Informationsblatt zu IT-Sicherheit und Datenschutz

für eine TASKO-Softwareinstallation (Cloud/SaaS)

1. Zweck, Geltung und Verhältnis zu AVV

- Dieses Informationsblatt stellt die wichtigsten technischen und organisatorischen Maßnahmen, Service-Standards sowie Datenschutz-Vorkehrungen im Zusammenhang mit dem cloudbasierten Betrieb der TASKO-Software durch die Donau Data Engineering GmbH dar. Es dient als Orientierung und Nachweis der Einhaltung aktueller Standards (u. a. DSGVO, NIS2, BSI).
- Neben einem separaten Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO wird zudem ein OnService-Vertrag geschlossen, der die Service- und Supportleistungen, den Cloud-Betrieb sowie weitere technische Rahmenbedingungen regelt. Der Anbieter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden.
  Die jeweils aktuellen Anlagen zum AVV (u. a. zu TOM, Subunternehmern, Weisungsbefugten) können unter https://tasko.info/download-center eingesehen und heruntergeladen werden.

2. Cloud-Betrieb und Hosting

- Die TASKO-Software wird ausschließlich in deutschen, ISO/IEC 27001-zertifizierten Rechenzentren der Hetzner Online GmbH betrieben.
- Die Bereitstellung erfolgt als Private Cloud gemäß Definition nach NIST SP 800-145 und gemäß BSI-Empfehlung:
  - Die Cloud-Infrastruktur ist exklusiv für den jeweiligen Kunden und dessen autorisierte Nutzer bestimmt.
  - Es findet eine vollständige Kundentrennung auf technischer und organisatorischer Ebene statt; ein Zugriff Dritter ist ausgeschlossen.
  - Die Anwendungsumgebung ist nicht öffentlich zugänglich und keine geteilte Nutzung mit anderen Organisationen möglich.
  - Die Verarbeitung und Speicherung personenbezogener Daten findet ausschließlich in der Private Cloud-Infrastruktur in Deutschland statt – eine Übermittlung in Drittstaaten ist ausgeschlossen, außer bei ausdrücklicher Zustimmung des Kunden und unter Einhaltung der DSGVO-Vorgaben.

3. Technische und organisatorische Maßnahmen (TOM)

- Transportverschlüsselung TLS 1.2/1.3; Verschlüsselung ruhender Daten (AES-256).
- Granulares Identity- & Access-Management mit Rollenrechten und verpflichtender Multi-Faktor-Authentifizierung (MFA).
- Kontinuierliches Security-Monitoring und revisionssichere Protokollierung sicherheitsrelevanter Vorgänge; zeitnahes Patch-Management; regelmäßige Sicherheits- und Penetrationstests durch externe Dienstleister.

- Ergänzend: Maßnahmen zu Zutritts-/Zugangs-/Zugriffskontrolle, Trennungskontrolle, Protokollierung, Malware-Schutz, Firewalls und Verfügbarkeitskontrolle gemäß dokumentierten TOM.

4. Service Level und Support

- Verfügbarkeit: mindestens 99,7 % pro Jahr; geplante Wartungsfenster sind ausgenommen.
- Support-Servicezeiten: werktags 08:00–17:00 Uhr; Reaktionszeiten laufen innerhalb der Servicezeiten.
    - S1 (kritisch): Reaktion innerhalb von 2 Stunden
    - S2 (hoch): Reaktion innerhalb von 4 Stunden
    - S3 (mittel): Reaktion innerhalb eines Werktages
    - S4 (niedrig): Reaktion innerhalb von 5 Werktagen
- Geplante Wartungen werden mindestens drei Werktage im Voraus angekündigt; Notfallwartungen können kurzfristig erfolgen.

5. Backups, Aufbewahrung und Wiederherstellbarkeit

- Tägliche Backups mit einer Aufbewahrungsfrist von mindestens 30 Tagen.
- Backups auf separatem Server in ISO/IEC-27001-Rechenzentrum der Hetzner Online GmbH in Deutschland; Übertragung und Ablage verschlüsselt (TLS/AES-256).
- Regelmäßige Wiederherstellungstests zur Überprüfung der Restore-Fähigkeit.

6. Sicherheitsvorfälle (Incident-Management)

- Der Anbieter informiert den Kunden unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung, über sicherheitsrelevante Vorfälle, inkl. Art/Umfang, betroffene Komponenten/Daten, Sofortmaßnahmen und geplante Abhilfe.
- Die Meldung umfasst insbesondere eine Beschreibung der Art des Vorfalls (mit Kategorien/ungefährer Zahl betroffener Personen/Datensätze, soweit möglich) sowie ergriffene/geplante Maßnahmen zur Behebung und Abmilderung.

7. Prüfrechte (Audit) des Kunden

- Der Kunde ist berechtigt, die Einhaltung der datenschutzrechtlichen und vertraglichen Vorgaben zu kontrollieren, u. a. durch Einsicht in Dokumentationen, Zertifikate, Prüfberichte und durch Remote- oder Vor-Ort-Audits nach vorheriger Ankündigung.
- Der Anbieter unterstützt die Durchführung von Kontrollen und stellt erforderliche Informationen/Nachweise zur Verfügung.
- Das Informationssicherheitsmanagement orientiert sich zusätzlich an einschlägigen EU-Vorgaben (u. a. NIS2-Richtlinie), sowie Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI; IT-Grundschutz).

8. Datenschutzrechtliche Grundsätze und Unterstützung

- Verarbeitung ausschließlich auf dokumentierte Weisungen des Kunden.
- Datenübermittlung in Drittländer nur unter den Voraussetzungen der Art. 44–49 DSGVO; ggf. mit vorheriger Zustimmung des Kunden.
- Unterstützung des Kunden bei Pflichten nach Art. 32–36 DSGVO (Technische/organisatorische Maßnahmen, Meldungen, DSFA, vorherige Konsultation) gemäß vereinbarten Unterstützungsleistungen.
- Home-Office-Verarbeitung nur unter Einhaltung der vereinbarten TOM; insbesondere keine unverschlüsselte lokale Speicherung und Sicherstellung angemessener Zugriffsschutzmaßnahmen.

9. Datenrückgabe, Löschung, Exit und Zurückbehaltungsrecht

- Nach Vertragsende: Rückgabe oder Löschung der personenbezogenen Daten binnen 30 Kalendertagen; Rückgabe in strukturiertem, maschinenlesbarem Format; abweichender erheblicher Mehraufwand kann gesondert vergütet werden.
- Kein Zurückbehaltungsrecht an personenbezogenen Daten, soweit dies zur Erfüllung gesetzlicher/vertraglicher Pflichten des Kunden erforderlich ist.

10. Mitwirkungspflichten des Kunden

- Der Kunde unterstützt den Anbieter angemessen, u. a. durch rechtzeitige Störungsmeldungen, Bereitstellung erforderlicher Informationen/Unterlagen, Beachtung von Sicherheitshinweisen und aktive Mitwirkung bei Behebungsmaßnahmen/Tests.

11. Orientierung an NIS2 und BSI-Empfehlungen

- Der Anbieter betreibt Informationssicherheit nach dem Stand der Technik und richtet sein Sicherheits- und Compliance-Vorgehen an einschlägigen EU-Vorgaben (u. a. NIS2) sowie BSI-Empfehlungen (z. B. IT-Grundschutz) aus, soweit auf die Leistungen anwendbar.

Oldenburg, den 19. Dezember 2025
Ort, Datum

- Geschäftsführer Donau Data Engineering GmbH -