Technische und Organisatorische Maßnahmen

Der Verantwortliche bestätigt, folgende Maßnahmen zur Einhaltung der Anforderungen an die Sicherheit der Datenverarbeitung ergriffen zu haben:

1. Zugangskontrolle

1.1. Der Zutritt zu den Räumlichkeiten der IT Services mpsna GmbH ist nur autorisierten Personen gestattet sowie deren Erfüllungsgehilfen. Außerhalb der Geschäftszeiten sind die Räumlichkeiten verschlossen sowie Kamera überwacht. Räume mit kritischer IT-Infrastruktur (Serverraum) sind stets verschlossen und nur für die Geschäftsleitung zugänglich.

2. Datenträgerkontrolle

2.1. Alle defekten oder auszutauschenden Medien werden ordnungsgemäße nach DIN 32757 vernichtet, dies bezieht elektronische sowie Papierträger mit personenbezogenen Daten mit ein.

2.2. Alle Mitarbeiter sind schriftlich darüber aufgeklärt, keine selbsttätigen Veränderungen an den Datenverarbeitungsanlagen vorzunehmen. Dies betriff explizit auch den Anschuss privater / mobiler Datenträger an die EDV.

3. Benutzerkontrolle

3.1. Der Zugang zu Arbeitsplatzrechner ist über einen zentralen Verzeichnisdienst (Active Directory) in Verbindung mit personalisierten Benutzerkennungen geregelt.

3.2. Die interne EDV-Richtline schreibt die Verwendung sicherer Passwörter (Kombination aus Sonderzeichen, Groß/Kleinschreibung und Zahlen) vor. Mitarbeiter sind angehalten beim Verlassen des Arbeitsplatzes ihren Bildschirm zu sperren.

3.3. Geräte, die nicht über die kabelgebundene Netzwerkinfrastruktur angebunden sind, können auf dem Betriebsgelände mittels verschlüsseltem WLAN in Verbindung mit einem zertifikatsbasierten VPN Zugang und außerhalb des Betriebsgeländes über einen zertifikatsbasierten VPN Gateway Zugriff auf das interne Unternehmensnetzwerk erhalten.

3.4. Die Kommunikation zwischen internem Netzwerk und dem Internet wird durch eine Firewall gesichert und sofern möglich verschlüsselt bzw. durch VPN-Netzwerke geschützt.

3.5. Jeder Arbeitsplatzrechner ist mit einem Virenscanner ausgestattet. Die Funktionsfähigkeit und Aktualität der Virenscanner wird zentral überwacht.

3.6. Es werden ausschließlich IT-Systeme eingesetzt, für die regelmäßige Sicherheitsupdates der Hersteller zur Verfügung stehen.

4. Zugriffskontrolle

4.1. Soweit softwareseitig unterstützt, erfolgt die Nutzerverwaltung unter Verwendung des zentralen Verzeichnisdienstes (Active Directory) im Single-Sign-On Verfahren. Für

Systeme, die eine Integration mit dem zentralen Verzeichnisdienst nicht zulassen, werden die internen Funktionen zur Nutzerverwaltung genutzt.

4.2. In beiden Fällen ist durch eine zentrale Zuordnung von Rollen und Rechten zu personalisierten Nutzerkennungen gewährleistet, dass die zur Benutzung von EDV-Anlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen bzw. diese verändern können, sofern sie hierfür berechtigt sind.

5. Transportkontrolle

5.1. Der Transport von Daten ist durchgehend verschlüsselt soweit es die Gegenstelle zulässt. Der Transport explizit von E-Mail ist soweit es die Gegenstelle anbietet ebenfalls verschlüsselt, sofern sich die Partner auf ein System einigen können. Der Abruf von E-Mails (Pop3/IMAP/Web) ist nur verschlüsselt erlaubt.

6. Datenintegrität sowie Eingabekontrolle

6.1. Die im Folgenden beschriebenen Maßnahmen dienen der Absicherung vor Datenverlust im Fall von unerwarteten technischen Störungen sowie äußeren Gefahren wie Feuer oder Wassereinbruch:

6.1.1. Einsatz von Antivirensoftware auf Arbeitsplatz-Rechnern und Servern.

6.1.2. Tägliche Backups sowie zusätzliche Replikation der virtuellen Server-Instanzen. Übernahme der Backups in ein räumlich getrenntes Langzeitarchiv.

6.1.3. Bereitstellung einer virtualisierten Server-Infrastruktur in klimatisierten Serverräumen.

6.1.4. Einsatz von RAID-Verfahren in den Storage-Systemen für die virtualisierte Serverumgebung.

6.1.5. Einsatz von USV-Systemen zur unterbrechungsfreien Stromversorgung und zum Schutz vor Überspannungen.

7. Trennungskontrolle

7.1. Alle erhobenen Daten, Webseiten, sowie per E-Mail oder schriftlich/mündlich, dienen lediglich dem Zweck der Auftragsbearbeitung sowie Buchführung. Für alle Werbezwecke werden Daten separat durch Zustimmung der Person erhoben und in separaten Datenbanken verwaltet. Es geschieht keine automatische Auswertung oder Zusammenführung von personenbezogenen Daten ohne Zustimmung.

8. Mitarbeiterschulung

8.1. Alle Mitarbeiter werden regelmäßig intern zum Umgang mit personenbezogenen Daten und dem Verhalten am EDV Arbeitsplatz sowie zur Passwortsicherheit unterwiesen.

Herten, den 23.05.2018