Anhang über technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

Technische und organisatorische Maßnahmen für Verantwortliche

Der Verantwortliche bestätigt Maßnahmen zur Einhaltung der Anforderungen an die Sicherheit der Datenverarbeitung ergriffen zu haben.

Dies sind folgende:

Pseudonymisierung und Verschlüsselung personenbezogener Daten

- Die kontaktbezogenen Daten, welche von Google Analytics gesammelt werden (Bsp. Verhalten auf der Webseite), werden anonymisiert und pseudonymisiert gespeichert. Die Funktion zur IP-Anonymisierung in Analytics setzt bei Nutzer-IPAdressen vom Typ IPv4 das letzte Oktett und bei IPv6-Adressen die letzten 80 Bits im Speicher auf null, kurz nachdem sie zur Erfassung an das Analytics-Datenerfassungsnetzwerk gesendet wurden.
- Die Verschlüsselung der kompletten Webseite wird mithilfe von SSL durchgeführt. Die einsetzten Zertifikate für die Verschlüsselung werden von GeoTrust bzw. LetsEncrypt erstellt und mindestens alle 89 Tage, spätestens nach 12 Monaten verlängert. Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.
- Bei Nutzung öffentlicher Netze, im Bezug auf personenbezogene Daten, wird eine Verschlüsselung vorgenommen,
- Zugang zu Systemen nur mit individuellen Benutzernamen und Kennwörtern,
- Berechtigte können nur auf für sie berechtigte Daten zugreifen,
- personenbezogene gespeicherte Daten können nur im Rahmen des Berechtigungskonzepts gelesen, kopiert, verändert oder entfernt werden,
- Verwendung fortlaufend aktualisierter Virenschutzsoftware, (ESET)
- Schutz des E-Mail-Verkehrs vor Viren und Spam, (ESET)
- Firewallsysteme, (ESET und Router)
- Sicherstellung einer hohen Widerstandsfähigkeit der DV-Systeme bei starkemZugriff bzw. starker Belastung, etwa durch Angriffe von außen, (ESET)
- Verwendung ausgetesteter Software, (ACRONIS,, MS Office, CEOS)
- In unseren Abrechnungs- und Datenbankprogrammen CEOS und Miclas wird jede Eingabe in einer Historie mit Zeitstempel und Benutzerkennung abgelegt, gleiches gilt für unsere Dokumentenverwaltung im Programm BITFARM,
- Trennung der Produktiv- von der Test- und Entwicklungsumgebung,
- Sperren von externen Schnittstellen, (USB, DVD-LW)
- Einsatz von Intrusion-Detection-System, (ESET)
- Verpflichtung der Mitarbeiter auf das Datengeheimnis,
- Alert-Meldung bei hoher Belastung und Ausfällen mit SMS-Benachrichtigung von IT-Personal,
- Virtualisierung/Dynamische Zuteilung,
- Hohe Passwortsicherheit, Regelmäßiger Wechsel,
- Kein Zugang für Unbefugte zu den Datenverarbeitungsanlagen,
- Während der Geschäftszeiten Zutritt zu Geschäftsräumen durch Mitarbeiter kontrolliert,

- Festlegung der berechtigten Personen in Listen für die sensiblen Bereiche der Rechenzentren,
- Einbruchschutzmaßnahmen u.a. durch ein abgeschlossenes Firmengelände, Alarmanlage mit Videoüberwachung und Wachschutzaufschaltung,
- Rauchwarnmelder mit Wachschutzaufschaltung,
- definierter Kreis von Zugangsberechtigten,
- Anzahl der Admins aufs Notwendigste begrenzt,
- Sichere Löschung bzw. Vernichtung von Datenträgern (ACRONIS) und physikalischen Dokumenten nach Ablauf der gesetzlichen Aufbewahrungspflichten, Beauftragt wurde dafür ein zertifiziertes Unternehmen,
- Verbot der Nutzung privater Datenträger,
- Empfang besetzt während Geschäftszeiten,
- Regelungen zur Beschaffung von Hard-und Software (durch ICD-E),
- Zentrales Rechtemanagement für Arbeitsplatz-PCs,
- Regelung und Kontrolle von externer Wartung und Fernwartung,
- Regelungen für Heimarbeitsplätze,
- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- Doppelt- oder Mehrfachvorhaltung aller Komponenten bei der Datenverarbeitung (z. B. Datensicherung und Spiegelung von Hardwarekomponenten), (ACRONIS),
- Datensicherungs- und Recoverykonzept, (ACRONIS)
- personenbezogene Daten sind ständig verfügbar und geschützt gegen zufällige Zerstörung oder Verlust durch regelmäßiges Backup,
- Sicherheitskopien, (RDX)
- unterbrechungsfreie Stromversorgung, (USV APS)
- Überwachungs- und Meldesysteme, (USV)
- Vertretungspläne für Personal.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Verarbeitung

- Regelmäßige Prüfung, ob/in welchem Umfang Zugangsrechte noch erforderlich sind,
- Auftragskontrolle bei Auftragsverarbeitung,
- Beauftragung von externen oder internen Prüfberichten,
- Durchführung von notwendigen Anpassungsmaßnahmen,
- Alle Sicherungssysteme unterliegen einer ständigen Anpassung, Kontrolle und Wartung.

Es liegen folgende Dokumentationen zu sonstigen Maßnahmen vor Datenschutzschulungen, Zertifikate etc. Unser interner Datenschutzbeauftragter ist zu erreichen unter der Mailadresse datenschutz@amvd.eu.

Mittwoch, 21. November 2018

Datum der Dokumentation

Unterschrift Verantwortlicher