Anlage gemäß Art. 28 DS-GVO:
Technische und Organisatorische Maßnahmen
nach Art. 32 DS-GVO

nach Artikel 32 Datenschutz-Grundverordnung (DS-GVO)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen hat die Henke Informatik GmbH (Auftragnehmerin) die folgenden technischen und organisatorischen Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Henke Informatik GmbH verarbeitet personenbezogene Daten an mehreren Standorten in Deutschland. Abhängig vom konkreten Auftragsinhalt findet die Verarbeitung nicht immer an allen Standorten statt.

Unterschiedliche Maßnahmen werden im Folgenden getrennt aufgelistet. Soweit die bei der Auftragnehmerin getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Die Maßnahmen bei der Auftragnehmerin können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

1. Vertraulichkeit

(ART. 32 ABS. 1 LIT. B DS-GVO)

1.1 Zutrittskontrolle

- Abschließbare Räume mit Sicherheitsschloss oder elektronischer Schließanlage
- Räume und Fenster sind außerhalb der Geschäftszeiten und bei Abwesenheit verschlossen
- Büro befindet sich im 1. Stock oder höher
- Besucheraufenthalte nur mit Begleitpersonen und unter vorheriger Anmeldung
- Restriktive Schlüsselregelungen, dokumentierte Ausgabe und Rücknahme von Schlüsseln und Transpondern

1.2 Zugangskontrolle

- Alle Rechner und Server verfügen über personalisierte Logins und Passwortschutz
- Verbot der Weitergabe von persönlichen Passwörtern
- Zugänge sind aufgaben- bzw. projektbezogen nur für die Leistungserbringer vergeben
- Firewalls in Firmennetzwerk vorhanden
- Passwortgeschützte Systeme nach vorgegebenen Richtlinien. Die Passwortrichtlinie legt eine Mindestlänge von mindestens 10 Zeichen sowie die Verwendung von mindestens 3 der folgenden vier Kategorien von Zeichen fest:
  - Kleinbuchstaben
  - Großbuchstaben
  - Sonderzeichen
  - Ziffern
- Einsatz von Multi-Faktor-Authentifizierung wo möglich und sinnvoll
- Eigener Passwort-Manager (z.B. Keepass) für jeden Mitarbeiter
- Verwendung eines Virtual Private Networks (VPN) für Zugriffe von Mitarbeitenden auf Firmennetze
- Sämtliche Server verwenden immer nur eine Minimalkonfiguration und werden regelmäßig gepatcht
- Für Mitarbeiter-Systeme und Arbeitsplätze gilt:
  - Verpflichtung zur Sperrung des Geräts bei Verlassen des Arbeitsplatzes
  - Verpflichtung zur vollständigen Verschlüsselung aller Datenträger in Geräten mit Zugriff auf personenbezogene Daten inklusive Backups
  - Verpflichtung zur verschlüsselten Übertragung von Daten (auch über externe Datenträger)
  - Verpflichtung zur Vermeidung und zum datenschutzkonformem Umgang von/mit

ausgedruckten Daten.

- Datenträger bei werden bei Nutzungsende durch sichere Verfahren überschrieben und damit gelöscht. Durch Einsatz datenschutzkonformer Verträge wird sichergestellt, dass defekte Datenträger und deren Inhalt unwiderbringlich zerstört werden.

1.3 Zugriffskontrolle

- Zugangsberechtigungen in Form von individuellen Benutzerprofilen.
- Vernichtung von Ausdrucken durch Aktenvernichter
- Protokollierung der Vernichtung von Datenträgern
- Produktive personenbezogene Daten im Rahmen der Dienstleistung KURSO (also Daten des Auftraggebers) werden ausschließlich in gesicherten Rechenzentren gespeichert und verarbeitet. Dies umfasst auch Backups.
- Abschließbare Schränke für sensible Daten in Papierform
- Mitarbeitenden ist es untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren. Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

1.4 Trennungskontrolle

- Trennung von:
  - Mitarbeiterdaten
  - Kundenkontaktdaten
  - Zugangsdaten
  - im Auftrag verarbeiteter Daten
  - Kundentestdaten (Projektarbeit, Kundenentwicklung)
  - Backup-Daten
  - Produktiv-/Test-/Entwicklungsdaten
- Trennung durch
  - Unterschiedliche Anwendungen
  - Unterschiedliche Berechtigungen/Zugangsdaten
  - Unterschiedliche Datenbanken
  - Unterschiedliche Rechenzentren/Hardware
  - Unterschiedliche Netzwerke

- Backups erfolgen auf separate Backupsysteme (eigene Hardware, andere Brandschutzzone). Backupsysteme holen zu sichernde Daten bei den produktiven Systemen ab. Sie können nicht von Produktivsystemen aus gesteuert/verändert/beeinflusst werden.

1.5 Pseudonymisierung und Verschlüsselung

(ART. 32 ABS. 1 LIT. A DS-GVO)

- Zugriffe auf Webapplikationen und Portale ausschließlich mit SSL / TLS.
- Sichere Verschlüsselung aller Datenübertragungen über öffentliche oder nicht selbstkontrollierte Netzwerke
- Richtlinie zur vollständigen sicheren Datenträgerverschlüsselung (hardware- oder softwaremäßig) für alle Datenträger außerhalb von gesicherten Rechenzentren
- Eine Pseudonymisierung der Daten ist derzeit nicht vorgesehen. Begründung: Die personenbezogenen Daten sind geschäftlicher, nicht privater Natur. In der Interessensabwägung überwiegen die geschäftlichen Interessen. Diese bestehen u.a. auch in der Sicherstellung einer Revisionssicherheit.
- Für Pseudonymisierung in von der Auftragnehmerin betriebenen Dienstleistungen (z. B. KURSO) ist ggf. der Auftraggeber verantwortlich.

