Datensicherheitskonzept der GEFAK

Allgemeine technische und organisatorische Maßnahmen

Stand: 15.11.2022

GEFAK Gesellschaft für angewandte Kommunalforschung mbH
Ockershäuser Allee 40b · 35037 Marburg
Tel.: +49 6421 1728-0 · Fax: +49 6421 1728-28
www.gefak.de · info@gefak.de
Amtsgericht Marburg HR B 1699
Geschäftsführer Dr. Ulrich Dewald, Christian Worm

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

1.1 Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Der Zutritt ist über eine Schlüsselregelung realisiert. Es existiert eine Dokumentation der Schlüsselvergabe sowie eine Verpflichtung der Schlüsselinhaber, einen etwaigen Verlust zu melden. Die Reaktion bei Verlust hängt von den Umständen ab und kann bis zum Austausch aller relevanten Schließzylinder reichen.

Ein Zutritt erfolgt grundsätzlich über den Empfang, unbeobachtet kann ein Zutritt nur widerrechtlich erlangt werden.

Das Reinigungspersonal ist sorgfältig ausgewählt und auf Geheimhaltung verpflichtet.

1.2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Der Zugang zu der Installation wird durch die Kombination von Benutzername und Benutzerpasswort erlangt. Das Passwort hat mindestens 20 Zeichen. Es existiert ein Benutzerstammsatz pro Benutzer. Nach dreimaliger Fehleingabe wird der entsprechende Account gesperrt und ist nur durch Mitarbeiter des Auftragverarbeiters wieder zu aktivieren. In einem solchen Falle wird das Passwort geändert.

Benutzerrechte sind vergeben.

Es kommt eine Hardware-Firewall mit IPS Möglichkeit zum Einsatz, ebenso ist ein Virenscanner vorhanden. Für den Zugriff von außen kommt VPN-Technik zum Einsatz.

Mobile Datenträger und die Datenträger von Notebooks sind verschlüsselt. Smartphones können im Verlustfalle aus der Ferne gelöscht werden.

1.3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Die jeweiligen Benutzer verfügen immer nur über diejenigen Systemberechtigungen, die sie für ihre jeweilige Arbeit benötigen. Die An- und Abmeldungen im System werden in Logdateien festgehalten. Die Verwaltung der Berechtigungen erfolgt durch den Administrator, ebenso die Einstellung und Überwachung der Passwortrichtlinie. Datenträger werden vor Wiederverwendung physisch gelöscht, sicher aufbewahrt und bei Bedarf verschlüsselt.

1.4 Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Die "Interne Mandantenfähigkeit" ist gegeben und wird im Rahmen der Zweckbindung genutzt. Bei pseudoanonymisierten Daten wird die Zuordnungsdatei getrennt aufbewahrt.

Funktionstrennung: Bei einer Fernwartung wird immer am Produktivsystem des Kunden gearbeitet. Eine Funktionstrennung ist in diesem Zusammenhang daher nicht möglich. Werden in der Folge der Fernwartung weitere Tests notwendig, so finden diese in einem Testsystem und nicht mit Echtdaten statt.

2. Integrität (Art. 32 Abs. 1 lit. b EU-DSGVO)

2.1 Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle ...

Für den Transport von Daten über eine Datenleitung wird VPN-Technik genutzt, die Weitergabe erfolgt, wenn möglich, in anonymisierter oder pseudonymisierter Form. Eine E-Mail-Verschlüsselung kann auf Basis von OpenPGP grundsätzlich geleistet werden, so der Verantwortliche dies wünscht und einen entsprechenden öffentlichen Schlüssel bereitstellt.

2.2 Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Tätigkeiten des Auftragsverarbeiters werden nicht in der Datenbank protokolliert. Ein Mitschnitt der Fernwartung (Videofile) wird spätestens auf Wunsch des Verantwortlichen angefertigt, wenn die Fernwartung über die reine Hilfestellung hinausgeht und Eingriffe am System vorgenommen werden. Ein Berechtigungskonzept existiert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

3.1 Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Die Daten werden in einem zweistufigen Backup-Verfahren sowohl ortsnah als auch ortsfern gesichert. Die ortsferne Sicherung erfolgt verschlüsselt. Die Sicherungen werden überwacht und protokolliert. Die Wiederherstellung wird stichprobenartig getestet. Eine Datensicherung wird an einem sicheren Ort aufbewahrt, diese ist verschlüsselt.

Die Vorhaltung der Daten erfolgt auf einem RAID Verbund. Der Serverraum verfügt über eine unterbrechungsfreie Stromversorgung, die Sensoren der Geräte überwachen diverse Umgebungsparameter, darunter auch die Temperatur. Im Brandfalle wird mit geeignetem Feuerlöscher gelöscht.

Der Serverraum liegt nicht unter sanitären Anlagen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO)

4.1 Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Die Zusammenarbeit zwischen Verantwortlichem und Auftragsverarbeiter ist in der zugehörigen AVV geregelt. So es zu Unterauftragsverhältnissen kommt, sind diese Auftragsverarbeiter sorgfältig ausgewählt. Ein Datenschutzbeauftragter ist bestellt, die Mitarbeiter sind auf die Verschwiegenheit verpflichtet.

Nach Beendigung des Auftrages werden alle personenbezogenen Daten vernichtet, so sie keinen anderweitigen Aufbewahrungsfristen unterliegen.

4.2 Datenschutzbeauftragter

Die GEFAK mbH hat einen externen Datenschutzbeauftragten bestellt, der dieses Datensicherheitskonzept mit erarbeitet und geprüft hat:

Henning Welz

von der Gesellschaft für Datenschutz Mittelhessen mbH, Auf der Appeling 8, 35043 Marburg

Tel: 06421 30979-0, E-Mail info@gdsm.de.