# DATA PROCESSING AGREEMENT

BETWEEN:

The Liberators Improve Your Team B.V., a legal entity incorporated under the laws of the Netherlands, having its registered office in (3544 DH) Utrecht at Parelmoervlinder 8 (hereinafter to be referred to as: the "**Controller**" or "**Customer**"),

AND

Exact Netherlands B.V., a legal entity incorporated under the laws of the Netherlands, having its registered office in (2629 JD) Delft at Molengraaffsingel 33 (hereinafter to be referred to as: the "**Processor**" or "**Exact**");

Controller and Processor will hereinafter jointly be referred to as the **"Parties**" and each individually as the "**Party**",

WHEREAS

I. The Processor is a developer and supplier of business software solutions for smaller and larger sized companies.

II. The Processor provides business software serving a wide range of branches and supporting multiple business processes to its customers (hereinafter to be referred to as: the "**Services**").

III. The Parties have concluded an Exact Online agreement for the use of Exact Online on which the Exact Online Terms & Conditions are applicable (hereinafter to be referred to as: the "**Service Agreement**").

IV. Pursuant to the provision of the Services and the Service Agreement, the Processor will be processing personal data (hereinafter to be referred to as: the "**Personal Data**") on behalf of the Controller in the course of the performance of the Service Agreement with the Controller. The Controller is obliged and wishes to protect and secure such information.

V. In consideration of the foregoing premises, Parties have agreed to enter into and execute this data processing agreement (hereinafter to be referred to as: the "**Data Processing Agreement**" and "**DPA**") under the following terms and conditions.

HEREBY AGREE AS FOLLOWS

## 1. Subject matter of this Data Processing Agreement

1.1. This Data Processing Agreement applies exclusively to the processing of Personal Data in the scope of the Service Agreement between the Parties for the provision of the Services. This DPA forms an integral part of the Service Agreement, and all the provisions of the Service Agreement are applicable on this DPA.

1.2. Terms such as "processing", "personal data", "controller" and "processor" shall have the meaning ascribed to them in the General Data Protection Regulation (*2016/679/EU*) (hereinafter to be referred to as: "**GDPR**").

1.3. Processor undertakes to process the Personal Data under the Service Agreement specified in **Exhibit 1** on behalf of the Controller for the purposes and in the course of the performance of the Service Agreement with the Controller.

## 2. The Controller and the Processor

2.1. The Processor will act as the processor as defined in article 4(8) GDPR and the Controller will act as the controller as defined in article 4(7) GDPR.

2.2. The Processor will only process the Personal Data in such manner and to the extent necessary for the provision of the Services under the Service Agreement, except as required to comply with a legal obligation to which the Processor is subject, or to follow instructions of the Controller. The Processor shall never process the Personal Data for any other purposes.

2.3. The Controller shall, in its use of the Services, process Personal Data in accordance with the requirements of data protection laws and regulations. For the avoidance of doubt, Controller's instructions for the processing of Personal Data shall comply with data protection laws and regulations. The Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Controller acquired the Personal Data. The Processor shall immediately inform the Controller if, in its opinion, an instruction provided by or on behalf of the Controller infringes the GDPR or other applicable data protection laws and regulations.

2.4. In the event the Controller is considered to be a processor within the meaning of article 4(8) GDPR, the Processor is considered to be a sub-processor and the terms and conditions of this DPA will remain in full force and effect.

## 3. Confidentiality

3.1. Without prejudice to any existing contractual arrangements between the Parties, the Processor will treat all Personal Data as strictly confidential. The Processor shall ensure that all persons authorized to process the Personal Data are bound to confidentiality. These obligations will not prevent a Party from sharing information with a third party to the extent such disclosure is mandatory under applicable law.

3.2. The Parties shall treat all information the Processor has to provide to the Controller by virtue of Article 4 of this DPA as strictly confidential.

## 4. Security and audit

4.1. Processor shall implement appropriate technical and organizational measures for the security of the processing of Personal Data, in order to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction or damage. Taking into account the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the Personal Data. An overview of these technical and organisational measures shall be attached to this DPA as **Exhibit 2**.

