Adresslabor
It´s that easy.

Annex to the Data Processing Agreement

Appropriate Technical and Organizational Measures (TOM)

Date: Mai 31th 2021

1. Organisational measures

Adresslabor is a sole proprietorship without employees. The owner is:

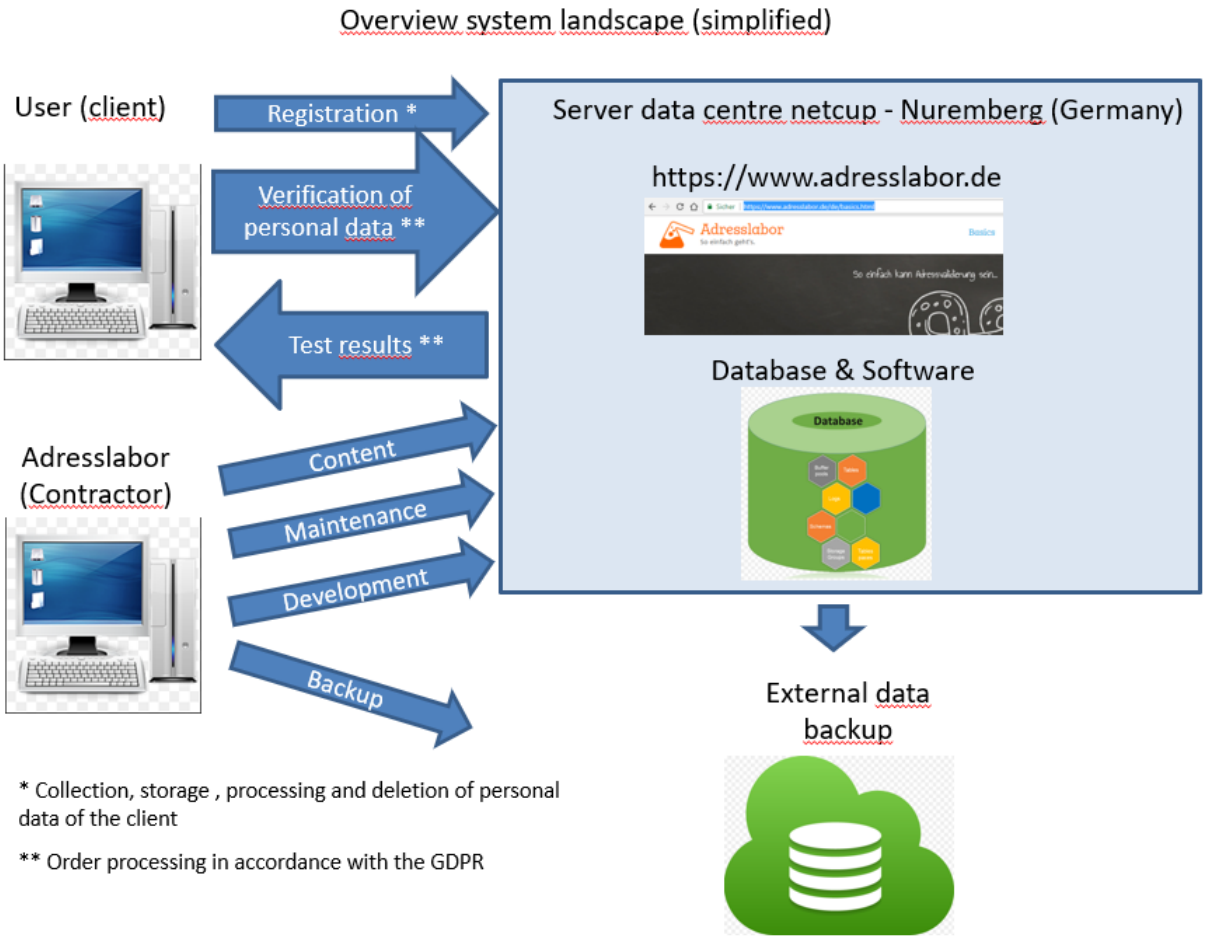
Rolf Paschold
www.adresslabor.de
Phone: +49 (0) 170 3 55 22 01
E-Mail: r.paschold@adresslabor.de

All external service providers (advertising agency for the website, IT developers for maintenance and support) who might have access to personal data have been obligated in writing to maintain company secrets and to comply with the basic data protection regulation GDPR.

Data protection officer: No data protection officer has been appointed. The legal basis for this is Article 37 GDPR and Section 38 (I) Sentence 2 BDSG. Adresslabor employs fewer than 10 persons who are permanently involved in the automated processing of personal data. Furthermore, the data processing is not subject to a data protection impact assessment and does not serve market or opinion research. The owner is responsible for compliance with the statutory data protection obligations.

System landscape and basic, automated processes

For a better understanding of the following TOM, this graphic should serve.



Both the website https://www.adresslabor.de (frontend) and the database and software for the Adresslabor products (backend) are located on a server rented from netcup GmbH (www.netcup.de). This server is located in Nuremberg, Germany.

The client (user/customer) creates a customer account with his free registration at http://www.adresslabor.de and enters his personal data, which are required for data processing and possible invoicing (registration). The customer's e-mail address serves as the unique user name, the customer himself assigns the password for access. This is hash-encrypted internally and cannot be read or viewed by anyone, including the client.

