: May 2026

Data Processing Agreement Boltrics Professionals B.V.

Comprised of:

Part 1. Data Pro Statement

Part 2. Standard clauses for data processing

NLdigital version march 2025

Part 1: Data Pro Statement

Along with the Standard Clauses for Data Processing, this Data Pro Statement constitutes the data processing agreement for the product or service provided by the company that has drawn up this Data Pro Statement.

General information

1. **This Data Pro Statement was drawn up by the following data processor (verwerker):**
   Boltrics Professionals B.V. (hereinafter also "**Boltrics**"), Galileïlaan 23b, 6716 BP Ede, The Netherlands, KVK: 08156615, VAT number: NL818818074B01. As of September 2026, Boltrics Professionals B.V. will be located at Galvanistraat 2, 6716 AE Ede, The Netherlands.

   If you have any queries about this Data Pro Statement or data protection in general, please contact:

   - *For questions regarding this Data Pro Statement, please contact: Senior Legal Counsel reachable at legal@boltrics.nl, telephone number: +31 318 742 550.*
   - *For security questions, please contact: Security reachable at security@boltrics.nl, telephone number: T: +31 318 742 550.*

   To the extent Boltrics processes personal data as a controller, Boltrics' Privacy Statement applies. The provisions of this Data Processing Agreement apply only insofar as Boltrics acts as a processor within the meaning of the GDPR.

2. **This Data Pro Statement shall enter into force in May 2026**
   We regularly revise the security measures described in this Data Pro Statement to safeguard that we are always prepared and up to date with regard to data protection. If this document is updated, we shall notify you of the revised versions through our regular channels.

3. **This Data Pro Statement applies to the following products and services provided by data processor**
   Boltrics' software solutions for logistics service providers consisting of:
   - Boltrics' 3PL software, with Microsoft Dynamics 365 Business Central underpinning the software, which software is modular in nature (the "**Boltrics Software**");
   - Boltrics Software + Datahub;
   - Boltrics Software + Web portal;
   - Boltrics Software + Boltrics App Platform;

   as well as support and maintenance services in relation to the Boltrics Software and other (IT) services provided by Boltrics to its customers as agreed between the Parties.

4. **Description of product(s)/service(s)**

   Boltrics Software
   Boltrics Software is a Software as a Service (SaaS) application that offers logistics service providers a solution for automating various business processes. Microsoft Business Central lies at the heart of Boltrics Software. Boltrics Software is modular in structure. The software offers WMS, TMS, Freight Forwarding, Finance, Customs, EDI solution (DataHub) and Customer Portal (Web Portal). For more information about

Boltrics Software and its various modules, please refer to the following link: Logistics software: WMS, TMS, FMS, Customs, Finance & CRM | Boltrics.

Boltrics Software + DataHub

DataHub is an EDI solution that connects to Microsoft Business Central. More information about DataHub can be found under the following link: Easily realize EDI integrations with Boltrics' DataHub | Boltrics.

Boltrics Software + Web Portal

Web Portal is a tool that allows customers to unlock data related to inventory management, shipments, quality control, wefts, reports, damages, results and invoices, among others, to their customers. More information about Web Portal can be found under the following link: Customer portal - Boltrics.

Boltrics Software + Boltrics App Platform

With Boltrics App Platform, customers can extend the capabilities of their logistics software to any mobile device. The App Platform is a single application center for all customer mobile devices. For more information about Boltrics App Platform, please refer to the following link App Platform - Boltrics.

Supporting (IT) services

Besides supplying software, Boltrics offers services such as implementation services, maintenance, support and consultancy work related to its software. For more information on Boltrics' support work, please refer to the following link Support, get your Boltrics solution back on track | Boltrics.

5. Intended use

Product/service is designed and built to process the following types of data:

General

Our products are designed and equipped to process the following data: All data to perform and support logistics processes in the areas of WMS, TMS, Freight Forwarding, Finance and Customs.
personal data provided to Boltrics in the context of an order granted to Boltrics for the provision of its services is used exclusively for the performance of the agreement entered into by you with Boltrics and other documented instructions from you as data controller, unless a provision of Union or Member State law applicable to Boltrics as a processor requires otherwise. In particular, Boltrics' processing consists of making its applications available, including the data entered and generated by you therein. In principle, Boltrics will not add, modify or delete personal data without instruction; automated changes may occur during updates or upgrades where the data structure is technically modified as part of the normal operation of the software.
Within the Boltrics Software, you may capture various types of personal data. Boltrics understands that you may enter such personal data, including any personal data fields or categories created by you, and that Boltrics will process such data solely on your behalf. You are responsible for assessing whether the purpose and nature of the processing are appropriate for the use of the Boltrics Software. You warrant to Boltrics that the processing of personal data as commissioned to Boltrics and/or carried out by you using the Boltrics Software does not violate applicable laws or regulations and does not infringe the rights of data subjects or third parties.
In principle, Boltrics processes only the following categories of personal data in connection with the formation and execution of the agreement or as registered by you in the course of using the Boltrics

