

Technische und organisatorische Maßnahmen

der

Grasenhiller GmbH
Sachsenstraße 2
92318 Neumarkt

Die nachfolgende Übersicht der technischen und organisatorischen Maßnahmen erfüllt die Auskunftspflicht der Fa. Grasenhiller GmbH, Neumarkt gegenüber Dritter gemäß Art. 32 DSGVO

Die mit markierten Punkte werden als Lösungen für die Anforderungen nach Art. 32 DS-GVO durch die Grasenhiller GmbH umgesetzt und eingehalten.

Detaillierte Auskünfte zu einzelnen Punkte können nach Rücksprache bei der Geschäftsleitung durch den Datenschutzbeauftragten mündlich erteilt werden.

Die Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen werden durch die Grasenhiller GmbH und den Datenschutzbeauftragten mindestens einmal jährlich geprüft.

Freigabe: 19.02.2024
Version: 2.7
Vertraulichkeitsstufe: öffentlich

I. Vertraulichkeit (Art. 32 Abs. 1 lit. BDS-GVO)

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- | | |
|---|--|
| <input type="checkbox"/> Alarmanlage | <input checked="" type="checkbox"/> Chipkarten-/Transponder-Schließsystem |
| <input type="checkbox"/> Schließsystem mit Codesperre | <input checked="" type="checkbox"/> Manuelles Schließsystem |
| <input type="checkbox"/> Biometrische Zugangssperren | <input type="checkbox"/> Videoüberwachung der Zugänge |
| <input type="checkbox"/> Lichtschranken / Bewegungsmelder | <input checked="" type="checkbox"/> Sicherheitsschlösser |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Personenkontrolle beim Pfortner / Empfang |
| <input type="checkbox"/> Protokollierung der Besucher | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |
| <input checked="" type="checkbox"/> Besucher nur in Begleitung von Mitarbeitern | |

2. Zugangskontrolle

Der Auftragnehmer sorgt dafür, dass die Personen, die berechtigt sind, das Datenverarbeitungssystem des Auftragnehmers zu nutzen, lediglich Zugang zu solchen Daten haben, die von ihrer Zugangsautorisierung abgedeckt sind. Dies geschieht durch:

- | | |
|--|---|
| <input checked="" type="checkbox"/> Zuordnung von Benutzerrechten | <input checked="" type="checkbox"/> Erstellen von Benutzerprofilen (Prozess zur Rechtvergabe bei Neueintritt, bei Abteilungswechsel und beim Austritt von Mitarbeitern) |
| <input checked="" type="checkbox"/> Passwortvergabe - Kennwortverfahren | <input type="checkbox"/> Authentifikation mit biometrischen Verfahren |
| <input checked="" type="checkbox"/> Authentifikation mit Benutzername / Passwort | <input checked="" type="checkbox"/> Zuordnung von Benutzerprofilen zu IT-Systemen |
| <input checked="" type="checkbox"/> Authentifizierung mit Chipkarten an MFP's | <input checked="" type="checkbox"/> Einsatz von VPN-Technologie |
| <input type="checkbox"/> Sperren von externen Schnittstellen (USB etc.) | <input checked="" type="checkbox"/> Sicherheitsschlösser |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input checked="" type="checkbox"/> Einsatz einer Software-Firewall |
| <input type="checkbox"/> Protokollierung der Besucher | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input checked="" type="checkbox"/> Einsatz einer Hardware-Firewall | <input checked="" type="checkbox"/> Automatische Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner) |
| <input checked="" type="checkbox"/> Passwortpolicy mit Mindestvorgaben | <input type="checkbox"/> Verschlüsselung von mobilen Datenträgern |
| <input type="checkbox"/> Verschlüsselung von Smartphone-Inhalten | <input checked="" type="checkbox"/> Kontrollierte Vernichtung von Datenträgern |

- | | |
|---|--|
| <input checked="" type="checkbox"/> Einsatz von Anti-Viren-Software | <input type="checkbox"/> Verschlüsselung von Datenträgern in Laptops / Notebooks |
| <input checked="" type="checkbox"/> Richtlinie Clean Desk | <input checked="" type="checkbox"/> Allg. Richtlinie Datenschutz und/oder Sicherheit |
| <input checked="" type="checkbox"/> Mobile Device Policy | |

