# DATA PROCESSING AGREEMENT

Effective from 2026-10-07

## 1. Purpose and application of the Agreement

### 1.1 Parties and contractual relationship

This Data Processing Agreement (the "DPA") applies between Hartic AB, company registration no. 559480-6217, Teknikvägen 3, 961 50 Boden, Sweden ("Hartic" or the "Data Processor"), and the customer that has entered into a Pricing Agreement regarding Hartic's services (the "Customer" or the "Data Controller"). Hartic and the Customer are each referred to as a "Party" and jointly as the "Parties".

The DPA forms an integral part of the Parties' Agreement and applies when Hartic processes personal data on behalf of the Customer in connection with the provision of Hartic's services. The DPA enters into force at the same time as the Pricing Agreement through which the Customer accedes to this DPA, unless the Parties have agreed otherwise in writing.

### 1.2 Order of precedence

In the event of a conflict between the DPA and other contractual documents, the DPA shall take precedence in matters concerning the processing of personal data on behalf of the Customer. In all other respects, the order of precedence set out in Hartic's General Terms and Conditions shall apply.

## 2. Roles and responsibilities

### 2.1 The Customer's role

The Customer is the Data Controller for the processing of personal data carried out on the Customer's behalf in Hartic's services and determines the purposes and essential means of the processing. The Customer is responsible, among other things, for ensuring that there is a valid legal basis for the processing, that data subjects receive the information required under applicable data protection legislation, and that the Customer's instructions to Hartic are lawful.

### 2.2 Hartic's role

Hartic is the Data Processor when Hartic processes personal data on behalf of the Customer. Hartic may only process such personal data in accordance with the Customer's documented instructions, this DPA, other applicable contractual documents, and applicable data protection legislation.

If Hartic considers that an instruction from the Customer infringes Regulation (EU) 2016/679 (the "GDPR") or other applicable data protection legislation, Hartic shall inform the Customer without undue delay, unless Hartic is prohibited from doing so by law.

### 2.3 Hartic's own processing

Processing for which Hartic itself determines the purposes and means, for example certain processing of business contacts, billing information, support administration or Hartic's own marketing, is not covered by this DPA. Such processing is described in Hartic's Privacy Policy.

## 3. Scope of processing

### 3.1 Subject matter, nature and purpose

Hartic processes personal data to the extent necessary to provide, operate, secure, maintain and administer the services ordered by the Customer. The processing may include, among other things, collection, recording, organisation, storage, consultation, analysis, compilation, transmission, making available, rectification, restriction, erasure and other processing required for the functionality of the Service.

The more detailed documented instructions are set out in this DPA, Appendix 1, the Customer's configuration and use of the Service, the Pricing Agreement, and other documented instructions agreed by the Parties in writing.

### 3.2 Duration

Processing may continue for as long as Hartic provides the Service to the Customer and thereafter only for the period required for return or erasure pursuant to Section 15, or where continued storage is required under Union law or Swedish law.

## 4. Customer instructions

### 4.1 Documented instructions

The Customer instructs Hartic to process personal data to the extent required to perform the Agreement and provide the functionality used by the Customer. The Customer's use of the Service's settings and functions, as well as written instructions from an authorised representative of the Customer, shall constitute documented instructions.

If the Customer requests processing that goes beyond the agreed Service or requires specific measures, the Parties may agree on the scope, timetable and any applicable fees before the work begins.

### 4.2 Transfers

Hartic may not transfer personal data to a third country or an international organisation other than in accordance with the Customer's documented instructions, this DPA and applicable data protection legislation. Rules regarding subprocessors and transfers to third countries are set out in Sections 11 and 12.

## 5. Confidentiality and access rights

Hartic shall ensure that persons authorised to process personal data on behalf of the Customer are subject to a confidentiality obligation or equivalent statutory duty of confidentiality and have access to personal data only to the extent required for their duties.

Hartic shall apply the principle of least privilege and take appropriate measures to prevent unauthorised access, alteration, disclosure or other unlawful processing.

## 6. Security of processing

### 6.1 Technical and organisational measures

Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, and the risks to the rights and freedoms of natural persons, Hartic shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Hartic's principal platform and customer data, including personal data stored in Hartic's service, are stored on servers in Sweden. Certain technical support services may involve limited personal data being processed by subprocessors in accordance with Sections 11 and 12.

