PUBLISHED ON: July 16, 2026

DATA PROCESSING AGREEMENT

between

Trusty Client - the Controller - hereafter named the "Client" -

and

Trusty AG, Bösch 82, 6331 Hünenberg, Switzerland - the Processor - hereafter named the "Service Provider" or the “Provider” -

1. Background and Scope

The Service Provider and the Client have entered into the principal contractual relationship, which is governed by the Terms of Service (the Terms). The latter stipulate terms and conditions for the use of the Service Provider’s web-based applications (the Applications) by the Client.

For the purpose and within the scope of providing any of the Applications under the said Terms, the Service Provider shall process personal data for the Client in accordance with the GDPR and this agreement.

If there is a discrepancy between this agreement and the Terms, this agreement shall take precedence in relation to the personal data processing, unless explicitly provided otherwise herein.

This agreement may be made available in different languages. In case of conflicts between the English version and any translation, the English version shall prevail.

2. Object, Nature and Purpose of Data Processing

The Service Provider is providing the web-based Applications with their primarily intended usages described in their respective Additional Terms to the Terms of Service. The Client decides how they use any of the Applications.

The personal data and other information that are intended to be collected and processed in the Applications are listed in the Appendix 1.

The data and information in the Appendix 1 shall be stored in the Application’s database operated by the Service Provider and hosted on a virtual server in the EU, all on behalf of and for the Client. Unless explicitly provided in this Agreement, no data are transferred to third countries outside of the European Economic Area without the prior consent of the Client and may only occur if the special conditions defined in Articles 44 et seq. of the GDPR are fulfilled.

The Service Provider shall process the said personal data and other information in the Application exclusively for operation and maintenance of the Applications, its webpages and database.

3. Technical and Organizational Measures

Technical and organizational measures, together with their implementation and observance, are detailed in Appendix 2. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

The Service Provider shall establish the security of the data in accordance the GDPR requirements. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems.

The technical and organizational measures shall be subject to technical progress and further development. In this respect, the Service Provider is permitted to implement alternative adequate measures. The safety level of the specified measures must not be compromised. Substantial changes must be documented.

4. Requests by Affected Persons

The Service Provider shall not correct, delete or restrict the processing of data on a direct request by affected persons. Insofar as an affected person contacts the Service Provider directly in this respect, the Service Provider will immediately forward this request to the Client without delay.

TRUSTY

5. Quality Assurance and Other Duties of the Service Provider

In addition to complying with the provisions of this agreement, the Service Provider shall comply with statutory obligations in accordance with Articles 28 to 33 of the GDPR; in this respect, the Service Provider shall particularly ensure compliance with the following requirements:

- Confidentiality in accordance with Article 28, paragraph 3, sentence 2, clause b, Article 29 and Article 32, paragraph 4. The Service Provider entrusts only such persons with the data processing defined in this agreement who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. The Service Provider and any person acting under its authority who has access to personal data may only process that data in accordance with the instructions of the Client (which includes the powers granted in this agreement and in the Terms) unless otherwise required to do so by law.
- The Service Provider and the Client shall, upon request, cooperate with the supervisory authority in the performance of their duties.
- The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to the processing of personal data under this agreement. This also applies insofar as the Service Provider is under investigation or is a party to an investigation by a competent authority in connection with infringements to any civil or criminal law, administrative rule, or regulation regarding the processing of personal data under this agreement.
- Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim of an affected person or a third party or any other claim in connection with the processing of personal data under this agreement, the Service Provider shall make every effort to support the Client to the best of his ability.
- The Service Provider shall regularly monitor the internal processes as well as the technical and organizational measures to ensure that the processing in its area of responsibility is executed in accordance with the requirements of the applicable data protection law and that the rights of the affected people are protected.
- Without undue delay and no later than 24 hours after the Service Provider has become aware of a security breach, the Service Provider shall notify the Client thereof in writing. This notification shall, at a minimum, and to the extent possible in light of the nature of the incident, include the following:
    - information on the nature of the identified security breach,
    - what categories of registered individuals are affected by it, and
    - the approximate number of the affected registered individuals, including categories of comprehensive personal data and the number of these in addition to what preventive or mitigating measures the Service Provider has implemented as a result of the found security breach.

The Service Provider shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments, and prior consultations referred to in Articles 32 to 36 of the GDPR.

6. Subcontracting

The Service Provider is engaging third party service providers (subcontractors) for the purpose of providing the Application. The list of subcontractors is provided in Appendix 1.

The Service Provider shall provide a 10 (ten) days advance notice before replacing the existing or engaging any new subcontractor. The Client may object in writing to the Service Provider's appointment of a subcontractor on reasonable grounds relating to data protection by notifying the Service Provider promptly in writing within 5 (five) days of receipt of the Service Provider's notice. Such notice shall explain the reasonable grounds for the objection. In such event, the parties shall discuss the Client's concerns in good faith with a view to achieving commercially reasonable resolution.

