DATENSCHUTZ IST VERTRAUENSSACHE!

Informationen zum Datenschutz und IT-Sicherheit

Version vom 21.11.2024

UND DAS VERTRAUEN UNSERER KUNDEN IST UNSER WICHTIGSTES GUT!

Wir arbeiten in fast allen Projekten mit sensiblen, personenbezogenen Daten, häufig sind das Test- oder Fragebogendaten. Diese Daten wurden uns anvertraut – von Bewerberinnen und Bewerbern, von Unternehmensvertretern, von Hochschulen oder – ganz allgemein – von Organisationen.
Daher sind der Schutz und die DSGVO-konforme Erhebung, Verarbeitung und Nutzung personenbezogener Daten für uns ein wichtiges Anliegen.
Für die Umsetzung gelten folgende Grundsätze:

Sicherheit:
Daten müssen gegen unbefugten Zugriff durch technische und organisatorische Maßnahmen geschützt sein. Einen umfassenden Maßnahmen-Katalog erhalten Sie zusammen mit unserer AVV zugestellt.

Vertraulichkeit:
Personenbezogene Daten dürfen niemand anderem, als im eigentlichen Zweck vorgesehen, zur Verfügung gestellt werden. Es muss natürlich verhindert werden, dass unbefugte Dritte darauf Zugriff erhalten, sie kopieren und/oder weiterverteilen können.

Integrität:
Datensätze dürfen nicht manipuliert werden können. Ihre Korrektheit muss gewährleistet werden, denn Sie vertrauen darauf und entscheiden auf der Basis dieser Daten.

Verfügbarkeit:
Die Systeme und Dienste müssen für Sie immer verfügbar sein und bleiben. Die Daten dürfen nicht durch Systemabsturz o.ä. verloren gehen. Denn dann würden viele wichtige Daten unwiederbringlich verloren gehen.

EXTERNER DATENSCHUTZBEAUFTRAGTER

Damit wir die obengenannte Sicherheit, die Vertraulichkeit, die Integrität und die Verfügbarkeit der Daten erreichen, lassen wir uns von einem erfahrenen Team von Datenschutzexperten der datenschutz süd GmbH beraten.

datenschutz süd GmbH
Wörthstraße 15
97082 Würzburg
office@datenschutz-sued.de

Der Geschäftsführer der datenschutz süd GmbH, Dr. iur. Christian Borchers (https://www.datenschutz-nord-gruppe.de/kontakt/ansprechpartner), ist unser externer Datenschutzbeauftragter.

INTERNER DATENSCHUTZKOORDINATOR

Daten zu schützen, hat nicht nur mit neuen Verträgen oder einer besonders guten Technik zu tun. Es ist auch eine Haltung!

Aus diesem Grund haben wir uns entschlossen, es nicht auf einem externen Expertenteam beruhen zu lassen, sondern uns auch intern vertieft zu qualifizieren. Hans-Jörg Didi fungiert daher neben seiner Rolle als Gesellschafter auch als interner Datenschutzkoordinator. Er ist damit betraut, die täglichen Abläufe aus dem Blickwinkel des Datenschutzes zu betrachten und laufend zu optimieren.

Hans-Jörg Didi
didi@itb-consulting.de

100% HOSTED IN EUROPE

Das französische Unternehmen Clever Cloud (https://www.clever-cloud.com/en/about) betreibt für uns ITB-Online Assessment (kurz IONA) als Platform as a Service.

Die Daten werden in drei Datencentern in Frankreich verarbeitet und zwar in …

- EQUINIX PA3 Paris IBX® Data Center in Saint Denis (Frankreich)
- EQUINIX PA4 Paris IBX® Data Center in Patin (Frankreich)
- Zayo Group Velizy Data Center in Vélizy-Villacoublay (Frankreich)

Weitere Sicherheitsinformationen (insbesondere Zertifizierungen) der drei Rechenzentren können Sie im Internet unter https://www.clever-cloud.com/en/security einsehen.

Welche Vorteile hat der Betrieb von IONA in diesen Rechenzentren?

- Alle drei Rechenzentren und auch der Cloud-Anbieter Clever Cloud selbst sind unter anderem nach DIN ISO/IEC 27001 zertifiziert.
- Die Speicherung und Verarbeitung Ihrer Daten erfolgt unter Erfüllung aller gängigen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO.

- Alle Daten werden in den Datenbanken mit LUKS und aes-xts verschlüsselt.
- Mit den drei genannten Rechenzentren erreichen wir eine Verfügbarkeit der Hostingumgebung im Jahresdurchschnitt von mindestens 99,9%; in den letzten 90 Tagen lag dieser Wert für die gesamte Applikation bei 99,998 % (Stand: 17.1.24). Der derzeitige Status sowie die Historie lassen sich über dieses Portal live verfolgen: https://status.iona-portal.com/
- Durch die moderne Architektur in einer Cloud-Umgebung werden in der Regel keine Wartungsfenster für Updates der Applikation benötigt („Zero-Downtime-Deployment"). Updates können somit eingespielt werden, während Testungen stattfinden.
- Bei steigender Beanspruchung der Plattform werden automatisiert weitere Ressourcen im Rechenzentrum bereitgestellt – die Plattform wächst somit automatisch mit den Anforderungen unserer Kunden.
- Backups werden mit dem Tool pgdump jeden Tag vorgenommen und verschlüsselt abgelegt. Insgesamt werden Backups 180 Tage aufbewahrt.

