Anlage 2 - Technische und organisatorische Maßnahmen

Stand: 04. September 2026

1. Allgemeine Grundsätze

1. Flatwise trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO.
2. Die Maßnahmen dienen insbesondere der Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der zur Verarbeitung von Auftragsdaten eingesetzten Systeme und Dienste sowie der Wiederherstellbarkeit und regelmäßigen Überprüfung des Schutzniveaus.
3. Die Maßnahmen werden entsprechend technischer Entwicklungen, geänderter Risiken und betrieblicher Anforderungen überprüft und erforderlichenfalls angepasst. Das insgesamt vereinbarte Schutzniveau darf dadurch nicht abgesenkt werden.

2. Zugriffs- und Berechtigungsmanagement

1. Zugriffe auf Auftragsdaten werden nach dem Grundsatz der Erforderlichkeit auf solche Personen beschränkt, die diese zur Erfüllung ihrer jeweiligen Aufgaben benötigen.
2. Erweiterte oder administrative Zugriffsrechte auf Produktivsysteme und Auftragsdaten werden auf einen begrenzten Personenkreis beschränkt und nur für betriebliche, technische, sicherheitsbezogene oder Supportzwecke eingeräumt.
3. Zugriffe im Rahmen von Support, Wartung oder Fehlerbehebung werden auf den für den jeweiligen Zweck erforderlichen Umfang beschränkt.
4. Nicht mehr benötigte Zugriffsberechtigungen sind zu entziehen; bei Änderungen von Aufgaben oder Verantwortlichkeiten sind Berechtigungen entsprechend anzupassen.
5. Mitarbeiter und sonstige berechtigte Personen mit Zugang zu Auftragsdaten sind zur Vertraulichkeit verpflichtet oder unterliegen einer entsprechenden gesetzlichen Verschwiegenheitspflicht.
6. Privilegierte Zugriffsberechtigungen werden dokumentiert und auf den hierfür erforderlichen Personenkreis beschränkt. Erteilung, Änderung und Entzug erfolgen anhand des jeweiligen Aufgaben- und Verantwortungsbereichs. Die Erforderlichkeit privilegierter Berechtigungen wird regelmäßig sowie anlassbezogen bei Änderungen von Aufgaben oder Verantwortlichkeiten überprüft.

3. Authentifizierung und Kontosicherheit

1. Der Zugang zur Flatwise-Anwendung erfolgt über individuelle Benutzerkonten und Authentifizierungsmechanismen.

2. Benutzerberechtigungen werden dem jeweiligen Konto und dessen Rolle beziehungsweise Berechtigungsumfang zugeordnet.
3. Für Endnutzer unterstützt Flatwise eine Mehrfaktor-Authentifizierung mittels TOTP. Einrichtung, Verifikation und Entfernung der Mehrfaktor-Authentifizierung sowie die technische Prüfung des erreichten Authentifizierungsniveaus sind in der Anwendung implementiert.
4. Privilegierte administrative Zugänge zu Infrastruktur-, Datenbank-, Hosting-, Entwicklungs- und sonstigen für den Produktivbetrieb maßgeblichen Systemen werden, soweit der jeweilige Dienst dies unterstützt, durch Mehrfaktor-Authentifizierung oder einen vergleichbaren zusätzlichen Authentifizierungsfaktor geschützt. Administrative Zugänge werden personenbezogen beziehungsweise nachvollziehbar zugeordnet und auf den erforderlichen Personenkreis beschränkt.

