Allgemeine Beschreibung der„technischen und organisatorischen Maßnahmen (TOM)“ gemäß Art. 32 EU-DSGVO

Version vom 28.05.2020

WIZARD COMPUTERSYSTEME GMBH („WIZARD“) betreibt zwei eigene Rechenzentren in Bremervörde. Dort und temporär bei Servicearbeiten im Netzwerk des Kunden vor Ort oder durch Fernwartung wird ggf. Auftragsverarbeitung durchgeführt. In diesem Rahmen sind "technische und organisatorische Maßnahmen (im folgenden *TOM*)" notwendig, die im Folgenden beschrieben werden. Im Rechenzentrum sind folgende Sicherheitsmaßnahmen vorhanden:

- Zutritts- und Zugangskontrolle
- Alarmanlage und 24/7h-Video-Überwachung
- 24/7 Alarmüberwachung durch Sicherheitsdienst
- mit unterbrechungsfreier Stromversorgung (USV)
- mit Dieselgenerator-Notstrombetrieb
- redundant ausgelegte Klimatisierung
- Brandmeldeüberwachung
- mehrere Internet-Anbindungen
- eignes AS 12923 multi-homed
- Peerings über DECIX in Hamburg und Frankfurt
- mit 24/7 Routing-Überwachung und Administration
- RZ-Fläche in mehrere Brandabschnitte geteilt
- 2 redundante RZ mit gegenseitigem Backup

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung oder Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Diese TOM beschreiben die Maßnahmen, die im Zuständigkeitsbereich von WIZARD als Auftragsdatenverarbeiter liegen. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen behält sich WIZARD vor, sofern das Schutzniveau nach EU-DSGVO nicht unterschritten wird.

I. Pseudonymisierung

Grundsätzlich können Daten mit einem Pseudonym, d.h. einem nicht personenbezogenen Namen, einer Nummer oder Ähnlichem versehen werden, welches eine Zuordnung erschwert. Wichtig für eine wirksame Pseudonymisierung ist dabei, dass die pseudonymisierten Daten ohne Hinzuziehung zusätzlicher Informationen keine Zuordnung erlauben. Als Auftragsverarbeiter trifft WIZARD keine Maßnahmen zur Pseudonymisierung, es sei denn, dass der Auftraggeber WIZARD hierzu beauftragt oder wenn sich eine Pseudonymisierung aus den jeweiligen Leistungsbeschreibungen der Produkte / Dienstleistungen von WIZARD ergibt.

II. Verschlüsselung

Daten können verschlüsselt werden. Hierbei wird die Information mit Hilfe eines kryptografischen Verfahrens in eine nicht leserbare Zeichenfolge verwandelt. Bei der Nutzung der Verschlüsselung bleibt der Personenbezug der Daten erhalten. Die Daten werden jedoch auf Basis von mathematischen Algorithmen so verändert, dass sie ohne Kenntnis des zugehörigen Schlüssels mit der aktuell verfügbaren Technik nicht lesbar gemacht werden können.

Zur Verschlüsselung setzt WIZARD für den elektronischen Transport Verschlüsselungsverfahren ein, die dem Stand der Technik entsprechen und ein Schutzniveau erreichen, das den Anforderungen z.B. von Berufsgeheimnisträgern (wie Steuerberatern, Wirtschaftsprüfern, Rechtsanwälten, Ärzten usw.) angemessen ist.

Dies sind für den elektronischen Transport zwischen Rechenzentrum

(1) und dem Verantwortlichem: Verbindungen über VPN oder TLS mit Zertifikaten oder Zwei-Faktor-Authentifikation.
(2) und Einzelpersonen: abgesichert mit Verschlüsselungsverfahren nach dem Stand der Technik
(3) und Mitarbeitern von WIZARD: Verschlüsselte Verbindung mit Zertifikaten oder Zwei-Faktor-Authentifikation.
(4) Mobile Endgeräte der WIZARD-Mitarbeiter werden - sofern hier personenbezogene Daten verarbeitet werden - verschlüsselt und mit Passwort geschützt.

III. Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste

Es soll verhindert werden, dass es zu unbefugter oder unrechtmäßiger Verarbeitung kommt. Hierunter fallen Maßnahmen, welche den Zutritt, Zugang und Zugriff auf Systeme und Dienste regeln (Beispiele: Bauliche Maßnahmen, Zugangskontrollen, Zugriffsrechte, Alarmanlagen). Ebenso soll die Integrität der Systeme geschützt werden. Daten sollen stets richtig und verlässlich sein und dürfen nicht unbeabsichtigt oder schadhaft geändert oder zerstört werden können.

A. Vertraulichkeit

Unbefugten ist der Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten im Auftrag verarbeitet werden, zu verwehren. Die Vertraulichkeit von Systemen (Hardware) und Diensten (Software) setzt im Rahmen der Verarbeitung zwingend ein Zugriffskonzept voraus, das mit Gruppen- und Benutzerrechten arbeitet und den Zugriff auf einzelne Daten im Rahmen der Verarbeitung abhängig von den erforderlichen Prozessen ermöglicht. Hierzu gehören auch Maßnahmen der Zutrittskontrolle, der Zugangskontrolle und der Zugriffskontrolle.

1. Benutzer-/Rechteverwaltung - Authentifizierung

WIZARD hat für am IT-System zugelassene Benutzer und angelegte Benutzergruppen Rechteprofile erstellt. In Anlehnung an die Maßnahme M 2.31 des BSI IT-Grundschutz (Dokumentation der zugelassenen Benutzer und Rechteprofile) umfasst dies insbesondere folgende Angaben:

(1) Rechtevergabe an zugelassene Benutzer
  - ✓ zugeordnetes Rechteprofil
  - ✓ Begründung für die Wahl des Rechteprofils
  - ✓ Zuordnung des Benutzers zu einer Organisationeinheit
  - ✓ Befristung der Einrichtung / Löschen in Benutzergruppe

(2) Rechtevergabe an zugelassene Gruppen
  - ✓ zugehörige Benutzer
  - ✓ Zeitpunkt der Einrichtung
  - ✓ Befristung der Einrichtung

2. Zutrittskontrolle

(1) Die Standorte sind 24/7 verschlossen.
(2) Die Räumlichkeiten sind durch eine Alarmanlage, die an einen Wachdienst aufgeschaltet ist, gesichert.
(3) In den Bereichen der Rechenzentren erfolgt eine Videoüberwachung.
(4) Der Ladenbereich bei WIZARD ist wochentags durchgehend von 09:00 Uhr bis 12:30 und von 14:30 Uhr – 18:00 Uhr besetzt.
(5) Alle Personen müssen sich im Ladengeschäft anmelden. Vor Einlassgewährung wird Rücksprache mit dem Besuchten gehalten. Der Besucher wird am Empfang abgeholt und wird stets von einem WIZARD-Mitarbeiter begleitet.
(6) Zusätzlich sind im gesamten Gebäude für die einzelnen Bereiche Sicherheitsschlösser verbaut. Die Schlüsselvergabe ist strikt geregelt und dokumentiert. Schlüssel werden nur an WIZARD-Mitarbeiter vergeben, die auf den Datenschutz verpflichtet sind. Dritte erhalten keine Schlüssel.
(7) Außerhalb der Arbeitszeiten sind die Gebäudetüren per Sicherheitsschlüssel verschlossen.
(8) Der Zutritt zum WIZARD-Rechenzentrum ist nur speziell autorisierten Mitarbeitern von WIZARD gestattet.
(9) Die Geschäftsleitung von WIZARD prüft periodisch die Notwendigkeit von Zutrittsberechtigungen für die Mitarbeiter.

