

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Stand: 21.10.2026 · Saniakte Fassung für die Website

Rolle	Angabe
Verantwortlicher	Ihre Organisation
Datenschutzkontakt des Verantwortlichen	Kontakt für den Datenschutz Ihrer Organisation
Auftragsverarbeiter (Betrieb von Saniakte)	Lucas Paulick, Friedensallee 1, 16556 Borgsdorf, kontakt@saniakte.de
Unterauftragnehmer (Rechenzentrum)	netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe, Deutschland
Serverstandort	Nürnberg, Deutschland

Diese Beschreibung umfasst die Anwendung und ihren Betrieb durch den Auftragsverarbeiter. Maßnahmen, die die Organisation selbst treffen muss, stehen in Abschnitt 7.

1. Vertraulichkeit

1.1 Zugangskontrolle zur Anwendung

- Der Zugang ist an persönliche Benutzerkonten gebunden. Es gibt keinen anonymen Zugang zu Einsatzdaten, ausgenommen der zeitlich begrenzte Protokolllink nach Abschnitt 1.4.
- Passwörter werden nicht im Klartext gespeichert, sondern als bcrypt-Hashwert mit Kostenfaktor 12. Der Kostenfaktor ist so gewählt, dass ein Prüfvorgang spürbar Rechenzeit kostet und Offline-Angriffe auf eine erbeutete Datenbank deutlich verlangsamt werden.
- Bei der Erstanmeldung ist ein Passwortwechsel erzwungen. Ein vom Administrator vergebenes Initialpasswort bleibt dadurch nicht dauerhaft gültig.
- Ein Passwortwechsel im laufenden Betrieb verlangt die Eingabe des aktuellen Passworts. Ausgenommen ist allein der erzwungene Erstwechsel, bei dem es kein selbstgewähltes Passwort gibt. Ohne diese Prüfung könnte eine übernommene Sitzung das Passwort rotieren und den Kontoinhaber aussperren.
- Jedes Konto kann zusätzlich einen zweiten Faktor einschalten (zeitbasierter Einmalcode, TOTP). Die Ersatzcodes liegen nur als Hashwert in der Datenbank.
- Nach acht Fehlversuchen binnen 15 Minuten ruht die Anmeldung eines Kontos für die Adresse, von der die Fehlversuche kamen. Zusätzlich ist die Zahl der Anmeldeversuche je Adresse begrenzt.
- Einrichtungslinks für neue Konten und zum Zurücksetzen des Passworts sind 72 Stunden gültig und werden in der Datenbank nur als Hashwert gespeichert.

1.2 Zugriffskontrolle innerhalb der Anwendung

- Drei Rollen: **admin** (Verwaltung), **zeugwart** (zusätzlich Fahrzeuge und Material pflegen und Materialhinweise lesen) und **helfer** (Dokumentation). Die Rolle wird serverseitig aus der Sitzung gelesen; sie ist nicht durch Eingaben des Clients beeinflussbar.
- Innerhalb eines Dienstes gibt es zusätzlich die Rollen Einsatzleitung, Schreiber und Helfer.
- Die Organisation legt einstellbare Rechte fest, je Recht „alle“ oder „nur Verwaltung“. Ab Werk der Verwaltung vorbehalten: Fahrzeuge und Material pflegen, Dokumente hinterlegen, Hilfeleistung einschränken, Dienste ausschreiben, Dienstberichte lesen. Ab Werk für alle: Dienste anlegen und abschließen, Materialhinweise lesen, eigenen Namen und eigenes Passwort ändern.
- Benutzerverwaltung, Organisationsdaten, Auskunft, Löschung und Datenschutzunterlagen sind ausschließlich der Rolle **admin** zugänglich.
- Die Dienstsicht der Organisation legt fest, welche Hilfeleistungen ein Konto ohne die Rolle **admin** sieht. Bei „Nur eigene“ (auch „Nur eigene, 24 Stunden“) sind das die Dienste, in die es eingeteilt ist, und von den Hilfeleistungen ohne Dienstzuordnung nur die selbst dokumentierten; fremde Hilfeleistungen ohne Dienst sieht ein Helfer nicht. Dieselbe Regel gilt für Liste, Detailseite, PDF, CSV und Sammel-PDF. Wer einen Dienst nicht sieht, kann sich auch nicht selbst eintragen, ihn wieder öffnen oder über die Dienstplanung die eigene Meldung zusagen; einen abgeschlossenen Dienst öffnet nur die Rolle **admin** wieder.
- Die Lagebildsicht legt fest, was ein Konto ohne Rolle im Dienst im Lagebild sieht (ab Werk nur die Aufträge).
- Öffentlich ohne Anmeldung erreichbar sind nur die Anmeldeseite, Impressum und Datenschutzerklärung, das Logo der Organisation, der zeitlich begrenzte Protokolllink und der Einrichtungslink.
- Ein Administrator kann weder sich selbst noch den letzten verbleibenden Administrator löschen. Damit bleibt die Installation stets bedienbar.