4. Mandantentrennung und Trennung technischer Umgebungen

1. Auftragsdaten unterschiedlicher Kunden werden innerhalb der Anwendung logisch voneinander getrennt. Zugriffe erfolgen innerhalb der jeweils vorgesehenen Benutzer-, Rollen-, Berechtigungs- und Eigentumsprüfungen.
2. Serverseitige Berechtigungs- und Eigentumsprüfungen verhindern, dass ein Nutzer allein durch Manipulation clientseitiger Anfragen auf Daten zugreift, für die keine Berechtigung besteht.
3. Für besonders schutzbedürftige Datenstrukturen werden, soweit vorgesehen, ergänzende datenbankseitige Zugriffsschutzmechanismen eingesetzt.
4. Entwicklungs-, Test- und Produktivumgebungen werden technisch als getrennte Umgebungen betrieben.
5. Produktivdaten werden außerhalb der eigentlichen Produktionsumgebung nur verarbeitet, soweit dies für einen konkret festgelegten technischen Zweck erforderlich ist, insbesondere für produktionsnahe Fehleranalyse, Release-Verifikation oder Wiederherstellungs- und Funktionsprüfungen.
6. Entwicklungs- und Testumgebungen, in denen ausnahmsweise Produktivdaten verarbeitet werden, werden technisch von der Produktionsumgebung getrennt betrieben. Der Zugriff ist auf den für den jeweiligen technischen Zweck erforderlichen privilegierten Personenkreis beschränkt. Eine Verwendung der Daten für fachliche Eigenzwecke, Schulungszwecke oder sonstige mit dem technischen Zweck unvereinbare Zwecke ist ausgeschlossen.
7. Solche Umgebungen werden nicht als dauerhaftes Parallelproduktivsystem verwendet. Insbesondere werden dort keine regulären neuen Kundenregistrierungen oder gewöhnlichen produktiven Geschäftsprozesse durchgeführt.
8. Eine aus Produktivdaten erzeugte Entwicklungs- oder Testkopie wird nach Wegfall des konkreten technischen Zwecks gelöscht beziehungsweise durch einen neuen kontrollierten Datenstand ersetzt, spätestens jedoch nach 30 Kalendertagen.

5. Verschlüsselung und Schutz von Zugangsdaten und Geheimnissen

1. Die Übertragung von Daten zwischen Client, Flatwise-Infrastruktur und angebundenen Diensten erfolgt über verschlüsselte Transportverbindungen nach dem jeweils eingesetzten Stand der Technik, insbesondere HTTPS/TLS.
2. Zugangsdaten, API-Schlüssel und sonstige technische Geheimnisse werden nicht als Bestandteil des ausgelieferten Clientcodes bereitgestellt, soweit sie für den serverseitigen Betrieb bestimmt sind.
3. Serverseitige Konfigurationswerte und Geheimnisse werden über hierfür vorgesehene Konfigurations- beziehungsweise Secret-Mechanismen verwaltet.
4. Datenbankmigrationen werden technisch darauf geprüft, dass definierte Secret-Muster nicht versehentlich in Migrationsdateien eingebracht werden.
5. Für produktiv eingesetzte Zugangsdaten, API-Schlüssel, Tokens und sonstige technische Geheimnisse bestehen dokumentierte Ablage-, Zugriffs- und Rotationsgrundsätze. Produktions- und Entwicklungsgeheimnisse werden soweit technisch möglich voneinander getrennt. Eine Rotation erfolgt insbesondere anlassbezogen bei Verdacht auf Offenlegung oder Kompromittierung, bei relevanten Berechtigungsänderungen sowie in sonstigen nach der jeweiligen Risikobewertung vorgesehenen Fällen.
6. Die primär über Supabase gespeicherten Datenbank- und Speicherobjektdaten werden nach Maßgabe der für Flatwise geltenden Anbieter- und Vertragsdokumentation verschlüsselt gespeichert. Für die dort eingesetzten Speichersysteme ist eine Verschlüsselung ruhender Daten insbesondere mittels AES-256 vorgesehen.

