Adresslabor
So einfach geht's.

Anlage zur Auftragsverarbeitung

Technische und organisatorische Maßnahmen (TOM)

Stand: 31.05.2021

1. Organisatorische Maßnahmen

Adresslabor ist ein Einzelunternehmen ohne Beschäftigte. Der Inhaber ist:

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

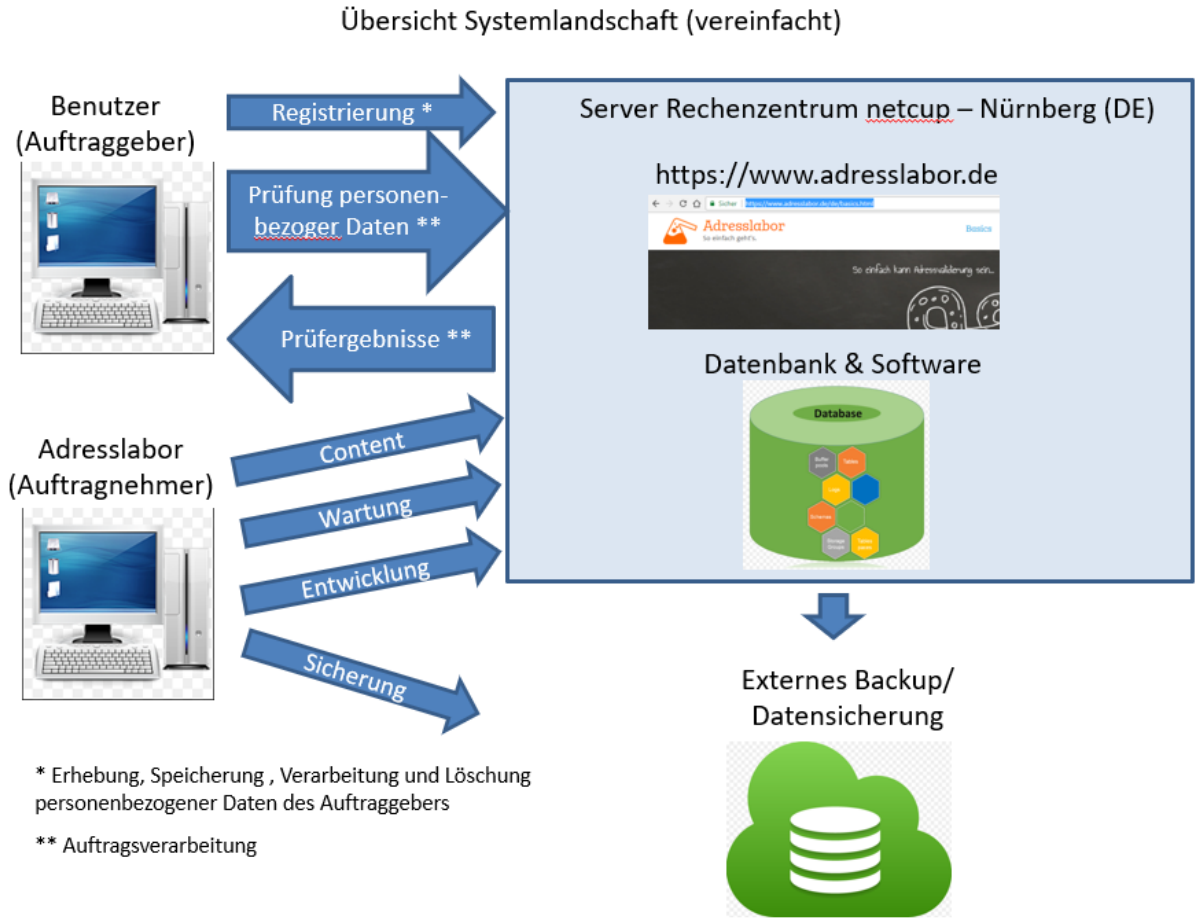
Alle externen Dienstleister (Werbeagentur für die Website, IT-Entwickler für Wartung und Support), die Zugriff auf personenbezogene Daten erhalten könnten, wurden schriftlich zur Wahrung der Betriebsgeheimnisse und Einhaltung der Datenschutz-Grundverordnung DSGVO verpflichtet.

Datenschutzbeauftragter: Es ist kein Datenschutzbeauftragten bestellt. Die Rechtsgrundlage hierfür ergibt sich aus Art. 37 DSGVO sowie § 38 Abs. I Satz 2 BDSG. Adresslabor beschäftigt weniger als 10 Personen, die ständig in der automatisierten Verarbeitung von personenbezogenen Daten tätig sind. Weiterhin unterliegt die Datenverarbeitung nicht einer Datenschutz-Folgeabschätzung und dient nicht der Markt- oder Meinungsforschung.