1.3 Sitzungsverwaltung

- Das Sitzungscookie wird mit den Merkmalen **secure**, **httpOnly** und **sameSite=lax** gesetzt: keine Übertragung über unverschlüsselte Verbindungen, kein Zugriff aus JavaScript, kein Mitsenden bei fremdinitiierten Anfragen aus Drittkontexten.
- Jede Anfrage prüft die Sitzung gegen den aktuellen Stand des Kontos (Sitzungsversion). Ein Wechsel oder Zurücksetzen des Passworts, ein eingelöster Einrichtungslink und „Alle Sitzungen beenden“ (durch die Person selbst oder die Verwaltung) beenden alle bestehenden Sitzungen des Kontos sofort. Den Passwortwechsel ohne bisheriges Passwort erhält nur eine Sitzung, die selbst mit dem Startpasswort entstand.
- Daneben setzt die Anmeldebibliothek (Auth.js) nur technisch notwendige Cookies für den Schutz vor gefälschten Anfragen (CSRF) und die Rückleitung nach der Anmeldung. Analyse-, Werbe- oder Social-Media-Dienste sind nicht eingebunden.

1.4 Protokolllinks

- Der Zugriffstoken für den anonymen Protokollabruf wird aus dem kryptographisch sicheren Zufallszahlengenerator von Node (**crypto.randomBytes**) erzeugt. Er ist nicht erratbar und nicht aus Einsatzdaten ableitbar.

- Der Token ist 48 Stunden gültig. Danach entzieht der Löschlauf ihn; der Link ist wirkungslos, das Protokoll bleibt über die Anmeldung erreichbar.
- Von selbst entsteht ein Link nur beim ersten Aufruf eines frischen Protokolls. Ein abgelaufener oder gelöschter Link wird nicht stillschweigend neu angelegt; einen neuen erzeugt nur ein Konto mit Schreibrecht an der Hilfeleistung ausdrücklich und nach Rückfrage, solange die Aufbewahrungsfrist läuft und die Verarbeitung nicht eingeschränkt ist. Das wird im Änderungsprotokoll festgehalten.
- Antworten mit Protokoll- oder Auskunftsinhalten tragen **Cache-Control: no-store**, damit sie nicht in Proxy- oder Browsercaches zurückbleiben.

1.5 Trennung

- Jede Organisation hat eine eigene Installation: eigene Container und eine eigene Datenbank. Es gibt keinen Mandantenbetrieb und keine gemeinsame Datenbank mehrerer Organisationen.
- Alle Installationen laufen auf einem gemeinsamen Server des Auftragsverarbeiters. Auf demselben Server laufen außerdem die Dienste des Anbieters (Website, Ticketdienst, Statusseite, Mailserver) sowie weitere Dienste des Betreibers, die nicht zu Saniakte gehören, jeweils in eigenen Containern.

2. Integrität

2.1 Transportverschlüsselung

- Der vorgelagerte Reverse Proxy Traefik erzwingt HTTPS. Zertifikate werden automatisch über Let's Encrypt bezogen und erneuert. Unverschlüsselte Aufrufe werden auf HTTPS umgeleitet.
- Für jede Installation sind folgende Sicherheitskopfelemente konfiguriert: **Strict-Transport-Security** (ein Jahr, einschließlich Subdomains), **X-Content-Type-Options: nosniff**, **X-Frame-Options: DENY** und **Referrer-Policy: strict-origin-when-cross-origin**. Seiten mit einem Einrichtungsslink senden **Referrer-Policy: no-referrer**.
- Die Anwendung ist nicht direkt aus dem Netz erreichbar; sie nimmt Anfragen nur über Traefik entgegen.

2.2 Eingabe- und Änderungskontrolle

- Jede Dokumentation trägt die dokumentierende Person als Verweis auf das Benutzerkonto und zusätzlich als unveränderlichen Namensvermerk. Der Vermerk bleibt auch nach Löschung des Kontos erhalten; ohne ihn wäre die Dokumentation nachträglich nicht mehr zuordenbar.
- Jede Auskunftserteilung wird protokolliert (Zeitpunkt, handelnder Administrator, Art und Bezug der Auskunft). Damit ist die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO erfüllt und die Auskunftsfunktion nicht als bequemer Datenexport nutzbar.
- Unterschriften werden nur gespeichert, wenn entweder ein Unterschriftenbild oder ein dokumentierter Grund für das Fehlen vorliegt. Datensätze ohne beides sind ausgeschlossen.