4.2. The availability and security of the Services will be audited by independent auditors annually and a control framework is designed managing defined risks in these areas. For some of the Services an ISAE 3402 type 2 report (or similar) is available upon the written request of the Controller. The Controller may have the right to audit Processor's compliance with its obligations under this DPA, up to one time per contractual year and at the Controller's costs, only if the Controller in its reasonable discretion believes that the Processor has violated a material obligation under this DPA, or if a competent data protection authority requests this. Subject to a motivated written proposal from the Controller and the approval of the Processor, such audit will be either performed by i) the Processor or ii) a qualified, independent third-party security auditor and in possession of the required professional qualifications bound by a duty of confidentiality (hereinafter to be referred to as: the "**Auditor**"). In the course of such audit, the Auditor may enter Processor's facilities during normal business hours and without unreasonably impacting Processor's business, in particular with no impact on the general IT security of the Processor, and examine Processor's work routines, set ups and technical infrastructure. At Processor's discretion or at Controller's specific written request, the Processor may provide evidence of the performance of its obligations and/or the suitability of the technical and organizational measures, as described in this DPA, by current third-party certifications, insofar available. For this purpose, Processor may also present up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security department or quality auditors) or suitable certification by way of an IT security or data protection audit.

## 5. Improvements to security

5.1. The Parties acknowledge that security requirements are constantly changing, and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Processor will therefore evaluate the measures as implemented in accordance with Article 4 from time to time and will tighten, supplement and improve these measures if this is reasonably commercially possible and required in order to maintain compliance with the requirements set out in Article 4.

5.2. The Controller has the right to request the Processor to take reasonable additional security measures, necessary to protect the interest of its customers and the Personal Data. The Processor will decide in its sole discretion if the additional security measures are reasonably commercially possible. Where an amendment to the Service Agreement (including any Annex thereto) is reasonable and necessary in order to execute such an instruction, the Parties shall negotiate an amendment to the Service Agreement in good faith.

## 6. Data Transfers

6.1. The Controller acknowledges and agrees that the Processor may transfer Personal Data to a country outside of the European Economic Area as required for the delivery of the Services as agreed upon in the Service Agreement, where Processor has a lawful basis for that transfer under Articles 44-49 GDPR.

## 7. Providing assistance

7.1. The Processor shall without undue delay after its detection, notify the Controller of any security breach with regard to the processing of the Personal Data. The notification will - as far as possible and available - include the nature of the security breach, the name and contact details of the data protection officer (at the time of this Data Processing Agreement to be reached via dpo@exact.com), the likely consequences of the security breach, and the measures that the Processor has taken or proposed to be taken in connection with the security breach. The Processor shall cooperate with the Controller and shall follow the Controller’s reasonable instructions with regard to a security breach, in order to enable the Controller to perform an investigation into the breach, as well as to enable the Controller to fulfil its obligations under Articles 32 to 36 GDPR. To the extent a security breach was caused by a violation of the requirements of this DPA by the Processor, the Processor shall make reasonable efforts to identify and to take suitable further steps in respect of the security breach.

7.2. The term “security breach” used in Article 7.1 shall be understood to mean: a breach of security as set out in Article 4 of this DPA leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

7.3. Any notifications pursuant to this Article 7 shall be addressed to the contact person of the Controller, i.e. the main user of the Services. The Controller may change the contact person for notifications pursuant to this Article 7, by implementing the change in the user interface (client portal) of the Services.

7.4. In case Processor receives a complaint or a request of a natural person with regard to the Personal Data (such as a request to access, request for rectification or request for erasure), Processor will notify Controller as soon as reasonably possible after receiving the complaint or request and will offer Controller – to the extent possible and for a reasonable fee – its assistance to the Controller in fulfilling its legal obligations.

7.5. Taking into account the nature of the processing and the information available to the Processor, the Processor will reasonably assist the Controller in complying with the obligations under Article 35 GDPR (Data Protection Impact Assessment/DPIA).

### 8. Contracting with Sub-Processors

8.1. The Controller acknowledges and agrees that the Processor may subcontract (part of) its activities under the Service Agreement consisting (partly) of the processing of the Personal Data or requiring Personal Data to be processed to any third party (hereinafter to be referred to as: the "**Sub-Processor**").

8.2. Processor may appoint or replace Sub-Processors, provided that Processor shall give notice of such changes and Controller does not legitimately object to such changes. Legitimate objections must contain reasonable and documented grounds relating to a Sub-Processor's non-compliance with applicable data protection legislation.

8.3. The Processor shall be responsible for the services provided by Sub-Processors in accordance with the Service Agreement, to the same extent the Processor would be liable if performing the services directly under the terms of this DPA, except as otherwise set forth in the Service Agreement.

