Anlage 1a

Technisch und organisatorische Maßnahmen (TOM)

Bzgl. der Vertraulichkeit der Daten sind folgende Maßnahmen umgesetzt:

1. Zutrittskontrolle.

   Über die Zutrittskontrolle wird sichergestellt, dass kein Unbefugter Zutritt zu den Datenverarbeitungsanlagen, mit denen die Daten verarbeitet oder genutzt werden, erlangt. Der Zutritt zu den o.g. Anlagen ist im Ennepe-Ruhr-Kreis nur über eine automatisierte Zugangskontrolle mit Transpondersystem möglich. Entsprechende Transponder besitzen nur die Mitarbeiter/innen der Abteilung ADV. Der Sicherheitsraum selbst ist mit einem Codeschloss versehen. Über die ausgehändigten Transponder sowie über den Personenkreis - die den Zugangscode kennen - wird eine Nutzungsberechtigung geführt. Den Zugangscode kennt nur ein bestimmter, zugelassener Personenkreis. Besucher dürfen nur in Begleitung eines Mitarbeiters/einer Mitarbeiterin der Abteilung ADV den Raum der Datenverarbeitung betreten. Zum Anmelden ist für diesen Zweck eine separate Wählanlage installiert.

2. Zugangskontrolle

   Mit der Zugangskontrolle wird verhindert, dass Unbefugte die Datenverarbeitungsanlagen nutzen können. Neben Benutzername und sicherem Passwort setzt der Ennepe-Ruhr-Kreis für alle mobilen Arbeitsplätze die Authentifizierung über „MobilePass+“ ein. Die Änderungen und Gestaltung von Passwörtern ist in der Dienstanweisung DA TUI geregelt. Alle externen Schnittstellen (USB-Ports, etc.) werden über eine Software administriert und überwacht. Darüber hinaus hat der Ennepe-Ruhr-Kreis eine für alle Beschäftigten gültige IT Sicherheitsrichtlinie erlassen.

3. Zugriffskontrolle

   Mit der Zugriffskontrolle wird sichergestellt, dass Nutzer/innen nur auf die Daten zugreifen können, für die sie eine Berechtigung besitzen. Dies wird über entsprechende Rollen- und Berechtigungsvergaben sichergestellt. Jeder Nutzer muss für die Programme, auf die er zugreifen muss, eine entsprechende Nutzungsberechtigung unterschreiben und vom entsprechenden Vorgesetzten gegenzeichnen lassen. Die Abteilung ADV erhält alle entsprechenden Nutzungsberechtigungen und vergibt entsprechend die Rollen bzw. Berechtigungen. Über die Protokollierung innerhalb des Softwareverfahrens wird die Eingabekontrolle gewährleistet (wer hat was wann gemacht).

4. Trennungskontrolle

   Der Trennungskontrolle wird mit Trennung von Test- und Echtsystem bzw. über die Mandantenfähigkeit des Softwareverfahrens Rechnung getragen.

5. Verfügbarkeit und Belastbarkeit

Über die Maßnahmen zur Verfügbarkeit und Belastbarkeit soll sichergestellt werden, dass die personenbezogenen Daten gegen zufälligen Verlust oder Zerstörung geschützt sind. Der Ennepe-Ruhr-Kreis hat hierfür alle Serversystem in einem Sicherheitsraum untergebracht. Dieser verfügt über eine redundante USV mit nachgeschaltetem Notstromdiesel, eine Löschanlage, eine Raumluftüberwachungsanlage und eine redundante Klimatisierung. Die Daten werden entsprechend einem festgelegten Sicherungskonzept gesichert. Die Datensicherung selbst wird in einem anderen Standort gelagert. Die Systeme selbst sind gleichfalls in einem anderen Standort gespiegelt.

Der Ennepe-Ruhr-Kreis lässt regelmäßig über Penetrationstests bzw. Sicherheitsüberprüfungen die vorgenommenen Sicherheitsvorkehrungen von externen Unternehmen überprüfen. Der Ennepe-Ruhr-Kreis setzt ein mehrstufiges Firewallsystem und Virenschutzsystem ein. Sowohl ein Intrusion Detection als auch ein Intrusion Prevention System werden beim Ennepe-Ruhr-Kreis eingesetzt.

Alle Ausfälle und Störungen werden über ein Monitoring System erfasst und protokolliert.