Mindestanforderungen der QUA-LiS an Technische und organisatorische Maßnahmen (TOM)

Die Bewerber müssen folgende Mindestanforderungen an Ihre TOM-Maßnahmen erfüllen. Der Nachweis kann in Form einer Eigenerklärung durch Unterzeichnung dieses Dokuments oder durch Zurverfügungstellung der eigenen TOM-Maßnahmen die die Mindestanforderungen erfüllen erfolgen. Die Mindestanforderungen sind farblich hervorzuheben. Maßnahmen die über die Mindestanforderungen hinausgehen werden nicht bewertet.

1. Vertraulichkeit gemäß Art. 32 Abs. 1 lit. b DSGVO

1.1 Zutrittskontrolle - Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen

- Manuelles Schließsystem
- Sicherheitsschlösser

Organisatorische Maßnahmen

- Schlüsselregelung/Liste
- Besucher in Begleitung durch Mitarbeitende
- Sorgfalt bei der Auswahl der Reinigungsdienste

1.2 Zugangskontrolle - Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen

- Login mit Benutzernamen und Passwort
- Anti-Virus-Software Clients
- Firewall und regelmäßige Aktualisierungen
- Einsatz VPN bei Remote-Zugriffen
- Automatische Desktopsperre
- **Verschlüsselung von QUA-LiS übermittelter Dateien mit LiSCrypt** (wird von QUA-LiS kostenlos zur Verfügung gestellt)

Organisatorische Maßnahmen

- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Richtlinie „Sicheres Passwort“
- Richtlinie „Löschen/Vernichten“
- Allgemeine Richtlinie Datenschutz und / oder Sicherheit

1.3 Zugriffskontrolle - Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen

- Aktenschredder mind. Stufe 3, cross cut)

Organisatorische Maßnahmen

- Verwaltung Benutzerrechte durch Administratoren

2. Integrität gemäß Art. 32 Abs. 1 lit. b DSGVO

2.1 Weitergabekontrolle - Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen

- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- Verschlüsselung vor der Weitergabe mit LiSCrypt (s.o.)

Organisatorische Maßnahmen

- Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- Weitergabe in anonymisierter oder pseudonymisierter Form

3. Verfügbarkeit und Belastbarkeit gemäß Art. 32 Abs. 1 lit. b DSGVO

3.1 Verfügbarkeitskontrolle - Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen

- Feuer- und Rauchmeldeanlagen

Organisatorische Maßnahmen

- Backup & Recovery-Konzept

4. Verfahren zu regelmäßigen Überprüfung, Bewertung und Evaluierung gemäß Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO

4.1 Datenschutz-Management

Organisatorische Maßnahmen

- Mitarbeitende geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeitenden mindestens 1x jährlich
- Das Unternehmen kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

4.2 Sicherheitsvorfälle

Technische Maßnahmen

- Einsatz von Firewall und regelmäßige Aktualisierungen
- Einsatz von Spamfiltern und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung

Organisatorische Maßnahmen

- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörden)
- Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen gemäß Art. 25 Abs. 2 DSGVO

Technische Maßnahmen

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

4.4 Auftragskontrolle - Maßnahmen, die gewährleisten, dass im Rahmen der Auftragsdatenverarbeitung personenbezogenen Daten nur nach Weisung des Auftraggebers verarbeitet werden (können)!

Organisatorische Maßnahmen

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Auswahl des Auftragnehmers unter Sorgfaltspflichtpunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standard-Vertragsklauseln
- Verpflichtung der Mitarbeitenden des Auftragnehmers auf Datengeheimnis
- Verpflichtung zur Bereitstellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen einer Bestellpflicht
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Eigenerklärung

Hiermit bestätigen wir, dass wir die in diesem Dokument aufgeführten Mindestanforderungen an die TOM-Maßnahmen uneingeschränkt erfüllen und dass diese ordnungsgemäß dokumentiert vorliegen.

Angaben zum Verantwortlichen

Name des Unternehmens:

Eintragung beim Registergericht:

Adresse:

E-Mail-Adresse:

Telefonnummer:

Website:

Angaben zum Datenschutzbeauftragten

Name, Vorname:

Adresse:

E-Mail-Adresse:

Telefonnummer:

Website:

_____

Datum, Unterschrift