Hartic's baseline security measures are described in Appendix 2. Hartic may develop and modify the security measures over time, provided that the overall level of protection is not materially reduced.

### 6.2 Customer responsibility for secure use

The Customer is responsible for its own user and access administration, for ensuring that only authorised persons are granted access to the Service, and for using available security features appropriately. The Customer controls user roles and access rights in the Service. Administrator privileges may only be assigned by an authorised administrator. Hartic supports strong authentication for users, including BankID where this login method is used.

## 7. Rights of data subjects

Taking into account the nature of the processing and to the extent possible, Hartic shall assist the Customer through appropriate technical and organisational measures so that the Customer can fulfil its obligations when data subjects exercise their rights under Chapter III of the GDPR, such as the rights of access, rectification, erasure, restriction, data portability or objection.

If Hartic receives a request from a data subject concerning personal data processed on behalf of the Customer, Hartic shall, unless otherwise required by law, refer the data subject to the Customer or forward the request to the Customer without responding to it substantively.

If a request entails work that materially exceeds the normal functionality of the Service, Hartic may, after informing the Customer, charge reasonable fees for specific assistance to the extent permitted by applicable data protection legislation and the Agreement.

## 8. Personal data breaches

### 8.1 Notification

Hartic shall notify the Customer without undue delay after becoming aware of a personal data breach concerning personal data processed on behalf of the Customer.

### 8.2 Information and assistance

To the extent the information is available, Hartic shall provide the information reasonably required by the Customer to assess the incident and fulfil its obligations under Articles 33 and 34 of the GDPR. Information may be provided in phases if all information is not available at the same time.

Hartic shall take reasonable measures to mitigate the consequences of the incident, prevent further unauthorised processing and assist the Customer with investigation and documentation. The Customer is responsible for deciding whether and how to notify the supervisory authority and inform data subjects, unless otherwise required by law.

## 9. Assistance under Articles 32-36 GDPR

Taking into account the nature of the processing and the information available to Hartic, Hartic shall assist the Customer to a reasonable extent in fulfilling obligations relating to security of processing, personal data breaches, data protection impact assessments and prior consultation with the supervisory authority under Articles 32-36 of the GDPR.

If the Customer's request for assistance concerns substantial work that is not included in the normal Service, the Parties may agree on reasonable compensation for such work, provided that Hartic has not caused the need for assistance through its own infringement.

## 10. Documentation, review and audits

### 10.1 Information

Upon request, Hartic shall make available to the Customer such information as is reasonably required to demonstrate that Hartic fulfils its obligations under Article 28 of the GDPR and this DPA.

### 10.2 Audits

The Customer has the right, itself or through an independent auditor, to review Hartic's compliance with this DPA. Reviews shall primarily, and to the extent possible, be conducted remotely using available documentation, reports, questionnaires, security information or equivalent materials. An on-site inspection or other more intrusive review may be carried out only where such documentation is not reasonably sufficient, where there are well-founded grounds to suspect a material compliance deficiency, or where such review is required by a competent supervisory authority. Such review shall be preceded by a written request and reasonable advance notice.

Audits shall be conducted during normal business hours and in a manner that minimises disruption to Hartic's operations and does not compromise the security or confidentiality of other customers or Hartic's trade secrets. An audit does not entitle the Customer to access other customers' data, source code, security keys or other information whose disclosure would create a security risk, except to the extent such access is expressly required by a competent supervisory authority. The Customer shall bear its own costs and Hartic's reasonable costs for the audit, unless the review identifies a material deficiency in Hartic's compliance with this DPA.

Limitations on frequency or cost responsibility do not apply to the extent a competent supervisory authority requires a review or where there are well-founded grounds to suspect a material infringement.

## 11. Subprocessors

### 11.1 General written authorisation

The Customer grants Hartic general written authorisation to engage subprocessors for processing covered by this DPA, provided that the requirements of this Section are complied with.

### 11.2 Current list

An up-to-date list of Hartic's subprocessors is available at www.hartic.se/subprocessors. The list shall at a minimum state the name of the subprocessor, the service or function provided, the type of personal data or processing

concerned, the relevant country or region of processing and, where applicable, the transfer mechanism used for transfers to a third country.

