Technisch-organisatorische Maßnahmen (TOM)

i. S. d. Art. 32 DS-GVO

Stand: 27.11.2026

1. Vorbemerkung zur Arbeits- und Betriebsumgebung

Die mint software GmbH arbeitet vollständig remote und unterhält keine eigenen Büro- oder Serverräume. Die Datenverarbeitung erfolgt auf zwei Ebenen:

- **Unternehmens-IT** – Sämtliche Kommunikation, Dokumentenablage und Archivierung erfolgen in Microsoft 365 (u. a. Teams, SharePoint, Outlook). Microsoft Entra ID regelt als zentrale Identitäts- und Zugriffsverwaltung den Zugang. Als Endgeräte werden ausschließlich firmeneigene Apple MacBooks eingesetzt.
- **Software-Plattform** – Die Produktivumgebung wird überwiegend bei Amazon Web Services in Rechenzentren in Frankfurt am Main und Irland betrieben. Ergänzend werden Dienste von Microsoft Azure (u. a. Dateispeicher, Warteschlangen, Schlüsselverwaltung, Monitoring sowie einzelne Produktivdienste) in der Europäischen Union (Frankfurt am Main) genutzt. Die Entwicklungsumgebung ist davon getrennt in Microsoft Azure eingerichtet.

Datenschutzrechtliche Rolle: Bei der Plattform schadensmeldung.digital sind die mint software GmbH und ihre gewerblichen Kunden (z. B. Werkstätten) für die Daten der Endkunden gemeinsam Verantwortliche nach Art. 26 DS-GVO, soweit nicht im Einzelfall eine Auftragsverarbeitung vereinbart ist. Bei den Modulen Dokumentcheck, KI-Telefonassistenz, Video, Eigene Rufnummer und Bildanonymisierung handelt die mint software GmbH als Auftragsverarbeiter nach Art. 28 DS-GVO. Die nachfolgenden Maßnahmen gelten für alle Produkte.

Physische Sicherungsmaßnahmen der Rechenzentren (Zutritt, Stromversorgung, Brandschutz, Klimatisierung) werden von diesen Anbietern erbracht und durch deren Zertifizierungen und Prüfberichte (u. a. ISO/IEC 27001, SOC 2 Type II, BSI C5) nachgewiesen. Die internen Sicherheitskonzepte der mint software GmbH (Datensicherung und Notfallwiederherstellung, Löschkonzept, Monitoring und Incident Response, sichere Softwareentwicklung) orientieren sich an ISO/IEC 27001:2022.

2. Vertraulichkeit (Art. 32 Abs. 1 b DS-GVO)

2.1 Zutrittskontrolle

Maßnahmen, die gewährleisten, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen im Unternehmen verwehrt wird.

mint software GmbH · Carl-Fischer-Str. 2 · 49084 Osnabrück · www.schadensmeldung.digital · info@mmmint.ai · +49 541 96328784
Amtsgericht Osnabrück HRB 215257 · Geschäftsführer Maximilian Stein · USt-IdNr. DE 334940239 · Steuernummer 65 200 38818
Sparkasse Osnabrück · IBAN DE03 2655 0105 1552 3779 52 · BIC NOLADE22XXX

- **Keine eigenen Büro- oder Serverräume** – Alle Mitarbeiter arbeiten remote. Es existieren keine unternehmenseigenen Räumlichkeiten, in denen Datenverarbeitungsanlagen betrieben werden.
- **Geschäftsanschrift** – Die Geschäftsanschrift dient ausschließlich dem Postempfang. Der Briefkasten ist durch eine Schließanlage gesichert.
- **Rechenzentren** – Die physische Zutrittskontrolle zu den Rechenzentren erfolgt durch die Betreiber AWS und Microsoft mittels mehrstufiger Zutrittskontrollen und ist durch deren Zertifizierungen nachgewiesen.
- **Arbeiten im Homeoffice und unterwegs** – Gearbeitet wird nur in Umgebungen, in denen Bildschirminhalte nicht von Unbefugten eingesehen werden können. Endgeräte werden nicht unbeaufsichtigt gelassen und bei Abwesenheit gesperrt.

