

Technische und organisatorische Maßnahmen gem. DSGVO

Kontrollziel	Beschreibung der Maßnahmen
0. Organisation	
Umsetzung des Datenschutzes	Ein interner Datenschutzbeauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus dem DSGVO eingesetzt.
Datenschutzbeauftragter	ENVISYS GmbH & Co. KG Prellerstraße 9 99423 Weimar
MitarbeiterInnen, die Kundendaten verarbeiten, sind auf die Umsetzung der technischen und organisatorischen Maßnahmen zu schulen	- Schulung fand am 22. Mai 2018 statt. Alle zuständigen MitarbeiterInnen waren anwesend bzw. wurden vorab geschult. - Bei Neueinstellungen werden die MA entsprechend geschult.
Die Verarbeitung von Daten ist hinsichtlich datenschutzrechtlicher Zulässigkeit zu dokumentieren.	Die Datenströme sind dokumentiert und die Zulässigkeit der Verarbeitung und Nutzung nach DSGVO nachgewiesen.
1. Vertraulichkeit	
Zutrittskontrolle	
Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	- Zutritt zu den Geschäftsräumen nur für MitarbeiterInnen entsprechend deren Aufgaben per überwachtem Schließsystem. - Zutritt für Besucher nur über den Empfang. - Kein Zutritt für Unbefugte zum Serverbereich. - Die Geschäftsräume sind mittels Alarmanlage gesichert.
Räume und Büros, in denen Datenverarbeitung stattfindet, sind vor Unbefugten zu schützen.	Kein Zutritt für Besucher in Räume, in denen Datenverarbeitung stattfindet.
Prüfung der Zutrittskontrollmaßnahmen	Der Datenschutzbeauftragte prüft die Zutrittskontrolle.
Zugangskontrolle	
Vergabe von Benutzerzugängen	Benutzerzugänge werden ausschließlich durch den Administrator/seinen Stellvertreter festgelegt. Die Rechtevergabe und Änderungen sind dokumentiert. Zugriff auf Daten nur durch strenge Passwörter möglich.

ENVISYS
GmbH & Co. KG
Prellerstraße 9
99423 Weimar
www.envisys.de

HRA 501373
Amtsgericht Jena
Umsatzsteuer-ID
DE 263992532

Persönlich haftend
ENVISYS Verwaltungs
GmbH
HRB 503769
Amtsgericht Jena
Geschäftsführer:
Winfried Schöffel M.A.

Bankverbindung
Ethik Bank eG
Kto. 3112985
BLZ 830 944 95
BIC GENO DE F1 ESN
IBAN
DE758309449400031129
85

Geschäftsführung
T: 0 36 43 / 4 95 27 10
F: 0 36 43 / 4 95 27 14
M: info@envisys.de

Vertrieb
T: 0 36 43 / 4 95 27 10
F: 0 36 43 / 4 95 27 14
M: vertrieb@envisys.de

Support
T: 0 36 43 / 4 95 27 20
F: 0 36 43 / 4 95 27 14
M: support@envisys.de

Gültigkeit von Benutzerzugängen	• Eine regelmäßige Revision der vergebenen Rechte erfolgt durch den Datenschutzbeauftragten.
Dokumentation von Benutzerzugängen	• Die Anlage und Veränderung von Benutzerzugängen ist im firmeninternen wiki dokumentiert.
Einschränkung von Administrationszugängen	• Es sind lediglich 2 Administrationszugänge (Administrator/Stellvertreter) vorhanden.
Schutz vor Zugriff auf Systeme/Anwendungen von außerhalb des Unternehmens	• Ein Zugriff von außerhalb auf das firmeninterne Netz ist für ausgewählte Mitarbeiter, mittels streng gesichertem Zugangsschutz, möglich.
Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	• Zugang zu den Computersystemen nur mit persönlichem Nutzernamen/Kennwort, wobei das Kennwort den Komplexitätsanforderungen der ENVISYS-Sicherheitsrichtlinie genügen muss. • Einsatz von Anti-Viren-Software. • Einsatz von Firewall-System.
Zugriffskontrolle	
Es ist zu 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.	• Zugriff auf Daten nur für Berechtigte entsprechend den Berechtigungskonzepten der ENVISYS für das jeweilige Anwendungssystem. • Zugriffsschutz auf Daten durch Passwort. • Die Passwörter werden ausschließlich vom Administrator vergeben und entsprechen einer hohen Passwortkomplexität. Die Passwörter werden nicht gespeichert. • Prüfung der ein- und ausgehenden Daten und E-Mails durch Firewall-System inkl. Virenschutz. • Virenschutz server- und clientseitig. • Protokollierung von Zugriffen und Änderungen auf Anwendungen und Löschung von Daten. • Die MitarbeiterInnen werden regelmäßig geschult und sensibilisiert.
Trennungskontrolle	
Daten, die zu unterschiedlichen Zwecken erhoben werden, sind getrennt voneinander zu bearbeiten.	• Die Daten werden in getrennten Bereichen gespeichert. • Zugriffskontrolle auf die Daten durch Passwörter.