ZUSÄTZLICHE INFORMATIONEN ZUR DATENVERARBEITUNG

Die ITB Consulting verpflichtet sich als Qualitätsdienstleister zu einer vertrauensvollen Abwicklung von Projekten. Neben den bereits angeführten, teilweise gesetzlich verpflichteten Maßnahmen zählt dazu für uns ergänzend:

- Vor Projektstart senden wir Ihnen unseren standardisierten Auftragsverarbeitungsvertrag zu. Wenn Sie einen eigenen Standardvertrag in Ihrem Unternehmen verwenden, prüfen wir diesen gerne hier intern.
- Alle Daten werden nur auf Servern der Europäischen Union verarbeitet. Die für das Hosting beauftragten Unternehmen sind ebenfalls in der Europäischen Union ansässig.
- Es werden nur jene Daten verarbeitet, die im ITB Online-Assessment selbst von den Teilnehmenden abgegeben wurden. Etwaige zusätzlich genutzte Hintergrunddaten werden im System transparent angeführt und angezeigt.
- Unsere Plattform ITB Online-Assessment legt die Form der Datenverarbeitung an unterschiedlichen Stellen allen Benutzern transparent offen. Unsere Standard-Datenschutzerklärung kann eingebunden werden, aber natürlich auch Ihre unternehmensspezifische.
- Es wird transparent auf die Möglichkeit hingewiesen, dass die Datenverarbeitung widerrufen werden kann. Ein solcher Widerruf kann im System direkt durch die HR-Manager eingesehen werden.
- Alle Daten werden – je nach Projekt – am Ende des Projekts gelöscht bzw. anonymisiert. Wann dies genau erfolgt, können Sie mit unseren Datenschutzbeauftragten abstimmen.

- Jegliche Datenübertragung zum ITB Online-Assessment sowie innerhalb des Systems findet über HTTPS und somit verschlüsselt, statt.

Darüber hinaus orientieren wir uns an allgemeinen Prinzipien wie beispielsweise der Zweckmäßigkeit der Datenerhebung. Dies bedeutet für uns, bspw. Soziodemographika (bspw. Alter, Geschlecht) nur im unbedingt notwendigen Ausmaß zu erheben und, wenn überhaupt, soweit wie möglich vergröbert (bspw. Alter in Alterskategorien statt in Jahren).

ZUSÄTZLICHE INFORMATIONEN ZUR SOFTWAREENTWICKLUNG BEI DER ITB

Die ITB Consulting verfolgt in der Softwareentwicklung einen modernen, agilen auf dem Scrum-Framework basierenden Entwicklungsansatz. Dabei werden Methoden und Werkzeuge eingesetzt, die aktuellen Industriestandards entsprechen und aktuell als „State of the Art“ in der Softwareentwicklung gelten.

Die Qualität der Software wird fortlaufend automatisiert im Entwicklungsprozess geprüft. Mit jedem Build durchläuft die Codebasis automatisierte Unit-Tests und es werden in regelmäßigen Abständen automatisierte Lasttests durchgeführt. Zusätzlich wird jedes Deployment von Fachexperten manuell auf einer dedizierten Testumgebung geprüft, um eine hohe Qualität und gute UX zu gewährleisten.

- Lasttests werden automatisiert über Tools wie Gatling und Grafana k6 durchgeführt, um die Belastbarkeit des Systems auch bei hoher Belastung sicherzustellen.

- System- und Integrationstests werden als sogenannte Black-Box-Tests durchgeführt und testen höhere Integrationsebenen der Komponenten.

- Unit-Tests bilden die Basis aller Tests. Sie testen viele, wenig komplexe Methoden automatisiert auf genau definierte Testfälle.

Bedarfsabhängig werden Penetrationtests durchgeführt, zuletzt im Oktober 2024.

In der Entwicklung kommen unter anderem folgende Entwicklungswerkzeuge und Methoden zum Einsatz:

- GitLab CI
- Code Climate
- JUnit, Mockito, AssertJ
- Jest
- npm audit
- OWASP Dependency Check
- CI / CD
- Unit Tests

- Pair Programming, Code Reviews

ZUSÄTZLICHE INFORMATIONEN ZU DEN EINGESETZTEN SOFTWARE-FRAMEWORKS

ENTWICKLER-STACK

Das ITB Online-Assessment ist modular aufgebaut und nutzt für verschiedene Teilbereiche unterschiedliche Technologien. Durch die Unterteilung in logische Module, unter anderem durch den Einsatz sogenannter Microservices, halten wir unsere Software übersichtlich. Zudem können die einzelnen Module separat aktualisiert, erweitert und verbessert werden, wodurch eine schnelle und flexible Entwicklung möglich wird. Bei hoher Last auf das System – zum Beispiel durch zahlreiche parallele Testungen – können die einzelnen Module außerdem unabhängig voneinander und vollautomatisch skaliert werden und damit auf die hohe Auslastung reagieren.

Die Frontends für die Testdurchführung sowie für die Administration nutzen u. a. die folgenden Technologien (Stand: November 2024):

- Angular 17
- Bootstrap 5

Diese Frontends greifen per HTTPS auf Service-Endpunkte zu (wir nutzen TLSv1.3 mit der Cipher suite AEAD-AES256-GCM-SHA384). Die dahinterstehenden Services wurden u.a. mit den folgenden Technologien entwickelt:

- Java 17 (Eclipse Temurin) und 11 (Ubuntu OpenJDK)
- Jakarta EE 8
- Spring Boot 2.6.7 und 2.7.14
- NestJS 8
- NodeJS 18

Für den Betrieb dieser Services setzen wir die folgenden Technologien ein:

- Wildfly 26
- Tomcat 9
- nginx 1.14.2 und 1.24.0
- Apache 2.4.60
- Docker

Für die Datenhaltung verwenden wir PostgreSQL 15 sowie für Logs Elasticsearch 7.5.2

Wenden Sie sich bei Fragen an …

Dr. Alexander Zimmerhofer, alexander.zimmerhofer@itb-consulting.de