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- | | |
|--|---|
| <input type="checkbox"/> Erstellen eines Berechtigungskonzepts | <input checked="" type="checkbox"/> Verwaltung der Rechte durch Systemadministrator |
| <input checked="" type="checkbox"/> Anzahl der Administratoren auf das „Notwendigste“ reduziert | <input checked="" type="checkbox"/> Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel |
| <input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | <input checked="" type="checkbox"/> Sichere Aufbewahrung von Datenträgern |
| <input checked="" type="checkbox"/> physische Löschung von Datenträgern vor Wiederverwendung | <input checked="" type="checkbox"/> ordnungsgemäße Vernichtung von Datenträgern |
| <input checked="" type="checkbox"/> Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) | <input checked="" type="checkbox"/> Protokollierung der Vernichtung von Datenträgern |
| <input type="checkbox"/> Verschlüsselung von Datenträgern | <input checked="" type="checkbox"/> Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken |
| <input checked="" type="checkbox"/> Regelung zur Wiederherstellung von Daten aus Backups | <input checked="" type="checkbox"/> Einsatz eines Spam-filters |

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- | | |
|---|---|
| <input checked="" type="checkbox"/> physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern | <input checked="" type="checkbox"/> Logische Mandantentrennung (softwareseitig) |
| <input checked="" type="checkbox"/> Erstellung eines Berechtigungskonzepts | <input type="checkbox"/> Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden |

- | | |
|---|---|
| <input type="checkbox"/> Versehen der Datensätze mit Zweckattributen/Datenfeldern | <input type="checkbox"/> Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System |
| <input checked="" type="checkbox"/> Festlegung von Datenbankrechten | <input checked="" type="checkbox"/> Trennung von Produktiv- und Testsystem |

II. Integrität (Art. 32 Abs. 1 lit. A und b DS-GVO)

1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- | | |
|--|---|
| <input checked="" type="checkbox"/> Einrichtungen von Standleitungen bzw. VPN-Tunneln | <input type="checkbox"/> Weitergabe von Daten in anonymisierter oder pseudonymisierter Form |
| <input checked="" type="checkbox"/> E-Mail-Verschlüsselung | <input type="checkbox"/> Erstellen einer Übersicht von regelmäßigen Ab- und Übermittlungsvorgängen |
| <input type="checkbox"/> Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen | <input checked="" type="checkbox"/> Beim physischen Transport: sichere Transportbehälter/-verpackungen |
| <input checked="" type="checkbox"/> Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen | <input checked="" type="checkbox"/> Datenaustausch über https-Verbindung |
| <input checked="" type="checkbox"/> Dokumentierte Verwaltung von Datenträgern - Bestandskontrolle | <input checked="" type="checkbox"/> Papierentsorgung mit Shredder gemäß Sicherheitsstufe mind. Stufe 3, cross cut |
| <input checked="" type="checkbox"/> Datenträgerentsorgung – sicheres Löschen durch physikalische Zerstörung oder durch Überschreiben der Festplatten | <input checked="" type="checkbox"/> Einsatz von VPN |
| <input checked="" type="checkbox"/> Bei Weitergabe: Übergabe mit Protokoll | <input checked="" type="checkbox"/> Dokumentation der Datenempfänger sowie deren Dauer der geplanten Überlassung mit Löschfristen |

2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter auf das Datengeheimnis | <input checked="" type="checkbox"/> Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. (Verfahrensverzeichnis) |
| <input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) | <input type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Klare Zuständigkeit für Löschungen

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Datensicherungskonzept
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal
- RAID-System/Festplattenspiegelung
- Getrennte Partitionen für Betriebssysteme und Daten
- Kontrolle des Sicherungsvorgangs

2. Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

Systeme müssen die Fähigkeit besitzen, mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.