Pseudonymisierung	
Es ist sicherzustellen, dass die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt.	• Alle mit der Verarbeitung personenbezogener Daten betrauten Personen wurden entsprechend verpflichtet. • Ein Datenschutzkonzept wird im Unternehmen eingesetzt und ist allen MitarbeiterInnen bekannt gemacht. • Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit, als auch eine konstante Sensibilisierung durch den Datenschutzbeauftragten bei den monatlich durchgeführten Mitarbeiterbesprechungen.
2. Integrität	
Weitergabekontrolle	
Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während eines 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 sind.	• Einrichtung von VPN-Tunneln. • E-Mail-Transport-Verschlüsselung. • Eine strikte Rechtevergabe sichert die Daten vor unberechtigt Zugriff.
Eingabekontrolle	
Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.	• Dateneingabe- und -änderung nur für Berechtigte, die über einen personalisierten, passwortgeschützten Zugang des Auftraggebers verfügen. • Protokollierung von Zugriffen und Änderungen auf Anwendungen und Löschung von Daten.
Es ist zu gewährleisten, dass Unterauftragnehmer ausschließlich die vom Auftraggeber vereinbarten personenbezogenen Daten bearbeiten.	• Sämtliche Unterauftragnehmer unterliegen den gleichen Vorgaben wie der Auftraggeber. • Entsprechende Verträge sind geschlossen. • Die Überprüfung der Unterauftragnehmer übernimmt der Datenschutzbeauftragte.
Es ist zu gewährleisten, dass personenbezogene Daten am Ende der Aufbewahrungsfrist gelöscht werden.	• Festlegung durch Vertragsbindung. • Bei Wegfall des Zweckes werden die Daten ebenfalls gelöscht.

3. Verfügbarkeitskontrolle	
Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	• Regelmäßiges und redundantes Backup (täglich differenziell, wöchentlich als Vollbackup, Kopie des Vollbackups in separatem alarmgeschützten Gebäude). • Monitoring-Systeme zur Systemüberwachung. • Schutz vor Diebstahl durch Alarmanlage. • Brandschutz- und Brandmeldemaßnahmen.
Es sind Schutzmaßnahmen zur Bekämpfung von Schadprogrammen zu gewährleisten.	• Ständig aktuelle Virens Scanner und Spamfilter im Einsatz. Die Systeme werden regelmäßig durch Updates aktualisiert.
Es ist zu sicherzustellen, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden.	• Physische Löschung bei funktionsfähigen Datenträgern und mechanische Zerstörung defekter Datenträger vor der Entsorgung.
Wiederherstellbarkeit	
Es ist zu sicherzustellen, dass im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich gewährleistet werden kann (rasche Wiederherstellbarkeit nach Art. 32 Abs. 1 lit.c DSGVO).	• Regelmäßiges und redundantes Backup (täglich differenziell, wöchentlich als Vollbackup, Kopie des Vollbackups in separatem alarmgeschützten Gebäude).
4. Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung	
Die Sicherheit der Datenverarbeitung ist regelmäßig durch geeignete Verfahren zu prüfen.	• Der Datenschutzbeauftragte überprüft regelmäßig die Einhaltung der technisch-organisatorischen Maßnahmen.
Auf Anfragen und Probleme ist kurzfristig zu reagieren (Incident-Response-Management).	• Einsatz eines Ticketsystems • Telefon- und E-Mail-Hotline
Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO).	• Keine Vorbelegung durch Haken. • Bei Anmeldung im System erfolgen keine Vorbelegungen. • Benutzer muss die Anmeldeinformationen selbst eintragen.
Auftragskontrolle	
Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	• Vertragswerk entspricht den Vorgaben der DSGVO. • Daten werden gem. den Anweisungen des Auftraggebers verarbeitet. • Der Datenschutzbeauftragte nimmt Beratungs- und Kontrollpflichten wahr.