Software: names, business contact details such as e-mail addresses and telephone numbers, and identification or technical data such as login credentials, user identifiers and IP addresses. Data subjects may include representatives and employees of your organization, authorized end users of the Boltrics Software, and, where applicable, your customers, suppliers or contractors. Prior to providing personal data to Boltrics, you shall obtain all required consents or authorizations from data subjects or third parties in accordance with applicable data protection laws.

Use of automated tools and AI

Boltrics may, in the performance of the Agreement, use automated tools and technologies, including artificial intelligence, machine-learning based solutions, or comparable technologies, including those provided by third parties.

Such technologies are used to support the processing activities carried out on behalf of the Customer and are not intended to independently determine the purposes or essential means of the processing.

Any output generated by such technologies is intended to be used in a supportive manner and is not intended, in itself, to produce legal or similarly significant effects for data subjects. The extent to which such output is used and relied upon remains subject to the Customer's use of the services and configuration thereof. Boltrics does not warrant the accuracy, completeness or suitability of any output generated by such technologies. Where relevant, appropriate human oversight can be applied.

Any such processing shall take place within the scope of Boltrics' role as processor and in accordance with the Customer's written instructions and this Data Processing Agreement.

Boltrics Software

Boltrics Software is designed and set up taking into account the following data considerations: customers manage their own data. Boltrics, as processor, does not control the Customer's data and will only access such data, where technically possible, at the Customer's request and/or where reasonably necessary for the performance of the agreement, including the performance, maintenance, security or support of the Boltrics Software. In principle, a limited number of Boltrics employees can access customer data for installation, maintenance and support purposes. They will, unless agreed otherwise or mandatory law requires otherwise, not change or add personal data, but only view it to solve a technical problem.

Boltrics Software is hosted in Microsoft Azure. By using the Microsoft product Business Central underlying Boltrics Software or other Microsoft products, personal data are also collected and processed by Microsoft. Microsoft may process personal data in accordance with its applicable terms and data protection commitments, including where the Customer accepts the Microsoft Customer Agreement or other relevant Microsoft terms. More information on the intended use and type of personal data processed by Microsoft can be found at Microsoft-privacyverklaring – Microsoft privacy[1] and more specifically in the customer agreement of Microsoft entered into with you: Licensing Documents (microsoft.com).[2]

Boltrics Software + DataHub

DataHub is designed and set up taking into account the following data considerations: customers manage their own data. Boltrics, as processor, does not control the Customer's data and will only access such data, where technically possible, at the Customer's request and/or where reasonably necessary for the

[1] See Microsoft Privacy Statement - Microsoft privacy for English language. Privacy statement accessed 22-02-2024, subject to and subject to change by Microsoft. Boltrics cannot make any representations, promises or warranties on behalf of Microsoft.
[2] Subject to change by Microsoft.

performance of the agreement, including the performance, maintenance, security or support of the Boltrics Software. In principle, a limited number of Boltrics employees can access customer data for installation, maintenance and support purposes. Unless otherwise agreed or mandatory law requires otherwise, they will not change or add personal data, but only view it to solve a technical problem.

Boltrics Software + Web portal

Web portal was designed and set up taking into account the following data considerations: customers manage their own data. All data from the Business Central environment is stored in the same continental region where the Business Central environment is hosted. Metadata about your company and environment, including the specified company name and logo, as well as pseudonymized data about users, may also be stored in other regions. Boltrics, as processor, does not control the Customer's data and will only access such data, where technically possible, at the Customer's request and/or where reasonably necessary for the performance of the agreement, including the performance, maintenance, security or support of the Boltrics Software. In principle, a limited number of Boltrics employees can access customer data for installation, maintenance and support purposes. Unless otherwise agreed or mandatory law requires otherwise, they will not change or add personal data, but only view it to solve a technical problem.

