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:	02.02.2021
Version:	2.4
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.

- ☐ Alarmanlage
- ☐ Schließsystem mit Codesperre
- ☐ Biometrische Zugangssperren
- ☐ Lichtschranken / Bewegungsmelder
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☒ Chipkarten-/Transponder-Schließsystem
- ☒ Manuelles Schließsystem
- ☐ Videoüberwachung der Zugänge
- ☒ Sicherheitsschlösser
- ☐ Personenkontrolle beim Pförtner / Empfang
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Tragepflicht von Berechtigungsausweisen

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:

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

☒ Einsatz von Anti-Viren-Software

☐ Verschlüsselung von Datenträgern in Laptops / Notebooks

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.

☐ Erstellen eines Berechtigungskonzepts

☒ Verwaltung der Rechte durch Systemadministrator

☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert

☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

☒ Sichere Aufbewahrung von Datenträgern

☒ physische Löschung von Datenträgern vor Wiederverwendung

☒ ordnungsgemäße Vernichtung von Datenträgern

☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

☒ Protokollierung der Vernichtung von Datenträgern

☐ Verschlüsselung von Datenträgern

☒ Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken

☒ Regelung zur Wiederherstellung von Daten aus Backups

4. Trennungskontrolle

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

☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

☒ Logische Mandantentrennung (softwareseitig)

☒ Erstellung eines Berechtigungskonzepts

☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern

☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

☒ Festlegung von Datenbankrechten

☒ 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.

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☒ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen
- ☒ Dokumentierte Verwaltung von Datenträgern - Bestandskontrolle
- ☒ Datenträgerentsorgung – sicheres Löschen durch physikalische Zerstörung oder durch Überschreiben der Festplatten
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☒ Beim physischen Transport: sichere Transportbehälter/-verpackungen
- ☒ Datenaustausch über https-Verbindung
- ☒ Papierentsorgung mit Shredder gemäß Sicherheitsstufe

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.

- ☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☒ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. (Verfahrensverzeichnis)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

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)
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☒ Datensicherungskonzept
- ☒ Testen von Datenwiederherstellung
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☒ Klimaanlage in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuerlöschgeräte in Serverräumen
- ☒ Erstellen eines Backup- & Recoverykonzepts
- ☐ Erstellen eines Notfallplans
- ☒ Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal

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
- ☒ Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates
- ☒ Räumlich getrennte Aufbewahrung von Sicherungsdatenträgern
- ☒ 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.

- ☒ Interne IT-Sicherheitsrichtlinie, Arbeitsanweisungen, Prozessbeschreibungen und Regelungen für Tests und Freigabe neuer Verfahren

2. Auftragskontrolle

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

- ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG
- ☒ Die Vertragsdurchführung erfolgt weisungsgebunden und wird regelmäßig kontrolliert
- ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)

☒ Auftragnehmer hat Datenschutzbeauftragten bestellt

☒ 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.

☒ Auskunftserteilung gegenüber dem Auftraggeber zu speziellen Verfahren oder Daten des Auftraggebers auf Anfrage

☒ 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