# DATA PROCESSING AGREEMENT (DPA)

Contract Reference: DPA-2025-042 | Effective Date: March 15, 2025 | Classification: CONFIDENTIAL

## PARTIES

\*\*Controller\*\*: TNO TECHNOLOGIES B.V., a company registered in the Netherlands with company number 12345678 and registered address at 123 Tech Street, Amsterdam, Netherlands ("Controller")

\*\*Processor\*\*: DATA SOLUTIONS LTD, a company registered in Ireland with company number 87654321 and registered address at 45 Processing Lane, Dublin, Ireland ("Processor")

## 1. INTRODUCTION

This Data Processing Agreement ("Agreement") forms part of the Service Agreement dated January 10, 2025 between the Controller and the Processor ("Service Agreement") and sets out the terms and conditions for the Processing of Personal Data by the Processor on behalf of the Controller.

## 2. DEFINITIONS

1. "GDPR" means the General Data Protection Regulation (EU) 2016/679.

2. "Personal Data" means any information relating to an identified or identifiable natural person as defined in Article 4(1) of the GDPR.

3. "Processing" means any operation performed on Personal Data as defined in Article 4(2) of the GDPR.

4. "Data Subject" means an identified or identifiable natural person to whom the Personal Data relates.

5. "Supervisory Authority" means an independent public authority established pursuant to Article 51 of the GDPR.

## 3. SCOPE AND PURPOSE OF PROCESSING

1. The Processor shall process the Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by Union or Member State law to which the Processor is subject.

2. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other data protection provisions.

## 4. TYPES OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS

1. Types of Personal Data to be processed:

- Contact information (name, email, phone number, address)

- Account credentials (username, encrypted password)

- Employment details (job title, department, employee ID)

- System usage data (login times, features accessed)

2. Categories of Data Subjects:

- Controller's employees

- Controller's customers

- Controller's business partners

## 5. PROCESSOR OBLIGATIONS

### 5.1 Confidentiality

The Processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### 5.2 Security Measures

1. The Processor shall implement appropriate technical and organizational measures to ensure security of the Personal Data, including:

- Pseudonymization and encryption of Personal Data

- Ensuring confidentiality, integrity, availability, and resilience of processing systems

- Ability to restore availability and access in the event of incidents

- Regular testing of security measures

2. The Processor shall implement the following specific security measures:

- Data encryption both in transit and at rest

- Multi-factor authentication for system access

- Regular security patching and updates

- Logging and monitoring of access and processing activities

- Regular security assessments and penetration testing

### 5.3 Sub-processors

1. The Processor shall not engage another processor without prior specific or general written authorization of the Controller.

2. Where the Processor engages another processor, the same data protection obligations as set out in this Agreement shall be imposed on that other processor.

3. The Processor shall remain fully liable to the Controller for the performance of that other processor's obligations.

### 5.4 Data Subject Rights

The Processor shall assist the Controller by appropriate technical and organizational measures for the fulfillment of the Controller's obligation to respond to requests for exercising the Data Subject's rights.

### 5.5 Data Breach Notification

1. The Processor shall notify the Controller without undue delay after becoming aware of a Personal Data breach.

2. The notification shall at least:

- Describe the nature of the breach

- Communicate the name and contact details of the data protection officer

- Describe the likely consequences of the breach

- Describe the measures taken or proposed to address the breach

### 5.6 Data Protection Impact Assessment

The Processor shall assist the Controller in ensuring compliance with obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and information available to the Processor.

### 5.7 Return or Deletion of Data

At the choice of the Controller, the Processor shall delete or return all the Personal Data to the Controller after the end of the provision of services relating to Processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data.

### 5.8 Audit and Compliance

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

## 6. LIABILITY AND INDEMNITY

1. The Processor shall be liable for damage caused by Processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Controller.

2. The Processor shall indemnify the Controller against all claims, liabilities, costs, expenses, damages and losses suffered by the Controller as a result of the Processor's breach of this Agreement.

## 7. TERM AND TERMINATION

1. This Agreement shall commence on the Effective Date and shall continue for the duration of the Service Agreement.

2. The obligations of the Processor with respect to Personal Data shall survive the termination of this Agreement for as long as the Processor continues to process Personal Data.

## 8. GOVERNING LAW AND JURISDICTION

This Agreement shall be governed by and construed in accordance with the laws of the Netherlands, and the parties submit to the exclusive jurisdiction of the courts of Amsterdam.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date:

FOR THE CONTROLLER:

Name: Johanna Vries

Position: Chief Information Security Officer

Date: March 15, 2025

FOR THE PROCESSOR:

Name: Sean O'Connor

Position: Data Protection Officer

Date: March 15, 2025