2.3 Datenhaltung

- Die Datenbank (PostgreSQL) ist nur im internen Docker-Netz der jeweiligen Installation erreichbar; sie hat keinen veröffentlichten Port. Zugriff hat allein die Anwendung dieser Installation.
- Unterschriften und das Organisationslogo liegen als Binärdaten in der Datenbank, nicht als Dateien im Dateisystem. Sicherung und Löschung bleiben dadurch atomar mit dem zugehörigen Datensatz; es gibt keinen zweiten Löschanforderung über das Dateisystem, der auseinanderlaufen könnte.

- Hochgeladene SVG-Logos werden mit **Content-Security-Policy: sandbox** und **Content-Disposition: inline** ausgeliefert, damit eingebettetes Skript nicht ausgeführt wird. Zulässig sind nur **image/png** und **image/svg+xml** bis 1 MB.

2.4 Eingaben ohne Netz auf dem Gerät

Im Einsatz fehlt oft der Empfang. Damit eine Dokumentation trotzdem nicht verloren geht, legt die Anwendung Eingaben, die den Server nicht erreichen, im Browser des Geräts ab (IndexedDB, Datenbank **saniakte-warteschlange**) und überträgt sie, sobald der Server wieder erreichbar ist. Das betrifft einfache Einträge, Protokolle samt Unterschriften, Bilder zu einem wartenden Protokoll, Nachträge, Logbucheinträge und den Dienststart.

- Gesundheitsdaten liegen nur so lange auf dem Gerät, bis der Server den Vorgang angenommen hat; danach wird er sofort gelöscht. Lehnt der Server ab (etwa wegen einer fehlenden Pflichtangabe oder fehlender Rechte), bleibt der Vorgang sichtbar mit der Meldung stehen, bis die Person ihn erneut sendet oder ausdrücklich verwirft. Still verworfen wird nichts.
- Beim Abmelden wird die Warteschlange vollständig geleert. Warten noch Einträge, fragt die Anwendung vorher, ob sie erst übertragen werden sollen („Es warten noch 2 Einträge – erst übertragen?“). So bleiben keine Gesundheitsdaten für das nächste Konto auf einem gemeinsam genutzten Gerät liegen. Das gilt auch für Einträge eines anderen Kontos, die noch auf dem Gerät warten: meldet sich auf einem gemeinsam genutzten Gerät eine zweite Person ab, werden nach ihrer Bestätigung auch diese gelöscht. Ist die Sitzung abgelaufen, bietet die Anwendung zuerst das neue Anmelden an; die Einträge bleiben dabei erhalten, und Löschen verlangt eine zweite Bestätigung. Beim Abmelden werden außerdem die zwischengespeicherten Seiten (Startseite, Formulare) gelöscht.
- Jeder Vorgang trägt die Kennung des Kontos, das ihn erfasst hat, und wird nur mit diesem Konto übertragen. Ist nach Ablauf der Sitzung ein anderes Konto angemeldet, wird der Vorgang nicht unter fremdem Namen gespeichert, sondern zur Prüfung markiert.
- Jeder Vorgang trägt eine zufällige Kennung (UUID), die als **Idempotency-Key** mitgeht und unter der der Server den Datensatz anlegt. Kommt derselbe Vorgang zweimal an, weil eine Antwort im Funkloch verloren ging, entsteht kein zweiter Datensatz; das gilt für Einsätze, Protokolle, Nachträge, Logbucheinträge und Bilder. Ein Protokoll und seine Unterschriften werden in einer Transaktion gespeichert: entweder beides oder nichts. Gehört die Kennung zu einem fremden Datensatz, antwortet der Server ohne Angaben dazu (409).
- Nachgereichte Nachträge und Logbucheinträge behalten den Zeitstempel des Eingangs beim Server; die tatsächliche Erfassungszeit wird am Text vermerkt. Damit lässt sich über die Warteschlange nichts rückdatieren.
- Für den Hinweis auf der Übersicht merkt sich das Gerät im **localStorage** nur Zahlen (wie viele Einträge übertragen wurden oder nicht) und die Kennung des zuletzt angemeldeten Kontos, keine Inhalte. Beides wird beim Abmelden gelöscht.
- Die Daten im Browser sind durch die Gerätesperre und die Trennung der Browser-Ursprünge geschützt, aber nicht zusätzlich verschlüsselt. Für Dienstgeräte sollte die Organisation daher eine Bildschirmsperre vorschreiben (siehe Abschnitt 7).

