
CCPA and CPRA Service Provider Contract

between

ABC SEARCH CLIENT

- the Business - hereafter named the "Client" -

and

ABC Transparency GmbH, 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 Application called "abc search" (the Application) 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 Application where the Client, as the business, can conduct searches for records on publicly available websites on its subjects of interest. The Application has been designed to work as a fraud, background checks and compliance investigation search tool, but, to the extent not regulated by the Terms, the Client decides how they use the Application.

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 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 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.

The Service Provider may claim compensation for support services which are not attributable to failures on the part of the Service Provider, with the hourly rate of 250 CHF (VAT not included).

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.

The Service Provider may assert a claim for remuneration for enabling Client's inspections with the hourly rate of 250 CHF (VAT not included).

The Service Provider may at its own discretion provide support to the Client in any other reviews conducted by the latter, including but not limited to completing Client's questionnaires on security, privacy, data processing and similar topics related to the Application. In such cases the Service Provider may assert a claim for remuneration with the hourly rate from the preceding paragraph.

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

The Client Data (as defined by the Terms) are regularly permanently deleted from the Application database, as described under article 5.3 of the Terms (Conducting Searches in Modules).

Upon termination of the Terms and consequently this agreement the Service Provider shall permanently delete any remaining personal data of the Client in the Application database, unless the Service Provider is legally obliged to store such information or permitted by applicable law to retain some or all of the personal information, which the Service Provider shall continue to protect from any further processing, except to the extent required by applicable law.

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 its website or through

the Application. Such amended Contract will become effective 10 (ten) days after its posting on the Server Provider's website.

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.

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.

ABC Transparency GmbH, Dejan Jasnic



ABC SEARCH CLIENT _____

Appendix 1 to the CCPA and CPRA Service Provider Contract

List of Personal Information and Other Information Processed in the Application:

- personal data relating to a subject of interest: first name, last name, year of birth, address, postal code of residence, VRM;
- personal data relating to the users of the Application authorised by the Client: first name, last name, email address.

List of subcontractors:

- AWS EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg;
 - Provides hosting of the Application on the virtual server in London, UK;
 - Provides notification email relay services.

Appendix 2 to the CCPA and CPRA Service Provider Contract

Technical and Organizational Measures

The Service Provider prevents unauthorized 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 password protected. 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.

All passwords in the Application are compressed with the Bcrypt algorithm. The Application uses Linux Iptables/Netfilter firewall.

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.

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.

The files are transferred using the standard POST method. All communication with the website of the Application, including file transfer, is encrypted using HTTPS ciphers.

After receiving the input Client Data, the respective Module adds this data to the list of subjects of interest and immediately deletes the uploaded Client Data file permanently. The list of subjects of interest is encrypted using AES-CBC cipher and stored in the Application database. In relation to the Companies House Module the data on the subjects of interest are saved in the User's browser and in the Application database.

Any Search Results data files are made available for download by the User immediately after the search is completed. After its download and no later than 10 minutes after its generation, the Search Results data file is permanently deleted from the Application server. In case of unsuccessful download or search the orphan files are detected and permanently deleted every 10 minutes. The list of subjects of interest is also permanently deleted from the Application server together with all temporary files. The data on a subject of interest for which an alarm has been set are encrypted and stored on the hosting server and are permanently deleted once the User deletes the alarm.

All searches in all the Modules, apart from searches using the alarm function and in the Companies House Module, are performed using the memory (RAM) of the server and do not create any unencrypted files containing the data on the subjects of interest, except for the Search Result File. Any search creates temporary files that are encrypted and are required to process the search query; the key is held by the Supplier.

For searches using the alarm function, the data on the subjects of interest are saved in the Application database for the purpose of conducting recurring searches. The data are permanently deleted as soon as the User disables the respective alarm.

The searches in the Companies House Module are performed using the memory (RAM). When a search result entity is selected for a Connection Search, these data are saved in the User's browser and in the Application database. The data are permanently deleted from the latter after the search is completed. The User can also select to conduct a Connection Search in the background and save the results in the Application; in this case the data are permanently deleted when the User deletes the saved results in the Application.

All access and traffic data are logged, and these logs are accessible to the Service Provider.

Terminated Application accounts are permanently deleted 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.

Subcontractors

Technical and organizational measures (herein also referred to as TOMs) relating to the hosting server are detailed in the agreement between the Service Provider and AWS EMEA SARL, Annex 1.

Said document is incorporated into this Agreement by reference and are available at <https://abctransparency.com>.

PUBLISHED ON 1.9.2023