Boltrics Software + Boltrics App Platform

Boltrics App Platform is designed and set up taking into account the following data considerations: customers manage their own data. Boltrics, as processor, does not control the Customer's data and will only access such data, where technically possible, at the Customer's request and/or where reasonably necessary for the performance of the agreement, including the performance, maintenance, security or support of the Boltrics Software. Data is processed in a manner intended to prevent direct identification of individuals, such as through anonymization or pseudonymization, where applicable. In principle, a limited number of Boltrics employees can access customer data for installation, maintenance and support purposes. Unless otherwise agreed or mandatory law prescribes otherwise, they will not change or add personal data, but only access it to solve a technical problem. The App Platform stores metadata about your environment in the same continental region as your Business Central environment and possibly in other regions as well.

Support and other (IT)-services

The following activities are carried out by Boltrics in its capacity as data processor, on behalf of and under the instructions of the customer:

- Where necessary for the performance of the services, Boltrics may share relevant contact details with its suppliers or sub-processors. Such sharing shall take place only to the extent necessary and in accordance with this Data Processing Agreement and applicable data protection laws.
- The Consultancy team processes your data to effectively address your issues.
- The Consultancy team processes your data to effectively implement our software solutions with you. This may include, for example, name and contact details of core users and steering committee members.
- The Integration department processes your data to effectively create integrations with your partners. If you provide personal data from these partners, your customers or other suppliers, including IT service providers, to Boltrics, you are responsible for ensuring that you have a valid legal basis and all required authorizations to provide such Personal Data to Boltrics.
- The Support Department processes your personal data to effectively resolve incidents.

- Boltrics IT Operations ("**Azure/Entra administrator(s)**") has full access to customer data for: installing a new version; implementing patches and hotfixes; and managing backups related to the applications that Boltrics manages. With approval from the Team Lead at Boltrics, employees of the Product Development Department may also be granted temporary access to customer data in necessary cases.

  Please provide us with the appropriate contact information for each issue.

- The processing of special categories of personal data or data regarding criminal convictions and offences or personal numbers issued by the government was not taken into account for this product/service.
  Customer needs to determine whether or not to use the aforementioned product/service to process such data.

6. Privacy by design/privacy by default

Boltrics uses standard Microsoft designs in its products to apply privacy by design. Microsoft applies privacy by design and privacy by default in its technical and business functions. More information can be found here General Data Protection Regulation - Microsoft GDPR | Microsoft Learn.[3] More on Microsoft Business Central security can be found here Microsoft Business Central security | Learn Boltrics (boltrics.com).
Boltrics Software and the underlying Microsoft Business Central database is run on Microsoft Azure. More about Microsoft Azure security can be found here Gegevensbescherming met Microsoft-privacyprincipes | Microsoft Vertrouwenscentrum[4].
For Boltrics' applications (other than Microsoft Business Central) or those managed by Boltrics:

- Applications outside Business Central contain as little data as possible. Whenever possible, data is stored exclusively in Business Central. Personal data is pseudonymized or anonymized whenever possible. Personal data in Business Central will be stored in the continental region where the Business Central environment is hosted. Data that allows access to data in Business Central (such as authentication credentials) is stored in a designated additional secure storage in Azure.
- Data stored outside Business Central is viewable from Business Central and can be managed from Business Central by the client.
- Blob data (actual messages), credentials and connection data are stored encrypted in DataHub.
- Data that Boltrics collects for statistical purposes and proactive troubleshooting is processed pseudonymously.
- Personal data is not pseudonymized where/when it is needed for the primary processes (contact with end users).
- Privacy controls are built directly into the system, process or business practice.
- Data in Business Central, App Platform, Web Portal and DataHub is encrypted at rest and in transit, in all layers of the architecture and throughout the data lifecycle.
- Boltrics has - unless otherwise agreed/agreed with the customer - by default implemented the most privacy-friendly settings in accordance with its customer's instructions. In addition, where necessary, the respective customer determines which data must be entered or which fields are made available and it is the customer himself who uploads data and enters, deletes and modifies data.

[3] General Data Protection Regulation - Microsoft GDPR | Microsoft Learn accessed 22-02-2024, subject to change. Boltrics cannot make any representations, promises or warranties on behalf of Microsoft.
[4] Data Protection with Microsoft Privacy Principles | Microsoft Trust Center, subject to change.