At the same time, the client receives his individual, unique "API Customer ID" and an "API Key" as a prerequisite for subsequent data processing via web service.

Only with the protected "Login" on adresslabor.de (e-mail and password) the pages "Single check" and "Bulk check" can be accessed.

Single check: Demo application for single, manually entered records to test for an extract of Adresslabor's products ("tests"). The user is shown the results of the test on the website.

Bulk check: Upload of Excel or CSV files with personal data, which are then tested in a batch process. After the checks are completed, the user receives an e-mail with a report on the results and can download the results file.

Web service: The web service is a REST API that allows an authorised user to check data from any application, such as an ERP system, a webshop check-out process or a CRM system. Triggered by a request to our server, the check starts at Adresslabor, the response with the check results usually comes immediately, within a few milliseconds (depending on the product).

The prerequisite for all three types of tests is a previously concluded agreement on commissioned processing in accordance with the GDPR.

All electronic communication between the user, adresslabor.com and the Adresslabor server is encrypted (https with SSL certificate). This also applies to the upload or download of files for the bulk check.

1. Anonymisation

Depending on the product, Adresslabor does not necessarily require personal data for the check. For example, the address check can be carried out exclusively with the information on country, postcode, city, street and house number, without reference to a person.

The Name-Check B2C requires first and last name and, if applicable, the salutation and a title, but no postal address.

This means that the client can largely control which data is transferred to Adresslabor for checking via the configuration of its processes.

Example:
A data record can be checked for a valid address (address check) and correct salutation/capitalisation (name check) at the same time, but it does not have to be.

Just as well, two separate checks can be started, one for the address only, one for the name only. Using a unique ID (e.g. customer number) on the data record, individual check results can be merged at the client.

2. Access control (physical securtiy)

Objective: Unauthorised access must be prevented. The term is to be understood spatially.

24/7 h video surveillance
In addition to mechanical access control, the data centre is also monitored around the clock by video. Any movement in the data centre triggers a message to a security company. If someone unauthorised is able to gain access to the data centre, security personnel are on site within minutes.

Source: https://www.netcup.de/ueber-netcup/rechenzentrum.php

3. Access control (environmental-related security)

Objective: The intrusion of unauthorized persons into the computer systems must be prevented.

- Password procedure (special characters, minimum length, regular change of password).
- Automatic blocking (pausing, blocking of access IP after 3 unsuccessful login attempts)
- One user master record per user

Objective: Unauthorised activities in IT systems outside of granted authorisations are to be prevented.

- Differentiated authorisations (profiles, roles)
- Access control via system log file (can be evaluated if required)
- Deletion of authorisations after leaving the company or changing service providers
- Firewall/ malware protection

4. Transfer control

Objective: Aspects of the transfer of personal data are to be regulated: Electronic transfer, data transport, transfer control.

- Encryption of transport routes: HTTPS with SSL certificates RSA 2048 bits (SHA256withRSA) for

  www.adresslabor.de
  api.adresslabor.de

- Restricted SSH access.
- Connection of subcontractors only encrypted according to the latest state of the art and with agreement on order processing GDPR.
- Logging of upload/download times per user and product for bulk checking (not of the personal data itself).
- Logging of web service requests (user, timestamp, product)

5. Input control

Objective: Traceability or documentation of data management and maintenance must be ensured.

- No overwriting of the requested data. Request data are retained after processing and are enriched with correction suggestions and/or result codes.
- The decision-making power to accept correction suggestions lies with the client.
- Deliberately no documentation and storage of the requested data and test results for data protection reasons.

6. Order control

Objective: Commissioned processing in accordance with instructions must be ensured.

The Client may obtain all relevant information on the Contractor's website before deciding on Adresslabor:

- Predefined services with product descriptions under "Details
- Demo videos for individual products under "Demo
- Disclosure of expected results under "Documentation
- Sample codes for various programming languages
- Free tests possible (10 € starting credit)
- The client then places his order and gives instructions by using the SaaS offer or purchasing credits.

7. Availability control

Objective: The data shall be protected against accidental destruction or loss.

Redundant, uninterruptible power supply

The data centre has a redundant power supply. This is also supported by a UPS and a diesel generator. Within the data centre, the redundancy is continued up to the individual servers [...].

Redundant, uninterruptible network connection

netcup GmbH is a direct member of RIPE, the allocation body in Europe for IP addresses. The data centre is connected to various nodes of the Internet, such as the DE-CIX, N-IX or the AMS-IX, through the integration into the Anexia Backbone Europe with multiple redundancy [...]. This creates very good fail-safety.

Redundante, unterbrechungsfreie Klimatisierung

Three independent air-conditioning units share the task of sufficiently cooling the equipment in the data centre. At least one air conditioner can fail without endangering the cooling. Each air conditioner is connected to the redundant, uninterruptible power supply. [...]
Source: https://www.netcup.de/ueber-netcup/rechenzentrum.php

Additions Addreslabor

- Weekly complete backup for website, database and software.
- Nightly backup of all transaction data (users, credit logs, ...).
- Destruction or loss is already excluded by the concept (no original data in processing).

8. Separation control

Objective: Data collected for different purposes must also be processed separately.

All data are processed separately for different purposes (storage, modification, deletion, transmission) through appropriate programming.

Adresslabor, Rolf Paschold (Owner)