Datenschutz und Informationssicherheit

Version v1.0.0 – Stand 17.02.2021

Management Summary

Allgemeines

«Hygeia» ist eine Contact-Tracing-Applikation für Schweizer Kantone. Sie unterstützt die Behörden in der Bekämpfung der COVID-19 Pandemie und wurde von den Kantonen St. Gallen, Appenzell Innerrhoden sowie Appenzell Ausserrhoden in Auftrag gegeben, um die vom BIT betriebene Plattform IES abzulösen.

Die Applikation sowie die dazugehörige Datenbank ist voll mandantenfähig und wird durch ein ausgeklügeltes Sicherheitssystem vor unbefugtem Zugriff geschützt. So können u.a. die Daten der einzelnen Mandanten bzw. Kantone nur durch passende Zugriffs-Token bearbeitet werden. Betrieben wird «Hygeia» unter der Domäne https://covid19-tracing.ch/.
Da im System besonders schützenswerte Personendaten bearbeitet werden, wurde der Informationssicherheit und dem Datenschutz höchste Priorität beigemessen (Data Protection by Design). Dies gilt sowohl für die Entwicklung der Applikation als auch für den Betrieb der Applikation und die Speicherung der Daten.

Die Funktionalität der Applikation wie auch die gespeicherten (Personen-)Daten stützen sich auf die «Weisung des BAG an die Kantone vom 11. Dezember 2020» inkl. des Anhangs («Minimal essential data»).

Zusammenfassung der verbleibenden Risiken

Bad Actor/Missbrauch
Nach wie vor verbleibt das Risiko eines Missbrauchs der Daten durch involvierte Personen die berechtigten Zugriff auf die Daten haben.
Massnahmen
Jeder Fall wird von mehreren Personen bearbeitet. Namentlich wird jeder Fall neben einem/einer Tracer*in auch von einem/einer Teamleiter*in kontrolliert. Zusätzlich wird jede Bearbeitung der Daten protokolliert. Dieses Protokoll kann durch die Benutzer*innen eingesehen werden, solange der Fall existiert. Das Löschen von Fällen ist mit einer separaten Berechtigung verknüpft, welche nur an Kader vergeben wird. Sämtliche Änderungen (inkl. Löschen von Fällen) werden zusätzlich direkt in der Datenbank protokolliert. Diese Einträge sind somit auch noch nach dem Löschen von Fällen vorhanden.

Angriffe auf das System
Unter Umständen könnte es auf einen direkten Angriff (z.B. DDOS) auf das System kommen.
Massnahmen
Das System ist kryptographisch mit einem IAM geschützt. Sämtliche aktuellen Massnahmen gemäss «Stand der Technik» im Bereich der Sicherheit auf der Web-Plattform wurden umgesetzt (SSL, Firewalls, Rate Limits etc.). Zusätzlich wird ein unabhängiges Security-Audit im Bezug auf direkte Angriffe auf das System durchgeführt werden, um dieses Risiko zu minimieren.

Zugriff zwischen Kantonen

Unter Umständen könnte es bei fehlerhafter Konfiguration zum Zugriff auf Daten zwischen den beteiligten Kantonen kommen.

Massnahmen

Das System bzw. die Applikation verwendet ein «Mandanten»-Konzept. Sämtliche Berechtigungen (z.B. um Personendaten einzusehen) sind auf Stufe der einzelnen Mandanten bzw. Kantone abgesichert. So muss jede Daten-bearbeitende Person via IAM explizit zum Zugriff auf die Daten des Mandanten berechtigt sein.

Abschliessende Bemerkungen

Im Bezug auf die verschiedenen Risiken wurden jeweils angemessene und dem Stand der Technik entsprechende Massnahmen getroffen. Durch die Einführung eines IAM's sowie eines detaillierten Berechtigungskonzeptes kann der Zugriff auf Daten sehr genau konfiguriert, eingeschränkt und nachvollzogen werden. Die gesamte Datenhaltung wird durch Anbieter*innen aus der Schweiz auf Schweizer Boden sowie unter anwendbarem Schweizer Recht sichergestellt. Die Betreiber*-innen der Infrastruktur sind ausserdem mit den relevanten ISO-Zertifikaten (namentlich ISO 27017, ISO 27018, ISO 27001, ISO 27002) ausgestattet.