7. **Data processor uses the Data Processing Standard Clauses for data processing, which are attached to the Agreement as an addendum.**

8. **Data Processor processes personal data (partially) outside the EU/EEA. Data processor has ensured in the following way that the personal data shall be protected to an appropriate standard:**

Data Processor may process personal data within and outside the EU/EEA.
Data Processor may rely on subprocessors and underlying service providers for the provision of the services. This may involve the processing of personal data in multiple jurisdictions, including outside the EU/EEA.
Where personal data is processed outside the EU/EEA, such processing shall take place in accordance with Chapter V of the GDPR.
Transfers of personal data to countries outside the EU/EEA shall only take place where at least one of the following conditions is met:

- the European Commission has issued an adequacy decision for the relevant country, territory or sector;
- appropriate safeguards are in place in accordance with Article 46 GDPR, such as the Standard Contractual Clauses (SCCs); or
- a derogation pursuant to Article 49 GDPR applies.

Tenant selection
The Customer is responsible for selecting and instructing the use of the tenant for the provision and receipt of the services by Boltrics.
The Customer acknowledges that such selection may result in the processing of personal data outside the EU/EEA and remains fully responsible for determining the appropriate data residency; selecting and configuring the relevant tenant, region or environment; and ensuring that such use complies with applicable data protection laws.
To the extent that access to Personal Data from outside the EU/EEA (for example by Customer or its users) qualifies as a transfer, Customer is responsible for ensuring that such transfer complies with applicable data protection laws.
Data Processor may, where required, inform Customer if an instruction is, in its reasonable opinion, in violation of applicable data protection laws.

9. **Data processor uses the following sub-processors:**

a. Microsoft B.V., Evert van de Beekstraat 354, 1118 CZ Schiphol, The Netherlands;
b. Microsoft Ireland Operations Limited, One Microsoft Place, Dublin 18, Ireland;

Please see the table below.

Sub-processor	Services	Processing location	Transfer mechanism
Microsoft	Azure, Business Central, Power Platform, Microsoft 365 and related platform services	EU/EEA and other jurisdictions depending on tenant, region and Microsoft services	Adequacy decision, SCCs and/or other valid transfer mechanism under Chapter V GDPR

Microsoft services are used for the provision of the services, including but not limited to Azure, Power Platform, and Microsoft 365.

Depending on the specific customer setup and contractual arrangements, Microsoft may act as a sub-processor to Boltrics, as a processor directly to the customer, or as an independent controller, depending on the specific processing activity and customer configuration. In many cases, customers maintain their own Microsoft tenant and contract directly with Microsoft. In such cases, Microsoft's role and responsibilities are governed by the customer's agreement concluded with Microsoft and/or the relavant applicable Microsoft terms. Further information on Microsoft's privacy and security practices can be found in the Microsoft Privacy Statement[5] and the Microsoft Trust Center.

Hosting and service architecture

Boltrics provides its services through a combination of cloud-based and customer-managed components. Boltrics processes personal data only within the scope of the services agreed with the Customer and in accordance with the instructions of the Customer.

Cloud-hosted services

Boltrics Software is built on Microsoft Dynamics 365 Business Central. Boltrics Software and its applications, including DataHub, the Boltrics App Platform and the Web Portal, are hosted on Microsoft Azure infrastructure. In this context, Boltrics procures platform and infrastructure services (PaaS/IaaS) from Microsoft and provides its solutions to customers as Software-as-a-Service (SaaS).
The location of data storage and processing within Microsoft Azure is determined by the Microsoft tenant configuration and the region selected by or on behalf of the Customer. Boltrics processes personal aata within the environment designated by the Customer and does not independently determine the tenant location.

Personal data collected and/or processed by Microsoft may be stored and processed in the Customer's region, in the United States, and in other jurisdictions where Microsoft or its affiliates, subsidiaries, or service providers operate, in accordance with Microsoft's applicable terms and data protection commitments.

[5] Microsoft Privacy Statement – Microsoft privacy subject to change.

Customer-managed components

Certain peripheral components and services (such as print services, telematics proxies, voice agents and other microservices) may be installed on infrastructure managed by the Customer. These components are not internet-facing and are operated within the Customer's own IT environment, for which the Customer remains responsible.

Development services

Boltrics may engage employees, contractors, temporary personnel and development partners acting under the authority, responsibility and instructions of Boltrics for development, maintenance and support activities related to the services. Such persons are subject to appropriate confidentiality, security and data protection obligations.To the extent such parties process Personal Data on behalf of Boltrics and qualify as sub-processors within the meaning of the GDPR, they shall be engaged in accordance with this Data Processing Agreement and applicable data protection laws.