2.2 Zugangskontrolle

Maßnahmen, die gewährleisten, dass Unbefugten der Zugang und somit die Nutzung von Datenverarbeitungsanlagen verwehrt wird.

- **Zentrale Identitätsverwaltung** – Die Arbeitskonten aller Mitarbeiter sind personengebunden und werden zentral in Microsoft Entra ID verwaltet. Die Anmeldung an Microsoft 365 und weiteren Diensten erfolgt, soweit technisch möglich, per Single Sign-on über Entra ID.
- **Mehr-Faktor-Authentifizierung** – Für alle Arbeitskonten in Entra ID, für administrative Konten bei Cloud- und Quellcode-Plattformen sowie für technische Administrations- und Entwicklerzugänge (z. B. Datenbankzugriff) ist eine Mehr-Faktor-Authentifizierung verpflichtend. Veraltete Anmeldeverfahren ohne MFA sind gesperrt.
- **Passwortrichtlinie** – Entra ID setzt Mindestanforderungen an Passwortlänge und -komplexität durch, verhindert die Verwendung bekannter unsicherer Passwörter und sperrt Konten bei wiederholten Fehlanmeldungen automatisch (Smart Lockout).
- **Passwortmanager** – Zur Verwaltung dienstlicher Zugangsdaten wird ein Passwortmanager eingesetzt, in dem Passwörter verschlüsselt gespeichert werden.
- **Endgeräte** – Es werden ausschließlich firmeneigene Apple MacBooks mit personengebundenem, passwortgeschütztem Benutzerkonto eingesetzt. Die Festplattenverschlüsselung (FileVault) ist auf allen Geräten aktiviert.
- **Geräteschutz** – Per Richtlinie vorgegeben sind: aktivierte macOS-Firewall, automatische Installation von Sicherheitsupdates, automatische Bildschirmsperre nach spätestens 5 Minuten Inaktivität sowie aktivierter integrierter Schadsoftwareschutz (XProtect, Gatekeeper).
- **Privilegierte Administratorkonten** – Für den Entra-Mandanten bestehen zwei dedizierte Administratorkonten, die nicht für den Tagesbetrieb genutzt werden. Für die Cloud- und Quellcode-Plattformen werden administrative Rechte über gesonderte, von den Arbeitskonten getrennte Konten bzw. Rollen vergeben.

mint software GmbH · Carl-Fischer-Str. 2 · 49084 Osnabrück · www.schadensmeldung.digital · info@mmmint.ai · +49 541 96328784
Amtsgericht Osnabrück HRB 215257 · Geschäftsführer Maximilian Stein · USt-IdNr. DE 334940239 · Steuernummer 65 200 38818
Sparkasse Osnabrück · IBAN DE03 2655 0105 1552 3779 52 · BIC NOLADE22XXX

- **Administrativer Zugang zur Produktion** – Für die Produktivumgebung bestehen zwei Administratorkonten. Ein dauerhafter direkter Zugriff auf Produktivdaten besteht nicht. Administrative Eingriffe erfolgen zeitlich begrenzt (Just-in-Time) über einen temporären, zusätzlich abgesicherten Zugangsserver (Jump-Box). Der Regelbetrieb erfolgt automatisiert über versionierte Infrastruktur- und Deployment-Definitionen (IaC).
- **Verschlüsselte Verbindungen** – Der Zugriff auf Plattform, Microsoft 365 und Cloud-Verwaltungsoberflächen erfolgt ausschließlich über verschlüsselte Verbindungen (TLS), unabhängig vom genutzten Netzwerk.
- **Protokollierung von Anmeldungen und administrativen Zugriffen** – Anmeldungen werden in Entra ID protokolliert. Administrative Zugriffe und Konfigurationsänderungen an der Cloud-Infrastruktur werden protokolliert (AWS CloudTrail, Azure Activity Log) und bei Auffälligkeiten ausgewertet.
- **Überprüfung der Zugangsberechtigungen** – Berechtigungen in der Quellcodeverwaltung und bei den Cloud-Plattformen werden regelmäßig sowie bei personellen Veränderungen überprüft.