Where the Service Provider engages a Sub-processor, it shall impose on such Sub-processor, by way of a contract or other legal act under Union or Member State law, the same data protection obligations as set out in this Agreement, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR.

The Service Provider shall remain fully liable to the Client for the performance of the Sub-processor's obligations under this Agreement.

7. The Client's Inspection Rights

The Client shall, at its own expense, have the right to conduct inspections, or have them conducted by independent third parties, with the purpose of verifying the Service Provider’s compliance with this agreement. Any inspection by the Client shall be announced to the Service Provider in good time.

The Service Provider shall ensure that the Client can verify the Service Provider's compliance with the obligations under Article 28 of the GDPR. The Service Provider is obligated to provide the Client with the necessary information upon request and in particular to provide proof of the implementation of the technical and organizational measures.

8. The Client’s Instructions

The Client shall immediately confirm any oral instructions in writing.

The Service Provider shall inform the Client immediately if it believes that an instruction violates data protection regulations. The Service Provider shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or alters said instructions.

9. Deletion and Return of Personal Data

Copies or duplicates of the data shall not be created without the knowledge of the Client, except for backup copies as far as they are necessary to ensure proper data processing as well as data required for compliance with statutory storage obligations.

Upon termination of the Terms in relation to any of the Applications and consequently this agreement, the Service Provider shall, at the choice of the Client, either i) permanently delete, or ii) enable the Client to export the data to itself, and then permanently delete all the existing copies, unless the Service Provider is legally obliged to store such data. The Client shall exercise its choice under (ii), and export any Client Data it wishes to retain, using the Application's export functionality during the retention period set out in Article 16.3 of the Terms; the Service Provider shall have no obligation to export or return the Client Data on behalf of the Client or any User. Upon the lapse of that retention period, the Service Provider shall permanently delete the Account, including the Client Data, from its production environment; the Account and the Client Data shall thereafter be permanently deleted from the Service Provider's backups in the ordinary course of its regular backup rotation cycle, and the Service Provider does not warrant or guarantee a specific date on which such deletion from backups will occur.

Notwithstanding the preceding provision, the Service Provider is entitled to save copies of data to the extent necessary to be able to document delivery of services as per the Terms or to defend itself against legal claims. In such a case, the Client’s personal data may be processed by the Service Provider for the stated purposes only.

Upon request, the Service Provider shall provide the Client with information on nature and the time of the data’s deletion.

10. Final Provisions

Modifications

The Service Provider reserves the right to change, modify, add, or remove portions of this Agreement at any time only for important reasons, in particular due to changes in applicable law, regulatory requirements, binding court decisions, or to reflect technical or organisational changes of the Application.

The Service Provider shall post such changes on https://trusty-compliance.com/documents and through the Application. The Client shall be notified of the change through the Application, and the changed and amended Agreement shall become effective ten (10) days after such notification.

The Client may object to such changes in writing within the ten (10) day notice period. In the event of an objection, the Agreement shall continue to apply unchanged until terminated by either Party in accordance with its terms.

If the Client does not object within the notice period, the changes shall become effective as notified.

Term of the Agreement

This agreement enters into force between the parties together with the Terms and also ceases to be in effect with the cancellation or any other termination of the Terms in relation to and in respect of any of the Applications.

The right to isolated extraordinary notice of cancellation hereby remains intact, as do statutory rights of rescission.

Jurisdiction

The parties agree that any claims and disputes that may arise from the agreement shall be settled by the court in Zug, Switzerland.

Contact

Should you have any complaints about how we handle your personal information, please contact us at support@trusty-compliance.com. If we are unable to resolve your complaint and you wish to take your complaint further, you may do so by contacting the relevant supervisory authority. You can find a list of EU supervisory authorities here.

Our appointed representatives:

- for the EU: Odvetniška družba Podjed, Kahne in partnerji o.p. – d.o.o., Štefanova ulica 13A, 1000 Ljubljana, Slovenia, tel: +386 1 43 00 310, email: info@podjed.si; lead contact person: Mr Luka Podjed

Our representatives are mandated by us to be addressed in addition to or instead of us by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with respective EU or UK data privacy regulation.

Note: As a Trusty Client you can request a signed version of this agreement to enable you to be compliant with your data protection obligations; please send your request to support@trusty-compliance.com

Appendix 1 to the Data Processing Agreement

List of Personal Data and Other Information Processed in the Application

All Applications

- personal data relating to the users of the Application authorised by the Client: first name, last name, email address;
- personal data relating to the person responsible for invoicing at the Client: first name, last name, email, telephone number.