### 11.3 New or replacement subprocessors

At least fourteen (14) calendar days before a planned change takes effect, Hartic shall inform the Customer electronically, normally by email to the Customer's registered contact person or administrator, of changes involving the engagement of a new subprocessor or the replacement of an existing subprocessor. The Customer shall be given the opportunity, within this period, to submit a written and objectively justified objection on data protection grounds. The current list of subprocessors is published at www.hartic.se/subprocessors.

If the Customer raises a justified objection, the Parties shall in good faith seek a reasonable solution. If no reasonable solution can be reached, Hartic may refrain from using the relevant subprocessor for the Customer or, if this is not practically possible, either Party may terminate the part of the Service affected by the objection. Such termination shall not affect other parts of the Agreement that can continue to be provided without the relevant subprocessor.

### 11.4 Agreements with subprocessors

Hartic shall, by written agreement, impose on each subprocessor data protection obligations that, to the relevant extent, provide at least the same level of protection as this DPA. Hartic remains fully liable to the Customer for the subprocessor's performance of its data protection obligations to the extent required by the GDPR.

## 12. Transfers to third countries

Where processing involves personal data being transferred to, stored in or made accessible from a country outside the EU/EEA, Hartic shall ensure that the transfer is carried out in accordance with Chapter V of the GDPR.

Depending on the circumstances, a transfer may be based on an adequacy decision, the EU-U.S. Data Privacy Framework for recipients participating in that framework, the European Commission's Standard Contractual Clauses, or another valid transfer mechanism. Where required, Hartic shall also implement supplementary technical, organisational or contractual safeguards.

Information about relevant subprocessors, processing regions and transfer mechanisms shall be set out in the current list of subprocessors at www.hartic.se/subprocessors.

## 13. Requests from public authorities

If Hartic receives a legally binding request from a public authority or other third party for disclosure of personal data processed on behalf of the Customer, Hartic shall, to the extent permitted by law, inform the Customer before the data are disclosed. Hartic shall disclose only the personal data it is legally required to disclose and, where appropriate, take reasonable measures to limit the request.

## 14. Anonymised data

In accordance with Hartic's General Terms and Conditions, Hartic may use statistics and data for product, methodology and business development after the data have been anonymised in such a way that neither individual data subjects nor the Customer can reasonably be identified. Once data have been irreversibly anonymised so that they no longer constitute personal data, they are no longer subject to this DPA or the GDPR.

## 15. Return and erasure

### 15.1 Upon termination of the Agreement

When the processing covered by the DPA ends, Hartic shall, at the Customer's choice, return or erase the personal data processed by Hartic on behalf of the Customer and erase existing copies, unless continued storage is required under Union law or Swedish law. If the Customer wishes the data to be returned or requests a specific data export, such request must be made no later than before termination of the Agreement and shall be handled to the extent technically possible and within the available functionality of the Service.

The Customer is responsible for using available export functions before the end of the contractual period or otherwise requesting any data export that the Customer requires after the Agreement has ended. If the Customer has not requested return of the data before termination of the Agreement, Hartic is entitled, from the day after the end of the contractual period, to close the Customer's account and commence erasure of the data. Hartic is not

obliged to keep the Service or the Customer's account available for any separate export period after the Agreement has ended. Specific assistance with data export may be agreed separately.

### 15.2 Backups

Hartic creates a backup of the production database once every twenty-four (24) hours. Backups are stored in Sweden and retained under the ordinary rotation and deletion routine for thirty-five (35) days. Personal data that remain in backups after ordinary erasure may during this period only be processed for restoration, security or other legally necessary purposes and are erased or overwritten when the ordinary backup cycle expires.

## 16. Liability

The Parties' liability for processing of personal data is governed by the GDPR, other applicable data protection legislation, this DPA and, where applicable, the other liability provisions of the Agreement. Nothing in this DPA limits liability that cannot be limited under mandatory law.

Each Party is responsible for its own obligations under applicable data protection legislation. The Customer is responsible for the lawfulness of the purposes, personal data and instructions determined by the Customer, while Hartic is responsible for ensuring that its processing as Data Processor is carried out in accordance with the Customer's documented instructions and Hartic's own obligations under the GDPR.