6. Hosting, Datenspeicherung, Datensicherung und Wiederherstellung

1. Die Flatwise-Anwendung wird auf von Hetzner betriebener Infrastruktur in Nürnberg, Deutschland, ausgeführt. Dort werden Auftragsdaten insbesondere während der Bearbeitung von Anfragen technisch verarbeitet.
2. Die primäre Speicherung von Datenbankdaten, Authentifizierungsdaten und in Flatwise gespeicherten Dokumenten erfolgt über Supabase. Das produktive Supabase-Projekt wird in der AWS-Region eu-north-1, Stockholm, Schweden, betrieben.
3. Die produktive PostgreSQL-Datenbank wird beim Datenbank-Dienstleister täglich gesichert.
4. Die Datenbanksicherungen werden rollierend für sieben Tage aufbewahrt und anschließend im regulären Sicherungszyklus überschrieben beziehungsweise entfernt.
5. Point-in-Time Recovery zwischen den jeweiligen Tagesständen ist derzeit nicht aktiviert und nicht Bestandteil des vereinbarten Sicherungskonzepts.
6. Die beschriebenen Datenbanksicherungen umfassen nicht die über den verwendeten Objektspeicher gespeicherten Dokumente und sonstigen Speicherobjekte. Für diese besteht derzeit kein gesondertes Backup, Versioning oder Point-in-Time-Restore. Die

technische Redundanz des produktiven Speichers ist von einem eigenständigen Backup zu unterscheiden.
7. Auf der von Hetzner betriebenen Infrastruktur bestehen derzeit keine gesonderten Hetzner-Backups von Auftragsdaten.
8. Die Wiederherstellbarkeit der bestehenden Datenbanksicherungen wird in angemessenen regelmäßigen Abständen sowie nach wesentlichen Änderungen des Sicherungs- oder Wiederherstellungsverfahrens praktisch überprüft. Die Ergebnisse werden dokumentiert. Ein bestimmtes RPO oder RTO wird nicht zugesichert.
9. Im Fall einer Wiederherstellung sind zwischenzeitlich wirksam gewordene Löschungen nach Maßgabe der vorgesehenen Löschprozesse erneut umzusetzen.

7. Protokollierung und technische Nachvollziehbarkeit

1. Flatwise setzt technische Protokollierung ein, soweit dies für Betrieb, Fehleranalyse, Sicherheit und Nachvollziehbarkeit erforderlich ist.
2. Serverprotokolle werden so gestaltet, dass unnötige Inhaltsdaten möglichst vermieden werden. Der allgemeine Request-Logger verarbeitet insbesondere keine POST-Request-Bodies und entfernt Query- beziehungsweise Fragmentbestandteile aus protokollierten Pfaden.
3. Anwendungsprotokolle können insbesondere Nutzerkennungen, Zeitpunkte, technische Pfade, aufgerufene Funktionen und für den Betrieb erforderliche technische Metadaten enthalten.
4. Allgemeine Anwendungsprotokolle werden derzeit grundsätzlich für 14 Tage, Fehlerprotokolle für 30 Tage vorgehalten und anschließend im Rahmen der vorgesehenen Rotation entfernt.
5. Für Fehlerdiagnose und technische Überwachung wird Sentry eingesetzt. Die Konfiguration ist darauf ausgerichtet, personenbezogene und fachliche Inhaltsdaten zu minimieren; die standardmäßige Übermittlung personenbezogener Identifikationsinformationen ist deaktiviert und sensible Inhalte werden soweit vorgesehen bereinigt beziehungsweise maskiert. Bei einem technischen Fehler kann ergänzend eine maskierte Aufzeichnung der unmittelbar vorausgehenden Bedienschritte verarbeitet werden. Texte und Eingaben werden dabei maskiert und Medieninhalte ausgeblendet. Eine gewöhnliche fortlaufende Sitzungsaufzeichnung wird nicht eingesetzt.
6. Protokolldaten werden nicht für mit dem jeweiligen Betriebs-, Sicherheits- oder Fehleranalysezweck unvereinbare Zwecke verwendet.

8. Verfügbarkeit, Monitoring und Wiederherstellung

1. Flatwise setzt technische und organisatorische Maßnahmen ein, um die Verfügbarkeit und Belastbarkeit der Anwendung entsprechend dem jeweiligen Risiko zu unterstützen.
2. Hierzu gehören insbesondere:
    a. Fehlerüberwachung auf Server- und Clientseite,
    b. technische Fehler- und Ereignisprotokollierung,
    c. Ratenbegrenzungen zum Schutz vor missbräuchlichen oder außergewöhnlichen Zugriffen,

    d. die in Abschnitt 6 beschriebenen Datenbanksicherungen sowie
    e. technische und manuelle Prüfungen des Systemzustands.
1. Flatwise trifft bei erkannten Störungen und Sicherheitsvorfällen angemessene Maßnahmen zur Eingrenzung, Fehleranalyse und Wiederherstellung.
2. Bestimmte Verfügbarkeitswerte, Wiederherstellungszeiten oder maximal zulässige Datenverlustzeiträume werden durch diese Anlage nicht zugesichert.

