DIGITALKEYCODE

## Anlage 1 zum Vertrag über Auftragsverarbeitung für digitalkeycode.com

Darstellung der bei der Makrolog AG gemäß Art. 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen (Stand 26.07.2021):

### Zutrittskontrolle

**Anforderung:**

Die Zutrittskontrolle verlangt, Unbefugten den körperlichen Zutritt zur Datenverarbeitungsanlage, mit der personenbezogene Daten verarbeitet werden, zu verwehren. Es soll verhindert werden, dass Personen, die dazu nicht befugt sind, unkontrolliert in die Nähe von Datenverarbeitungsanlagen kommen.

Realisierte Maßnahmen:

- Das Rechenzentrum des beauftragten Hosting-Providers (Amazon Web Services am Standort Frankfurt) ist nach dem Cloud Computing Compliance Controls Catalogue, C5 des BSI sowie nach ISO/IEC 27018:2019 zertifiziert und erfüllt damit die Anforderung.

### Zugangskontrolle

**Anforderung:**

Im Gegensatz zur Zutrittskontrolle ist hiermit der Schutz vor einem Eindringen unbefugter Personen in das EDV-System selbst, also dessen Benutzung, beabsichtigt. Es müssen daher Maßnahmen getroffen werden, die das unberechtigte Eindringen in die EDV-Systeme verhindern.

Realisierte Maßnahmen:

- Richtlinien zur sicheren Wahl und dem ordnungsgemäßen Umgang mit Passwörtern
- Zugriff auf Serversysteme mit persönlicher Schlüsseldatei über eine verschlüsselte Verbindung mittels SSH (Secure Shell) für alle Benutzer
- Zusätzliche Passwortverschlüsselung der persönlichen Schlüsseldatei
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern

### Zugriffskontrolle

**Anforderung:**

Maßnahmen der Zugriffskontrolle müssen geeignet sein, zu gewährleisten, dass ausschließlich die zur Benutzung des Systems berechtigten Personen auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

**Realisierte Maßnahmen:**

- Trennung von Berechtigungsbewilligung (organisatorisch) durch Geschäftsleitung von technischer Ausführung durch Administratoren
- Schlüssel sind eindeutig autorisierten Benutzern zugeordnet (siehe auch Zugangskontrolle SSH)
- Produktspezifische Steuerung mit welchen Schlüsseln auf die Serversysteme zugegriffen werden darf
- Nur der Besitzer einer Anwesenheitsliste kann auf die von ihm erfassten personenbezogenen Daten zugreifen. Die Authentifizierung erfolgt über die Telefonnummer mit einem per SMS zugesandten PIN-Code.

## Weitergabekontrolle

**Anforderung:**

Maßnahmen zur Weitergabekontrolle müssen geeignet sein, um sicherzustellen, das personenbezogene Daten bei der Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Realisierte Maßnahmen:

- Genereller Einsatz von HTTPS oder sonstiger geeigneter Verschlüsselung bei Übertragung
- Der Zugriff auf personenbezogene Daten erfolgt nur nach Authentifizierung (siehe auch Zugriffskonstrolle)
- Der Zugriff auf das interne Netzwerk des Auftragnehmers erfolgt grundsätzlich über verschlüsselte VPN-Verbindungen

## Eingabekontrolle:

**Anforderung:**

Die Maßnahmen zur Eingabekontrolle müssen gewährleisten, dass alle sicherheitsrelevanten Abläufe und alle Vorgänge, die personenbezogene Daten betreffen, durch das System protokolliert (geloggt) werden.

**Realisierung:**

- Die Datenerfassung erfolgt durch die Personen selbst, die die personenbezogenen Daten zur Verfügung stellen.

- Die Protokollierung erfolgt implizit durch Abspeichern in der jeweiligen Anwesenheitsliste, d.h. Speicherung und Protokollierung sind ein und derselbe Vorgang.

**Auftragskonktrolle:**

**Anforderung:**

Die Auftragskontrolle verpflichtet den Auftragsverarbeiter, den Auftrag, bei dem personenbezogenen Daten verarbeitet oder genutzt werden, gemäß den Vorschriften des Datenschutzes und den Vorgaben des Auftraggebers abzuwickeln und dem Auftraggeber als verantwortliche Stelle Kontrollen vor Ort zu ermöglichen. Maßnahmen zur Auftragskontrolle müssen sicherstellen, dass die überlassenen Daten nur im Rahmen des Auftrages verarbeitet werden können.

**Realisierung:**

- Verpflichtung aller Mitarbeiter auf die Einhaltung der Regeln in Bezug auf Daten-, Fernmelde- und Geschäftsgeheimnis
- Belehrung / Unterweisung der Mitarbeiter in Bezug auf die relevanten datenschutzrechtlichen Regelungen
- Prüfung und Sicherstellung der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit durch Einsatz von BSI/ISO-zertifizierten Hosting-Dienstleistern

**Verfügbarkeitskontrolle:**

**Anforderung:**

Maßnahmen zur Verfügbarkeitskontrolle müssen sicherstellen, dass personenbezogene Daten nicht unbeabsichtigt zerstört werden oder „verloren“ gehen.

**Realisierung:**

- Einsatz von virtuellen Plattformen
- Nutzung redundanter Infrastrukturen beim Hosting-Provider
- Monitoring aller Systeme zur Erkennung von Störungen
- Regelmäßige Backups (mindestens alle 24h)

**Trennungskontrolle:**

**Anforderung:**

Maßnahmen der Trennungskontrolle müssen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können. Eine Trennung darf nicht nur auf einem System oder nur auf dem Hauptsystem realisiert sein, sondern muss für die davon betroffenen Verfahren insgesamt durchgängig umgesetzt sein.

**Realisierung:**

- Trennung von Entwicklungs- und Produktivsystemen durch unterschiedliche virtuelle Maschinen.
- Speicherung der digitalkeycode-Daten in speziell gesicherten exclusiv für digitalkeycode genutzten virtuellen Maschinen.