## 17. Term and amendments

The DPA remains in force for as long as Hartic processes personal data on behalf of the Customer. Provisions which by their nature are intended to survive termination of the Agreement, including provisions on confidentiality, erasure and liability, shall remain in force for as long as relevant.

Hartic may update this DPA where required due to changes in legislation, regulatory requirements, or technical and organisational changes, provided that the amendment does not materially reduce the Customer's rights or the protection of personal data. Material amendments shall be notified to the Customer within a reasonable period before they take effect. Changes affecting commercial terms shall be handled in accordance with the Pricing Agreement.

## 18. Governing law and dispute resolution

The DPA shall be interpreted and applied in accordance with Swedish law, taking into account directly applicable EU law. Disputes shall be handled in accordance with the provisions on governing law and dispute resolution in Hartic's General Terms and Conditions.

## Appendix 1 - Description of processing

### A. Subject matter and purpose

Processing of personal data for the purpose of providing Hartic's digital platform, Hartic Core and the modules and functions ordered by the Customer, including user administration, surveys, pulses, analysis, reporting, follow-up, action support, customer support, technical operations and security.

### B. Categories of data subjects

- The Customer's employees and staff.
- Managers, leaders, administrators and other users to whom the Customer grants access to the Service.
- Consultants, contractors or other persons whom the Customer chooses to include in surveys or other processing in the Service.
- Other data subjects whose personal data the Customer itself enters into the Service within the scope of the agreed functionality.

### C. Categories of personal data

- Name, work-related email address and other contact details provided by the Customer.
- Organisation, organisational affiliation, group, position, role and access rights.
- User and account information as well as technical identifiers and log data.
- Responses to surveys and pulses, free-text responses, results, summaries and related analytical data.

- Data processed in the modules and functions activated by the Customer, for example work-environment-related data, risk and health rounds, deviations or other information the Customer chooses to record.
- Other personal data entered into the Service by the Customer or its users within the scope of the agreed functionality.

**D. Special categories of personal data**

Depending on the questions, free-text fields, modules and functions used by the Customer, the processing may include special categories of personal data under Article 9 of the GDPR, in particular data concerning physical or mental health, as well as other privacy-sensitive data. The Customer is responsible for ensuring that such processing is permitted and that the necessary legal basis and any specific conditions for the processing are fulfilled.

**E. Duration of processing**

For the duration of the Agreement and thereafter only to the extent required for return, erasure, backup or statutory retention under the DPA.

## Appendix 2 - Technical and organisational security measures

Hartic applies security measures adapted to the risk of the processing and continuously develops those measures. The measures include, among other things, the following areas:

**A. Access and authorisation management**

- Access rights are limited according to job duties and the principle of least privilege.
- Access to the production environment and customer data is limited to authorised members of Hartic's technical team where such access is required for operations, support, security, troubleshooting or development. Privileged administrative access to development and production environments, including Azure, is protected by multi-factor authentication (MFA).
- The Customer controls user roles and access rights in the Service. Administrator privileges may only be assigned by an authorised administrator. The Service supports strong authentication for users, including BankID where this login method is used.

**B. Protection of data and communications**

- Hartic's principal production databases and backups are stored on servers in Sweden.
- Communications with the Service are protected using appropriate encrypted transport protocols.
- The production database is backed up once every twenty-four (24) hours. Backups are stored in Sweden and retained for thirty-five (35) days under Hartic's ordinary rotation and deletion routine.

**C. Operations, logging and continuity**

- Relevant technical events are logged and monitored to the extent necessary for operations, troubleshooting, traceability and security.
- Procedures are in place for backup, restoration and the handling of disruptions and personal data breaches.
- Security-related events are handled in accordance with internal incident procedures.

**D. Development and change management**

- Security aspects are considered in the development, modification and maintenance of the Service.
- Access to production environments is limited to authorised persons within Hartic's technical team and privileged access is protected by MFA.

**E. Organisational measures**

- Personnel and other persons who are granted access to personal data are subject to confidentiality obligations and relevant internal instructions.
- Subprocessors are selected and managed in accordance with the requirements of the DPA and applicable data protection legislation.
- Security measures are evaluated and adapted when the risk landscape, technology or processing changes.