3. Vertraulichkeit (Art. 32 Abs. 1 a, b DS-GVO)

3.1 Zugriffskontrolle

Maßnahmen, die den Zugriff auf Daten durch Unbefugte verhindern sowie Informationen vor unerlaubter Kenntnisnahme, Veränderung oder Löschung schützen.

- **Rollenbasiertes Berechtigungskonzept** – Zugriffsberechtigungen werden nach dem Need-to-Know- und Least-Privilege-Prinzip vergeben – in der Plattform, in Microsoft 365 (SharePoint- und Teams-Berechtigungen) und in der Cloud-Infrastruktur (IAM, Azure-Berechtigungsgruppen, Kubernetes-RBAC).
- **Berechtigungsprozess** – Vergabe, Änderung und Entzug von Berechtigungen bei Eintritt, Wechsel und Austritt von Mitarbeitern erfolgen nach einem festgelegten Ablauf über die zentrale Identitätsverwaltung. Nicht angebundene Anbieterkonten werden im selben Ablauf manuell entzogen.
- **Verschlüsselung besonders schutzbedürftiger Daten** – Bank- und sensible Konfigurationsdaten werden zusätzlich auf Anwendungsebene verschlüsselt. Die Schlüssel werden in Azure Key Vault verwaltet.
- **Löschkonzept** – Ein Löschkonzept nach DIN 66398 legt je Datenkategorie Aufbewahrungsfristen, Löschauslöser und das Löschverfahren fest. Anwendungs- und Geschäftsdaten werden nicht automatisch nach Ablauf einer Frist gelöscht, sondern wenn ein Löschauslöser eintritt (Antrag einer betroffenen Person, Vertragsende eines Kunden, Wegfall des Zwecks). Stehen gesetzliche Aufbewahrungspflichten (z. B. für Rechnungen) einer Löschung entgegen, werden die Daten bis zum Fristablauf aufbewahrt und danach gelöscht. Abgerechnete Rechnungen und signierte Dokumente können in der Anwendung nicht gelöscht werden. Zugehörige Dateien im

mint software GmbH · Carl-Fischer-Str. 2 · 49084 Osnabrück · www.schadensmeldung.digital · info@mmmint.ai · +49 541 96328784
Amtsgericht Osnabrück HRB 215257 · Geschäftsführer Maximilian Stein · USt-IdNr. DE 334940239 · Steuernummer 65 200 38818
Sparkasse Osnabrück · IBAN DE03 2655 0105 1552 3779 52 · BIC NOLADE22XXX

Dateispeicher werden einschließlich früherer Versionen im Rahmen des Löschverfahrens manuell entfernt.

- **Papierlose Arbeitsweise** – Eingehende Post wird digitalisiert und in Microsoft 365 abgelegt. Die Papieroriginale werden anschließend vernichtet.
- **Keine externen Datenträger** – Externe Datenträger (z. B. USB-Sticks, externe Festplatten) werden nicht eingesetzt.
- **Rückgabe und Löschung von Endgeräten** – Bei Austritt werden Endgeräte zurückgegeben und vor einer Weiterverwendung vollständig gelöscht.
- **Verpflichtung auf Vertraulichkeit** – Alle Mitarbeiter sind schriftlich auf die Vertraulichkeit und den Datenschutz verpflichtet (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DS-GVO).

3.2 Trennungskontrolle

Maßnahmen, die gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden.