10. **Data processor shall support their clients in the following way when they receive requests from data subjects:**
You can create a ticket via support with requests for an export, modification or deletion of data or submit a request to do so via security@boltrics.nl. If the request involves costs, you will be informed in advance. Boltrics will notify you of any requests received directly from data subjects regarding data subjects' rights under applicable privacy laws, including but not limited to requests for access, rectification, deletion, restriction of processing or transfer of personal data. Boltrics will only comply with such a request if you have instructed Boltrics in writing to do so.

11. **Data processor shall support their clients with Data Protection Impact Assessments (DPIA) in the following manner:**
Where the Customer is required to do so, the Data Processor shall, upon reasonable request, provide reasonable assistance with a Data Protection Impact Assessment (DPIA). Boltrics will cooperate with Data Privacy Impact Assessments in the following manner:
    - You will contact Boltrics by email at security@boltrics.nl
    - You make clear what assistance you require from Boltrics
    - Boltrics will provide the desired cooperation as soon as possible and may charge additional costs in accordance with its usual hourly rate.

12. **Once the Agreement with a client has been terminated, data processor shall delete personal data it processes on behalf of client within *three months*, in such a manner that the data can no longer be used and shall be rendered inaccessible,** unless retention of certain personal data is required or reasonably necessary pursuant to applicable law, the agreement concluded with the Customer, this data Processing Agreement, Boltrics' Privacy Statement, or for purposes related to security, backup, audit, compliance, dispute handling, the establishment, exercise or defence of legal claims, or the continuity and integrity of the services.
If, in the Customer's judgment as controller of the personal data, certain personal data should no longer be retained and applicable laws do not provide otherwise, Boltrics shall, upon written request of the Customer, delete the specified personal data and certify such deletion.

13. **Returning of personal data once the Agreement has been terminated**

At Customer's written request, and where technically feasible, Boltrics shall return such personal data in a commonly used and machine-readable format, subject to applicable fees.
These obligations do not apply to the extent Boltrics is required to retain personal data under statutory retention obligations or where Boltrics acts as controller. Further details are set out in Article 30 (Obligations upon termination) of *NLdigital Terms 2025*.

For the avoidance of doubt, the obligations set out in Articles 12 and 13 apply only to personal data processed by Boltrics in the context of the Boltrics Software and related services, within components and services that are under the direct control of Boltrics. Personal data stored or otherwise processed within Microsoft products and services (including, but not limited to, Microsoft Dynamics 365 Business Central and Azure), including data residing in the Customer's tenant, is subject to the applicable terms and conditions of Microsoft and any agreements between the Customer and Microsoft. Boltrics does not determine the storage location, retention, or deletion of such data and does not have independent control over such environments. To the extent Boltrics has access to such personal data for implementation, support or service purposes, such access is limited, temporary in nature, and subject to the applicable Microsoft terms and technical limitations. Such personal data remains under the control and responsibility of the Customer and/or Microsoft, and falls outside the scope of the return and deletion obligations referred to in Articles 12 and 13.

Security policy

14. **Data processor has implemented the following security measures to protect their product or service:**

Boltrics implements and maintains appropriate technical and organizational measures to protect its products, including services, and to safeguard personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. These measures take into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the risks to the rights and freedoms of natural persons, and relevant security standards and frameworks, including, where applicable, the NIS2 Directive and ENISA guidelines.

Boltrics maintains a structured risk management framework as part of its Information Security Management System ("**ISMS**"). Risk assessments are performed periodically and, where appropriate, upon significant changes to systems, services or the threat landscape. Identified risks, including risks related to third-party dependencies such as cloud providers, are documented and addressed through appropriate risk treatment measures. Security measures are selected and implemented taking into account the outcome of such risk assessments, the sensitivity of the personal data, the criticality of the systems involved and/or the potential impact on the rights and freedoms of data subjects.

In particular, the following applies:

- **Pseudonymisation**
  Personal data is pseudonymised where feasible and appropriate, taking into account the nature and purpose of the processing. In particular, pseudonymisation is applied for logging, monitoring, analytics, telemetry, performance analysis and troubleshooting purposes. Personal data is not pseudonymised where this would prevent or materially impair the primary functionality of the services or the performance of contractual obligations.

