Technische und organisatorische Maßnahmen

(Art. 32 DSGVO)

Die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen gelten für die Produktumgebung von Dronesolut. Berücksichtigt werden insbesondere die Verarbeitung von Nutzer- und Planungsdaten in der Web-/Mobile-App, die Speicherung von Drohnentelemetriedaten über einen separaten Microservice mit Datenhaltung in Supabase sowie optionale Zusatzfunktionen wie die KI-gestützte Dokumentenauslese (für z.B. Genehmigungen). Die aktuelle Liste der eingesetzten Auftragsverarbeiter und Unterauftragsverarbeiter wird in einer separaten Anlage geführt.

1. Pseudonymisierung und Verschlüsselung personenbezogener Daten

- Data Masking von Authentifizierungsdaten und Verarbeitung von Zugangsdaten ausschließlich in technisch geschützter Form.
- Verschlüsselung gespeicherter Daten auf den eingesetzten Plattformen und Infrastrukturen, soweit dies vom jeweiligen Dienst bereitgestellt wird.
- Datentransfers ausschließlich über verschlüsselte Verbindungen nach dem Stand der Technik, insbesondere TLS.
- Verschlüsselte API-Kommunikation zwischen Web/Mobile-App, Telemetrie-Microservice und Supabase-Datenbank.
- Datenminimierung bei optionalen Funktionen; im Rahmen der KI-Auslese werden nur aktiv freigegebene Dokumente verarbeitet.

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zugangs- und Zutrittskontrolle

- Administrative Zugriffe auf Produkt- und Systemumgebungen sind auf berechtigte Personen beschränkt.
- Endgeräte mit administrativem Zugriff sind passwortgeschützt und gegen unbefugten Zugriff zu sichern.
- Die physische Sicherheit der Rechenzentren (AWS, Supabase) wird durch die jeweils eingesetzten Infrastruktur- und Plattformdienstleister gewährleistet.

Speicher- und Zugriffskontrolle

- Es besteht ein Berechtigungskonzept zur Verwaltung von Benutzerrechten.
- Unterschiedliche Zugriffsberechtigungen gelten für Lesen, Schreiben und Löschen von Daten.
- Die Anzahl administrativer Berechtigungen wird auf das notwendige Maß reduziert.
- Planungsdaten, Telemetriedaten und optionale Dokumentenverarbeitung werden systemseitig getrennt verarbeitet.
- Produktiv-, Test- und Entwicklungsumgebungen sind organisatorisch und technisch voneinander zu trennen, soweit solche Umgebungen vorhanden sind.

Benutzerkontrolle

- Personen mit Zugriff auf personenbezogene Daten werden auf Vertraulichkeit verpflichtet.
- Mitarbeitende und berechtigte Personen werden zu Datenschutz- und Informationssicherheitsanforderungen sensibilisiert.

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Datenintegrität
- Regelmäßige Software- und Sicherheitsupdates der eingesetzten Systeme und Komponenten.
- Absicherung von Anwendungen, Schnittstellen und Infrastrukturen durch geeignete Netzwerk- und Zugriffsschutzmaßnahmen.
- Protokollierung und Überwachung sicherheitsrelevanter Ereignisse, soweit technisch vorgesehen und erforderlich.

Weitergabekontrolle

- Soweit Daten über das Internet oder interne Schnittstellen übertragen werden, erfolgt dies verschlüsselt.
- Die Web-/Mobile-App greift auf Telemetriedaten ausschließlich über definierte APIs und anhand einer Missions- oder Referenz-ID zu.
- Eine Übermittlung an weitere Dienstleister erfolgt nur auf dokumentierter Grundlage und im erforderlichen Umfang.

Auftragskontrolle

- Auswahl der Auftragnehmer unter Sorgfaltsgesichtspunkten, insbesondere im Hinblick auf Datenschutz und Informationssicherheit.
- Klare vertragliche Regelungen zum Umfang der Verarbeitung personenbezogener Daten.
- Prüfung neuer Dienstleister vor Aufnahme der Verarbeitung; bestehende Dienstleister werden über die separate Liste der eingesetzten Auftragsverarbeiter und Unterauftragsverarbeiter dokumentiert.
- Soweit eine Datenverarbeitung im Auftrag durchgeführt wird, werden mit den eingesetzten Dienstleistern entsprechende Verträge nach Art. 28 DSGVO oder funktional gleichwertige Datenschutzvereinbarungen geschlossen.

4. Verfügbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Die Verfügbarkeit der Produktumgebung richtet sich nach den jeweils eingesetzten Cloud-, Plattform- und Datenbankdiensten.
- Für Planungsdaten in der Web-/Mobile-App und für Telemetriedaten in der separaten Datenbank sind angemessene Backup-, Restore- und Wiederherstellungsmechanismen vorzuhalten, soweit diese durch die eingesetzten Dienste bereitgestellt werden.
- Die Telemetrie-Verarbeitung über MQTT, Microservice, Datenbank und API ist so auszugestalten, dass Datenverluste, unberechtigte Zugriffe und längere Ausfälle möglichst vermieden werden.
- Die getroffenen Maßnahmen werden regelmäßig auf Aktualität, Angemessenheit und Wirksamkeit überprüft und bei wesentlichen Änderungen an Architektur, Dienstleistern oder Produktfunktionen fortgeschrieben.