Anlage 1

Technische und organisatorische Maßnahmen (TOM) des Auftragnehmers i.S.d. Art. 32 DSGVO der Firma blau direkt GmbH & Co. KG

Erläuterung:

Firmen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschrift der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die Firma blau direkt GmbH & Co. KG erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1 Zutrittskontrolle

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

Maßnahmen:
- Manuelles Schließsystem
- Chipkarten-/Transponder-Schließsystem mit regelmäßiger Prüfung der Zutrittsrechte
- Sicherheitsschlösser
- Schlüsselregelung
- Personenkontrolle beim Empfang
- Sorgfältige Auswahl von Reinigungspersonal
- stichprobenartig eingesetzte mobile Kameraüberwachung mit WLAN-gestützer Bildübertragung
- Besucher in Begleitung durch Mitarbeiter

1.2. Zugangskontrolle:

Erläuterung:
Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint.

Maßnahmen:
- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort (Hochsicherheitspasswörter mit Passwortmanagement & Controlling)
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Sperren von externen Schnittstellen (USB)
- Schlüsselregelung
- Personenkontrolle beim Empfang
- Sorgfältige Auswahl von Reinigungspersonal
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall

- Einsatz einer Software-Firewall
- Richtlinie „Sicheres Passwort"
- Richtlinie „Löschen / Vernichten"
- Richtlinie „Clean desk"
- Allgemeine Richtlinien zum Datenschutz und/oder Sicherheit
- Anleitung „Manuelle Desktopsperre"

1.3. Zugriffskontrolle

Erläuterung:
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.

Maßnahmen:
- Passwortrichtlinie: (Hochsicherheitspasswörter mit Passwortmanagement & Controlling)
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Dienstleistern zur Aktenvernichtung Protokollierung der Aktenvernichtung mit Aktenvernichtungszertifikaten
- Einsatz Berechtigungskonzepte
- Minimale Anzahl an Administratoren
- Verschließbare Aktenschränke
- Verwaltung von Benutzerrechten durch Administratoren

1.4. Trennungskontrolle

Erläuterung:
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen:
- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern Logische Mandantentrennung (softwareseitig)
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem
- Steuerung über Berechtigungskonzept

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. A DSGVO; Art. 25 Abs. 1 DSGVO)

Erläuterung:
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden könne, sofern diese zusätzlichen Informationen gesondert aufbewahrtwerden und entsprechende technische und organisatorische Maßnaßmen unterliegen.

Maßnahmen:
- Interne Anweisung, personbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren.

2. Integrität (Art. 32 Abs. 1 lit . B DSGVO)

2.1. Weitergabekontrolle

Erläuterung:
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.

Maßnahmen:
- Einrichtungen von VPN-Tunneln
- E-Mail-Verschlüsselung
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen.
- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- Weitergabe in anonymisierter oder pseudonymisierter Form

2.2. Eingabekontrolle

Erläuterung:
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:
- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. B DSGVO)

3.1. Verfügbarkeitskontrolle

Erläuterung:
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen:
- Unterbrechungsfreie Stromversorgung (USV)
- Lüftungsanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen
- RAID System / Festplattenspiegelung
- Einsatz von Server Anti-Viren Software

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. D DSGVO; Art. 25 Abs. 1 DSGVO)

4.1. Incident-Response-Management

Erläuterung:
Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Maßnahmen:
- Einsatz von Firewall und regelmäßigen Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Intrusion-Detection-Systemen
- Intrusion-Prevention-Systemen
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen und Datenpannen
- Dokumentierter Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Einbindung von DSB und zuständige Datenschutzbehörde bei Sicherheitsvorfällen und Datenpannen
- Dokumentation von Sicherheitsvorfällen und Datenpannen

4.2. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Erläuterung:
Privacy by design / privacy by default

Maßnahmen:
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

4.3. Auftragskontrolle

Erläuterung:
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen:
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- vorherige Prüfung der Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer

4.4. Datenschutz-Management

Maßnahmen:
- Interner Datenschutzbeauftragter
- Mitarbeiter werden geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter findet statt
- Die Datenschutz-Folgenabschätzung wird bei Bedarf durchgeführt

- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mindestens jährlich durchgeführt
- Sicherheitskonzepte werden dokumentiert
- Software-Lösung für Datenschutz-Management im Einsatz
- Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
- Benutzerrechtevergabe wird dokumentiert und regelmäßig kontrolliert
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter nach Bedarf / Berechtigung.

Stand: 22.05.2018