Sicherheits- und Datenschutzkonzept der infra.run Service GmbH

24. April 2024

infra.run Service GmbH
Wilhelmine-Gemberg-Weg 14, 10179 Berlin
Geschäftsführung: Leonie Hannig, Markus Otto, Andreas Steinhauser
Steuernummer: 30/358/51857 Ust-IdNr: DE340100821
HRB 225307 B, Amtsgericht Berlin-Charlottenburg

Inhaltsverzeichnis

1 Sicherheitskonzept **3**
1.1 Allgemeiner Überblick . . . 3
1.2 Organisatorisches und Rahmenbedingungen . . . 3
1.3 IT-Systemarchitektur . . . 3
1.4 Schutz . . . 4
1.5 Vorgaben . . . 4
1.6 Kontrolle . . . 5

2 Datenschutzkonzept **6**
2.1 Ziel des Datenschutzkonzepts . . . 6
2.2 Präambel . . . 6
2.3 Datenschutzpolitik und Verantwortlichkeiten im Unternehmen . . . 6
2.4 Rechtliche Rahmenbedingungen im Unternehmen . . . 7

3 Bestehende technische und organisatorische Maßnahmen **8**
3.1 Softwareentwicklung und -installation . . . 8
3.2 Vertraulichkeit . . . 8
Zutrittskontrolle . . . 8
Zugangskontrolle . . . 9
Zugriffskontrolle . . . 10
Datenträgerkontrolle . . . 11
Trennungskontrolle . . . 11
Pseudonymisierung . . . 11
3.3 Integrität . . . 12
Weitergabekontrolle . . . 12
Eingabekontrolle . . . 12
3.4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO) . . . 13
Verfügbarkeitskontrolle . . . 13
Rasche Wiederherstellbarkeit . . . 13
3.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO) . . . 14
Auftragskontrolle . . . 14

1 Sicherheitskonzept

1.1 Allgemeiner Überblick

Die infra.run Service GmbH (kurz infra.run) erbringt IT-Dienstleistungen für Auftraggeber. Dies geschieht primär durch das Hosting von OpenSource Software.

Im Unternehmen gibt es die Geschäftsführung, fest angestellte Administrator:innen, fest angestellte Projektmanager:innen, freischaffende Administrator:innen, freischaffende Softwareentwickler:innen und Volunteers. Administrator:in bezeichnet eine Person, die Zugang zu einem oder mehreren Hosts hat und dort Super-User (root-) Rechte erlangen und Services installieren, löschen und konfigurieren kann. Personen können mehrere Rollen besetzen.

Dieses Sicherheitskonzept bezieht sich auf alle Bereiche, in denen Daten von Auftraggebern verarbeitet werden und alle Personen, die Administrator:innen sind und Zugang zu solchen Bereichen haben.

1.2 Organisatorisches und Rahmenbedingungen

Alle Mitarbeiter:innen sind frei in der Wahl ihres Arbeitsplatzes. Zentrale Büroräume, in denen Tätigkeiten als Administrator:innen durchgeführt werden, gibt es nicht. Einzig notwendige Voraussetzung für die Arbeit bei infra.run ist eine Internetanbindung mit ausreichender Bandbreite. Dies stellt besondere Anforderungen an die individuellen Sicherheitsmaßnahmen der Administrator:innen, die im Folgenden erläutert werden.

1.3 IT-Systemarchitektur

Infra.run betreibt eigene Server-Hardware in Rechenzentren in Deutschland und insbesondere in solchen Rechenzentren, die weder direkt noch indirekt im Eigentum von nicht-deutschen Unternehmen stehen und gemäß Gesetzeslage in ihrem Ursprungsland verpflichtet wären, den staatlichen Diensten ihres Ursprungslandes Daten zur Verfügung zu stellen (z. B. USA PATRIOT Act). Infra.run nutzt ausschließlich Rechenzentren, die mindestens ISO27001-zertifiziert sind. Sollten die von infra.run selbst betriebenen Ressourcen nicht ausreichen (beispielsweise aufgrund von Kapazitätsspitzen), werden Hardware oder virtuelle Maschinen bei ebensolchen Hostern bzw. Rechenzentren zusätzlich angemietet.