- **Encryption**
  Personal data is encrypted at rest and in transit using industry-standard encryption mechanisms, unless this is not technically feasible or would materially impair the functionality of the services. Encryption is applied across relevant components of the architecture, including databases, storage, backups and network communications.
- **Confidentiality, integrity, availability and resilience**
  The confidentiality, integrity, availability and resilience of the products and data are safeguarded through a combination of technical, organisational and contractual measures, including access controls, authentication and authorisation mechanisms, logical separation of customer environments, monitoring, vulnerability management, secure configuration and employee confidentiality obligations. Boltrics' services are hosted on Microsoft Azure and Microsoft Dynamics 365 Business Central, which operate in accordance with internationally recognised security standards and certifications (including ISO 27001 and SOC 1 / SOC 2), while Boltrics remains responsible for the security measures applicable to the services it provides.
- **Incident response and recovery**
  Boltrics has implemented incident response, backup and recovery procedures designed to help ensure that, in the event of a physical or technical incident, the availability of and access to Personal data can be restored in a timely manner. Regular backups are performed, recovery procedures are tested, and incident handling processes are periodically reviewed and improved.

Further details regarding the implemented security measures are described in the *Information Security & Cybersecurity Overview* or may be made available upon reasonable request, subject to applicable confidentiality and security restrictions. Detailed internal security policies are not publicly disclosed for security reasons. More information on Boltrics' security measures, including FAQ, can be found here.

15. **Data processor conforms to the principles of the following Information Security Management System (ISMS):** Boltrics operates an ISMS that has been developed taking into account relevant ENISA guidelines[6], which refers to internationally recognized standards such as ISO (27001). Boltrics' ISMS and Security policy incorporate a PDCA-cycle (of continuous improvement), and take into account the principles underlying the EU NIS2 Directive.

16. **Data processor has obtained the following labels and certificates**
    - Data Pro Verified
    - Boltrics has obtained the Certified for Microsoft Dynamics seal of approval, the highest standard for partner-developed software.

Data breach protocol

17. **In the event something does go wrong, data processor shall follow the following data breach protocol to ensure that clients are notified of incidents:**
    This protocol applies to any Personal Data Breach as defined in Article 4(12) GDPR, including incidents involving the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

[6] TECHNICAL IMPLEMENTATION GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures JUNE 2025, VERSION 1.0

If Boltrics becomes aware of a Personal Data Breach, or reasonably suspects that a Personal Data Breach with a potential risk to the rights and freedoms of natural persons may have occurred, Boltrics shall inform you, Customer, without undue delay, in accordance with the obligations set out in this Data Processing Agreement.

Where possible, Boltrics shall provide at least the following information:

(i) the nature of the breach, including, where possible, the categories of data subjects concerned and the approximate number of data subjects concerned;

(ii) the categories of personal data concerned and, where possible, the approximate number of personal data records concerned;

(iii) the identified or expected consequences of the breach for the processing of the personal data and the data subjects concerned; and

(iv) the measures that Boltrics has taken or proposes to take to address the breach, including, where applicable, measures to mitigate its possible adverse effects.

Notifications shall be made to the contact person designated by you for such purpose. You are responsible for providing Boltrics with the relevant written contact details. Notification shall take place by telephone or e-mail.

Whether or not a Personal Data Breach must be notified to the competent supervisory authority and/or communicated to data subjects remains the responsibility of you as the controller, in accordance with Articles 33 and 34 GDPR. Upon request, Boltrics shall provide reasonable cooperation in connection with such notification or communication obligations.

Boltrics shall take reasonable measures necessary to contain, investigate and mitigate the effects of the Personal Data Breach.

Further details regarding Boltrics' internal incident and data breach handling procedures are laid down in Boltrics' internal data breach response policy. Such internal procedures are maintained for internal governance purposes and do not limit or replace the notification obligations set out in this Data Processing Agreement. Additional information may be provided where appropriate, subject to applicable confidentiality and security restrictions.

Part 2: Standard Clauses for Data Processing

Version: March 2025

Along with the Data Pro Statement, these standard clauses constitute the data processing agreement. They also constitute an annex to the Agreement and to the appendices to this Agreement, e.g. any general terms and conditions which may apply.

Article 1. Definitions

The following terms have the following meanings ascribed to them in the present Standard Clauses for Data Processing, in the Data Pro Statement and in the Agreement:

1.1 **Dutch Data Protection Authority (AP):** the supervisory authority defined in Section 4.21 of the GDPR.

1.2 **GDPR:** the General Data Protection Regulation.

1.3 **Data Processor**: the party which, in their capacity as an ICT supplier, processes Personal Data on behalf of their Client as part of the performance of the Agreement.

1.4 **Data Pro Statement**: statement issued by Data Processor in which they provide information such as the intended use of their products and/or services, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects.

1.5 **Data Subject**: a natural person who can be identified, directly or indirectly.

