

# ANLAGE 2

## TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

zum AVV gemäß Art. 28 Abs. 3 lit. b und lit. c sowie Art. 32 DSGVO

### 1. Ziel, Geltungsbereich, Aktualisierung

1.1 Diese TOM gewährleisten ein dem Risiko angemessenes Schutzniveau unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung (Art. 32 DSGVO).

1.2 Die TOM gelten für alle Leistungen von WISNOTS im Rahmen der Auftragsverarbeitung, insbesondere Entgegennahme und Aufbereitung von Vorgangsdaten, Einreichung bei zuständigen Stellen, Bearbeitung von Rückfragen sowie Speicherung und Bereitstellung des Vorgangsstatus.

1.3 WISNOTS darf TOM weiterentwickeln, sofern das Schutzniveau nicht unterschritten wird. Eine Überprüfung erfolgt mindestens jährlich sowie anlassbezogen.

### 2. Zugriffskontrolle und Authentifizierung

#### 2.1 Rollen- und Berechtigungskonzept

- Rollenbasierte Zugriffskontrolle (RBAC)
- Least-Privilege- und Need-to-Know-Prinzip
- Trennung von Aufgaben für privilegierte Tätigkeiten, soweit organisatorisch sinnvoll
- Mandantentrennung: Vorgangsdaten verschiedener Verantwortlicher sind logisch getrennt; ein Zugriff über Mandantengrenzen hinweg ist ausgeschlossen

#### 2.2 Authentifizierung

- Multifaktor-Authentifizierung für administrative und privilegierte Zugänge
- Sicherer Passwort- und Credential-Umgang
- Authentifizierung der Nutzer des Verantwortlichen über Einmalcode an die hinterlegte E-Mail-Adresse

#### 2.3 Administrative Zugriffe und Netzwerk

- Zugriff auf administrative Systeme ausschließlich über gesicherte Kanäle
- Segmentierung sensibler Administrationsschnittstellen

#### 2.4 Joiner/Mover/Leaver

- Geregelter Prozess zur Vergabe, Änderung und Entziehung von Zugriffsrechten
- Zeitnahe Sperrung bei Offboarding oder Rollenwechsel

### 3. Umgang mit Zugangsdaten zu Portalen Dritter

3.1 Zugangsdaten des Verantwortlichen zu Installateurverzeichnissen und Portalen von Netzbetreibern werden in einem dedizierten Secret Store verschlüsselt gespeichert und nie im Klartext abgelegt oder protokolliert.

3.2 Der Zugriff ist auf autorisierte Personen beschränkt, erfolgt ausschließlich zur Bearbeitung konkreter Vorgänge und wird protokolliert.

3.3 Der Verantwortliche kann Zugangsdaten jederzeit selbst ändern oder deren Löschung verlangen. Die Löschung erfolgt unverzüglich.

3.4 Zugangsdaten werden nicht an Dritte weitergegeben und nicht in Backups außerhalb des Secret Stores gespeichert.

#### **4. Besonders schutzbedürftige Datenfelder**

4.1 Felder mit erhöhtem Schutzbedarf, insbesondere Bankverbindung, Geburtsdatum und Steuer-Identifikationsnummer, werden nur erfasst, soweit die zuständige Stelle sie verlangt.

4.2 Der Zugriff auf diese Felder ist auf den zur Vorgangsbearbeitung erforderlichen Personenkreis beschränkt und wird gesondert protokolliert.

#### **5. Protokollierung, Nachvollziehbarkeit, Monitoring**

##### **5.1 Logging**

- Protokollierung sicherheitsrelevanter Ereignisse (Authentifizierung, Administrationsaktionen, Zugriffe auf Vorgangsdaten, kritische Systemereignisse)
- Manipulationsschutz der Logs, soweit technisch und organisatorisch möglich

##### **5.2 Aufbewahrung von Logs**

- Aufbewahrung nur solange erforderlich für Sicherheits- und Nachweiszwecke
- Richtwert: in der Regel bis zu 12 Monate; Anpassung nach Risikolage, gesetzlichen Vorgaben oder Weisung des Verantwortlichen

5.3 Monitoring: Zentrales Monitoring und Alerting zur Erkennung von Anomalien und sicherheitsrelevanten Ereignissen

#### **6. Verschlüsselung und Schlüsselmanagement**

6.1 Übertragung: Transportverschlüsselung nach Stand der Technik (TLS 1.3, mindestens TLS 1.2)

6.2 Ruhende Daten: Verschlüsselung nach Stand der Technik (AES-256 oder gleichwertig)

##### **6.3 Schlüsselmanagement**

- Schlüsselverwaltung über geeignete Mechanismen (KMS oder gleichwertig)
- Zugriff auf Schlüsselmaterial streng beschränkt und protokolliert
- Schlüsselrotation regelmäßig und anlassbezogen, Richtwert mindestens jährlich sowie bei Sicherheitsvorfällen

6.4 Datenminimierung: Es werden nur die Daten erhoben und gespeichert, die für die Einreichung bei der jeweils zuständigen Stelle erforderlich sind.