9. Sichere Softwareentwicklung und Änderungsmanagement

1. Änderungen an der Software und Datenbankstruktur erfolgen über kontrollierte Entwicklungs- und Bereitstellungsprozesse.
2. Im Entwicklungsprozess werden unter anderem automatisierte Linting-, Formatierungs- und Typprüfungen eingesetzt.
3. Für Datenbankmigrationen besteht eine dokumentierte, fortlaufende Migrationshistorie. Bereits angewendete Migrationen werden durch Hash-Prüfungen gegen nachträgliche unkontrollierte Änderungen geschützt.
4. Technische Prüfungen verhindern unter anderem definierte Secret-Muster in Datenbankmigrationen.
5. Datenbankänderungen werden über dokumentierte Release-Abläufe mit technischen Prüfungen und menschlicher Freigabe vor der Anwendung auf die jeweilige Zielumgebung durchgeführt.
6. In der CI werden technische Prüfungen und Smoke-Tests eingesetzt.
7. Sicherheitsrelevante Schwachstellen, Softwareabhängigkeiten und Herstellerhinweise werden im Rahmen des Entwicklungs- und Wartungsprozesses überprüft. Hierzu werden insbesondere Sicherheitsinformationen der eingesetzten Anbieter und Abhängigkeiten sowie technische Dependency-Prüfungen herangezogen. Festgestellte Schwachstellen werden nach Risiko, Ausnutzbarkeit und Bedeutung für die eingesetzten Systeme bewertet und entsprechend priorisiert behandelt.
8. Für intern eingesetzte KI- und Entwicklungswerkzeuge bestehen Vorgaben zur Begrenzung von Produktivzugriffen und zur Vermeidung unkontrollierter Änderungen an Produktivsystemen.

10. Schutz von Datei-Uploads und Eingaben

1. Datei-Uploads werden technisch auf zulässige Formate und Größen beschränkt.
2. Für Uploads besteht derzeit ein technisches Größenlimit von 50 MB.
3. Neben einer Prüfung des angegebenen MIME-Typs erfolgt serverseitig eine Prüfung charakteristischer Dateiinhalte beziehungsweise Dateisignaturen („Magic Bytes“), um Abweichungen zwischen deklariertem und tatsächlichem Dateityp zu erkennen.
4. Technische Eingaben werden serverseitig validiert, soweit dies für die jeweilige Funktion und den Schutz der Anwendung erforderlich ist.
5. Ratenbegrenzungen und weitere technische Schutzmechanismen dienen der Begrenzung missbräuchlicher oder außergewöhnlicher Nutzung.

11. Datenschutzvorfälle

1. Sicherheits- und Datenschutzvorfälle werden nach ihrer Erkennung untersucht und entsprechend Art und Schwere des Vorfalls behandelt.
2. Flatwise trifft angemessene Maßnahmen zur Eindämmung erkannter Vorfälle, zur Untersuchung ihrer Ursache und zur Verringerung des Risikos einer Wiederholung.
3. Verletzungen des Schutzes personenbezogener Daten, die Auftragsdaten betreffen, werden nach Maßgabe des § 9 AVV behandelt und dokumentiert.
4. Zugriffe und erforderliche technische Maßnahmen im Rahmen der Incident-Behandlung werden auf den jeweils erforderlichen Umfang beschränkt.