Für die Einhaltung der gesetzlichen Datenschutzpflichten steht der Inhaber ein.

Systemlandschaft und grundlegende, automatisierte Prozesse

Zum besseren Verständnis der folgenden TOM soll diese Grafik dienen.



Sowohl die Internetseite https://www.adresslabor.de (Frontend) als auch die Datenbank und die Software für die Produkte von Adresslabor (Backend) liegen auf einem netcup GmbH angemieteten Server (www.netcup.de). Dieser Server steht in Nürnberg, Deutschland.

Der Auftraggeber (Benutzer/ Kunde) erstellt mit seiner kostenlosen Anmeldung auf www.adresslabor.de ein Kundenkonto und erfasst seine personenbezogenen Daten, die zur Auftragsabwicklung und einer eventuellen Rechnungsstellung benötigt werden (Registrierung). Als eindeutiger Benutzername dient die E-Mail-Adresse des Kunden, das Passwort für den Zugang vergibt der Kunde selbst. Dieses wird intern Hash-verschlüsselt und kann von niemandem ausgelesen oder eingesehen werden, auch nicht vom Auftraggeber.

Gleichzeitig erhält der Kunde seine individuelle, eindeutige „API Customer ID“ und einen „API Key“ als Voraussetzung für eine spätere Auftragsverarbeitung via Webservice.

Erst mit dem geschützten „Login“ auf adresslabor.de (E-Mail und Passwort) kann auf die Seiten „Einzelprüfung“ und „Massenprüfung“ zugegriffen werden.

Einzelprüfung: Demo-Anwendung für einzeln, manuell erfasste Datensätze zum Test für einen Auszug der Produkte („Tests“) von Adresslabor. Dem Benutzer werden die Ergebnisse der Prüfung auf der Internetseite angezeigt.

Massenprüfung: Upload von Excel- oder CSV-Dateien mit personenbezogenen Daten, die dann im Batchverfahren geprüft werden. Nach Abschluss der Prüfungen erhält der Benutzer eine E-Mail mit einem Bericht zu den Ergebnissen und kann die Ergebnisdatei herunterladen.

Webservice: Der Webservice ist eine REST-API, mit der ein autorisierter Benutzer Daten von beliebigen Anwendungen aus prüfen lassen kann, zum Beispiel ERP-System, Check-out Prozess des Webshops oder ein CRM-System. Ausgelöst durch eine Anfrage („Request“) an unseren Server startet die Prüfung bei Adresslabor, die Antwort („Response“) mit den Prüfergebnissen kommt in der Regel sofort, innerhalb von wenigen Millisekunden (je nach Produkt/Test).

Voraussetzung für alle drei Arten der Prüfungen ist eine zuvor geschlossene Vereinbarung zur Auftragsverarbeitung nach DSGVO.

Die komplette elektronische Kommunikation zwischen dem Benutzer, adresslabor.de und dem Server von Adresslabor ist dabei verschlüsselt (https mit SSL-Zertifikat). Das gilt auch für den Upload bzw. Download von Dateien für die Massenprüfung.

1. Anonymisierung

Adresslabor benötigt - je nach Produkt – nicht zwingend personenbezogene Daten zur Prüfung. So kann z.B. der Adress-Check ausschließlich mit den Informationen zu Land, PLZ, Ort, Straße und Hausnummer durchgeführt werden, ohne Bezug zu einer Person.

Der Name-Check B2C benötigt Vor- und Nachname und ggf. die Anrede und einen Titel, aber keine postalische Adresse.

Damit kann der Auftraggeber über die Konfiguration seiner Prozesse weitgehend selbst steuern, welche Daten an Adresslabor zur Prüfung übertragen werden.

Beispiel:
Ein Datensatz kann gleichzeitig auf gültige Adresse (Adress-Check) und korrekte Anrede/ Groß-Kleinschreibung (Name-Check) geprüft werden, muss aber nicht.

Genauso gut können zwei voneinander getrennte Prüfungen gestartet werden, einmal nur die Adresse, einmal nur der Name. Über eine eindeutige ID (z.B. Kundennummer) am Datensatz können einzelne Prüfergebnisse beim Auftraggeber zusammengeführt werden.

2. Zutrittskontrolle

Ziel: Ein unbefugter Zutritt ist zu verhindern. Der Begriff ist räumlich zu verstehen.

24/7 h Videoüberwachung

Neben einer mechanischen Zutrittskontrolle wird zudem das Rechenzentrum rund um die Uhr per Video überwacht. Jede Bewegung im Rechenzentrum löst eine Meldung bei einem Sicherheitsunternehmen aus. Sollte sich jemand Unbefugtes Zutritt zum Rechenzentrum verschaffen können, ist Sicherheitspersonal in wenigen Minuten vor Ort.

