**Technische und organisatorische Maßnahmen (TOM) zur Gewährleistung der Sicherheit der Verarbeitung von Jan-Lukas Knoch („PicShop.me“)**

**A. Maßnahmen zur Pseudonymisierung**

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

**B. Maßnahmen zur Verschlüsselung**

Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text / Information mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird:

- Symmetrische / Asymmetrische Verschlüsselung
- Blockalgorithmen (z. B. AES, 3DES)

**C. Maßnahmen zur Sicherung der Vertraulichkeit**

**1. Zutrittskontrolle**

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren:

Beschreibung des Zutrittskontrollsystems:

- Automatisches Zutrittskontrollsystem
- Manuelles Schließsystem (Notausgänge)
- Sicherheitsschlösser
- Absicherung der Gebäudeschächte
- Türen mit Knauf auf der Außenseite
- Schlüsselregelung / -liste
- Kontrollsystem für Besucher

**2. Zugangskontrolle**

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Beschreibung des Zugangskontrollsystems:

- Login mit Benutzername und Passwort
- Login mit biometrischen Daten und 2-Factor Authentifizierung
- Sperre des Anmeldevorgangs nach festgelegter Zahl von Versuchen
- Zeitgesteuerte Desktopsperre
- Firewalls auf Clients aktiviert
- Dedizierte Firewall
- Anti-Virus-Software auf Clients installiert (Defender auf Windows)

- Verriegelung des Server-Schranks
- Verschlüsselung Dateisystem „Clients“ (Notebook, Desktop)
- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen / eines Benutzerstammsatzes „i. S. v. Rechtemanagement“
- Zentrale Passwortvergabe
- „Passwort“- und „Home-Office“-Richtlinie
- Anleitung „Manuelle Desktopsperre“

**3. Zugriffskontrolle**

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung des Zugriffskontrollsystems:

- Einsatz eines zentralen netzbasierten Authentisierungsdienstes für Benutzer
- Verwendung von Kennwort-Management-Systemen
- Papier wird sicher vernichtet (Bsp. Aktenvernichter-Sicherheitsstufe P-3)
- Datenträger, die nicht mehr sicher gelöscht werden können, werden sicher vernichtet Einsatz von Berechtigungskonzepten
- Regelungen zur Einrichtung, Einteilung von Benutzerkennungen, Benutzergruppen und Rechteprofilen
- Benutzerkennungen und Berechtigungen werden nur auf Basis des tatsächlichen Bedarfs und der Notwendigkeit zur Aufgabenerfüllung vergeben („Need-to-know“-Prinzip)
- Jede Benutzerkennung ist eindeutig und einer Person zugeordnet
- Benutzer und Benutzerkennungen dürfen nur über administrative Rollen eingerichtet und gelöscht werden
- Restriktive Rechtevergabe für Outsourcing-Dienstleister („Need-to-know“-Prinzip)

**4. Trennungsgebot**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Beschreibung des Trennungskontrollvorgangs:

- Trennung von Produktiv- und Testumgebung (Entwicklerumgebung)
- Getrennte physikalische Aufbewahrung von Clients und der verwendeten Datenbanken von Clients
- Ausschließlich Administratoren haben Zugriff auf administrative Funktionen und Schnittstellen
- Ein Identitäts- und Berechtigungsmanagement ist im Einsatz (Authentifizierungsserver mit Zugang zu Kernsystem)
- Benutzer- und Gruppen-IDs kommen jeweils nur einmal vor

**D. Maßnahmen zur Sicherung der Integrität**

**1. Datenintegrität**

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden:

Beschreibung der Datenintegrität:

- Einspielen neuer Releases und Patches mit Release- / Patchmanagement
- Funktionstest bei Installation und Releases/Patches durch die IT-Abteilung

**2. Transportkontrolle**

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

Beschreibung der Transportkontrolle:

- Verwendung eines Verschlüsselten Kommunikationsprotokolls auf dem Webserver (https)
- Ausschluss von physischen Transporten von Datenträgern

**3. Eingabekontrolle**

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

Beschreibung des Eingabekontrollvorgangs: In einer separaten Tabelle in der Datenbank wird aufgezeichnet, welche Änderungen der relevanten Daten des Benutzeraccounts durch die Mitarbeiter von Jan-Lukas Knoch („PicShop.me“) oder den Kunden (Fotografen) vorgenommen werden.

**E. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit**

**1. Verfügbarkeitskontrolle**

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beschreibung des Verfügbarkeitskontrollsystems:

- Datensicherungsverfahren
- Möglichkeit von Rollbacks
- USV (Unterbrechungsfreie Stromversorgung)
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums

**2. Rasche Widerherstellbarkeit**

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen zur raschen Widerherstellbarkeit:

- Datensicherungsverfahren
- Geeignete Versionsverwaltung des Quellcodes (Entwickler)
- Automatisches Monitoring mit E-Mail-, SMS- und Telefon-Benachrichtigung
- Notfallmanagement
- Mitarbeiter für Notfallmanagement sensibilisiert

**3. Zuverlässigkeit**

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Beschreibung der Maßnahmen zur Zuverlässigkeit:

- Automatisches Monitoring mit E-Mail-, SMS- und Telefon-Benachrichtigung
- IT-Notdienst 24/7

**F. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung**

**1. Überprüfungsverfahren**

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren:

- Datenschutz-Management
- Externer Datenschutzbeauftragter (DSB) ist bestellt
- Mitarbeiter werden regelmäßig geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter
- Formalisierte Prozesse für Datenschutzvorfälle (insb. regelmäßige Einbindung des Datenschutzbeauftragten)
- Weisungen des Auftraggebers werden dokumentiert
- formalisiertes Auftragsmanagement

**2. Auftragskontrolle**

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

Beschreibung der Maßnahmen zur Auftragskontrolle:

- Vorherige Prüfung vom Auftragnehmer bzgl. getroffener Sicherheitsmaßnahmen und deren Dokumentation
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insb. in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU StandardVertragsklauseln
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen einer Bestellpflicht
- Vereinbarung von wirksamen Kontrollrechten gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Weisungen des Auftraggebers werden dokumentiert
- formalisiertes Auftragsmanagement

Letzte Aktualisierung: 01.11.2022