Sicherheitsrelevante Systembeschreibung

Ansprechpartner / Verantwortlichkeiten

Systembetreiber
Betreiber des Systems ist die JOSHMARTIN GmbH, St. Gallen.

Inhaber der Daten
Inhaber der Daten ist der jeweilige Mandant bzw. der Kanton, vertreten durch dessen berechtigten Beauftragten. Diesem obliegt es, die Applikation und Daten bei entsprechenden Instanzen zu melden und ggf. genehmigen zu lassen.

Anwendungsverantwortliche
Anwendungsverantwortliche ist die JOSHMARTIN GmbH, St. Gallen.

Benutzerkreis
Der Benutzerkreis konsolidiert sich wie folgt:

- Von Amts wegen berechtigte Personen der jeweiligen Gesundheitsdepartemente der Mandanten.
- Im Tracing tätige Personen (Tracer*innen, Teamleiter*innen, Stabsstellen) welche von den Mandanten beauftragt und berechtigt werden.
- Administrator*innen der Applikationen (wenige Angestellte der JOSHMARTIN GmbH, St. Gallen).

Weitere Stellen
Verantwortlich für den Betrieb der Plattform ist die CAOS AG, St. Gallen.

Beschreibung des Gesamtsystems

«Hygeia» ist eine Contact-Tracing-Applikation auf Mandanten-Basis für Schweizer Kantone. Für den ordnungsgemässen Betrieb sowie Konfiguration, Zugriffsrechte und Rechtevererbung wird ein rollenbasiertes Zugriffsmodell verwendet.

Rollen

Tracer*innen: Diese*r «traced» die Fälle und erfasst die entsprechenden Daten. Jede/r Tracer*in ist einem/einer Teamleiter*in zugeordnet.

Superuser*innen: Tracer*innen, die auch eine Support-Funktion (via Chat und Telefon) gegenüber den anderen Tracern sowie Supervisoren übernehmen. Superuser testen auch neue Funktionen und Bugfixes.

Supervisor*innen bzw. Teamleiter*innen: Im Tracing sind diese für die Kontrolle von Fällen sowie für die Datenqualität zuständig. Ebenfalls kommt ihnen die Funktion der Beantwortung von fachlichen Fragen der Tracer*innen zu.

Viewer*innen: Personen, die Zugriff auf die Fall-Daten brauchen, diese jedoch nicht bearbeiten müssen und somit auch nicht dürfen. Beispiele: Person, die beim Gesundheitsdepartement angestellt sind, eine Analyse der Fälle vornehmen müssen oder auch Kantonsärzte. Die Zugriffe auf das System (bzw. die Ausstellung der für den Zugriff notwendigen Access Tokens) werden protokolliert.

Statistic-Viewer*innen: In dieser Rolle können Statistiken angeschaut werden. Diese Rolle berechtigt lediglich zur Ansicht der Statistiken.

Data-Exporter*innen: Kontaktpersonen, welche Kontakt zu einem Fall hatten und in einem anderen Kanton wohnen, müssen dem jeweiligen Kanton im geeigneten Format mitgeteilt werden. Der Data-Exporter kann für alle Mandanten, welche nicht selber mit dem Hygeia-System arbeiten, die Fall-Daten im BAG-Format herunterladen und sie diesen Kantonen zur Verfügung stellen.

Admin: Admins können Rollen einrichten und Rechte vergeben (ausser das Recht auf Admin). Die Admins werden durch JOSHMARTIN eingerichtet; dies ist i.d.R nur eine Person pro Mandant.

Webmaster: Der Webmaster hat das Recht Applikations-Konfigurationen anzupassen (z.B. die Adresse des SMTP-Servers für den Mailversand). Diese Rolle berechtigt nicht zur Ansicht von Fall-Daten oder anderen Personendaten.