Specific for Trusty Whistleblowing

- personal data relating to a whistleblower (reporting person), if provided: first name, last name, email address, telephone number, relationship toward the Client;
- personal data relating to the persons suspected to be involved and the persons being aware of the violation/wrongdoing, if provided: full name, position, organization; a factual description of the violation/wrongdoing, as well as a description of the circumstances of the incident, including time and place of the incident.

Specific for Trusty QuickScreen 360

- personal data relating to the contact person of the business partner: first name, last name, email address, telephone number, title/role;
- personal data relating to the business partner's officers, directors and executives: first name, last name, year of birth, country of residence, title, sanction lists records, politically exposed persons records;
- personal data relating to the business partner's owners: first name, last name, year of birth, country of residence, ownership percentage, sanction lists records, politically exposed persons records;
- personal data of contacted public officials as provided by the supplier;
- personal data relating to the screened individual: first name, last name, year of birth, country of residence, sanction lists records, politically exposed persons records, adverse media records.

List of subcontractors:

- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany;
    - Hosting of the backend of the Applications (Whistleblowing, QuickScreen 360, EUDR Passport and the Academy administration), including the primary database, search index and file storage, on virtual servers in Nuremberg, Germany.
- AWS EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg;
    - Provides notification email relay service;
- OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland;
    - Provides artificial intelligence service for assessments of sanctions search results quality;
- Salesforce, Inc. Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105, United States;
    - Provides hosting of the PolicyApp and Academy frontend App on the virtual server in Europe through their product Heroku;
- Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland;
    - Azure OpenAI Service; artificial-intelligence processing for adverse-media and sanctions result analysis, policy summarisation and translation, training-content generation and document validation. Regions: Germany (EU) and Sweden Central (EU).
- Stripe Payments Europe, Limited (SPEL), 3 Dublin Landings, North Wall Quay, Dublin 1, D01 C4E0, Ireland;
    - Provides payment processing services;
- CRIF AG, Hagenholzstrasse 81, 8050 Zurich, Switzerland;
    - Provides information on politically exposed persons via their AML GUARD Service;
- Zoho Corporation GmbH, Trinkausstraße 7, 40213 Düsseldorf, Germany;
    - Provides CRM services and Client email campaigns using data centers in Amsterdam and Dublin.
- SerpApi, LLC, 5540 N Lamar Blvd #12, Austin, TX 78751, United States;
    - Search-engine results for adverse-media screening.

- ScrapingBee SAS, Clever Cloud SAS 4 rue Voltaire 44000 Nantes France;
    - Retrieval of web page content of adverse-media sources.

Appendix 2 to the Data Processing Agreement

Technical and Organizational Measures

The Service Provider prevents unauthorized internal access to the Application by applying security updates regularly by using state of the art technology, hence securing critical network access points. Allocation of authorisations to the Service Provider's staff is revision-proof.

Electronic access to the Application by the Client is protected through password authentication or OAuth2 login methods. After opening of the Client Application Account, the initial user password is required to be changed by the Client and is not known to the Service Provider. The Client's password is determined by the Client himself; the password must comply with predefined guidelines relating to the minimum number of characters and numbers. The Client is responsible for authorising and opening additional user accounts for the Application.

The Application data are physically or logically isolated and saved separately from other Service Provider's data. Backups of data are performed using a similar system of physical or logical isolation. Backups of all Application data are performed daily.

Resilience measures such as security programs (firewalls, encryption programs, spam filters) and monitoring of all relevant servers are employed.

In order to ensure confidentiality, the Whistleblowing Application does not store IP addresses and time stamps.

The Application supports functioning in a server farm and ensures uninterrupted functioning (24x7x365). Any scalability for performance and additional services is provided. No licensed programs are used. The software is using open-source solutions (MySQL, Apache, Laravel, jQuery, Bootstrap).

SSL/TLS encryption is used to ensure security and privacy during data transfer. Textual data from the contents of the reports and from the communication channel with a whistleblower are encrypted with the symmetric AES CBC algorithm using the OpenSSL extension. Files are encrypted using AES 256 CTR cipher. All passwords in the Application are compressed with the Bcrypt algorithm. The Application uses Linux Iptables/Netfilter firewall.

In relation to the Whistleblowing Application only pseudonymisation of whistleblower data is provided with randomly generated usernames for each whistleblower individually.

The program records an audit trail for each entry/insight/change. All access and key events are logged, and these logs are accessible to the Service Provider, if necessary.

Terminated Application accounts are permanently deleted and overwritten.

The Client may delete contents from the Application (for example individual reports in the Whistleblowing Application); the Client is additionally warned when such content deletions are permanent and overwritten.

The Service Provider regularly mandates a third party provider to perform a web-application penetration test on the Application and subsequently resolves identified security vulnerabilities, if any.

Technical and organizational measures relating to the subcontractors are available on the Client's request sent to support@trusty-compliance.com