3. Zugangskontrolle

(1) Zunächst greifen alle Maßnahmen der voran beschriebenen Zutrittskontrolle.
(2) Alle Systeme im Rechenzentrum und im Verantwortungsbereich von WIZARD (Arbeitsplatz-PC’s, Server, Router, usw.) verfügen mindestens über ein Zugangskontrollsystem (UserID, Passwort). Es gibt vorgeschriebene Regeln zur Passwortvergabe. Dies betrifft die notwendige Komplexität, die Lebensdauer des Passwortes sowie die Wiederverwendung alter Passwörter.
(3) Zur Prüfung der Wirksamkeit der Absicherungsmaßnahmen werden bei sensiblen Systemen in Zeitabständen Penetrationen durchgeführt.
(4) Arbeitsplatz-PC-Sicherheit sowie WTS-Sitzungen:
  - ✓ Benutzerkennung mit mindestens 8-stelliger Passwortvergabe. Jeder User bekommt eine eigene Benutzerkennung mit eigenem Passwort. (Netzwerk Authentifizierung).
  - ✓ Automatische passwortgeschützte Bildschirm- und PC-Sperren.
  - ✓ Alle Mitarbeiter von WIZARD werden kontinuierlich angewiesen, ihre PC‘s bei kurzzeitigem Verlassen des Arbeitsplatzes zu sperren. Die Einhaltung dieser Anweisung wird strengstens überwacht.
  - ✓ Für alle Remote-Zugänge bei WIZARD geschieht der Zugang grundsätzlich mit einer 2-Faktor-Autorisierung.
(5) Zugangskontrolle zu Systemen zur Auftragsbearbeitung:
  - ✓ Die zur Benutzung von IT-Systemen Berechtigten dürfen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen.
  - ✓ Im Auftrag verarbeitete Daten dürfen bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.
  - ✓ Die eingesetzten IT-Systeme haben ein dediziertes Rechtesystem, das ermöglicht, Datenzugriffe und -veränderungen auf Basis von Rollen und individuellen Berechtigungen zu vergeben.
  - ✓ Es gibt vorgeschriebene Regeln zur Passwortvergabe.

4. Zugriffskontrolle

Innerhalb des WIZARD-Netzwerks werden für verschiedene User unterschiedliche Berechtigungsrollen vergeben. So wird gewährleistet, dass ein Nutzer nur auf solche Verzeichnisse oder Bereiche Berechtigungen erhält, die er auch sehen darf.

- ✓ Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen.
- ✓ Zusätzlich ist das WIZARD-Netzwerk in differenzierte Netzsegmente eingeteilt. User können folglich nur auf entsprechend freigegebene Server zugreifen.

5. Zugriff auf das Rechenzentrum

- ✓ Der Zugriff erfolgt nur über VPN-Verbindungen oder über WIZARD-eigene Punkt-zu-Punkt-Glasfaserstrecken.
- ✓ Die Datenübertragung zwischen WIZARD und den lokalen Netzen der Auftragnehmer oder anderen Kommunikationspartnern erfolgt soweit möglich verschlüsselt.
- ✓ Auf die Server der Auftraggeber im WIZARD-Rechenzentrum, im Rahmen der Auftragsverarbeitung, kann von den WIZARD-Mitarbeitern über das WIZARD-Firmennetzwerk nicht direkt zugegriffen werden. Hier erfolgt der Zugriff immer über eine dazwischengeschaltete Sicherheits-Ebene (Admin-Server). Hier werden auch alle Zugriffe kontinuierlich protokolliert und die Zugriffe von der WIZARD-Geschäftsleitung turnusmäßig stichprobenartig anhand der erteilten Auftragsverarbeitungs-Aufträge und den Einträgen im Ticket-System überprüft.
- ✓ Die IT-Systeme von WIZARD werden kontinuierlich auf die Wirksamkeit eingesetzter Maßnahmen gegen das Eindringen seitens unbefugter Dritter getestet.

6. Sicherheitsmaßnahmen bei Fernwartung

- ✓ Der Aufbau der Fernwartungsverbindung darf nur durch den Auftraggeber erfolgen; Fernwartungsarbeiten dürfen nur mit seiner Zustimmung begonnen werden.
- ✓ WIZARD protokolliert die Fernwartungsaktivitäten mit Datum, Uhrzeit und Benutzerkennung.