- **Mandantentrennung** – Personenbezogene Datensätze sind einem Mandanten zugeordnet. Nutzer erhalten ausschließlich Zugriff auf die Daten ihres Mandanten. Dateien werden in mandantenbezogenen Speicherbereichen abgelegt.
- **Trennung der Umgebungen** – Produktiv- und Entwicklungsumgebung sind in getrennten Konten bzw. Abonnements betrieben. Zugangsdaten der Produktivumgebung sind aus der Entwicklungsumgebung nicht zugänglich und umgekehrt. In Test- und Entwicklungsumgebungen werden keine unmaskierten Produktivdaten verwendet.
- **Kunden- und projektbezogene Berechtigungen** – Zugriffsberechtigungen auf kunden- und projektbezogene Daten werden, soweit möglich, auf die jeweils zuständigen Mitarbeiter beschränkt.

4. Integrität (Art. 32 Abs. 1 b DS-GVO)

4.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass bei der Weitergabe von Daten ein unberechtigter Zugriff, unbefugte Kenntnisnahme oder unbeabsichtigter Abfluss verhindert wird.

- **Transportverschlüsselung** – Datenübertragungen zur Plattform, zu Schnittstellenpartnern und zu Speicherdiensten über öffentliche Netze erfolgen verschlüsselt nach aktuellem Stand der Technik (TLS 1.2 oder höher). Interne Verbindungen laufen innerhalb abgeschotteter privater Netze der Cloud-Anbieter. Die Zertifikate werden automatisiert verwaltet.
- **Verschlüsselung gespeicherter Daten** – Datenbanken, Objektspeicher und Datensicherungen der Plattform sind im Ruhezustand verschlüsselt (u. a. AWS KMS, AES-256, Azure Storage Service Encryption), ebenso die Daten in Microsoft 365. Endgeräte sind per FileVault verschlüsselt.

mint software GmbH · Carl-Fischer-Str. 2 · 49084 Osnabrück · www.schadensmeldung.digital · info@mmmint.ai · +49 541 96328784
Amtsgericht Osnabrück HRB 215257 · Geschäftsführer Maximilian Stein · USt-IdNr. DE 334940239 · Steuernummer 65 200 38818
Sparkasse Osnabrück · IBAN DE03 2655 0105 1552 3779 52 · BIC NOLADE22XXX

- **Kontrollierter Datenaustausch** – Dokumente werden vorzugsweise über berechtigungsgesteuerte Freigaben in SharePoint/OneDrive bzw. über Freigabelinks der Plattform geteilt, nicht als E-Mail-Anhang. E-Mails werden, sofern von der Gegenstelle unterstützt, transportverschlüsselt (TLS) übertragen.
- **Kein öffentlicher Zugriff auf Speicher** – Öffentlicher Zugriff auf die produktiven Objektspeicher ist deaktiviert.
- **Keine Datenträger zum Datentransport** – Private oder externe Datenträger werden nicht zum Datentransport eingesetzt.

4.2 Eingabekontrolle

Maßnahmen, die eine nachträgliche Überprüfung ermöglichen, wann und von wem personenbezogene Daten in Systemen eingegeben, verändert oder gelöscht wurden.

