CCPA and CPRA Service Provider Contract

Between

Trusty Client - the Business - hereafter named the "Client" -

and

Trusty AG, Bösch 82, 6331 Hünenberg, Switzerland - the Service Provider - hereafter named the "Service 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 the Application under the said Terms, the Service Provider shall process personal information for the Client in accordance with the CCPA and CPRA and this contract.

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

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

2. Purpose of 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 information and other information that are intended to be collected and processed in the Application are listed in the Appendix 1.

The Service Provider shall process the said personal information and other information in the Application exclusively upon documented instructions from the Client for operation and maintenance of the Application, its webpages and database, which comprise the business purpose.

3. Technical and Organizational Measures

The Service Provider shall assist the Client through appropriate technical and organisational measures to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorised or illegal access, destruction, use, modification or disclosure. 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 information in accordance with the CCPA and CPRA requirements. The measures to be taken are measures of information 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. Consumers' Rights

With regards to the consumers' right to delete, the Service Provider shall cooperate with the Client in responding to a verifiable consumer request, and at the direction of the Client, shall delete or enable the Client to delete and shall

TRUSTY

notify any of its own service providers or contractors to delete personal information about the consumer collected, used, processed or retained by the Service Provider, except to where and to the extent permitted to retain the personal information pursuant to an exemption under the CCPA and/or CPRA. The Service Provider shall notify any service providers, contractors or third parties who may have accessed personal information from or through the Service Provider, unless the information was accessed at the direction of the Client, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.

The Service Provider shall not be required to comply with a deletion request submitted by the consumer directly to the Service Provider. Insofar as a consumer contacts the Service Provider directly in this respect, the Service Provider will immediately forward this request to the Client without delay.

With regards to the consumers' right to know what personal information is being collected, right to access personal information and right to know what personal information is sold or shared and to whom, the Service Provider shall provide assistance to the Client with respect to the Client's response to a verifiable consumer request, including, but not limited to, by providing to the Client the consumer's personal information in the Service Provider's possession and by correcting inaccurate information or by enabling the Client to do the same as it relates to the collection of personal information for the business purpose.

5. Quality Assurance and Other Duties of the Service Provider

In addition to complying with the provisions of this contract, the Service Provider shall comply with applicable obligations of the CCPA and the CPRA, providing the required level of privacy protection and also acknowledges that it shall not:

- Sell or share the personal information processed on behalf of the Client;
- Retain, use or disclose the personal information processed on behalf of the Client for any purpose other than for the business purpose or as otherwise permitted by this contract;
- Retain, use or disclose the information processed on behalf of the Client outside of the direct business relationship between the Service Provider and the Client, except where the Service Provider has engaged a subcontractor to assist in the provision of the services;
- Combine the personal information that the Service Provider receives from, or on behalf of, the Client with personal information that it receives from, or on behalf of, another person, or collects from its own interaction with the consumer, provided that the Service Provider may combine personal information to perform any business purpose as required by the Client and in compliance with the CCPA and/or the CPRA provisions.
- Share or process the personal information processed on behalf of the Client for targeted and on cross-context behavioural advertising.

The Service Provider certifies that it understands these restrictions and will comply with them. The Service Provider shall notify the Client if it determines that it can no longer meet its obligations under the CCPA and/or the CPRA.

With regards to assistance commitments, the Service Provider will, upon Client's written instructions and upon proof of such a communication, provide reasonable assistance to the Client to enable the Client to respond to any correspondence, inquiry or complaint received from a consumer for the California Attorney General in connection with the collection and processing of personal information.

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.

Where the Service Provider engages any other person to assist it in processing personal information for a business purpose on behalf of the Client or if any other person engaged by the Service Provider engages another person to assist in processing personal information for that business purpose, it shall notify the Client of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in this contract.

7. The Client's Inspection Rights

The Client has, at its own expense, the right to take reasonable and appropriate steps to ensure that the Service Provider uses the personal information processed on behalf of the Client in a manner consistent with the Client's obligations under the CCPA and/or the CPRA and to stop and remediate any unauthorised use of personal information. Any steps taken by the Client shall be announced to the Service Provider in good time.

8. The Client's Instructions

Any instructions shall be provided by the Client to the Service Provider by means of a written contract.

The Service Provider shall inform the Client immediately if it believes that an instruction violates CCPA and/or CPRA provisions. 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

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, at its sole discretion, to change, modify, add, or remove portions of the Contract at any time by posting such changes on https://trusty-compliance.com/documents website or through the Application. The Clients already subscribed to any Application will be notified on the change and amendment through the Application and for them such changed and amended contract will become effective 10 (ten) days after the posting in the Application.

The Client is obliged to check the contract periodically for changes. Continued use of the Application after such changes have become effective constitutes the Client's binding acceptance of such changes.

Term of the Contract

This contract 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.

Liability

The Service Provider shall not be liable for the obligations of the Client for which it provides services. The Service Provider shall only be liable for its own violation of its obligations under the CCPA and/or CPRA.

Jurisdiction

This contract shall be governed by and constructed in accordance with the governing law and jurisdiction as specified in the Terms, unless otherwise agreed by the Client and the Service Provider or unless otherwise required by the CCPA and/or CPRA.

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

Appendix 1 to the CCPA and CPRA Service Provider Contract

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 CCPA and CPRA Service Provider Contract

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