- ✓ WIZARD darf von den eingeräumten Zugriffsrechten nur in dem für die Durchführung der Fernwartungsarbeiten unerlässlich notwendigen Umfang Gebrauch machen.
- ✓ WIZARD darf personenbezogene Daten nur dann vom DV-System des Auftraggebers herunterladen und auf den eigenen Systemen speichern, wenn zuvor die Erlaubnis des Auftraggebers in Textform vorliegt.
- ✓ Der Auftraggeber ist berechtigt, die Fernwartungsarbeiten von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.
- ✓ WIZARD muss personenbezogene Daten, die bei der Fernwartung übermittelt wurden, unverzüglich löschen oder dem Auftraggeber zurückgeben, wenn sie für die Durchführung der Fernwartungsarbeiten nicht mehr erforderlich sind.

B. Integrität

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten ist zu reduzieren. Die Integrität von Systemen und Diensten erfordert die Absicherung gegen Manipulationen.
Dazu zählen:

- ✓ die Wahrung der referentiellen Sicherheit in Datenbanken
- ✓ die Protokollierung von Änderungen
- ✓ das Durchführen von Plausibilitätsprüfungen
- ✓ die Verhinderung der Eingabe ungültiger Werte
- ✓ die Verhinderung der ungewollten Löschung, Überschreibung oder Änderung von Daten

Es ist sicherzustellen, dass Programme und Daten nicht verfälscht und/oder falsche Daten verarbeitet werden, damit sie nicht unbemerkt fehlerhafte Ergebnisse erzeugen oder Funktionen ausführen, die nicht erwünscht sind.
Die persönliche Verantwortung jedes WIZARD-Mitarbeiters für die Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen wird bei WIZARD durch jährliche Schulungsmaßnahmen, weitergehende Seminare und zentral bereitgestellte Informationen gestärkt.
In den Sicherheitsbereichen des WIZARD-Rechenzentrums gilt ein grundsätzliches Fotografierverbot. Das Verbot ist für alle Benutzer verbindlich geregelt, es wird von den Führungskräften und vom Sicherheitsdienst überwacht.
Für den Sicherheitsbereich des WIZARD-Rechenzentrums haben nur wenige, besonders autorisierte Mitarbeiter Zutritt. Jeder Zutritt wird protokolliert.

1. Weitergabekontrolle

WIZARD stellt sicher, dass personenbezogene Daten bei der elektronischen Übertragung, beim Transport oder bei der Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Hierzu wählt WIZARD geeignete Maßnahmen wie Verschlüsselung o.Ä. bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger.
Sicherung bei der elektronischen Übertragung:

- ✓ Bei der elektronischen Übertragung von Auftragnehmerdaten in das WIZARD-Rechenzentrum sind alle Verbindungen über einen VPN-Tunnel verschlüsselt.
- ✓ Die elektronische Übertragung von Auftragnehmerdaten in das WIZARD Rechenzentrum wird protokolliert.
- ✓ Bevor die elektronische Übertragung stattfindet, wird geprüft, ob diese zulässig ist.

Sicherung bei der Lagerung und Transport:

- ✓ Es besteht ausreichender Zugriffsschutz zwischen dem Speichern der Daten auf den Datenträgern und dem Transport. Die Datenträger liegen in Bremervörde in einem gesicherten Raum und dort in Datensicherungsschränken, die nur Mitarbeitern mit einer entsprechenden Berechtigung zugänglich sind.
- ✓ Der Transport von Sicherungsdatenträgern wird ausschließlich durch eigene WIZARD-Mitarbeiter in verschlossenen speziellen Transportboxen durchgeführt.
- ✓ Alle Datenexporte verlassen das Unternehmen nur verschlüsselt.
- ✓ Datenexporte werden durch das Vier-Augen-Prinzip geprüft

2. Eingabekontrolle

Maßnahmen zur Gewährleistung der nachträglichen Überprüfung und Nachvollziehbarkeit der Datenverwaltung und -pflege, insbesondere hinsichtlich Eingabe, Veränderung oder Löschung von Daten.
Scannen von Dokumenten:

- ✓ Im Scanprozess wird protokolliert, welcher Mitarbeiter ein Dokument bearbeitet hat.
- ✓ Alle Vorgänge werden protokolliert. Protokolle werden stichpunktartig ausgewertet.

Erfassung von Kundendaten:

- ✓ WIZARD erfasst nur Kundendaten, die auftragsrelevant sind.

3. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten lediglich entsprechend den Weisungen des jeweiligen Auftraggebers verarbeitet werden.
WIZARD hat hierzu die folgenden Maßnahmen festgelegt:

- ✓ Schriftliche Vereinbarungen und Verträge
- ✓ Klare Abgrenzung der Kompetenzen und Pflichten zwischen WIZARD und Auftraggeber
- ✓ Festlegung der Sicherheitsmaßnahmen
- ✓ Weisungsbefugnisse eindeutig definiert
- ✓ Vor-Ort-Kontrollen
- ✓ Vereinbarungen zur Auftragsverarbeitung nach Art. 28 der EU-DSGVO

4. Trennungskontrolle

Es ist sicher zu stellen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können.
Stichpunktartig hier die wichtigsten Maßnahmen, die WIZARD umgesetzt hat:

- ✓ Trennung von Produktiv- und Test-System
- ✓ Getrennte Ordnerstrukturen (Mandantenfähigkeit)
- ✓ Getrennte Tables in der Datenbank
- ✓ Getrennte Datenbanken
- ✓ Getrennte Server

5. Löschen von Daten

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es die Zwecke, für die sie verarbeitet werden, erforderlich machen. Die Leistungsbeschreibungen von WIZARD für Produkte und Dienstleistungen (einsehbar unter www.wizard.de), die Kundenaufträge und die Vereinbarungen zur Auftragsverarbeitung nach Art. 28 der EU-DSGVO mit den Auftraggebern sehen hier verschiedene Löschkonzepte vor.
Vernichtung von Datenträgern:
Datenträger werden zentral in eigens hierfür vorgehaltenen verschlossenen speziellen Behältern bei WIZARD zwischengelagert und nach spätestens 6 Monaten nach DIN-66399 („Büro- und Datentechnik – Vernichtung von Datenträgern Teil 3: Prozess der Datenträgervernichtung, Februar 2013" nach Schutzklasse 3 und Sicherheitsstufe 4) von einem externen Entsorger Datenschutz-konform vernichtet, mit dem WIZARD eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 EU-DSGVO hat.
Die Löschung von Kundendaten auf ASP-, und Server-Housing-Systemen oder bei Cloud-Speicher-Lösungen liegt in der Verantwortung der Auftraggeber und wird von WIZARD nur nach ausdrücklicher schriftlicher Weisung durchgeführt. Die Aufbewahrungsfristen der Daten werden im Rahmen der vertraglichen Beauftragung durch den Kunden vorgegeben bzw. ergeben sich aus den gesetzlichen Aufbewahrungsfristen.

6. Mandantentrennung

Zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet. Daten von Auftraggebern werden im Rahmen der Auftragsverarbeitung getrennt verarbeitet, verwaltet und logisch getrennt.

7. Protokollierung

Die Verarbeitung von manuell im Auftrag verarbeiteten Daten werden grundsätzlich protokolliert und der Verantwortliche (Auftraggeber) erhält jeweils umgehend nach der Tätigkeit per E-Mail eine Beschreibung der durchgeführten Arbeiten.
Die Dateneingabe und die Verarbeitung der im Auftrag verarbeiteten Daten erfolgen ausschließlich nach dem mit dem Auftraggeber festgelegten Verfahren.

C. Verfügbarkeit

WIZARD stellt sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden. Alle Alarmierungspläne, Handlungsanweisungen, Notfallregelungen sowie Wiederanlaufpläne sind in einem elektronischen Notfallhandbuch festgehalten. WIZARD führt eine laufende Überwachung der Nutzung der Dienste und der Auslastung der Systeme durch. WIZARD hat ein Notfallkonzept umgesetzt, das z. B. Maßnahmen zur Abwehr von Angriffen aus dem Internet beinhaltet. Dieses Notfallkonzept wird laufend fortgeschrieben und regelmäßig auf Wirksamkeit geprüft.
Für die IT-Infrastruktur von WIZARD sind hier einige wesentliche Maßnahmen stichpunktartig genannt:

