Technische und organisatorische Maßnahmen

Grundeigentümer-Verband Hamburg von 1832 e.V.

Glockengießerwall 19

20095 Hamburg

Die personenbezogenen Daten der Online-Formulare werden in einem Rechenzentrum in Köln verarbeitet. Die technischen und organisatorischen Maßnahmen leiten sich weitgehend von den Maßnahmen des Rechenzentrum-Betreibers ab.

Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1	Zutrittskontrolle
Maßnahmen der Zutrittskontrolle, die es Unbefugten verwehren, sich den IT-Systemen, Datenverarbeitungsanlagen sowie den vertraulichen Akten und Datenträgern physisch zu nähern.	
Sicherheitsbereich Rechenzentrum: Festgelegte Sicherheitsbereiche Individuelle Zutrittsberechtigungsvergabe Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt nur für autorisierte Personen Dokumentation von Zutrittsberechtigungen Zutrittsdokumentation Rollenabhängige Zutrittsregelungen für die Mitarbeiter Sicherheitsbereich mit Eingangskontrolle **Sicherheitsbereich Geschäftsräume:** Empfang Zentrales Schliesssystem Zeitschloss, ab 18 Uhr kein Zutritt ohne Schlüssel Tägliche Kontrolle durch Sicherheitsdienst Serverräume durch elektronisches System und Einbruchmeldesysteme zusätzlich gesichert	

2	Zugangskontrolle

Maßnahmen der Zugangskontrolle, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Sicherheitsbereich Rechenzentrum und Geschäftsräume:

Zusätzliche Zugangsbeschränkung der Serverräume

Änderung der Standardkennwörter aller System- und Infrastrukturkomponenten

Protokollierung von Rechenzentrum Mitarbeitern relevanten Aktivitäten (Anmeldung, Abmeldung,

Zugangsverweigerungen, etc.)

Schutz der Infrastruktur durch Hardware-Firewalls

Schutz der Infrastruktur durch Einbruchmeldeanlagen

Zugangsbeschränkungen für bestimmte IP-Adressbereiche

VPN-Beschränkungen

Portregeln/Sperrung von nicht erforderlichen Ports

Externer Zugang nur über sichere Verbindungen (VPN, RDP, SSL oder vergleichbar)

W-LAN-Verschlüsselung

Antivirus-Software auf allen Systemen

Regelmäßige Software-Updates

Benutzerauthentifizierung für Systemzugang- und/oder Anwendungszugriff erforderlich

Verschlüsselte Speicherung von User-Passwörtern

Vertraulichkeitserinnerungen

Interne und ggf. externe Audits

Netzwerksegmentierung

3	Trennungskontrolle

Ist im Unternehmen die Trennungskontrolle gewährleistet, indem personenbezogenen Daten so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist?

Sicherheitsbereich Rechenzentrum und Geschäftsräume:

Logische Datentrennung: Separate Datenbanken oder strukturierte Dateiablage

Separate Instanzen für Entwicklungs- und Produktivsysteme (Sandboxes)

Spezifische Genehmigungsregelung für die Datenbank und den Anwendungszugriff / Berechtigungskonzept

4	Zugriffskontrolle

Maßnahmen der Zugriffskontrolle, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Sicherheitsbereich Rechenzentrum:

Schriftliche Verpflichtung aller Mitarbeiter auf das Datengeheimnis

Rollenbasiertes Berechtigungskonzept

Dokumentation der Vergabe von Zugriffsrechten

Strenge administrative Aufgabentrennung

Geregeltes Löschen / Entsorgen von Datenträgern wie Festplatten, CDs, DVDs, USB-Sticks

Vernichtung von physikalischen Medien nach DIN 32757 oder vergleichbaren Standards

Regelmäßige Sicherheitsprüfungen

Kontrollierter Zugang zu E-Mails und Internet

Trennung von Anwendungs- und Administrationszugängen

Regelmäßige Sicherheits-Updates

Nutzung eines Aktenvernichters

Überwachung und Protokollierung allgemeiner Benutzeraktivität

Verbot der Nutzung von privaten Datenträgern

Sicherheitsbereich Geschäftsräume:

Schriftliche Verpflichtung aller Mitarbeiter auf das Datengeheimnis

Rollenbasiertes Berechtigungskonzept

Geregeltes Löschen / Entsorgen von Datenträgern wie Festplatten, CDs, DVDs, USB-Sticks

Regelmäßige Sicherheitsprüfungen

Kontrollierter Zugang zu E-Mails und Internet

Regelmäßige Sicherheits-Updates

Nutzung eines Aktenvernichters

Verbot der Weitergabe von Kennwörtern

Verbot der Nutzung von privaten Datenträgern

Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

5	Eingabekontrolle

Maßnahmen der Eingabekontrolle die feststellen, wer personenbezogene Daten in Systeme eingegeben, geändert oder entfernt hat und die die Überprüfbarkeit dessen gewährleisten.

