Data Processing Agreement (DPA)

Mödling, 10.08.2026

SCHUHFRIED GmbH, Hyrtlstraße 45, 2340 Mödling, Austria
Tel. +43/2236/42315-0 | info@schuhfried.com | www.schuhfried.com
Residence: Mödling, FN 104661p
Regional court: Wr. Neustadt, UID No. ATU 19273809

SCHUHFRIED
psychometrics for you

TABLE OF CONTENTS

1. DEFINITIONS AND INTERPRETATION 3
2. PROCESSING OF COMPANY PERSONAL DATA 4
3. PROCESSOR PERSONNEL 5
4. SECURITY 5
5. SUBPROCESSING 5
6. DATA SUBJECT RIGHTS 6
7. PERSONAL DATA BREACH 6
8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION .. 6
9. DELETION OR RETURN OF COMPANY PERSONAL DATA 7
10. AUDIT RIGHTS 7
11. DATA TRANSFERS 7
12. GENERAL TERMS 8

Last modified: August 10th, 2026

This Data Processing Agreement (“Agreement”) forms part of the Contract for Services under SCHUHFRIED GmbH's Terms and Conditions (the “Principal Agreement”) between

SCHUHFRIED GmbH, Hyrtlstraße 45, 2340 Mödling, Austria

*(referred to as the “**Processor**”)*

and

(referred to as the “**Company**”, which is to be understood as any business or organization using the Services, regardless of its legal form).

This Agreement governs the specific requirements of Data Protection Laws to the extent that the Company's use of SCHUHFRIED Services involves the processing of Personal Data subject to Data Protection Laws.

The term of this Agreement shall follow the term of the Principal Agreement. Terms not defined herein shall have the meaning as set forth in the Principal Agreement.

WHEREAS

A) The Company acts as a Data Controller (the “Controller”).

B) The Company wishes to subcontract certain Services (as defined below), which involve the processing of Personal Data, to SCHUHFRIED GmbH, acting as a Data Processor (the “Processor”).

C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) and other applicable data protection laws.

D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1) “**Agreement**” means this Data Processing Agreement and all Schedules;

1.2) “**Company Personal Data**” means any Personal Data related to the Company or the Company's customers, employees, or test persons processed in connection with the Principal Agreement;

1.3) “**Contracted Processor**” means a Subprocessor;

1.4) “**Data Protection Laws**” means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.5) “**EEA**” means the European Economic Area;

1.6) “**EU Data Protection Laws**” means the GDPR as transposed into or supplemented by the domestic legislation of each EU Member State, and as amended, replaced or superseded from time to time;

1.7) “**GDPR**” means EU General Data Protection Regulation 2016/679;

1.8) “**Data Transfer**” means:

- 1.8.1) a transfer of Company Personal Data from the Controller to the Processor or a Contracted Processor; or
- 1.8.2) an onward transfer of Company Personal Data from the Processor to a Subprocessor, or between two establishments of a Subprocessor;

1.9) “**Services**” means the Vienna Test System online (VTS online) platform and related services provided by SCHUHFRIED GmbH and associated support and maintenance services. The details of the Services and applicable pricing are set out in the Principal Agreement and on SCHUHFRIED's website.

1.10) “**Subprocessor**” means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Controller in connection with this Agreement.

The terms “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority” shall have the same meaning as in the GDPR or other applicable Data Protection Law, and their cognate terms shall be construed accordingly.

2. PROCESSING OF COMPANY PERSONAL DATA

Processor shall:

2.1) comply with all applicable Data Protection Laws in the Processing of Company Personal Data;

2.2) not process Company Personal Data other than on the Controller's documented instructions as set out in this section 2;

Controller instructs Processor to process Company Personal Data to:

2.3) provide the Services and related technical support, including the operation of VTS online for psychological assessment purposes;

2.4) fulfill legal obligations or resolve disputes;

2.5) carry out internal tasks aimed at optimizing the security, privacy, reliability, and functionality of the Services;

2.6) carry out internal reporting, operational monitoring, and other similar internal tasks necessary for the delivery of the Services.

3. PROCESSOR PERSONNEL

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement and/or to comply with Data Protection Laws and other relevant legislation in the context of that individual's duties to the Processor. Processor shall ensure that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. SECURITY

In accordance with Article 32(1) of the GDPR, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing. These measures shall be designed to protect the rights and freedoms of natural persons, considering the risks of varying likelihood and severity, including the risk of a Personal Data Breach.

The Processor shall assess the risks associated with processing activities and apply measures consistent with the requirements of Article 32(1) GDPR, ensuring the security of Company Personal Data at all times. An overview of SCHUHFRIED's technical and organizational measures is available in the SCHUHFRIED Trust Center.

5. SUBPROCESSING

Subject to this Agreement, the Company grants general authorization to the Processor to engage Subprocessors and to disclose or transfer Company Personal Data to them. The Company acknowledges and approves the list of Subprocessors (see Subprocessors), understanding that this list may be updated by the Processor from time to time. The Company shall be informed of material changes to the Subprocessor list in accordance with SCHUHFRIED's notification process.

The Processor shall ensure that Subprocessors are subject to an agreement with the Processor no less restrictive and protective than this Agreement with respect to the protection of Company Personal Data, to the extent applicable to the nature of the services provided by the Subprocessor.