Administrator:innen stehen entweder betriebseigene, mobile Computer zur Verfügung oder sie nutzen eigene Geräte. In beiden Fällen ist es ausdrücklich gestattet, die Geräte auch für private Zwecke zu verwenden. Die Systemressourcen sind, wie im

Datenschutzkonzept beschrieben, strikt getrennt. Auf Privatgeräten liegt die Verantwortung ausdrücklich bei den Mitarbeiter:innen. Sie werden zur Wahrnehmung dieser Verantwortung intern besonders geschult.

1.4 Schutz

Infra.run verarbeitet im Auftrag unter anderem Daten von z. B. Schulkindern, Patient:innen, Journalist:innen und somit Daten mit einem besonders hohen Schutzbedarf. Hierbei handelt es sich um verschiedene Datenarten, z. B. Benutzername, Klarname, E-Mail-Adresse, Wohnort, Telefonnummer, Text-/Audio- und Video-Streams von Konferenzteilnehmer:innen, Notizen von Lehrkräften zu Personen und Noten, Arbeitsergebnisse, Testergebnisse und Lernfortschritte. Der Schutz dieser Daten vor unberechtigtem Zugriff hat oberste Priorität. Hierfür hat infra.run diverse Regeln und Mechanismen etabliert, die insbesondere im Datenschutzkonzept detailliert beschrieben werden.

1.5 Vorgaben

Die folgende Aufzählung gibt eine Übersicht über die Maßnahmen, die infra.run getroffen hat, um die Daten der Nutzer:innen zu schützen:

- Zugangssperren: Die zur Administration verwendeten Geräte werden durch die Mitarbeiter:in vor unberechtigtem Zugriff geschützt.
- Datensparsamkeit: infra.run erhebt, verarbeitet und speichert Daten nur in dem für die Aufrechterhaltung des Betriebs erforderlichen Umfang.
- Verschlüsselung: infra.run stellt sicher, dass sämtliche Datenübertragung zwischen den von ihr betriebenen Services und deren Nutzer:innen ausschließlich über gemäß den Empfehlungen des BSI transportverschlüsselte Kanäle erfolgt.
- Vier Augen Prinzip: Produktivsysteme werden von mindestens zwei Personen gemeinsam bedient. Dies verhindert Missbrauch und vermeidet Fehler.
- Nachvollziehbarkeit: Alle Aktionen der Administrator:innen auf Produktivsystemen werden für 90 Tage aufgezeichnet.
- Hoher Automatisierungsgrad: Systeme werden im Sinne der Reproduzierbarkeit und Fehlerreduktion ausschließlich automatisiert aufgesetzt und konfiguriert.
- Virtualisierung: Administrative und andere Tätigkeiten werden durch Virtualisierung voneinander getrennt.
- Tenant-Trennung: User-Daten unterschiedlicher Nutzer:innen-Gruppen werden z. B. durch Virtualisierung, logische Trennung von Datenbanken und getrennte Schnittstellen weitestgehend voneinander separiert.

- Update-Prozess: Alle durch infra.run betriebenen Services werden kontinuierlich auf Updates überprüft. Sicherheitsrelevante Updates werden schnellstmöglich installiert.
- Aktive Sicherheitskontrolle: Infra.run überprüft anlassbezogen die betriebenen Services auf Schwachstellen und Sicherheitslücken und meldet etwaige Funde an die entsprechenden Entwickler:innen im Rahmen einer „responsible disclosure“ und schaltet betroffene Funktionen ggf. vorübergehend ab oder schafft falls möglich externe Sicherheitsschranken.

1.6 Kontrolle

Die Kontrolle der Einhaltung der im Sicherheits- und Datenschutzkonzept beschriebenen Regeln und Maßnahmen wird durch die Geschäftsführung verantwortet und kontinuierlich durchgeführt. Diese Dokumente werden durch die Geschäftsführung bei Bedarf angepasst. Nach jeder Anpassung werden die Administrator:innen über die Änderungen informiert.

