

Data Processing Agreement (Professional Services)

Effective 8-Oct-2025

This Data Processing Agreement ("**DPA**") is entered into between:

1. **Customer** ("**Controller**"); and
2. **Acterus B.V.**, with its registered office at Achtseweg 159M, 5651 GW Eindhoven, The Netherlands ("**Processor**").

Preamble

This DPA is incorporated into the Professional Services Agreement or statement of work ("**the Agreement**") between the Controller and the Processor. The Controller uses the SyncForce software-as-a-service platform

("the Platform") provided by SyncForce B.V., and has engaged the Processor to provide Professional Services related to the Platform. This DPA governs the processing of Personal Data by the Processor's personnel when accessing the Platform on behalf of the Controller.

1. Definitions

All capitalized terms not otherwise defined herein shall have the meaning given to them in the GDPR. "Personal Data," "Processing," "Data Subject," and "Personal Data Breach" shall have the meanings ascribed to them in the GDPR.

2. Scope and Purpose of Processing

2.1 Instructions: The Processor shall only access and Process Personal Data within the Platform to the extent necessary to perform the Professional Services outlined in the Agreement and in accordance with the Controller's documented instructions.

2.2 Details of Processing: The details of the processing activities are set forth in **Annex I**.

3. Obligations of the Processor

3.1 Authorised Personnel: The Processor shall ensure that its personnel authorized to access the Controller's data within the Platform are subject to a strict duty of confidentiality and are trained in the responsible handling of Personal Data.

3.2 Security: The Processor shall implement and maintain appropriate technical and organisational measures to ensure the security of its own systems, networks, and devices used by its personnel to access the Platform. As part of these measures, the

Processor maintains an information security management system (ISMS) that is certified against the ISO/IEC 27001 standard. These measures, described in **Annex III**, are designed to prevent a Personal Data Breach originating from the Processor's environment. The Controller acknowledges that the security of the Platform itself is the responsibility of SyncForce B.V. under a separate agreement.

3.3 Personal Data Breach: In the event of a Personal Data Breach affecting the Controller's Personal Data that is caused by the Processor's personnel or originates from the Processor's systems, the Processor shall notify the Controller without undue delay after becoming aware of it.

3.4 Sub-processing: The Controller provides a general written authorisation for the Processor to engage the sub-processors listed in Annex II. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of other sub-processors, thereby giving the Controller the opportunity to object to such changes.

3.5 International Transfers: The Processor shall ensure that any personnel accessing the Controller's Personal Data are located within the European Economic Area (EEA). No access to or transfer of Personal Data outside the EEA shall occur without a valid transfer mechanism in place as required by Data Protection Law.

3.6 Assistance and Deletion: The Processor shall provide reasonable assistance to the Controller in responding to Data Subject Rights requests. Upon termination of the Agreement, the Processor shall cease all access to the Controller's Personal Data, and all personnel access rights shall be revoked. The Processor will not retain any copies of the Personal Data.

4. Liability

The liability of each party under this DPA shall be subject to the limitations of liability set out in Section 10 of the Professional Services Agreement (PSA).

ANNEX I: DETAILS OF PROCESSING

- **A. List of Parties**
 - **Data Controller:** As defined in the Agreement.
 - **Data Processor:** Acterus B.V.
- **B. Description of Processing**
 - **Categories of Data Subjects:** Controller's employees and other end users of the SyncForce Platform.
 - **Types of Personal Data:** Full name and business email address of end users stored within the SyncForce Platform.
 - **Subject-Matter and Nature of the Processing:** The Processor's authorized personnel will access the Controller's instance of the SyncForce Platform to provide Professional Services, including but not limited to, implementation, configuration, training, and technical support. Activities may include viewing, creating, or modifying user profiles as directed by the Controller.
 - **Purpose of the Processing:** To deliver the Professional Services as defined in the Agreement and any applicable SoW or Order Form.
 - **Duration of the Processing:** For the term of the professional services engagement as defined in the Agreement.

ANNEX II: SUB-PROCESSORS

The Controller provides a general authorisation for the Processor to engage the sub-processors listed below. The Processor shall inform the Controller of any intended changes to this list, thereby giving the Controller the opportunity to object.

Sub-processor Name	Service Provided	Location
Viv-it Services Srl	Professional Services and Support	Romania (EEA)

ANNEX III: TECHNICAL AND ORGANISATIONAL SECURITY MEASURES (Processor's Environment)

The Processor has implemented and maintains a comprehensive Information Security Management System (ISMS) that is certified against the ISO/IEC 27001 standard. This ISMS underpins the following measures to secure its corporate environment and personnel access:

- **Personnel Security:** Personnel with access to customer data are subject to confidentiality agreements and undergo regular security and data protection training.
- **Endpoint Security:** All company-issued devices used to access customer environments are managed, encrypted, and protected with anti-malware software.
- **Access Control:** Access to customer environments is restricted to authorized personnel on a need-to-know basis. Multi-factor authentication is enforced for accessing sensitive systems, including customer platforms where available.
- **Data Minimisation:** Processor's personnel are instructed to only access the minimum amount of Personal Data necessary to perform their assigned tasks. No Personal Data is to be downloaded or stored locally from the customer's Platform instance unless explicitly authorized by the Controller for a specific task.