- **Protokollierung in der Plattform** – Die Plattform protokolliert Aktivitäten mit Nutzer, Aktion, Zielobjekt und Zeitpunkt sowie die Statushistorie von Vorgängen. Die Protokolle werden gemäß Löschkonzept aufbewahrt und gelöscht.
- **Dokumentation von Löschungen** – Löschungen von Vorgängen werden im Aktivitätsprotokoll mit Nutzer, Zeitpunkt und Objekt erfasst. Löschungen aufgrund von Anfragen Betroffener oder bei Vertragsende eines Mandanten werden zusätzlich mit Umfang und Grund dokumentiert und schriftlich bestätigt.
- **Protokollierung in Microsoft 365** – Aktivitäten in Microsoft 365 werden im Microsoft-365-Überwachungsprotokoll (Audit-Log) erfasst.
- **Protokollierung von Infrastruktur- und Codeänderungen** – Änderungen an der Cloud-Infrastruktur werden protokolliert (AWS CloudTrail, Azure Activity Log). Änderungen an Anwendung und Infrastruktur sind über die Versionsverwaltung nachvollziehbar (Pull Requests, Release-Historie).
- **Aufbewahrung sicherheitsrelevanter Protokolle** – Selbst gespeicherte sicherheitsrelevante Protokolle (u. a. AWS CloudTrail einschließlich der Sicherungs- und Wiederherstellungsvorgänge, Zugriffs- und Datenbank-Auditprotokolle) werden 12 Monate aufbewahrt. Protokolle der Plattformanbieter (Azure Activity Log, Entra ID, GitHub) werden gemäß deren Standardaufbewahrung vorgehalten. Bei Sicherheitsvorfällen werden relevante Protokolle zusätzlich als Beweismittel gesichert.
- **Versionierung** – SharePoint und OneDrive versionieren Dokumente. Versehentlich geänderte oder gelöschte Dokumente können wiederhergestellt werden.

mint software GmbH · Carl-Fischer-Str. 2 · 49084 Osnabrück · www.schadensmeldung.digital · info@mmmint.ai · +49 541 96328784
Amtsgericht Osnabrück HRB 215257 · Geschäftsführer Maximilian Stein · USt-IdNr. DE 334940239 · Steuernummer 65 200 38818
Sparkasse Osnabrück · IBAN DE03 2655 0105 1552 3779 52 · BIC NOLADE22XXX

5. Auftragsverarbeitung (Art. 28 und Art. 32 Abs. 4 DS-GVO)

5.1 Auftragskontrolle

Maßnahmen, die gewährleisten, dass Daten, die im Auftrag verarbeitet werden, ausschließlich gemäß den Vorgaben des Auftraggebers verarbeitet werden.

- **Verarbeitung nur auf Weisung** – Soweit die mint software GmbH als Auftragsverarbeiter tätig ist, werden personenbezogene Daten ausschließlich auf Grundlage eines Auftragsverarbeitungsvertrags und entsprechend den Weisungen des Auftraggebers verarbeitet.
- **Gemeinsame Verantwortlichkeit** – Soweit die mint software GmbH mit Kunden gemeinsam verantwortlich ist, sind Zuständigkeiten, Informationspflichten, Betroffenenrechte und das Vorgehen bei Datenschutzverletzungen in einem Vertrag nach Art. 26 DS-GVO geregelt.
- **Übersicht der Unterauftragsverarbeiter** – Eine Übersicht der Dienstleister, die im Auftrag personenbezogene Daten verarbeiten oder Zugriff darauf haben können, wird gepflegt – u. a. Hosting und Cloud-Dienste (AWS, Microsoft Azure), Kommunikation (Microsoft 365, Amazon SES, Twilio, Telnyx, WhatsApp über Twilio), KI-Dienst (OpenAI mit EU-Datenresidenz und Zero Data Retention), Video (Mux), Bildanonymisierung (deepsight) sowie Softwareentwicklung (GitHub, GitGuardian). Mit diesen Unterauftragsverarbeitern bestehen Auftragsverarbeitungsverträge.
- **Datenhaltung und Drittlandtransfer** – Die Plattformdaten werden in Rechenzentren innerhalb der EU gespeichert. Für die gesondert lizenzierten Module Video und Angebote gilt abweichend: Videos werden bei Mux, Inc. gespeichert und ausgeliefert (Speicherung bei Google Cloud in den USA; EU-U.S. Data Privacy Framework). Soweit Anbieter ihren Sitz in einem Drittland haben, erfolgt die Absicherung über EU-Standardvertragsklauseln bzw. das EU-U.S. Data Privacy Framework.
- **Auswahl und Kontrolle von Dienstleistern** – Dienstleister werden vor Beauftragung nach Datenschutz- und Sicherheitskriterien ausgewählt. Ihre Nachweise (Zertifikate, Prüfberichte) werden bei Beauftragung und anlassbezogen geprüft.
- **Rückgabe und Löschung bei Vertragsende** – Bei Auftragsverarbeitung erhält der Auftraggeber bei Vertragsende auf Wunsch einen Export seiner Daten in strukturierter Form (einzelne Vorgänge, Formulare, Rechnungen und Nachrichten). Anschließend werden die Daten nach einem festgelegten Verfahren manuell gelöscht und die Löschung schriftlich bestätigt.
- **Datenschutzbeauftragter** – Ein externer Datenschutzbeauftragter ist bestellt. Er unterweist die Mitarbeiter im Datenschutz und wird bei datenschutzrelevanten Fragestellungen einbezogen.