Authentisierung

Jede Person, die auf Daten eines Mandanten zugreifen muss, wird zwingend über das IAM-System «Zitadel» identifiziert und authentifiziert. Rollen und Berechtigungen werden dort parametriert. Weitere Informationen dazu vgl. unten bei «Kommunikationsmatrix».

Backup

- Die Datenbank wie auch die Applikation wird laufend in einem «point in time»-Verfahren durch CAOS AG bzw. deren Infrastruktur-Betreiber*in Cloudscale gesichert. Storage Nodes werden auf Infra-level auf mehrere physikalische Standorte verteilt.

- Das IAM-System «Zitadel» wird durch CAOS AG betrieben und ist hochverfügbar. Das System ist für einen georedundanten Betrieb ausgelegt und die Daten werden georedundant gesichert (Redundanzgrad 3).

Support/SLA

Der Support wird durch JOSHMARTIN gemäss dem SLA (separates Dokument) gewährleistet. JOSHMARTIN zieht bei Bedarf die Betreiberinnen des Hostings (CAOS AG sowie cloudscale.ch AG) bei.

Beschreibung der zu bearbeitenden Daten

Die Umsetzung der zu bearbeitenden Personen- und Falldaten in Hygeia orientiert sich streng an den Anforderungen gemäss Weisung des Bundesamtes für Gesundheit (BAG). Details sind dieser Weisung zu entnehmen.

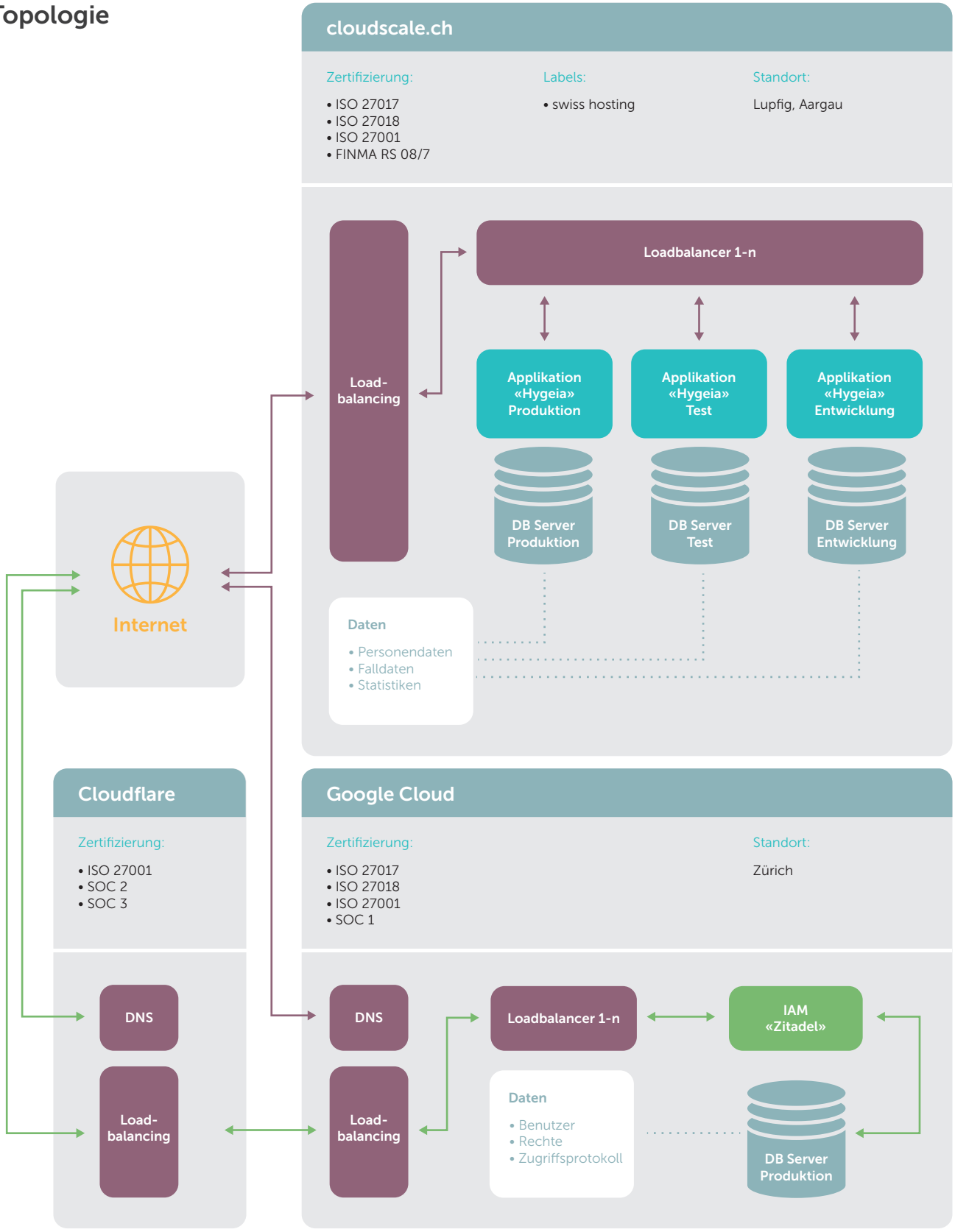
Personendaten: Dazu gehören Name, Adresse, Kontaktmöglichkeiten (u.a. Telefon, Mail) und Arbeitsumfeld, Impf-Status etc. Eine Person kann in mehrere Fälle involviert sein, sei es als Kontakt eines Indexfalles (=möglicher Indexfall) oder als Indexfall selber. Vgl. dazu auch «Personenbezogene Daten» in den Sektionen «Variablen pro isoliertem COVID-19-Fall» und «Variablen pro Kontaktperson in Quarantäne» in o.e. Weisung.