- ✓ Zugangskonzept für das Gebäude
- ✓ redundante Storagesysteme
- ✓ Mehrstufiges Backupkonzept
- ✓ RAID Verfahren bei Storagesystemen
- ✓ Datenübertragung und Datenspiegelung
- ✓ Cluster-Betrieb und redundante Systeme
- ✓ Server werden live überwacht
- ✓ WIZARD hält Ersatzteile und Ersatzgeräte vor bzw. hat mit Herstellern Wartungsverträge mit entsprechenden Service-Level-Agreements (SLA) und kurzen Reaktionszeiten, um bei einem Komponentenausfall umgehend einen Ersatzbetrieb sicherstellen zu können, der geeignet ist, die Rechenzentrumsleistungen grundsätzlich aufrecht zu erhalten.
- ✓ Regelmäßige Wartungen gewährleisten die Betriebsbereitschaft, die Leistungsfähigkeit sowie das Qualitätsniveau der Systeme.
- ✓ Das Einspielen von Patches und Hotfixes erfolgt regelmäßig, sobald diese verfügbar sind und nach WIZARD-internen Tests freigegeben wurden.
- ✓ Die Server- und Storage-Systeme im WIZARD-Rechenzentrum werden durch den Einsatz von Managed-Service-Softwareagenten permanent überwacht.
- ✓ Das Monitoring und das Management der gesamten RZ-Systemlandschaft trägt zum Erhalt der Betriebsbereitschaft sowie der Leistungsfähigkeit der Systeme bei.

D. Belastbarkeit

Die Belastbarkeit umfasst u.a., dass Systeme ausreichend dimensioniert sind, um Verarbeitungen ohne Ausfälle und Wartezeiten durchführen zu können. Ebenso ist hiermit die Toleranz eines Systems gegenüber Störungen gemeint, die in der IT allgemein als „Resilienz" beschrieben wird („Resiliens" = die Fähigkeit von technischen Systemen, bei Störungen bzw. Teil-Ausfällen nicht vollständig zu versagen, sondern wesentliche Systemdienstleistungen aufrechtzuerhalten). Dies umfasst auch die Ausfallsicherheit der IT-Systeme und Dienste.
Die für unternehmenskritische Prozesse eingesetzten IT-Systeme sind hochredundant ausgelegt. WIZARD verfügt über eine skalierbare IT-Architektur, die eine schnelle und flexible Reaktion auf die Veränderung der Bedingungen durch Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall sicherstellt.
An dieser Stelle sei auch auf den Notfallplan von WIZARD verwiesen. Sämtliche Maßnahmen werden durch permanentes Monitoring überwacht und dokumentiert. Zusätzlich prüft WIZARD durch regelmäßige Wiederanlauf-Tests die ordentliche Funktionsweise aller getroffenen Maßnahmen.
Für die Anbindung von lokalen Kunden-Netzwerken an das Internet bietet WIZARD den abgesicherten Internet-Zugang eZEUS. Bei eZEUS sorgt eine Vielzahl von Mechanismen für die Absicherung gegen Gefahren aus dem Internet (z.B. Proxy-Systeme, Firewalls, Viren-Scanner, Filter-Systeme usw.).

IV. Wiederherstellbarkeit

Als weitere technische Maßnahme beschreibt Art. 32 Abs. 1 lit. c) DSGVO die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.
Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu diesen durch einen physischen oder technischen Zwischenfall ist zu reduzieren.
WIZARD hat hierzu u.a. folgende Maßnahmen etabliert:

- ✓ Sicherung der Installationen
- ✓ Sicherung der Daten
- ✓ Sicherung von Systemdateien und Datencontainern
- ✓ Sicherung von LOG-Dateien
- ✓ Sicherung von Benutzerkonten

V. Organisatorische Maßnahmen

Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen und zur Gewährleistung der Sicherheit der Verarbeitung bei WIZARD etabliert.
Die Einsicht der Protokolle der Hard- und Software-Komponenten der Infrastruktur gehört zu den täglichen Aufgaben des zuständigen IT-Administrators. Darüber hinaus ist ein System der Benachrichtigung bzw. Alarmierung bei automatisierten Vorgängen eingerichtet.