Verstöße gegen die im Sicherheits- und Datenschutzkonzept dargestellten Regeln und Maßnahmen können zu Abmahnung oder fristloser Kündigung führen. Des Weiteren können Verstöße auch zu zivil- und/oder strafrechtliche Konsequenzen haben. Alle Mitarbeiter:innen, egal ob sie Freelancer oder Festangestellte sind, werden vor Arbeitsbeginn hierüber informiert.

2 Datenschutzkonzept

2.1 Ziel des Datenschutzkonzepts

Das Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Dokumentation die für die infra.run Service GmbH (kurz infra.run) relevanten datenschutzrechtlichen Aspekte darzustellen und die Umsetzung der gesetzlichen Anforderungen zu gewährleisten. Das Datenschutzkonzept dient allen Mitarbeiter:innen von infra.run als Leitfaden für den Umgang mit personenbezogenen Daten. Es kann auch als Grundlage für datenschutzrechtliche Prüfungen z. B. durch Auftraggeber im Rahmen der Auftragsverarbeitung genutzt werden. Dadurch soll die Einhaltung der europäischen Datenschutz-Grundverordnung (DS-GVO) nicht nur gewährleistet, sondern auch der Nachweis der Einhaltung geschaffen werden.

2.2 Präambel

Infra.run bietet Hosting von BigBlueButton Videokonferenzen als skalierbaren Service an. Weitere geplante Dienstleistungen sind das Hosting des Lernmanagementsystems Moodle und des Instant Messengers Matrix, sowie der Single-Sign-On Lösung Keycloak und der Cloud-Software Nextcloud. Zusätzlich kann auch von infra.run selbst entwickelte Software zum Einsatz kommen.

Das Angebot richtet sich insbesondere an Schulen und Bildungseinrichtungen, Organisationen mit gesellschaftlichem Mehrwert und NGOs. Die infra.run Service GmbH wurde explizit mit dem Anspruch gegründet, eine datenschutzkonforme Alternative zur Nutzung von Dienstleistern zu bieten, deren Umgang mit Daten und dem Schutz dieser Daten bestenfalls fragwürdig ist. Der Schutz und die Sicherheit personenbezogener Daten wurde daher bereits bei beim Aufbau der Firma berücksichtigt. Das Team von infra.run setzt sich aus IT-Spezialist:innen und IT-Sicherheitsexpert:innen mit langjähriger Erfahrung zusammen.

2.3 Datenschutzpolitik und Verantwortlichkeiten im Unternehmen

Infra.run bietet IT-Dienstleistungen an, die es Nutzern ermöglichen, miteinander zu kommunizieren und Daten auszutauschen. Unser erklärtes Ziel ist es hierbei, einen optimalen Service anzubieten und gleichzeitig die minimal notwendige Menge von Nutzerdaten zu verarbeiten. Die Prozesse sind darauf ausgelegt, nur die für Betrieb und

Abrechnung notwendigen Daten zu erheben und zu speichern und dabei die Daten vor unbefugten Zugriffen zu schützen.

Infra.run besteht aus einem Kernteam von 10 Personen und wird im Bedarfsfall von externen Freelancern und Ehrenamtlichen unterstützt. Die Geschäftsführung der Firma besteht aus Leonie Hannig, Markus Otto und Andreas Steinhauser, die auch operativ verantwortlich sind. Alle Mitarbeiter:innen von infra.run haben die Möglichkeit, ausschließlich remote zu arbeiten.

Entscheidungen über neue Dienstleister, Hardware oder Software werden im Team diskutiert und gefällt. Hierdurch wird die in der Firma und im Kreis der Freelancer/Ehrenamtlichen vorhandene Expertise bezüglich Leistungsfähigkeit und Sicherheit der zu evaluierenden Technologien optimal genutzt.

Bei der Auswahl von Software wird darauf geachtet, dass diese OpenSource ist, wodurch eine hohe Verlässlichkeit und Sicherheit der Software gewährleistet werden kann. Für externe Dienstleistungen werden ausschließlich Anbieter mit Sitz in Deutschland ausgewählt, dies gilt ebenfalls für Rechenzentren. Insbesondere wird darauf geachtet, dass die Unternehmen vollständig und ausschließlich europäischem, vorzugsweise aber deutschem Recht unterworfen sind.

