Technische und Organisatorische Maßnahmen zur IT-Sicherheit

Version 2

Stand: 25.05.2020

Dokumenten ID: 1296891979

Inhaltsverzeichnis

Anlage 2 der Auftragsverarbeitungsvereinbarung

Die edjufy GmbH (nachfolgend Auftragnehmer) ergreift die folgenden technischen und organisatorischen Maßnahmen bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten für die gleichnamige Plattform edjufy.

§1 Zutrittskontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass der unbefugte Zutritt zu Datenverarbeitungsanlagen, auf denen personenbezogenen Daten verarbeitet, gespeichert und genutzt werden, verhindert wird.

Folgende Maßnahmen werden hierfür ergriffen:

- Überwachung der Zugänge zu Datenverarbeitungsanlagen
- Vergabe von Zugangsberechtigungen ausschließlich an autorisierte Personen
- Zutritt zu Datenverarbeitungsanlagen bzw. Allen relevanten Räumen nur für autorisierte Personen (Autorisierte Mitarbeiter sowie Besucher nur in Begleitung von autorisierten Mitarbeitern)
- Protokollierung des Zutritts zu Datenverarbeitungsanlagen

§2 Zugangskontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass der unbefugte Zugriff zu Datenverarbeitungsanlagen, auf denen personenbezogenen Daten verarbeitet, gespeichert und genutzt werden, verhindert wird.

Folgende Maßnahmen werden hierfür ergriffen:

- Zugriff ausschließlich durch autorisierte Mitarbeiter mit individuellen Zugangsdaten
- Verwendung von Zwei-Faktor Authentifizierung
- Zugriff auf Datenverarbeitungsanlagen ausschließlich über abgesichertes VPN (Virtual Private Network)

§3 Zugriffskontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten, dass zur Nutzung von Datenverarbeitungsanlagen autorisierten Personen ausschließlich auf die ihrer Berechtigung unterliegenden Daten zugreifen können. Des weiteren wird verhindert, dass personenbezogene Daten ohne entsprechende Berechtigung nicht gelesen, geändert, kopiert oder gelöscht werden können.

Folgende Maßnahmen werden hierfür ergriffen:

- Datenzugriff nur für berechtigte Personen
- Schutz gegen unberechtigte interne sowie externe Zugriffe
- Unterweisung von Mitarbeitern bezüglich der individuellen Zugriffsrechte

§4 Eingabekontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass keine personenbezogenen Daten in die Datenverarbeitungssysteme zusätzlich eingegeben oder entfernt wurden sowie eine entsprechende Überprüfung möglich ist.

Folgende Maßnahmen werden hierfür ergriffen:

- Erstellung eines Audit-Trails bei der Eingabe, Änderungen und Löschung von Daten
- Versionierung von Datenbeständen um Änderungen nachzuvollziehen
- Verschlüsslung von Datenbeständen
- Zugriffsbeschränkungen beim Zugriff auf Datenbestände

§5 Weitergabekontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass bei der Übertragung und dem Transport von personenbezogenen Daten diese nicht durch unbefugte dritte gelesen, kopiert, verändert oder gelöscht werden können.

Folgende Maßnahmen werden hierfür ergriffen:

- Verschlüsslung von Datenübertragungen mit gängigen Verschlüsselungstechniken wie z.B. HTTPS Verbindungen (SSL)
- Versand von E-Mail Nachrichten ausschließlich über verschlüsselte Verbindungswege (SSL/TLS)
- Einsatz von verschlüsselten VPN (Virtual Private Network) Verbindungen zur Verbindung mit Datenverarbeitungsanlagen
- Verschlüsslung von internen und externen Speichermedien (Festplatten Verschlüsslung)

§6 Verfügbarkeitskontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass es nicht zum unbeabsichtigten Verlust oder zur Zerstörung von Datenbeständen kommt.

Folgende Maßnahmen werden hierfür ergriffen:

- Regelmäßige Datensicherung auf externen und gesicherten Speichermedien
- Regelmäßige Überprüfung der Datensicherungen auf eine mögliche Wiederherstellbarkeit

§7 Auftragskontrolle

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass die Auftragsdatenverarbeitung von personenbezogene Daten auf Basis der mit dem Auftraggeber geschlossenen Auftragsverarbeitungsvereinbarung durchgeführt wird. Hierfür wird insbesondere auch auf die in der Auftragsverarbeitungsvereinbarung vereinbarte Weisungsbefugnis hingewiesen.

§8 Trennung der Verarbeitung für verschiedene Zwecke

Der Auftragnehmer sowie die beauftragten Unterauftragsverarbeiter gewährleisten durch geeignete Maßnahmen, dass Datenbestände welche für unterschiedliche Zwecke erhoben werden, getrennt verarbeitet werden können.

Folgende Maßnahmen werden hierfür ergriffen:

- Getrennte Verarbeitung zweckgebundener Datenbestände
- Trennung von Test- und Produktionssystemen