mint software GmbH · Carl-Fischer-Str. 2 · 49084 Osnabrück · www.schadensmeldung.digital · info@mmmint.ai · +49 541 96328784
Amtsgericht Osnabrück HRB 215257 · Geschäftsführer Maximilian Stein · USt-IdNr. DE 334940239 · Steuernummer 65 200 38818
Sparkasse Osnabrück · IBAN DE03 2655 0105 1552 3779 52 · BIC NOLADE22XXX

6. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b, c DS-GVO)

6.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten vor (zufälliger) Zerstörung und Verlust geschützt sind.

- **Rechenzentrumsinfrastruktur** – Unterbrechungsfreie Stromversorgung, Brandschutz, Klimatisierung und redundante Netzanbindung werden durch die Rechenzentrumsbetreiber sichergestellt und durch deren Zertifizierungen nachgewiesen.
- **Redundanter Betrieb** – Die Datenbank wird mit Instanzen in mehreren räumlich getrennten Verfügbarkeitszonen betrieben (AWS Frankfurt), der zentrale Dateispeicher der Plattform ist zonenredundant ausgelegt.
- **Datensicherung der Datenbank** – Die Datenbank wird fortlaufend gesichert und kann auf einen Zeitpunkt innerhalb des Aufbewahrungszeitraums von 30 Tagen wiederhergestellt werden (Point-in-Time-Recovery). Zusätzlich wird täglich eine Sicherung in einen gegen Löschung geschützten Sicherungstresor kopiert und dort 30 Tage aufbewahrt. Die Datenbank ist gegen versehentliches Löschen geschützt.
- **Datensicherung der Objektspeicher** – Die Dateien im zentralen Dateispeicher der Plattform sind versioniert und zonenredundant gespeichert. Gelöschte Dateien und Container können innerhalb von 30 Tagen wiederhergestellt werden; zusätzlich ist eine zeitpunktbezogene Wiederherstellung möglich. Eine Löschsperre verhindert das versehentliche Entfernen des Speicherkontos.
- **Schutz kryptografischer Schlüssel** – Die Schlüssel in Azure Key Vault sind gegen versehentliches und vorzeitiges Löschen geschützt. Schlüsselsicherungen werden getrennt abgelegt.
- **Löschung und Datensicherungen** – Gelöschte Daten werden nicht einzeln aus Sicherungen entfernt. Sie verbleiben dort bis zum Ablauf der jeweiligen Aufbewahrungsfrist der Sicherungen (Datenbank 30 Tage) und werden dann automatisch gelöscht. Bis dahin sind die Sicherungen verschlüsselt, nur für berechtigte Administratoren zugänglich und werden ausschließlich zur Wiederherstellung genutzt, nicht für die laufende Verarbeitung. Wiederherstellungen erfolgen in der Regel gezielt für einzelne Mandanten. Nach einer vollständigen Wiederherstellung werden zwischenzeitlich erfolgte Löschungen manuell erneut durchgeführt.
- **Überwachung der Sicherungen** – Fehlgeschlagene Sicherungen lösen automatisch einen Alarm aus.
- **Infrastructure as Code (IaC)** – Infrastruktur und Cluster-Konfiguration sind vollständig als Code beschrieben und können reproduzierbar wiederhergestellt werden.
- **Überwachung und Alarmierung** – Plattform und Anwendungen werden kontinuierlich überwacht (Anwendungstelemetrie, Fehlerraten, Latenz). Die Erreichbarkeit wird von mehreren

