**ARBEITSMATERIAL**

**3/7 MUSTER (TOM)**

**Liste der Technische und organisatorische Maßnahmen**

aus: Datenbank und Datenschutz gehören zusammen

Die Themenreihe „**Datenbank und Datenschutz gehören zusammen**“

ist eine Kooperation mit Dirk Wolf,

dem Datenschutzbeauftragten des Deutschen Fundraising-Verbandes (DFRV).

Sie erreichen Dirk Wolf

für Rückfragen und Buchung

unter: wolf@skriptura.de

DATENWELTEN bietet Ihnen als kostenfreie Basics:

1. MUSTER Verzeichnis von Verarbeitungstätigkeiten (VVT)
2. VORLAGE Auftragsverarbeitungsvertrag (AVV)
3. MUSTER Liste der Technische und organisatorische Maßnahmen (TOM)
4. MUSTER-Datenschutzrichtlinie
5. PODCAST (ab März 2023): Die gängigsten Datenschutz-Pannen bei der Nutzung einer Fundraising-Datenbank
6. Zum Nachschlagen „Aufbewahrungsfristen“

Des Weiteren finden Sie im Shop:

1. ****VIDEO (ab März 2023)

Die zehn wichtigsten ToDos für eine DSGVO-konforme Datenbank-Nutzung

**Muster Liste der Technischen und organisatorischen Maßnahmen**

*Folgendes Muster ist als Gedankenstütze zu verstehen. Bitte sehen Sie sich jeden einzelnen Punkt an und passen ihn an die bei Ihnen vorliegenden Gegebenheiten an. Ist ein Punkt bei Ihnen gar nicht vorhanden, löschen Sie ihn bitte. Gibt es zu einem Thema etwas, was hier nicht vermerkt ist, fügen Sie ihn bitte hinzu.*

**Technische und organisatorische Maßnahmen**

**1.** **Vertraulichkeit** (Art. 32 Abs. 1 Buchstabe b DSGVO)

* Zutrittskontrolle

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

* Bereiche sind in verschiedene Sicherheitsbereiche unterteilt
* Zugänge sind gegen unbefugten Zugang gesichert
* Alarmanlage (Einbruchmeldesystem)
* Zugangsauthentisierung (Schlüsselregelung, Chipkartensystem)
* Sicherheitsschlösser
* Besucherregelung (Begleitung, Besucherausweis, Protokollierung)
* Sicherheits- und Wachdienst (Wochenende);
* Zugangskontrolle
* Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
* Zugangsschutz zu allen DV-System durch Benutzerauthentisierung
* Es existieren Passwortkonventionen
* Authentisierung mit Benutzername / Passwort
* Zuordnung von Benutzerrechten
* Sperren von externen Schnittstellen (USB etc.)
* Erstellung und Zuordnung von Benutzerprofilen
* Einsatz von Anti-Viren-Software
* Einsatz einer Hard- und Software-Firewall
* Verschlüsselung (bei entsprechendem Bedarf);
* 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.

* Anzahl der Administratoren auf das „Notwendigste“ reduziert
* Regelungen und Verfahren zum Anlegen, Ändern und Löschen von Berechtigungsprofilen
* Prozess zur Beantragung, Genehmigung, Vergabe und Rückgabe von Zugriffsberechtigungen ist implementiert
* Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
* Einsatz von Aktenvernichtern
* Sichere Aufbewahrung von Datenträgern
* Ordnungsgemäße Vernichtung von Datenträgern;
* Trennungskontrolle

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

* Trennung von Produktiv und Testsystem
* Es werden nur solche Daten erhoben, gespeichert und verarbeitet die unmittelbar dem eigentlichen Zweck dienen.
* Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
* Technische und Operative Regelung und Maßnahmen zur Sicherstellung der getrennten Verarbeitung;

**2. Integrität** (Art. 32 Abs. 1 Buchstabe b DSGVO)

* 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.

* Es findet eine Protokollierung statt.
* Die Festlegung ist dokumentiert und den betroffenen Mitarbeitern bekannt.
* Die Verbindung zu den Backendsystemen ist geschützt.
* Es existiert eine Verfahrensregelung über den Einsatz von Datenträgern.
* Datenträgerverwaltung – Durchführung regelmäßiger Bestandskontrollen.
* Es gibt Regelungen zur datenschutzkonformen Vernichtung von Datenträgern.
* Die Vernichtung wird dokumentiert.
* Bei Übertragungen werden dem Stand der Technik entsprechenden Verschlüsselungsverfahren eingesetzt.
* Eingabekontrolle

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

* Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (Protokollierung)
* Es existiert eine Dokumentation der Eingabeberechtigungen;

**3. Verfügbarkeit** **und Belastbarkeit** (Art. 32 Abs. 1 Buchstabe b DSGVO)

* Verfügbarkeitskontrolle

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

* Es existiert ein Backup-Konzept.
* Verantwortliche Personen und Vertreter sind benannt.
* Unterbrechungsfreie Stromversorgung (USV)
* Klimaanlage im Serverraum
* Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverraum
* Regelmäßige Prüfung von Notstromaggregat und Überspannungsschutzeinrichtung sowie permanente Überwachung der Betriebsparameter
* Lagerung von Datensicherungen in feuer- und wassergeschützten Datensicherheitsschränken, bzw. zusätzlich extern.
* Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Buchstabe d DSGVO; Art. 25 Abs. 1 DSGVO)
* Datenschutz-Management
* Vorfalls-Reaktionsplan
* Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
* Auftragskontrolle