Alle von infra.run durchgeführten Verarbeitungstätigkeiten wurden dokumentiert. Das Verzeichnis von Verarbeitungstätigkeiten wurde am 02.03.2021 erstellt und wird anlassbezogen aktualisiert bzw. ergänzt und ansonsten jährlich auf Aktualität überprüft. Eine digitale Version liegt für alle Mitarbeiter:innen zugänglich in der firmeninternen Nextcloud. Der Datenschutzbeauftragte ist Dr. Thomas Pudelko, erreichbar unter datenschutz@t-pudelko.de. Die Meldung an die Aufsichtsbehörde erfolgte am 13.01.2021.

Die Dokumentation der Technischen und organisatorischen Maßnahmen wurde am 21.12.2020 fertiggestellt und wird anlassbezogen aktualisiert. Alle Mitarbeiter:innen, dies umfasst neben Festangestellten auch Freelancer und Ehrenamtliche, haben eine Verpflichtung auf Vertraulichkeit und Beachtung des Datenschutzes unterzeichnet.

Alle Mitarbeiter:innen wurden über die in diesem Dokument aufgeführten Maßnahmen informiert und werden regelmäßig geschult. Die Einhaltung der Vorgaben für die Arbeit an den Systemen wird von einem sachkundigen Mitglied der Geschäftsführung spontan und unregelmäßig wiederkehrend überprüft.

2.4 Rechtliche Rahmenbedingungen im Unternehmen

Die für infra.run zu beachtenden rechtlichen Regelungen sind insbesondere die DSGVO sowie weitere gesetzliche Regelungen wie das GmbH-Gesetz, das Bundesdatenschutzgesetz (BDSG) und das Bürgerliche Gesetzbuch. Die Verarbeitung der vom Auftraggeber stammenden personenbezogenen Daten erfolgt ausschließlich zur Erfüllung der vertraglich vereinbarten Pflichten und mit Einwilligung des Auftraggebers.

3 Bestehende technische und organisatorische Maßnahmen

3.1 Softwareentwicklung und -installation

Die Softwareentwicklung der von infra.run betriebenen Services werden von den Mitarbeiter:innen begleitet und beobachtet sowie fallweise auf Codequalität, Aktualität der verwendeten Software-Komponenten und Sicherheit überpüft. Ggf. werden problematische Komponenten mittels OS-spezifischen Härtungswerkzeugen (AppArmor, systemd-basierter Isolation, seccomp) zusätzlich abgesichert. Neue Softwareversionen werden schnellstmöglich getestet und ausgerollt. Bei sicherheitsrelevanten Updates werden kurze Reaktionszeiten garantiert.

Softwareinstallationen werden zur Fehlervermeidung und zur Sicherstellung der Reproduzierbarkeit ausschließlich über „Ansible“ durchgeführt. Ggf. werden Systeme in „Containern“ ausgerollt. Diese Container werden ausschließlich aus von infra.run selbst erzeugten und konfigurierten „images“ erzeugt. Services oder Softwarekomponenten, die keinen „state“ halten, erhalten keine Updates, sondern werden gelöscht und neu erzeugt, sobald eine neue Version vorliegt und von infra.run erfolgreich getestet wurde. So werden Konfigurationsfehler durch Updates vermieden.

3.2 Vertraulichkeit

Zutrittskontrolle

Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt.

Maßnahmen:

Sofern von infra.run Büroräume unterhalten werden, befinden sich hier keine personenbezogenen Daten bzw. Verkehrsdaten des Vertragspartners. Die Büroräume sind mehrfach mittels Schließanlagen gesichert.

infra.run besitzt eigene Server. Diese Server stehen bei ISO 27001-zertifizierten Rechenzentrums-Dienstleistern und verfügen über Zugangskontrollen, die nur Berechtigten physischen Zutritt erlauben.

Durch ständige Aktualisierung der „SSH“-Schlüssel wird sichergestellt, dass der administrative Zugang zu physischen bzw. virtuellen Maschinen nur berechtigten Perso-

nen mit gültigen persönlichen Schlüsseln gestattet ist. Eine Anmeldung durch Passwörter wird unterbunden.