Individuals who support SCHUHFRIED's technical product development (including sole traders and freelancers) and who act under SCHUHFRIED's direct authority, integrated into its teams and without autonomous decision-making power over any processing, are classified by SCHUHFRIED as employee-equivalent within the meaning of Article 4(10) and Article 29 GDPR. Such individuals are not treated as Subprocessors under this Agreement. The criteria and obligations applicable to this classification are described in SCHUHFRIED's Organizational Measures.

6. DATA SUBJECT RIGHTS

Taking into account the nature of the processing, Processor shall provide reasonable assistance to the Company to fulfill the Company's obligations to respond to requests to exercise Data Subject rights under Data Protection Laws.

Processor shall:

6.1) promptly notify the Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2) ensure that it does not respond to that request except on the documented instructions of the Controller or as required by applicable laws to which the Processor is subject, in which case the Processor shall, to the extent permitted by applicable laws, inform the Controller of that legal requirement before the Processor responds to the request.

7. PERSONAL DATA BREACH

The Processor shall manage any Personal Data Breach in compliance with applicable Data Protection Laws and its internal Personal Data Breach procedures. In the event of a Personal Data Breach affecting Company Personal Data, the Processor shall notify the Company without undue delay, providing sufficient information to enable the Company to fulfill its obligations under Data Protection Laws, including informing Data Subjects where necessary.

The Processor shall cooperate with the Company and take reasonable steps as directed by the Company to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

Each party shall bear the costs of investigation, remediation, mitigation, and other related costs to the extent a Personal Data Breach is caused by that party.

Each party shall bear the costs of any fines, penalties, damages, or other related amounts imposed by an authorized regulatory body, governmental agency, or court of competent jurisdiction to the extent arising from that party's breach of its obligations under this Agreement.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Processor shall provide reasonable assistance to the Company with any data protection impact assessments and prior consultations with Supervisory Authorities or other competent data privacy authorities that the Controller reasonably considers to be required by Articles 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to processing of Company Personal Data by the Contracted Processors and taking into account the nature of the processing and information available to the Processor.

9. DELETION OR RETURN OF COMPANY PERSONAL DATA

Upon cessation of any Service involving the processing of Company Personal Data, the Processor shall delete all Company Personal Data to the extent permitted by applicable laws and in accordance with the Processor's Principal Agreement and data retention policy. The Company may export their data prior to account closure; requests made after account deletion can no longer be fulfilled.

Details of SCHUHFRIED's data retention and deletion practices are described in the Customer data lifecycle section of the Trust Center documentation.

10. AUDIT RIGHTS

Subject to this section 10, the Processor shall make available to the Company on request all information reasonably necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the processing of Company Personal Data by the Contracted Processors.

The Company shall not exercise its audit rights more than once per calendar year except following a Personal Data Breach or an instruction by a regulatory authority. The Company shall give the Processor at least sixty (60) days' prior written notice of its intention to conduct an audit. Audits shall be conducted during the Processor's business hours, shall not disrupt the Processor's operations, and shall ensure the protection of the Company's, Processor's, and other Data Subjects' Personal Data. The Processor and the Company shall mutually agree in advance on the date, scope, duration, and applicable security and confidentiality controls. The Company acknowledges that signing a non-disclosure agreement may be required prior to the conduct of the audit. The Company shall bear all costs reasonably incurred by the Processor in connection with an audit, including staff time and any third-party costs.

Information and audit rights of the Company only arise under this section 10 to the extent that the Agreement does not otherwise provide them with information and audit rights meeting the relevant requirements of Data Protection Law.

11. DATA TRANSFERS

The Processor shall only transfer or authorize the transfer of Company Personal Data to countries within the EU/EEA or to countries subject to an adequacy decision as provided for in Article 45 GDPR. Company Personal Data processed under this Agreement is hosted and processed within the European Union (Microsoft Azure West Europe region, Netherlands).

If a transfer of Company Personal Data to a country outside the EU/EEA or a country without an adequacy decision is required — for example, in the context of Subprocessor services — the Parties shall ensure that the Personal Data is adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU-approved standard contractual clauses or other transfer mechanisms as provided for by Data Protection Laws. The Processor shall be authorized to perform such transfers to Subprocessors

provided that adequate safeguards are implemented with regard to the nature of the transfer.

12. GENERAL TERMS

Compliance with Applicable Laws. Processor will process Company Personal Data in accordance with this Agreement and Data Protection Laws applicable to its role under this Agreement. Processor is not responsible for complying with Data Protection Laws that are solely applicable to the Company by virtue of its business, sector, or jurisdiction.

Confidentiality. Each party must keep confidential any information it receives about the other party and its business in connection with this Agreement ("**Confidential Information**") and must not use or disclose that Confidential Information without the prior written consent of the other party, except to the extent that:

- (a) disclosure is required by law; or
- (b) the relevant information is already in the public domain through no fault of the Parties.

Notices. All notices and communications given under this Agreement must be in writing and will be sent by email. The Controller shall be notified by email sent to the address associated with its account under the Principal Agreement. The Processor shall be notified by email sent to: datenschutz@schuhfried.com.

Governing Law and Jurisdiction. This Agreement shall be governed by Austrian law and the applicable law of the European Union. Any disputes, actions, claims or causes of action arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the competent courts of Mödling, Austria.

In case of discrepancy between the German version of this Agreement and any translated version, the German version shall prevail.

Signature Company

Signature SCHUHFRIED GmbH