#### **7. Backup, Wiederherstellung, Verfügbarkeit**

##### **7.1 Backups**

- Regelmäßige Backups nach Backup-Konzept, Richtwert täglich
- Schutz gegen unbefugte Veränderung, soweit verfügbar
- Speicherung ausschließlich innerhalb der Europäischen Union (Convex, AWS eu-west-1, Irland)

7.2 Wiederherstellung: Richtwert RTO 24 Stunden, RPO 24 Stunden

7.3 Restore-Tests: Wiederherstellbarkeit wird in angemessenen Intervallen getestet, Richtwert mindestens jährlich sowie anlassbezogen

## **8. Schwachstellenmanagement und sichere Entwicklung**

### **8.1 Vulnerability-Management**

- Regelmäßige Schwachstellenanalysen, mindestens jährlich, risikobasiert häufiger
- Priorisierte Behebung kritischer Findings innerhalb angemessener Fristen

### **8.2 Patch- und Update-Management: Sicherheitsupdates werden risikobasiert und zeitnah eingespielt**

### **8.3 Secure Development**

- Code-Reviews nach Vier-Augen-Prinzip, soweit praktikabel
- Secrets-Management: keine Zugangsdaten oder Schlüssel im Code
- Trennung von Entwicklungs-, Test- und Produktivumgebungen
- In Test- und Entwicklungsumgebungen werden keine produktiven personenbezogenen Daten verwendet

## **9. Incident Response**

### **9.1 Dokumentierter Prozess inklusive Rollen und Verantwortlichkeiten (Erkennung, Eindämmung, Behebung, Nachbereitung)**

### **9.2 Bearbeitung sicherheitsrelevanter Vorfälle unverzüglich nach Bekanntwerden. Meldung von Verletzungen des Schutzes personenbezogener Daten an den Verantwortlichen gemäß AVV, Richtwert innerhalb von 48 Stunden nach Kenntniserlangung**

### **9.3 Ursachenanalyse und Maßnahmenplan, Richtwert innerhalb von 30 Tagen**

## **10. Personal und Organisation**

### **10.1 Personen mit Zugriff auf personenbezogene Daten sind zur Vertraulichkeit verpflichtet**

### **10.2 Regelmäßige Datenschutz- und Security-Schulungen, Richtwert jährlich**

### **10.3 Regelmäßige Überprüfung privilegierter Berechtigungen und zeitnahe Entziehung nicht mehr erforderlicher Rechte**

## **11. Unterauftragsverarbeiter**

- Einsatz nur nach Maßgabe des AVV
- Vertragliche Verpflichtung auf gleichwertige Datenschutzpflichten gemäß Art. 28 Abs. 4 DSGVO
- Drittlandbezug nur unter Einhaltung der Art. 44 ff. DSGVO
- Aktueller Stand siehe Anlage 3

## **12. Löschung und Rückgabe**

- Rückgabe oder Löschung personenbezogener Daten nach Beendigung gemäß AVV
- Löschung nach Stand der Technik (sichere Löschung, kryptographische Löschung, Schlüsselvernichtung)
- Backups: Löschung im Rahmen des rollierenden Backup-Konzepts; bis dahin keine produktive Nutzung, Zugriff strikt beschränkt

## **13. KI-Verarbeitung**

- Nutzung ausschließlich des EU-Endpunkts von Requesty in Frankfurt am Main; eine Umleitung auf andere Endpunkte ist technisch ausgeschlossen

- Nutzung ausschließlich freigegebener Modellbereitstellungen in EU-Regionen; Anfragen an nicht freigegebene Modelle werden vom Endpunkt abgewiesen, ohne Ausweichen auf andere Modelle
- keine Protokollierung oder Zwischenspeicherung von Anfrageinhalten bei Requesty (Zero Data Retention)
- keine Verwendung von Vorgangsdaten zum Training von KI-Modellen
- Protokollierung des je Verarbeitungsschritt verwendeten Modells im Vorgang

Berlin, 28.09.2026

WISNOTS GmbH