Zugangskontrolle

Die Zugangskontrolle verhindert Unbefugten den Zugang zu Datenverarbeitungssystemen.

Maßnahmen:

Der Zugriff für Mitarbeiter:innen von infra.run zu den Verwaltungssystemen erfolgt ausschließlich über „SSH“ im public-private-key Verfahren und erzeugt auf den Servern ein revisionssicheres Audit Logging. Hier werden alle Aktionen der Mitarbeiter:innen aufgezeichnet. Alle Logs werden zentral auf einem Logging-Server gespeichert.

Private „SSH“-Schlüssel sind zusätzlich mit einem persönlichen Kennwort gesichert. Die eingesetzte Kennwortrichtlinie gibt vor, dass Passwörter mindestens 12 Zeichen lang sind und u.a. aus Buchstaben und mindestens einer Ziffer bzw. Sonderzeichen bestehen müssen. Die Anforderungen folgen der internen Kennwort-Richtlinien des ISMS gemäß ISO 27001.

Es haben zu den Systemen nur die Personen Zugang, die jeweils mit der Administration des jeweiligen Systems direkt betraut sind. Dritte Personen haben keinen Zugang zu den Systemen. Sollte eine fachliche Unterstützung gewünscht sein, werden solche Personen, sofern eine rechtskräftige Vertragsbeziehung und eine unterzeichnete Verschwiegenheitserklärung vorliegen, über eine „tmux“ Session mit eigenem „upterm“-Server oder über einen geteilten Bildschirm in einem Videoconferencing-Tool eingebunden, sodass die Aufsicht immer bei berechtigten Personen liegt.

Passworte, Application-Secrets und API-Keys werden im shared Password-Manager gespeichert. Hierzu haben in- und externe Mitarbeiter:innen nur jeweils zu den für sie relevanten Secrets Zugang.

Generell erfolgt der Zugriff zu den Verwaltungssystemen ausschließlich über folgende Interfaces:

- Interne Verwaltungsinterfaces, welche mittels TLS gemäß der Mindeststandards des BSI (mindestens TLS 1.2 mit Forward Secrecy) verschlüsselter Kommunikation erreichbar sind
- reine remote-shell mittels des verschlüsselten „SSH“-Protokolls
- Im Falle des Verwaltungsinterfaces erfolgt die Benutzerauthentifizierung mittels einer Nutzernamen und Passwort Kombination.
- Im Falle des Zugangs mittels Remote Shell erfolgt eine Authentifizierung mittels private/public-Key Verfahren, wobei die Schlüssel zusätzlich noch über ein Passwort gesichert sind. Der Zugriff ist zusätzlich ausschließlich über eine Firewall/DMZ möglich.

Ausscheidenden Mitarbeiter:innen wird der Zugriff sofort gesperrt. So genannte Gast-Accounts oder auch nicht-personengebundene/anonyme Accounts werden nicht zur Verfügung gestellt.

Restriktive Firewall-Settings erlauben ausschließlich den Zugang zu den Services über die explizite Öffnung der benötigten Ports. Es werden jeweils systembezogen mehrstufige Schutzmechanismen sowohl auf Netzwerk- als auch auf OS- und ggf. Applikationsebene etabliert, um diese vor DDOS- und brute-force-Angriffen zu schützen.

Sicherheit von Arbeitsgeräten Die Mitarbeiter:innen nutzen für ihre Arbeit wahlweise Computer, die durch infra.run zur Verfügung gestellt werden und ausschließlich zur Administration zu verwenden sind oder Geräte ihrer Wahl. Hierfür ist die Voraussetzung, dass der Computer lediglich als Hostsystem für Virtualisierungen dient, von denen eine ausschließlich betrieblichen Zwecken dient und vollständig isoliert ist. Daneben können eine oder mehrere weitere Virtualisierungen für andere Zwecke nutzbar gemacht werden. Das Hostbetriebssystem darf für keine weiteren Aufgaben als die Virtualisierung bzw. Herstellung der Netzwerkanbindung genutzt werden. Die Geräte sind nach Stand der Technik konfiguriert und abgesichert. Die Festplatten sind nach Stand der Technik verschlüsselt. Für den passwortgestützten Endgerätezugang bzw. die Festplattenverschlüsselung sind starke Passworte nach Empfehlung des BSI zu verwenden.