3. Verfügbarkeit und Belastbarkeit

- Sicherung: täglich um 02:30 Uhr je Installation ein vollständiger Datenbankauszug (**pg_dump**), sofort mit **gpg** (AES256) verschlüsselt. Jede Sicherung wird nach dem Schreiben vollständig eingelesen und geprüft (entschlüsselbar und lesbar); der Klartext liegt dafür nur kurz in einem Ordner, auf den allein der Betriebsnutzer zugreifen kann, und wird sofort gelöscht. Aufbewahrung 30 Tage; gelöscht wird erst nach einer geglückten neuen Sicherung.
- Vor jeder Aktualisierung einer Installation wird zusätzlich eine Sicherung der Datenbank angelegt. Sie ist nicht verschlüsselt, liegt in einem Ordner, auf den allein der Betriebsnutzer zugreifen kann, und wird nach 30 Tagen gelöscht.
- Ablage der Sicherungen: auf demselben Server. Eine Kopie außerhalb dieses Servers besteht derzeit nicht; sie ist in Vorbereitung.
- Außer den Kartendiensten für die Standortsuche und, falls eingeschaltet, dem Diktat und den Benachrichtigungen (siehe Verzeichnis von Verarbeitungstätigkeiten) ruft die Anwendung keine externen Dienste auf.
- Der Löschlauf bricht bei einem Fehler an einem einzelnen Datensatz nicht ab. Der betroffene Datensatz wird vermerkt und im nächsten Durchlauf erneut versucht.

4. Löschung und Speicherbegrenzung

- Ein wiederkehrender Löschlauf entfernt automatisch nach Fristablauf: abgelaufene Protokolllinks sowie Einsätze samt Protokolldatei, Unterschriften und zugehörigen Links nach 10 Jahren.
- Gelöscht wird hart, nicht anonymisiert. Es bleiben keine Restdatensätze zurück, deren Anonymität später bestritten werden könnte.
- Über jeden Löschlauf wird ein Löschprotokoll geführt, das ausschließlich Umfang (Anzahl), Bereich und Zeitraum enthält – keine Namen, keine Kennungen. Es belegt gegenüber der Aufsichtsbehörde, dass gelöscht wurde, ohne selbst ein Personendatenspeicher zu sein.
- Einsatzstatistiken bleiben als reine Monatszählung ohne Personenbezug erhalten.
- Vor Fristablauf steht die Verarbeitungseinschränkung nach Art. 18 DSGVO zur Verfügung: Der Datensatz wird aus allen Listen und Suchen ausgeblendet und ist nur noch bei ausdrücklichem Direktaufruf durch die Rolle **admin** sichtbar. Ein PDF, die Unterschriftsbilder, das Sammel-PDF und der öffentliche Protokolllink werden für eingeschränkte Datensätze nicht mehr ausgegeben. Die Auskunft nach Art. 15 DSGVO erfolgt über die Auskunftsseite als JSON-Datei; die Unterschriftsbilder werden nur auf gesonderten Wunsch herausgegeben.
- Sicherungen enthalten gelöschte Datensätze noch bis zum Ablauf ihrer Aufbewahrung von 30 Tagen (Abschnitt 3).

5. Protokollierung auf Serverebene

- Die Anwendung schreibt keine aufgerufenen Adressen und keine Query-Strings in ihre Protokolle. Ihre Container-Protokolle sind in der Größe begrenzt.
- Ob und in welchem Umfang der vorgelagerte Reverse Proxy Zugriffe protokolliert, beschreibt diese Fassung noch nicht; die Angabe wird nachgereicht.

6. Auftragsverarbeitung

- Saniakte wird vom Auftragsverarbeiter Lucas Paulick betrieben; Grundlage ist der Vertrag zur Auftragsverarbeitung (in der Anwendung unter Dokumente abrufbar).
- Unterauftragnehmer für das Rechenzentrum: netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe, Deutschland, Standort Nürnberg, Deutschland.
- Weitere Empfänger einzelner Daten (Kartendienst, Push-Dienste der Browserhersteller, Diktat) nennt das Verzeichnis von Verarbeitungstätigkeiten.

7. Pflichten und Vorkehrungen

7.1 Pflichten der Organisation

- Alle Nutzerinnen und Nutzer auf Vertraulichkeit und, soweit einschlägig, auf die Schweigepflicht nach § 22 Abs. 1 Nr. 1 lit. b BDSG verpflichten.
- Regeln für die Erfassungsgeräte festlegen: Bildschirmsperre, Geräteverschlüsselung, Verlust sofort der Verwaltung melden.
- Konten ausgeschiedener Personen zeitnah löschen.
- Den Ablauf bei Datenpannen (eigene Unterlage) bekannt machen.
- Diese Maßnahmen regelmäßig überprüfen (Art. 32 Abs. 1 lit. d DSGVO).

7.2 Beim Auftragsverarbeiter

- Tägliche verschlüsselte Sicherung nach Abschnitt 3.
- Meldung von Datenpannen an die Organisation unverzüglich, spätestens 24 Stunden nach Kenntnis (Vertrag zur Auftragsverarbeitung § 7 Abs. 4).