Falldaten: Unter einem Fall werden sämtliche Informationen zu einem Fall abgelegt inkl. der notwendigen Verknüpfungen u.a. auf Personen bzw. deren Personendaten, zugehörigem Kanton und bearbeitendem/r Tracer*in. Zu den Informationen gehören (soweit bekannt und notwendig) Kontakt-Ort, Datum, Tracing-Phasen, Aufenthaltsort während der Isolation bzw. Quarantäne, Klinische Informationen (z.B. Symptome), Auftraggeber bzw. Meldeeinheit des Tests bei Indexpersonen, Krankenhausaufenthalte etc. Vgl. dazu auch die Sektion «Variablen pro isoliertem COVID-19-Fall» und «Variablen pro Kontaktperson in Quarantäne» in o.e. Weisung.

Statistiken: Diese Daten entstehen «automatisch» mit dem Betrieb bzw. dem Arbeiten mit der Hygeia-Applikation. Sie können nur betrachtet werden.

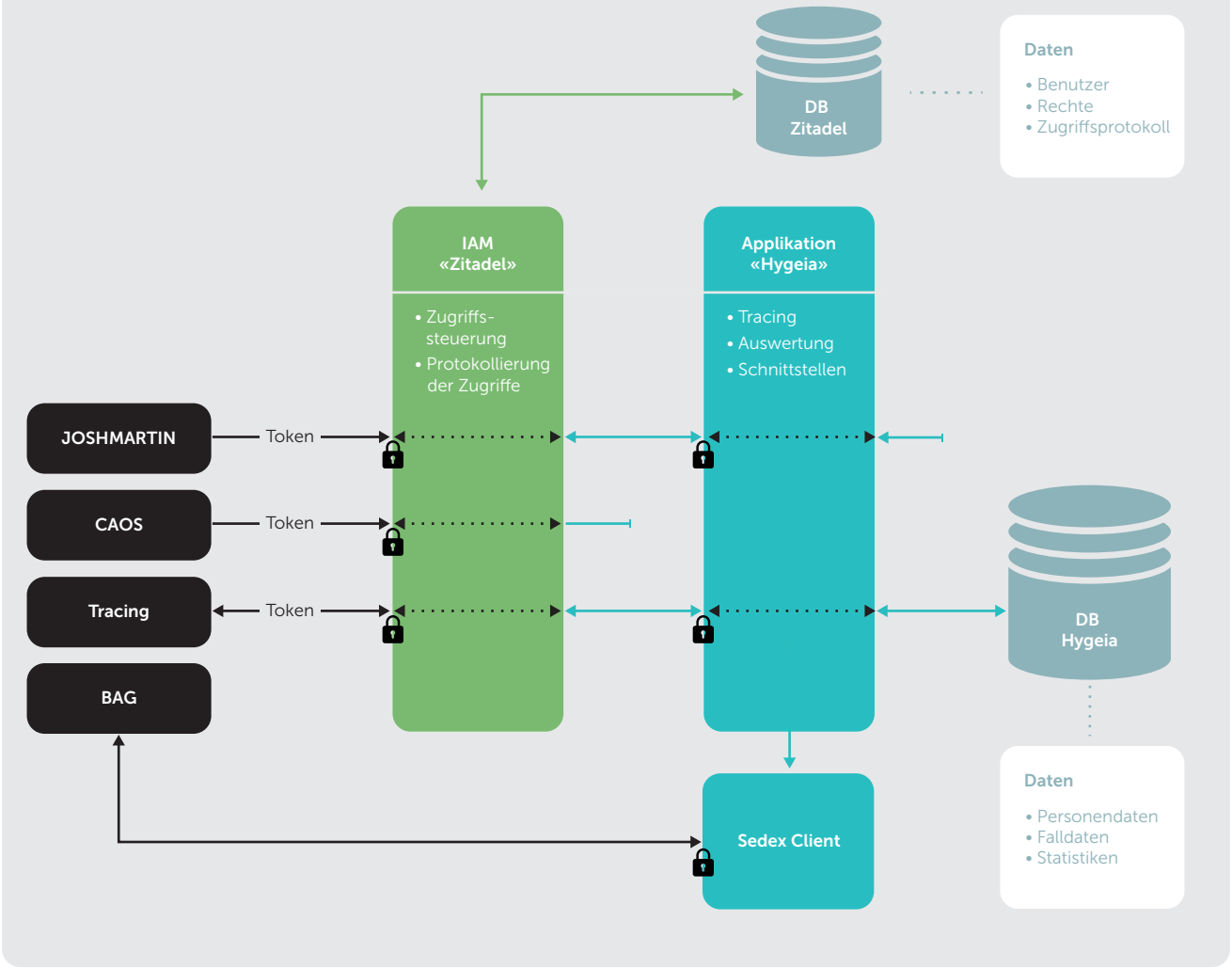
Standard-Datensätze (Organisationen): Diese Daten sind teilweise von der Weisung vorgegeben bzw. müssen für das Contact-Tracing erhoben werden (Organisationen).

Topologie


cloudscale.ch
Zertifizierung:
• ISO 27017
• ISO 27018
• ISO 27001
• FINMA RS 08/7
Labels:
• swiss hosting
Standort:
Lupfig, Aargau
Loadbalancer 1-n
Load-balancing
Applikation «Hygeia» Produktion
Applikation «Hygeia» Test
Applikation «Hygeia» Entwicklung
DB Server Produktion
DB Server Test
DB Server Entwicklung
Daten
• Personendaten
• Falldaten
• Statistiken
Internet
Cloudflare
Zertifizierung:
• ISO 27001
• SOC 2
• SOC 3
DNS
Load-balancing
Google Cloud
Zertifizierung:
• ISO 27017
• ISO 27018
• ISO 27001
• SOC 1
Standort:
Zürich
DNS
Load-balancing
Loadbalancer 1-n
IAM «Zitadel»
Daten
• Benutzer
• Rechte
• Zugriffsprotokoll
DB Server Produktion