- Backup-Verfahren – Datenspeicherung auf RAID-Systemen
- Räumlich getrennte Aufbewahrung von Sicherungsdatenträgern
- Unverzögliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates
- Verwendung redundanter Serversysteme als Ausfallsicherheit und zur Aufrechterhaltung des Betriebs in Aktualisierungs- und Updatephasen

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. D DS-GVO; Art. 25 Abs. 1 DS-GVO)

1. Organisationskontrolle

Anforderungen aus diesem Vertrag werden in internen Sicherheitsrichtlinien umgesetzt.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Interne IT-Sicherheitsrichtlinie, Arbeitsanweisungen, Prozessbeschreibungen und Regelungen für Tests und Freigabe neuer Verfahren | <input checked="" type="checkbox"/> Externer Datenschutzbeauftragter:
Oliver Fouquet, Fürther Straße 98-100, 90429 Nürnberg, Tel.: 0911/3238653, Mobil: 0176 767 14 298, E-Mail info@metropoldata.de |
| <input checked="" type="checkbox"/> Mitarbeiter geschult und auf das Datengeheimnis verpflichtet | <input checked="" type="checkbox"/> Regelmäßige Sensibilisierung der Mitarbeiter (jährlich) |
| <input checked="" type="checkbox"/> Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz | <input checked="" type="checkbox"/> Datenschutzfolgeabschätzung wird bei Bedarf durchgeführt |
| <input checked="" type="checkbox"/> Die Organisation erfüllt die Informationspflichten nach Art. 13 und 14 DSGVO | <input checked="" type="checkbox"/> Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen |
| <input checked="" type="checkbox"/> Ein Überprüfung der Wirksamkeit der Technischen Maßnahmen wird mind. Jährlich durchgeführt. | <input checked="" type="checkbox"/> Prozess zur Erkennung von Datenpannen |
| <input checked="" type="checkbox"/> Einbindung des DSB und ISB in Sicherheitsvorfälle und Datenpannen | <input checked="" type="checkbox"/> Nachbearbeitung von Datenpannen |

2. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Art. 5, Abs. 1 DSGVO und §§ 53, 62 BDSG)

- | | |
|---|--|
| <input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) | <input checked="" type="checkbox"/> Die Vertragsdurchführung erfolgt weisungsgebunden und wird regelmäßig kontrolliert |
| <input checked="" type="checkbox"/> schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) | <input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis |
| <input checked="" type="checkbox"/> Auftragnehmer hat Datenschutzbeauftragten bestellt | <input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
| <input checked="" type="checkbox"/> Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation | <input checked="" type="checkbox"/> Beauftragung auf Basis eines AV-Vertrags nach DSGVO bzw. EU-Standardvertragsklauseln |
| <input checked="" type="checkbox"/> Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer | <input checked="" type="checkbox"/> Regelung zum Einsatz von Subunternehmern |
| <input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags | |

3. Weisungskontrolle

Daten, die vom Auftraggeber an den Auftragnehmer übermittelt werden, dürfen ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers verarbeitet werden.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Auskunftserteilung gegenüber dem Auftraggeber zu speziellen Verfahren oder Daten des Auftraggebers auf Anfrage | <input checked="" type="checkbox"/> Für die Mitarbeiter des Auftragnehmers bindende Richtlinien und Arbeitsanweisungen, die sich aus dem jeweiligen Verfahren ergeben. |
|--|--|

Datum

Verantwortlicher für die Erstellung (in Druckbuchstaben)

Unterschrift des Verantwortlichen

Dokumentenhistorie

Versionsnummer	Anpassungsdatum	Grund der Anpassung	Name
1.0	09.05.2016	Aktualisierung	Karner/Iberler
1.1	08.05.2016	Aktualisierung	Iberler
2.0	20.05.2018	Aktualisierung DS-GVO	Iberler
2.1	18.06.2018	Aktualisierung	Iberler
2.2	12.02.2019	Prüfung / Aktualisierung	Iberler
2.3	05.02.2020	Prüfung / Aktualisierung	Iberler
2.4	02.02.2021	Prüfung / Aktualisierung	Iberler
2.5	11.05.2021	Prüfung / Aktualisierung	Iberler
2.6	20.06.2022	Prüfung / Aktualisierung	Iberler
2.7	19.02.2024	Prüfung / Aktualisierung	Iberler