1.6 **Client:** the party on whose behalf Data Processor processes Personal Data. Client can either be the controller (the party who determines the purpose and means of the processing) or another data processor.

1.7 **Agreement**: the agreement concluded between Client and Data Processor, based on which the ICT supplier provides services and/or products to Client, the data processing agreement forming part of this agreement.

1.8 **Personal Data** any and all information regarding a natural person who has been or can be identified, as defined in Article 4.1 of the GDPR, processed by Data Processor as required under the Agreement.

1.9 **Data Processing Agreement**: the present Standard Clauses for Data Processing, which, together with Data Processor's Data Pro Statement (or similar such information), constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

Article 2. General provisions

2.1 The present Standard Clauses for Data Processing apply to all Personal Data processing operations carried out by Data Processor in providing their products and services, as well as to all Agreements and offers. The applicability of Client's data processing agreements is explicitly rejected.

2.2 The Data Pro Statement, and particularly the security measures described in it, may be adapted from time to time to changing circumstances by Data Processor. Data Processor shall notify Client in the event of

significant revisions. If Client in all reasonableness cannot agree to the revisions, Client shall be entitled to terminate the data processing agreement in writing, stating their reasons for doing so, within thirty days of having been served notice of the revisions.

2.3 Data Processor shall process the Personal Data on behalf of Client, in accordance with the written agreed upon instructions provided by Client by Data Processor.

2.4 Client or their customer shall serve as the controller within the meaning of the GDPR, shall have control over the processing of the Personal Data and shall determine the purpose and means of processing the Personal Data.

2.5 Data Processor shall serve as the processor within the meaning of the GDPR and shall therefore not determine the purpose and means of processing the Personal Data, and shall not make any decisions on the use of the Personal Data and other such matters.

2.6 Data Processor shall implement the GDPR as laid down in the present Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to Client to assess, on the basis of this information, whether Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organisational measures in order to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.

2.7 Client shall guarantee Data Processor that they act in accordance with the GDPR, that they provide a high level of protection for their systems and infrastructure at all time, that the nature, use and/or processing of the Personal Data are not unlawful and that they do not violate any third party's rights.

2.8 Administrative fines imposed on Client by the Dutch Data Protection Authority cannot be recovered from Data Processor.

Article 3. Security

3.1 Data Processor shall implement the technical and organisational security measures set out in their Data Pro Statement. In implementing the technical and organisational security measures, Data Processor shall take into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing and the intended use of their products and services, and the risk in processing the data of varying likelihood and severity inherent to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of Data Processor's products and services.

3.2 Unless explicitly stated otherwise in the Data Pro Statement, the products and services provided by Data Processor shall not be equipped to process special categories of personal data or data relating to criminal convictions and offences.

3.3 Data Processor seeks to ensure that the security measures they shall implement are appropriate for the manner in which Data Processor intends to use the products and services.

3.4 In Client's opinion, said security measures provide a level of security that is tailored to the risk inherent in the processing of the Personal Data used or provided by Client, taking into account the factors referred to in Article 3.1.

3.5 Data Processor shall be entitled to adjust the security measures they have implemented if to their discretion such is necessary for a continued provision of an appropriate level of security. Data Processor shall record any significant adjustments they chooses to make, e.g. in a revised Data Pro Statement, and shall notify Client of said adjustments where relevant.

3.6 Client may request Data Processor to implement further security measures. Data Processor shall not be obliged to honour such requests to adjust their security measures. If Data Processor makes any adjustments to their security measures at Client's request, Data Processor is entitled to invoice Client for the costs associated with said adjustments. Data Processor shall not be required to actually implement the requested security measures until both Parties have agreed upon them in writing.

Article 4. Data breaches

4.1 Data Processor does not guarantee that their security measures shall be effective under all circumstances. If Data Processor discovers a data breach within the meaning of Article 4 sub 12 of the GDPR, they shall notify Client without undue delay. The "Data Breach Protocol" section of the Data Pro Statement outlines the way in which Data Processor shall notify Client of data breaches.

4.2 It is up to the Controller (the Client or their customer) to assess whether the data breach of which Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (Client or their customer) shall at all times remain responsible for reporting data breaches which must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR. Data Processor is not obliged to report data breaches to the Dutch Data Protection Authority and/or to the Data Subject.

4.3 Where necessary, Data Processor shall provide further information on the data breach and shall assist Client to meet their breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information available to Data Processor.

4.4 If Data Processor incurs any reasonable costs in doing so, they are entitled to invoice Client for these, at the rates applicable at the time.