12. Datenminimierung, Löschung und Aufbewahrung

1. Flatwise ist darauf ausgerichtet, technische Verarbeitungen und Protokollierungen auf die für die jeweilige Funktion, Sicherheit und Fehleranalyse erforderlichen Daten zu beschränken.
2. Auftragsdaten werden nach Maßgabe der vertraglichen Funktionen, der Weisungen des Kunden und der in § 10 AVV beschriebenen Rückgabe- und Löschregeln gelöscht.
3. Temporäre technische Verarbeitungen werden entsprechend ihrer Funktion möglichst kurz vorgehalten.
4. Für Auftragsdaten in Entwicklungs- und Testumgebungen gelten ergänzend die in Abschnitt 4 festgelegten Zweckbindungs- und Löschfristen.
5. Für die derzeitige Walter-Verarbeitung gelten ergänzend die besonderen Regelungen des Abschnitts 13.
6. Gesetzlich erforderliche oder in eigener Verantwortlichkeit von Flatwise verarbeitete Vertrags-, Abrechnungs-, Sicherheits- und Nachweisdaten werden von den Auftragsdaten getrennt nach den hierfür geltenden Speicher- und Löschregeln behandelt.

13. Besondere Schutzmaßnahmen für den KI-Assistenten Walter

1. Walter greift nicht unmittelbar und uneingeschränkt auf die Datenbank zu. Datenzugriffe erfolgen über serverseitig definierte Funktionen.
2. Der verfügbare Toolzugriff wird durch ein serverseitiges Register, die jeweiligen Produkteinstellungen, Benutzerberechtigungen und die technische Umgebung begrenzt.
3. Für jeden Datenabruf gelten die Berechtigungs- und Eigentumsprüfungen des jeweils eingeloggten Nutzers.
4. Walter besitzt im Go-live-Umfang keinen Toolzugriff auf Dokumente oder Dateien, Bankverbindungen oder Kontotransaktionen.
5. Schreibende Änderungen werden nicht autonom durch das Sprachmodell ausgeführt. Ein von Walter vorbereiteter Kalendereintrag muss über den hierfür vorgesehenen gesonderten Freigabemechanismus ausdrücklich bestätigt werden.

6. Walter trifft keine eigenständigen automatisierten Entscheidungen mit rechtlicher oder vergleichbar erheblicher Wirkung über natürliche Personen.
7. Der Gesprächskontext wird von Flatwise nicht als dauerhafter Chatverlauf gespeichert. Im Browser wird er nur temporär bis insbesondere zum Neuladen, Abmelden, Nutzerwechsel oder Beginn eines neuen Chats vorgehalten. Serverseitig besteht der zusammengesetzte Prompt nur für die Dauer des jeweiligen Verarbeitungsvorgangs, derzeit höchstens etwa 45 Sekunden.
8. Aufrufe an Azure OpenAI erfolgen mit deaktivierter anwendungsseitiger Gesprächsspeicherung (store: false).
9. Die für Walter verwendete Azure-Ressource befindet sich in Sweden Central (Schweden). Das eingesetzte Modelldeployment wird als Data Zone Standard innerhalb der EU Data Zone betrieben. Die Modellverarbeitung kann nach Maßgabe der Microsoft-Produktkonfiguration innerhalb dieser EU Data Zone auch in anderen EU-Regionen stattfinden. Das für Walter vorgesehene Deployment ist gpt-5.6-luna.
10. Für das Modelldeployment ist die reguläre Missbrauchs- und Sicherheitsüberwachung von Microsoft aktiviert. Diese ist von der anwendungsseitigen Einstellung store:false zu unterscheiden. Soweit in besonderen Fällen eine menschliche Prüfung entsprechend gekennzeichneter Inhalte erforderlich wird, erfolgt diese nach den für EWR-Bereitstellungen geltenden Microsoft-Regelungen durch hierfür autorisierte Prüfer im EWR.
11. Walter begrenzt die Zahl aufeinanderfolgender Toolaufrufe und unterliegt technischen Zeit- und Ratenbegrenzungen.
12. Technische Walter-Protokolle enthalten keine beabsichtigte Speicherung des Chatverlaufs, der vollständigen Prompts oder Antworten. Die allgemeinen Protokollfristen gemäß Abschnitt 7 bleiben unberührt.