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

3. Zugangskontrolle

Ziel: Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

- Kennwortverfahren (Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Automatische Sperrung (Pausenschaltung, Sperrung der Zugriffs-IP nach 3 misslungenen Login-Versuchen)
- Ein Benutzerstammsatz pro User

4. Zugriffskontrolle

Ziel: Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

- Differenzierte Berechtigungen (Profile, Rollen)
- Zugriffskontrolle über System-Logfile (bei Bedarf auswertbar)
- Löschung von Berechtigungen nach Firmenaustritten oder Wechsel eines Dienstleisters
- Firewall/ Virenschutz

5. Weitergabekontrolle

Ziel: Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle.

- Verschlüsselung der Transportwege: HTTPS mit SSL-Zertifikaten RSA 2048 bits (SHA256withRSA) für

  www.adresslabor.de
  api.adresslabor.de

- Eingeschränkter SSH-Zugang.
- Anbindung von Unterauftragnehmern nur verschlüsselt nach neuestem Stand der Technik und mit Vereinbarung zur Auftragsverarbeitung DSGVO
- Protokollierung Upload-/ Downloadzeiten pro Benutzer und Produkt für die Massenprüfung (nicht der personenbezogenen Daten selbst)
- Protokollierung der Webservice-Anfragen (Benutzer, Zeitstempel, Produkt)

6. Eingabekontrolle

Ziel: Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und –pflege ist zu gewährleisten.

- Kein Überschreiben der angefragten Daten. Anfragedaten bleiben auch nach der Verarbeitung erhalten und werden mit Korrekturvorschlag und/ oder Ergebniscodes angereichert.
- Die Entscheidungsgewalt zur Übernahme von Korrekturvorschlägen liegt beim Auftraggeber.
- Bewusst keine Dokumentation und Speicherung der angefragten Daten und Prüfergebnisse aus Datenschutzgründen

7. Auftragskontrolle

Ziel: Die weisungsgemäße Auftragsverarbeitung ist zu gewährleisten.

Der Auftraggeber kann sich vor seiner Entscheidung für Adresslabor alle relevanten Informationen auf der Website des Auftragnehmers einholen:

- Vordefinierte Leistungen mit Produktbeschreibungen unter „Details
- Demo-Videos zu einzelnen Produkten unter „Demo“
- Offenlegung der zu erwartenden Ergebnisse unter „Dokumentation“
- Beispielcodes für verschiedene Programmiersprachen
- Kostenlose Tests möglich (10 € Startguthaben)
- Danach erteilt der der Auftraggeber seinen Auftrag und die Weisung durch Inanspruchnahme des SaaS-Angebots bzw. den Kauf von Credits.

8. Verfügbarkeitskontrolle

Ziel: Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Redundante, unterbrechungsfreie Stromversorgung

Das Rechenzentrum verfügt über eine redundante Stromzuführung. Diese wird zudem über eine USV und einen Diesel-Generator gestützt. Innerhalb des Rechenzentrums wird die Redundanz bis zu den einzelnen Servern fortgeführt […].

Redundante, unterbrechungsfreie Netzwerkanbindung

Die netcup GmbH ist direktes Mitglied bei der RIPE, der Vergabestelle in Europa für IP-Adressen. Das Rechenzentrum ist durch die Einbindung in den Anexia Backbone Europe mehrfach redundant an diverse Knotenpunkte des Internets, wie dem DE-CIX, N-IX oder dem AMS-IX angebunden […]. Dadurch wird eine sehr gute Ausfallsicherheit geschaffen.

Redundante, unterbrechungsfreie Klimatisierung

Drei unabhängige Klimaanlagen teilen sich die Aufgabe, die Geräte im Rechenzentrum ausreichend zu kühlen. Mindestens eine Klimaanlage kann ausfallen, ohne dass die Kühlung gefährdet ist. Jede Klimaanlage ist an der redundanten, unterbrechungsfreien Stromversorgung angeschlossen. […]

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

Ergänzungen Adresslabor:

- Wöchentliche Komplett-Sicherung für Website, Datenbank und Software.
- Nächtliche Sicherung aller Bewegungsdaten (Benutzer, Credit-Logs, …)
- Zerstörung oder Verlust ist schon durch das Konzept ausgeschlossen (keine Originaldaten in der Verarbeitung)

9. Trennungskontrolle

Ziel: Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Alle Daten werden durch entsprechende Programmierung getrennt für unterschiedliche Zwecke verarbeitet (Speicherung, Veränderung, Löschung, Übermittlung)

Adresslabor – Rolf Paschold (Inhaber)