Data Processing Agreement

between

ABC SEARCH CLIENT

- the Controller - hereafter named the "Client" -

and

ABC Transparency GmbH, Bösch 82, 6331 Hünenberg, Switzerland

- the Processor - 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 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 Application where the Client, as the data controller, 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 data and other information that are intended to be collected and processed in the Application are listed in the Appendix 1.

The data and information in the Appendix 1 shall be processed in the Application's database operated by the Service Provider and hosted on a virtual server selected by Client in the registration form, all on behalf of and for the Client. No data are transferred outside the country of

the selected virtual server 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.

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.

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.

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.

The Service Provider shall provide a 10 (ten) days advance notice before 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.

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.

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

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.

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 data.

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 Agreement at any time by posting such changes on its website or through the Application. Such amended Agreement will become effective 10 (ten) days after its posting on the Server Provider's website.

The Client is obliged to check the Agreement 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 Agreement

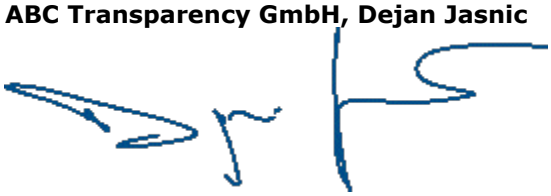
This Agreement enters into force between the parties together with the Terms and also ceases to be in effect with the cancellation or any other termination of the Terms.

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.

ABC Transparency GmbH, Dejan Jasnic



ABC SEARCH CLIENT_____

Appendix 1 to the Data Processing Agreement

List of Personal Data 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 Data Processing Agreement

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