Technisch Organisatorische Maßnahmen
der AGENTUR JOHANNES JAROLIM
Stand 01.05.2018

1. Standardmaßnahmen.

AGENTUR JOHANNES JAROLIM sieht zum Schutz personenbezogener Daten im Rahmen der folgenden Standardverarbeitungsvorgängen, welche

- nur im geringen Ausmaß personenbezogene Daten über Strafdaten und strafrechtliche Verurteilungen bzw. besondere Kategorien von personenbezogenen Daten beinhalten und
- auch sonst nur kein oder nur ein geringes Risiko aufweisen

folgende technische und organisatorische Maßnahmen

- zur Sicherstellung der Vertraulichkeit der Datenverarbeitung,
- zur Sicherstellung der Integrität der Datenverarbeitung,
- zur Sicherstellung der Verfügbarkeit der Datenverarbeitung,
- zur Sicherstellung der Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung,
- zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den
- Zugang zu den personenbezogenen Daten bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen und
- zur Sicherstellung der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

in den nachfolgenden Bereichen vor:

Organisationskontrolle

- Schriftliche Regelungen über den Betrieb, die Abläufe, die Sicherheit der Datenverarbeitung
- IT-Sicherheitsrichtlinien sowie Arbeits- und Verfahrensanweisungen
- Regelungen über Sicherung des Datenbestandes
- Festlegen der Tätigkeiten der Mitarbeiter durch Stellenbeschreibungen
- Erstellen Verarbeitungsübersicht (internes Verfahrensverzeichnis)

Zutrittskontrolle

- Zutritt ausreichend abgesichert über Zutrittskontrollsystem

Zugangskontrolle

- Zentrale und sichere Aufbewahrung Administrator-Passwörter
- Administratorzugang ist Passwort länger als 8 Zeichen
- Bildschirmsperre mit Loginzwang
- Nutzen der Kurztasten zur Bildschirmsperre
- Externer Zugriff nur über VPN

Zugriffskontrolle

- differenzierte Berechtigungen (Rollenberechtigungskonzept)
- Auswertung von Logfiles

Weitergabekontrolle

- HTTPS Protokoll
- Mailanlagen mit PB Daten als ZIP nur bis mittlerer Schutzbedarf
- Kennwort nicht mit/bei den Daten (mit extra Mail)
- VPN

Eingabekontrolle

- Logfiles
- Protokollierung
- differenzierte Berechtigungen Auswertung von Logfiles bezüglich "Zugang" und "Zugriff"
- Auswertungen der Logfiles, bezüglich Erfassen, ändern und löschen der Daten
- Einsatz von Anwendungssoftware mit "Rollenkonzepten"
- Einsatz von Anwendungssoftware mit "differenzierbaren Rechten"

Auftragskontrolle

- Unterweisung der Mitarbeiter zum Datenschutzaspekt
- vertragliche Regelungen als Auftragsdatenverarbeiter
- Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Verantwortlichen/Auftraggebers

Verfügbarkeitskontrolle

- Feuerlöscher beim Serverraum
- Backup-Konzept
- Datensicherung
- Unterbrechungsfreie Stromversorgung (USV)
- Rauchverbot in Server-und PC-Arbeitsräumen
- Datenarchivierung
- Einspielung Sicherheitspatches
- Spamfilter
- Virenschutz

Trennungskontrolle

- Trennung besonders sensibler Daten
- Unterschiedliche Subnetze
- Interne Zugriffssicherung
- Zweckbindung im Verfahrensverzeichnis definiert

Johannes Jarolim, PMP · Senior Web Development · Maria-Cebotari-Straße 6 · 5020 Salzburg
UID ATU67692026 · Telefon +43 (0)664 4047489 · office@jarolim.com · www.jarolim.com