2. Integrität

(ART. 32 ABS. 1 LIT. B DS-GVO)

2.1 Weitergabekontrolle

- Weitergabe an Dritte nur nach Weisung des Auftraggebers
- Weitergabe auf elektronischem Wege ausschließlich über sichere Kommunikationskanäle
- Anhänge von E-Mails als ZIP Dateien auf Basis von AES 256 bit verschlüsselt. Passwort per Telefon. Generelle Strategie der Vermeidung von Weitergabe per E-Mail.
- Richtlinie zur E-Mail Nutzung belehrt und verpflichtet die Mitarbeiter
- Versand von Datenträgern verschlüsselt
- Mitarbeiter der Auftragnehmerin sind zur Geheimhaltung verpflichtet.

2.2 Eingabekontrolle

2.2.1 Durch Mitarbeitende von Henke Informatik

- Eingaben durch Mitarbeiter nur über personalisierte Logins inkl. Logging/Protokollierung
- Dokumentation von Zuständigkeiten für die Daten
- Automatische Protokollierung bestimmter Aktionen / Systemprozesse

2.2.2 Durch Mitarbeitende des Auftraggebers

- Die Verantwortung für die Eingabekontrolle in von der Auftragnehmerin betriebenen Dienstleistungen (z. B. KURSO) obliegt dem Auftraggeber. Die Eingabekontrolle wird durch die Auftragnehmerin – sofern möglich – unterstützt. Insbesondere stellen personalisierte Benutzeraccounts Teil der Eingabekontrolle dar.

3. Verfügbarkeit und Belastbarkeit

(ART. 32 ABS. 1 LIT. B DS-GVO)

3.1 Verfügbarkeitskontrolle

- Regelmäßige Datensicherung und Prüfung selbiger
- Abhängig vom Servicelevel/auf Kundenwunsch weitere Maßnahmen vereinbar

Zusätzlich gehostete Dienstleistungen (z. B. KURSO):

- Die Systeme der Auftragnehmerin sind durch technische Maßnahmen wie Firewalls und Abwehrmechanismen gegen Angriffe geschützt.
- Systeme der Auftragnehmerin sind ausfallsicher ausgelegt.
- Produktivdatenbanken sind mindestens in einem zweiten Brandabschnitt gespiegelt
- Stündliche Datensicherung von Produktivdaten in separaten Brandabschnitt mit einer Vorhaltezeit von 30 Tagen
- Regelmäßige Tests u. a. der Datensicherung
- Früherkennung von systemkritischen Zuständen durch Monitoring und Alerting
- Weitere Maßnahmen, insbesondere in Rechenzentren, siehe TOM der Subunternehmer laut AV-Vertrag
- Regelmäßige, wenn möglich automatisierte Updates.

3.2 Sicherstellung der Belastbarkeit

- Vorhaltung von Puffern (Ressourcen) zum Abfangen unerwarteter Lastspitzen
- Monitoring

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(ART. 32 ABS. 1 LIT. D DS-GVO)

- Interne und technische Audits mit den Sicherheitsverantwortlichen
- Regelmäßige Schulungen/Wissensaufbau der Mitarbeitenden zu Datenschutz und IT-Sicherheit (Awareness)
- Regelmäßige Einschätzung möglicher Risiken und Ausarbeitung von angemessenen Maßnahmen zu deren Vermeidung
- Berücksichtigung der einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), soweit als Auftragsverarbeiter von Bedeutung

4.1 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(ART. 25 DS-GVO)

- Interne Richtlinien für Softwareentwickler bei Eigenentwicklungen
- Anwendung von datenschutzfreundlichen Voreinstellungen
- Berücksichtigung des Datenschutzes bei Auswahl und Einsatz von Systemen / Technologien

4.2 Auftragskontrolle

- Auftragsverarbeitung nur nach Abschluss eines AV-Vertrages mit Auftraggeber
- Erteilung von Weisungen in schriftlicher oder elektronischer Form
- Schriftliche Bestätigung von mündlichen Weisungen
- Regelung zur Datenlöschung/-vernichtung bei Auftragsbeendigung
- Regelmäßige Kontrolle der Umsetzung
- Vertragliche Vereinbarung von Konventionalstrafen bei Zuwiderhandlungen möglich
- Strenge Auswahl von Dienstleistern, Prüfung und Abschluss eine AV-Vertrages mit Subunternehmern

4.3 Transparenz

- Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO (sowohl als Verantwortlicher als auch als Auftragsverarbeiter)
- TOM, AV-Vertragsvorlage und Datenschutzerklärung als Teil des Web-Auftritts

5. Intervenierbarkeit

- Dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
- Nachverfolgbarkeit der Aktivitäten des Verantwortlichen zur Gewährung der Betroffenenrechte
- Einrichtung eines Verfahrens für das Zusammenspiel zwischen Verantwortlichem und Auftragsverarbeiter für den Umgang mit Vorgängen Betroffener
- Operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten
- Regelmäßige Erinnerung zur Mitwirkungspflicht

6. Nichtverkettung

- Einsatz eines Rollenkonzepts zur Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
- Programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten
- Verbot von Backdoors bei der Softwareentwicklung
- Funktionstrennung gemäß Rollenkonzept
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements und eines sicheren Authentisierungsverfahrens
- geregelte Zweckänderungsverfahren (unter Berücksichtigung von Rechtsgrundlage, Erforderlichkeit, Vereinbarkeit)
- Durchführung regelmäßiger Maßnahmen zur Awareness