Zugriffskontrolle

Infra.run hat zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen:

Arbeiten an Produktivsystemen, oder „staging“ bzw. Testsystemen mit echten, personenbezogenen Daten werden ausschließlich im vier-Augen-Prinzip durchgeführt. Hierfür kommt die Software „upterm“ in Kombination mit „tmux“ zum Einsatz.

Logs werden in einem zentralen Logging-System verschlüsselt und maximal drei Tage lang gespeichert. Es werden ausschließlich für den Betrieb der Servcies notwendige Daten aufgezeichnet. Eine Verlängerung dieser Zeit kann durch den Auftraggeber für bis zu zwei Wochen unter Nennung eines nachvollziehbaren Grundes schriftlich verlangt werden und führt unsererseits zu einer Meldung bei der/dem zuständigen Datenschutzbeauftragten. Eine Herausgabe von personenbezogenen bzw. biometrischen Daten erfolgt nur auf richterlichen Beschluss. Auf Verlangen durch die Staatsanwaltschaft oder Polizei kann eine Herausgabe nur bei rechtlicher Verpflichtung (Art.6 Abs. 1c DS-GVO) oder nachgewiesenem berechtigten Interesse (Art.6 Abs. 1f) und bestehendem Ermittlungsverfahren unter Nennung der Ermittlungsnummer oder bei Gefahr

im Verzug erfolgen. Es werden nur Daten mit Zweckbezug herausgegeben. Grundsätzlich herrscht bei infra.run das Gebot der Datensparsamkeit.

Grafische Administrations-Interfaces werden wo immer möglich vermieden, da hier ein revisionssicheres Audit Logging sehr schwierig ist. Ggf. erfolgt ein Zugang über zwei-Faktor-Authentifizierung.

Der Zugriff auf die Bestands- und Betriebsdaten unterliegt einer Rechtekontrolle (Rollen), die Einzelpersonen oder Gruppen mit minimalen Zugriffsrechten versieht. So hat beispielsweise der Bereich Buchhaltung keinen Zugriff auf die hier betrachteten Daten. Der Zugriff ist somit je nach Mitarbeiterrolle nur auf Teildaten möglich. Hierbei ist ein kompletter Export aller Daten beispielsweise nicht möglich. Jeglicher Zugriff erfolgt verschlüsselt.

Datenträgerkontrolle

Datenträger werden nach Kündigung nach einem definierten Verfahren mehrfach überschrieben (Festplatten) oder per Erase bzw. Secure-Erase gelöscht (SSDs) und nach Prüfung wieder eingesetzt.

Defekte Festplatten und Papierdokumente werden von einem externen Dienstleister fachgerecht physisch und datenschutzkonform gemäß DIN 66399 (Sicherheitsstufe 5) vernichtet.

Trennungskontrolle

infra.run hat zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen:

Die personenbezogenen Daten verschiedener „tenants“ werden, sofern deren Verarbeitung erforderlich ist (Personalisierung von Services, Zugang zu Accounts etc.) in logisch vollständig voneinander getrennten Datenbanken realisiert. Wo technisch sinnvoll möglich, werden die Services zusätzlich durch Virtualisierung (Container oder virtuelle Maschinen) voneinander getrennt. Bei Managed Servern- und Cloud-Vertragspartnern werden Daten physisch oder logisch von anderen Daten getrennt gespeichert. Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

Pseudonymisierung

Für die Pseudonymisierung ist der Auftraggeber verantwortlich.

3.3 Integrität

Weitergabekontrolle

Infra.run hat zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle).

Maßnahmen:

Alle von infra.run betriebenen Services sind durch User ausschließlich über transportverschlüsselte Verbindungen erreichbar. Bei TLS-Verbindungen werden Downgrade-Attacken mittels HSTS verhindert.

