ght GmbH Elektronik im Verkehr
Schafhofstraße 2
90411 Nürnberg

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß DSGVO

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

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen ist zu reduzieren.

>> Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen, etc.

Technische und organisatorische Maßnahmen:

- Abgestufte Zutrittsregelung.
- Zutrittsrechte werden über Schlüsselregelung dokumentiert.
- Während der Geschäftszeiten ist der Empfang dauerhaft besetzt (Besucheranmeldung).
- Zutritt für Gäste (Wartungstechniker, Lieferanten, Besucher etc.) nur unter Aufsicht.

>> Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern, etc.

Technische und organisatorische Maßnahmen:

- Es existiert eine Passwort- und Benutzerverwaltung.
- Ein vom System vorgegebener Änderungszyklus der Benutzerpasswörter an allen Computerarbeitsplätzen ist eingerichtet (Änderungszyklus).
- An Arbeitsplatzrechnern, an welchen personenbezogene Daten verarbeitet werden, sind Bildschirmschoner eingerichtet, welche nach 15 Minuten aktiviert werden und nur durch erneute Passworteingabe entsperrt werden können.
- An Terminal-Servern, an welchen personenbezogene Daten verarbeitet werden, erfolgt eine Zwangstrennung bei Inaktivität nach dreißig Minuten. Ein erneutes Anmelden ist nur durch Passworteingabe möglich.

>> Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen, etc.

Technische und organisatorische Maßnahmen:

- Benutzerprofile sind mit Lese- und teilweise Schreibrechten versehen.
- Datenzugriffe werden protokolliert und im Verdachtsfall ausgewertet.
- Datenzugriffe werden über abgestufte Verzeichnisberechtigungen gewährt.

>> Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing, etc.

Technische und organisatorische Maßnahmen:

- Softwareseitiger Ausschluss (Mandantentrennung)
- Dateiseparierung
- Trennung über Zugriffsregelung (Datenbankprinzip)

>> Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Technische und organisatorische Maßnahmen:

- Als Auftragsverarbeiter trifft die ght GmbH zusätzlich zu Maßnahmen die durch den Verantwortlichen im Rahmen der Beauftragung vorgenommen werden, keine weiteren Maßnahmen zur Pseudonymisierung.

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

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.

>> Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur, etc.

Technische und organisatorische Maßnahmen:

- Protokollierung der Datenübermittlungsstelle/-wege, welche im Verdachtsfall ausgewertet werden können.
- Externe Zugriffe erfolgen über VPN Clients.

>> Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Dokumentenmanagement, Protokollierung, etc.

Technische und organisatorische Maßnahmen

- Externe Zugriffe erfolgen über VPN Clients.
- Schulungsmaßnahmen für Softwarenutzung
- Zugriffs- und Änderungsprotokollierung auf Datenbankebene.

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

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 Nichtverfügbarkeit von im Auftrag verarbeiteten Daten ist zu reduzieren.

>> Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/ offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Meldewege und Notfallpläne; Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO), etc.

Technische und organisatorische Maßnahmen:

- Durchführung von stündlichen, täglichen und wöchentliche Backups nach definiertem Backupplan
- Einsatz von USV-Geräten
- Einsatz von RAID-Systemen
- Einsatz von Hot-Standby Redundanz-Systemen
- Einsatz von Cold-Standby Redundanz-Systemen

>> Belastbarkeit der Systeme

Datenverarbeitungssysteme & – Dienste müssen auch belastbar sein. Dies bedeutet einerseits, dass etwa ein Webserver auch bei kurzfristig starker Beanspruchung durch viele gleichzeitige Anfragen zuverlässig die angeforderten Daten liefert, als auch die Fähigkeit, externen Angriffen etwa durch Hacker zu widerstehen bzw. diese zu überstehen, z.B. Skalierende Systeme, Denial of Service – Abwehrtechniken, RAID-Systeme, Virenschutz, Firewall.

Technische und organisatorische Maßnahmen:

- Es existieren Sicherheitseinrichtungen wie Firewall, Virenschutz, VPN Zugänge, Netzwerkkennungen.
- Die Firewall verfügt über Erkennungsmechanismen für DoS und DDoS Angriffe.
- Server werden virtualisiert betrieben. CPU und Speicher werden dynamisch zugewiesen.
- Alle Server werden auf RAID Systemen mit einer Fehlertoleranz von mindestens einer HDD pro RAID betrieben.

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

Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu betreiben.

>> Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Technische und organisatorische Maßnahmen:

- Es wird keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen durchgeführt.

>> Innerbetriebliche Organisation

a. Prozesse, die zur Einhaltung der technisch- organisatorischen Maßnahmen dienen wie z.B. Interne Verhaltensregeln, Datenschutzmanagementsystem, Audits (ISO 27001) etc.

b. Prozesse der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen im IT-Bereichen wie z.B. Datensicherheitskonzept, Störfallplan, Wiederanlaufplan.

c. Einhaltung des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy by Design/Privacy by Default) z. B. Auswahl datenschutzfreundlicher Technologien bei der Beschaffung

Technische und organisatorische Maßnahmen:

a. <u>Datenschutzmanagement</u>

- Nur Mitarbeiter die auf die Einhaltung der datenschutzrechtlichen Vorgaben verpflichtet wurden, dürfen die für ihren Aufgabenbereich entsprechenden Daten verarbeiten.
- Es existieren interne Verhaltensrichtlinien sowie ein Datenschutz Handbuch.
- Alle Mitarbeiter werden in regelmäßigen Abständen (min. jährlich) zum Thema Datenschutz per E-Learning geschult und sensibilisiert.
- In einem Organigramm sowie in Stellenbeschreibungen sind Verantwortlichkeiten und Befugnisse der einzelnen Mitarbeiter festgelegt und im Unternehmen bekannt gemacht. Dieses wird in regelmäßigen Abständen von der obersten Leitung im Rahmen der ISO 9001 Zertifizierung überprüft.

b. <u>Störfallmanagement</u>

- Die Einhaltung der technisch- organisatorischen Maßnahmen werden jährlich (Audit) durch den Datenschutzbeauftragten überprüft und gegebenenfalls angepasst.

c. <u>Datenschutz durch Technikgestaltung</u>

- Auswahl datenschutzfreundlicher Technologie bei der Beschaffung
- (Fern)zugriffe erfolgen ausschließlich über verschlüsselte Verbindungen