mint software GmbH · Carl-Fischer-Str. 2 · 49084 Osnabrück · www.schadensmeldung.digital · info@mmmint.ai · +49 541 96328784
Amtsgericht Osnabrück HRB 215257 · Geschäftsführer Maximilian Stein · USt-IdNr. DE 334940239 · Steuernummer 65 200 38818
Sparkasse Osnabrück · IBAN DE03 2655 0105 1552 3779 52 · BIC NOLADE22XXX

europäischen Standorten aus extern geprüft. Kritische Alarme werden automatisch an die zuständigen Techniker zugestellt.

- **Notfallplan** – Ein schriftliches Notfall- und Wiederherstellungskonzept legt Szenarien, Zuständigkeiten, Eskalationswege und Wiederherstellungsverfahren fest. Wiederherstellungen erfolgen nach Möglichkeit zunächst in einer isolierten Umgebung.
- **Wiederherstellungstests** – Die Wiederherstellung der Datenbank aus den Sicherungen wird monatlich automatisiert getestet. Zusätzlich findet jährlich ein Notfalltest statt. Ergebnisse und Folgemaßnahmen werden dokumentiert.
- **Microsoft 365** – Die Daten in Microsoft 365 werden von Microsoft georedundant gespeichert. Versionierung und Papierkorb ermöglichen die Wiederherstellung versehentlich gelöschter Inhalte.
- **Archivierung** – Geschäftsdokumente werden in Microsoft 365 archiviert. Archivierung und Datensicherung sind getrennte Verfahren.
- **Penetrationstests** – Externe Penetrationstests können nach gesonderter Vereinbarung mit dem Kunden durchgeführt werden.

7. Sichere Softwareentwicklung (Art. 25, Art. 32 DS-GVO)

7.1 Entwicklungs- und Freigabeprozess

Maßnahmen, die gewährleisten, dass Sicherheit und Datenschutz bereits bei der Entwicklung der Software berücksichtigt werden.

- **Versionskontrolle** – Der gesamte Quellcode wird in GitHub verwaltet. Der Zugriff ist rollenbasiert und personengebunden, Mehr-Faktor-Authentifizierung ist für alle Mitglieder verpflichtend.
- **Branch Protection** – Direkte Änderungen an den produktiven Branches sind technisch unterbunden; Administratoren können dies in dokumentierten Ausnahmefällen (z. B. Versionsfreigaben) umgehen. Änderungen werden über Pull Requests übernommen.
- **Code-Reviews und Vier-Augen-Prinzip** – Änderungen werden vor der Übernahme von mindestens einer weiteren Person geprüft und freigegeben. Ergänzend unterstützt ein KI-gestütztes Review; es ersetzt die menschliche Freigabe nicht.
- **Automatisierte Tests und Prüfungen** – Build und automatisierte Tests laufen bei Pull Requests in der Build-Pipeline.
- **Abhängigkeitsmanagement** – Bekannte Schwachstellen in Drittbibliotheken werden automatisiert erkannt und Aktualisierungen automatisch vorgeschlagen (GitHub Dependabot). Schwachstellen werden nach Schweregrad priorisiert und behoben.
- **Secret Scanning** – Jeder Push und jeder Pull Request wird auf versehentlich eingecheckte Zugangsdaten und Schlüssel geprüft (GitGuardian). Aufgedeckte Zugangsdaten werden unverzüglich widerrufen und erneuert.