Alle Mitarbeiter:innen sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen. Sämtliche für den Betrieb des vorliegenden Dienstes benötigten Daten verbleiben innerhalb eines Rechenzentrums. Unabhängig von dem vorliegenden Vertrag sichert infra.run die Weitergabe wie folgt:

- Protokollierung der Datenverarbeitung
- Verschlüsselung der Daten
- Kontrollierter Zugriff ausschließlich verschlüsselt bzw. hinter Firewall/DMZ
- Im Falle der Vertragskündigung wurde die Übergabe sämtlicher Daten an den Auftraggeber vereinbart. Die Übergabe der Daten wurde elektronisch vereinbart, d.h. somit ebenfalls verschlüsselt, z. B. PGP.
- Ein Transport auf herkömmlichen Weg findet in der Regel keine Anwendung. Dieser Transport würde folgende Maßnahmen erfordern:
  - Transport der Daten durch Boten
  - Erstellen von Begleitpapieren
  - Prüfung der Daten auf Richtigkeit und Vollständigkeit
- Festplatten bzw. Papierdokumente werden ausschließlich über professionelle Entsorger datenschutzkonform vernichtet.

Eingabekontrolle

Infra.run hat zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).

Maßnahmen:

Interne Verwaltungssysteme von infra.run protokollieren Änderungen an Kundenstammdaten. Alle Aktionen der Mitarbeiter:innen werden aufgezeichnet, die dabei entstehenden Logs werden zentral auf einem Logging-Server gespeichert. Jeglicher Zugriff wird wie folgt unterschieden:

- Art der Nutzung (Neuanlage, Veränderung, Löschung des Datensatzes)
- Zeitpunkt der Nutzung bzw. des Ereignisses
- ausführende Person (Benutzerkennzeichen)

Die Änderung der Daten erfolgt gemäß Zutritts- und Zugangskontrolle.

3.4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Infra.run hat zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung, bewusste Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).

Maßnahmen:

Dem Verlust von Daten wird durch regelmäßige Backups (je nach betrieblicher Relevanz minimal täglich, maximal wöchentlich) vorgebeugt. Eine Klassifizierung erfolgt nach logischen und physischen Schäden/Datenverlust. Der maximale Datenverlust bedingt durch logische Fehler beträgt 24h. Physischem Datenverlust wird durch Einsatz von gespiegelten oder per RAID gesicherten Datenspeichern vorgebeugt. Das Risiko eines Datenverlustes ist vorhanden, jedoch durch die getroffenen Maßnahmen auf ein Minimum reduziert. Alle relevanten Systeme sind mit einem Monitoring versehen. Der Einsatz erfolgt im Rechenzentrum vollumfänglich mit USV.

Das Risiko von bewusster Zerstörung wird durch die oben beschriebenen Maßnahmen so weit wie möglich reduziert.

Rasche Wiederherstellbarkeit

Maßnahmen:

Für alle internen Systeme ist innerhalb des Monitorings eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

Automatisierte Backup-Systeme stellen eine Wiederherstellbarkeit der Anwender:innen-Daten sicher. Backups erfolgen ausschließlich verschlüsselt. Besonders relevante Services (Identity-Management, Lastverteilung, Datenbanken etc.) werden im HA-Setup bzw. als Cluster oder im „hot-standby“ etabliert.

3.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Auftragskontrolle

Infra.run hat zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Vertragspartners verarbeitet werden können (Auftragskontrolle).

Maßnahmen:

Es gibt ausschließlich verschlüsselten und personalisierten Zugang zu den Systemen, auf denen die Daten verarbeitet werden (public-key basiertes „SSH“). Alle Aktivitäten werden geloggt und können jederzeit nachvollzogen werden. Der Zugriff auf die Systeme ist auch nicht allen Admins möglich, sondern nur denen, die mit der Wartung dieser Server betraut sind.

Des Weiteren werden alle Mitarbeiter:innen von infra.run in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung. Regelmäßige Audits mit dem Vertragspartner sichern ab, dass Änderungen an Diensten bzw. technischen oder datenschutzrelevante Rahmenbedingungen auf mögliche Änderungen bzw. Risiken geprüft werden. Infra.run hat einen Datenschutzbeauftragten beziehungsweise einen Ansprechpartner für Datenschutz bestellt. Dieser ist durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.