Article 5. Confidentiality

5.1 Data Processor shall ensure that the persons processing Personal Data acting under its authority have committed themselves to confidentiality.

5.2 Data Processor shall be entitled to provide third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or order issued by a competent government authority.

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by Data Processor to Client, and any and all information provided by Data Processor to Client detailing the technical and organisational security measures included in the Data Pro Statement are

confidential and shall be treated as such by Client and shall only be disclosed to authorised employees of Client. Client shall ensure that their employees comply with the requirements described in this article.

Article 6. Term and termination

6.1 This data processing agreement constitutes part of the Agreement, and any new or subsequent agreement arising from it and shall enter into force at the time of the conclusion of the Agreement and shall remain effective for an indefinite period.

6.2 This data processing agreement shall end by operation of law upon termination of the Agreement or upon termination of any new or subsequent agreement arising from it between parties.

6.3 If the data processing agreement is terminated, Data Processor shall delete all Personal Data they currently store and which they have obtained from Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data can no longer be used and shall have been *rendered inaccessible*. Alternatively, if such has been agreed, Data Processor shall return the Personal Data to Client in a machine-readable format.

6.4 If Data Processor incurs any costs associated with the provisions of Article 6.3, they shall be entitled to invoice Client for said costs. Further arrangements relating to this subject can be laid down in the Data Pro Statement.

6.5 The provisions of Article 6.3 do not apply if Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such instances, Data Processor shall only continue to process the Personal Data insofar as such is necessary by virtue of their statutory obligations. Furthermore, the provisions of Article 6.3 shall not apply if Data Processor is the Controller of the Personal Data within the meaning of the GDPR.

Article 7. The rights of Data Subjects, Data Protection Impact Assessments (DPIA) and auditing rights

7.1 Where possible, Data Processor shall cooperate with reasonable requests made by Client relating to Data Subjects who invoke their rights from Client. If Data Processor is directly approached by a Data Subject, they shall refer the Data Subject to Client where possible.

7.2 If Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, Data Processor shall cooperate with such, following a reasonable request to do so.

7.3 Data Processor will lend their cooperation to Client's requests for the deletion of personal data insofar as Client cannot carry this out themself.

7.4 Data Processor shall be able to demonstrate their compliance with their requirements under the data processing agreement by means of a valid Data Processing Certificate or an equivalent certificate or audit report (third-party memorandum) issued by an independent expert.

7.5 In addition, at Client's request, Data Processor shall provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If, in spite of the foregoing, Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, Client shall be entitled to have an audit performed (at their own expense) not more than once every year by an independent, certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The scope of the audit shall be limited to verifying that Data Processor is complying with the arrangements made regarding the processing of the Personal Data as set forth in the present data processing agreement. The expert shall be subject to a duty of confidentiality with regard to his/her findings and shall only notify Client of matters which cause Data Processor to fail to comply with their obligations under the data processing agreement. The expert shall furnish Data Processor with a copy of his/her report. Data Processor shall be entitled to reject an audit or instruction issued by the expert if to their discretion the audit or instruction is inconsistent with the GDPR or any other law, or that it constitutes an unacceptable breach of the security measures they have implemented.

7.6 The parties shall consult each other on the findings of the report at their earliest convenience. The parties shall implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. Data Processor shall implement the proposed measures for improvement insofar as to their discretion such are appropriate, taking into account the processing risks associated with their product or service, the state of the art, the costs of implementation, the market in which they operate, and the intended use of the product or service.

7.7 Data Processor shall be entitled to invoice Client for any costs they incur in implementing the measures referred to in this article.

Article 8. Sub-processors

8.1 Data Processor has specified in the Data Pro Statement whether Data Processor uses any third parties (sub-processors) to help them process the Personal Data, and if so, which third parties.

8.2 Client hereby authorises Data Processor to hire other sub-processors to meet their obligations under the Agreement.

8.3 Data Processor shall notify Client of any changes concerning the addition or replacement of the third parties (sub-processors) hired by Data Processor, e.g. through a revised Data Pro Statement. Client shall be entitled to object to such changes. Data Processor shall ensure that any third parties they hire shall commit to ensuring the same level of Personal Data protection as the security level Data Processor is bound to provide to the Client pursuant to the Data Pro Statement.

Article 9. Other provisions

These Standard Clauses for Data Processing, along with the Data Pro Statement, constitute an integral part of the Agreement. Therefore, any and all rights and obligations arising from the Agreement, including any applicable general terms and conditions and/or limitations of liability, shall also apply to the data processing agreement.