mint software GmbH · Carl-Fischer-Str. 2 · 49084 Osnabrück · www.schadensmeldung.digital · info@mmmint.ai · +49 541 96328784
Amtsgericht Osnabrück HRB 215257 · Geschäftsführer Maximilian Stein · USt-IdNr. DE 334940239 · Steuernummer 65 200 38818
Sparkasse Osnabrück · IBAN DE03 2655 0105 1552 3779 52 · BIC NOLADE22XXX

- **Verwaltung von Zugangsdaten** – Produktive Zugangsdaten werden verschlüsselt verwaltet (u. a. SOPS, Azure Key Vault) und nicht im Klartext im Quellcode abgelegt.
- **Kontrollierte Deployments** – Der Produktivzustand wird automatisiert aus der Versionsverwaltung abgeglichen (GitOps). Produktiv-Releases sind den zugrunde liegenden Pull Requests zugeordnet.

8. Überprüfung, Bewertung, Evaluierung von Maßnahmen (Art. 32 Abs. 1 d DS-GVO)

8.1 Kontrollverfahren

Maßnahmen, die eine regelmäßige Überprüfung, Kontrolle und – sofern notwendig – Anpassung von Sicherungsmaßnahmen gewährleisten.

- **Regelmäßige Überprüfung der technisch-organisatorischen Maßnahmen** – mindestens jährlich sowie bei wesentlichen Änderungen der Systeme oder Prozesse.
- **Regelmäßige Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten (VVT)**
- **Regelmäßige Überprüfung von Datenverarbeitungsprozessen inkl. Dokumentation**
- **Betroffenenrechte** – Als Auftragsverarbeiter unterstützt die mint software GmbH den Auftraggeber bei der Beantwortung von Anfragen Betroffener (Art. 28 Abs. 3 lit. e DS-GVO) und leitet direkt eingehende Anfragen an ihn weiter. Bei gemeinsam verantworteten Verarbeitungen und eigenen Verarbeitungen bearbeitet die mint software GmbH Anfragen Betroffener selbst.
- **Prozess zum Umgang mit Sicherheits- und Datenschutzvorfällen** – Vorfälle werden nach einem festgelegten Verfahren erkannt, nach Schweregrad klassifiziert, eingedämmt, dokumentiert und nachbetrachtet. Als Auftragsverarbeiter meldet die mint software GmbH Verletzungen des Schutzes personenbezogener Daten dem Auftraggeber unverzüglich nach Bekanntwerden (Art. 33 Abs. 2 DS-GVO) und unterstützt ihn bei der Meldung an die Aufsichtsbehörde. Bei gemeinsam verantworteten und eigenen Verarbeitungen meldet die mint software GmbH meldepflichtige Verletzungen innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde (Art. 33 Abs. 1 DS-GVO) und informiert gemeinsam verantwortliche Kunden unverzüglich.
- **Einbeziehung des Datenschutzbeauftragten** – bei wesentlichen Änderungen oder der Einführung neuer Datenverarbeitungsverfahren.

9. Zertifizierungen und internationale Standards

Die mint software GmbH verfügt derzeit über keine eigenen Zertifizierungen. Die internen Sicherheitskonzepte orientieren sich an ISO/IEC 27001:2022. Die eingesetzten Infrastruktur- und Plattformanbieter (AWS, Microsoft) sind u. a. nach ISO/IEC 27001 zertifiziert und verfügen über SOC-2-Type-II-Berichte sowie BSI-C5-Testate. Die Nachweise sind über die Anbieter abrufbar.

mint software GmbH · Carl-Fischer-Str. 2 · 49084 Osnabrück · www.schadensmeldung.digital · info@mmmint.ai · +49 541 96328784
Amtsgericht Osnabrück HRB 215257 · Geschäftsführer Maximilian Stein · USt-IdNr. DE 334940239 · Steuernummer 65 200 38818
Sparkasse Osnabrück · IBAN DE03 2655 0105 1552 3779 52 · BIC NOLADE22XXX