Kommunikationsmatrix

Parteien und Zugriff



Beschreibung der zugrundeliegenden Technik

Die als Basis verwendete Software wird mindestens einmal monatlich auf (sicherheitsrelevante) Aktualisierungen überprüft und nach Eignungstests aktualisiert. Für die Kernkomponenten Elixir bzw. Erlang werden Patch-Versionen (gem. «SemVer» [https://semver.org/lang/de/]: sicherheitsrelevante Aktualisierungen) regelmässig automatisch deployed.
Sämtliche Änderungen (Programmcode, verwendete Versionen der Basiskomponenten etc.) werden in Form von VCS (Git) protokolliert. Dasselbe gilt für sämtliche Änderungen auf Infrastruktur-Level (GitOps). Beides wird in Git-Repositories der JOSHMARTIN GmbH zentral abgelegt und gesichert.

Plattform (gehosted bei cloudscale.ch AG)

- Orchestrator: Kubernetes - v1.18.8 (Stand 27.01.2021)
- OS: Linux CentOS - v7 (Stand 27.01.2021)

Encryption / TLS / DNS

- TLS >= 1.2
- Cipher Suites (TLS 1.2)
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
- Cipher Suites (TLS 1.3)
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- HSTS
- Forward Secrecy
- Certificate Transparency
- OCSP Stapling
- DNSSEC

Applikation

- Language: Elixir - v1.11.3 (Stand 27.01.2021)
- Language: Erlang - v23.2.3 (Stand 27.01.2021)
- DB: Postgres - v12.4 (Stand 27.01.2021)

Sicherstellung des ordnungsgemässen Betriebes der Applikation und Notfallkonzept

Betrieb

Der ordnungsgemässe Betrieb wird durch die beteiligten Organisationen (JOSHMARTIN / CAOS) sichergestellt.

Notfallkonzept

Monitoring: ein ständiges Monitoring mit Escalation wird durch die beteiligten Organisationen durchgeführt.

SLA: darin werden die Servicezeiten geregelt.

Einhaltung / Überprüfung der Schutzmassnahmen

Der/die IT-Sicherheitsbeauftragte des entsprechenden Mandanten hat jederzeit vollen Zugriff auf die Zugriffsprotokolle im IAM («Zitadel») und kann weitere sicherheitsrelevante Auskünfte im Rahmen der im SLA festgelegten Kommunikationswege jederzeit beim Betreiber der Plattform anfordern.

Test / Abnahme der Informationssicherheits-Funktionen

Interne Tests sowie Tests der Auftraggebenden haben ergeben, dass keine sicherheitsrelevanten Lücken in der Applikation, der verwendeten Datenbank sowie dem IAM-System bestehen.

Im Verlaufe des ersten Semesters 2021 ist ein Sicherheits-Test (Penetration-Test) durch eine externe Firma geplant. Verhandlungen mit möglichen Anbieter*innen haben bereits stattgefunden.

Liquidation

Bei einer allfälligen Liquidation der Applikations-Daten wird pro Mandant wie folgt vorgegangen:

- Datenübergabe (verschlüsselt und in maschinenverarbeitbarem Format) an Berechtigte des Mandanten (in Form eines BAG Med Exports).
- Unwiderrufbares Löschen der aktiven Daten dieses Mandanten.
- Deaktivieren WebSMS für den Mandanten bzw. dessen Rollen.
- Entfernen des Mandanten sowie den zugeordneten Rollen und Berechtigungen aus dem IAM «Zitadel».
- Deaktivieren des Mandanten im Kernsystem.
- Beim letzten Mandanten: Abschalten der Plattform sowie löschen aller Backups.

Involvierte Unternehmungen

- JOSHMARTIN GmbH
  Neugasse 51, 9000 St. Gallen
  +41 71 511 72 50
  info@joshmartin.ch
- CAOS AG
  Teufener Strasse 19, 9000 St.Gallen
  +41 71 575 76 47
  hi@caos.ch
- Cloudscale.ch AG
  Venusstrasse 29, 8050 Zürich
  +41 44 55 222 55
  hallo@cloudscale.ch