Sicherheitsbereich Rechenzentrum:

Rollenabhängige Zugriffsbeschränkungen

Applikationsbasierte Überprüfung der Eingabeberechtigung

Protokollierung der relevanten Prozesse (Speicherung, Verarbeitung, Modifizierung, Abrufen,

Übertragung, Löschung, etc.)

Protokollierung von administrativen Änderungen

Konzept zur Datenlöschung

Sicherheitsbereich Geschäftsräume:

Rollenabhängige Zugriffsbeschränkungen

Applikationsbasierte Überprüfung der Eingabeberechtigung

Konzept zur Datenlöschung

6	Weitergabekontrolle

Maßnahmen der Weitergabekontrolle die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur kontrolliert und dokumentiert weitergegeben werden.

Sicherheitsbereich Rechenzentrum:

Weitergabe nur nach Weisung

Sicherheitsbereich Geschäftsräume:

Verschlüsselung von Datenträgern

Fernwartungskonzept

Weitergabe nur nach Weisung

Transportverschlüsselung

Allgemeine Verschlüsselung

Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

7	Verfügbarkeitskontrolle

Schutzmaßnahmen der Verfügbarkeitskontrolle gegen einen zufälligen Verlust oder eine zufällige Zerstörung von elektronischen Daten, Akten und Datenträgern.

Sicherheitsbereich Rechenzentrum:

Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag

Unterbrechungsfreie-Stromversorgung (USV)

Feuer und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr

Ein flächendeckendes Wasser- und Brandfrühsystem (VESDA) reagiert bereits bei geringer Überschreitung definierter Grenzwerte, um größere Schäden zu verhindern

Kühl- und Löschgassystem

Disaster-Recovery-Mechanismen für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust

Tägliche inkrementelle Datensicherung

Wöchentliche vollständige Datensicherung

Wöchentliche Backups auf separat gespeicherten physischen Medien oder auf physikalisch getrennten Systemen

Der Kraftstoffvorrat ist für mindestens 16 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich

Geräte zur Überwachung der Temperatur und Feuchtigkeit

Notfallplan

Externe Audits und Sicherheitstests

Klar definierte Verwaltungsaufgaben für Auftraggeber und Auftragnehmer

Sicherheitsbereich Geschäftsräume:

Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag

Unterbrechungsfreie-Stromversorgung (USV)

Feuer und/oder Rauchmelder verfügt über eine direkte Aufschaltung zu einem örtlichen Wachdienst

Disaster-Recovery-Mechanismen für die Datenwiederherstellung

Tägliche inkrementelle Datensicherung an zwei Standorten

Automatisierte Überprüfung auf Funktionsfähigkeit der Datensicherung

Notfallplan

Klar definierte Verwaltungsaufgaben für Auftraggeber und Auftragnehmer

Automatisierte Backuptests

Verfahren zur regelmäßigen Überprüfung und Bewertung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

8	Auftragskontrolle

Maßnahmen der Auftragskontrolle die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Sicherheitsbereich Rechenzentrum und Geschäftsräume:

Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers

Definition von Rollen für unterschiedliche Aufgaben

Aufteilung der Zuständigkeiten

Festgelegte Ansprechpartner für Änderungsanfragen

Regelmäßige Kontrolle externer Dienstleister

Regelmäßige Datenschutz-Unterweisung der Mitarbeiter

Regelmäßige Besprechungen mit den bestellten Datenschutzbeauftragten in Bezug auf Betriebsprozesse, welche die Verarbeitung von personenbezogenen Daten betreffen

Verpflichtung der Mitarbeiter auf das Datengeheimnis

Kontrollrechte der Auftraggeber bei der Auftragsdatenverarbeitung

Subunternehmer werden auf die gleichen Regelungen und Bestimmungen verpflichtet wie der Grundeigentümer-Verband selbst

Automatisierte Kontrollmechanismen oder technische Beschränkungen, mit denen die Datenverarbeitung entsprechend den Weisungen des Auftraggebers sichergestellt wird

Fern-Zugriff erfolgt nur mit starker Verschlüsselung, erfordert eine Benutzerauthentifizierung und unterliegt strikten Regeln zur Zugriffsbeschränkung