8.4. The Processor shall arrange that Sub-Processors are bound by similar confidentiality obligations as under this DPA.

8.5. Processor shall ensure that Sub-Processors are subject to data protection obligations of at least the same degree as agreed upon in this DPA.

### 9. Returning or Destruction of Personal Data

9.1. Upon termination of this DPA, the Processor shall either destroy or return all Personal Data to the Controller.

### 10. Liability and Indemnity

10.1. The liability and indemnification clauses as agreed between the Parties in the Service Agreement and accompanying Exact Online Terms & Conditions will also be applicable on the obligations recorded in this DPA.

### 11. Duration and Termination

11.1. This DPA shall come into effect on the date on which it is signed by both Parties and shall continue as long as the Service Agreement is in effect, or - if this period lasts longer - as long as Personal Data is processed by the Processor under this DPA.

11.2. Termination or expiration of this DPA shall not discharge the Parties from its confidentiality obligations pursuant to Article 3.

### 12. Miscellaneous

12.1. In the event of any inconsistency between the provisions of this DPA and the provisions of the Service Agreement, the provisions of this DPA shall prevail.

12.2. Any amendment to this DPA is only valid after written approval from both Parties.

12.3. This DPA is governed by the laws as agreed upon in the Service Agreement. Any disputes arising out or in connection with this DPA shall be brought exclusively before the competent court as agreed upon in the Service Agreement.

(*signature page follows*)

**The Liberators Improve Your Team B.V.**

On behalf of Agilistic B.V.

Name: C. Verwijs

Title: Co-founder

Date: 03/11/2024

**The Liberators Improve Your Team B.V.**

On behalf of The Learning Facilitator B.V.

Name: P.M. Overeem

Title: Co-founder

Date: 03/11/2024

DocuSigned by:

37AEDFA1AE4249A...

**Exact Netherlands B.V.**

Name: Marcel van de Sandt

Title: Chief Customer Success Officer

Date: 13 maart 2024 | 13:37 CET

**Exhibit 1 the extent, type and purpose of the planned collection, processing or use of data; the type of data and group of persons affected**

| | |
|---|---|
| the extent of the processing data | **Data entered by or under the responsibility of the customer is stored and processed if and to the extent requested by the customer.** |
| type and purpose of the collection, processing or use of data | **The purpose is to provide customers with services to support its business by providing insight and processing capabilities for its data** |
| the type of data | **All personal data entered by the customer, which may include e-mail addresses, names and addresses of persons, and other types of data.** |
| and group of persons affected | **Mainly employees of the customer, contacts of the customer from external companies such as its customers or prospective customers and their respective employees.** |

**Exhibit 2 General technical and organizational measures**

## 1. Access control to premises and facilities

*Unauthorized access (in the physical sense) must be prevented.*
Technical and organizational measures to control access to premises and facilities, particularly to check authorization:

- Access control system
- ID reader, chip card
- Door locking
- Security staff
- Surveillance facilities
- Alarm system, video/CCTV monitor

## 2. Access control to systems

*Unauthorized access to IT systems must be prevented.*
Technical (ID/password security) and organizational (user master data) measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, change of password)
- Automatic blocking (e.g. password or timeout)
- Creation of one master record per user

## 3. Access control to data

*Activities in IT systems not covered by the allocated access rights must be prevented.*
Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses:

- Differentiated access rights (profiles, roles, transactions and objects)
- Reports
- Access
- Change
- Deletion

## 4. Disclosure control

*Aspects of the disclosure of personal data must be controlled: electronic transfer, data transport, transmission control, etc.*
Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

- Encryption/tunneling (VPN = Virtual Private Network)
- Logging
- Transport security

## 5. Input control

*Full documentation of data management and maintenance must be maintained.*
Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:

- Logging and reporting systems

**6. Task control**

*Commissioned data processing must be carried out according to instructions.*

Measures (technical/organizational) to segregate the responsibilities between the Controller and the Processor:

- Unambiguous wording of the contract
- Formal commissioning (request form)
- Criteria for selecting the Agent
- Monitoring of contract performance

**7. Availability control**

*The data must be protected against accidental destruction or loss.*

Measures to assure data security (physical/logical):

- Backup procedures
- Mirroring of hard disks, e.g. RAID technology
- Uninterruptible power supply (UPS)
- Remote storage
- Anti-virus/firewall systems
- Disaster recovery plan

**8. Segregation control**

*Data collected for different purposes must also be processed separately.*

Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:

- "Internal client" concept / limitation of use
- Segregation of functions (production/testing)