DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

Maßnahmen zur Gewährleistung der Schutzziele

Allgemeiner Nachweis der technischen und organisatorischen Maßnahmen TOMs (auch Anlage zum AV-Vertrag)

DSGVO (Art. 5 i. V. m. Art. 25, Art. 28 und Art. 32 DSGVO)

Die Gewährleistungsziele finden ihren ganz wesentlichen Anker in den Grundsätzen der Verarbeitung personenbezogener Daten in Art. 5 DSGVO, die wiederum den Schutzauftrag aus Art. 8 der Charta der Grundrechte der Europäischen Union aufnehmen.

Die DSGVO verpflichtet die verantwortlichen Stellen und verarbeitenden Organisationen dazu, zur Gewährleistung des grundrechtlichen Schutzes der Rechte der Betroffenen sowie gegen unbefugte Zugriffe durch Dritte die dafür angemessenen technischen und organisatorischen Maßnahmen (insbes. Art. 32 DS-GVO) auszuwählen und im Rahmen der Technikgestaltung und datenschutzfreundlicher Voreinstellungen gem. Art. 25 DSGVO einzusetzen und zu prüfen (Art. 32 I d). Der Verantwortliche ist für die Einhaltung der Grundsätze der Verarbeitung nach Art. 5 Abs. 1, 24 DSGVO verantwortlich und muss dessen Einhaltung nachweisen können. Weitere Erläuterungen finden sich in ErwGr 39 „Grundsätze der Datenverarbeitung“.

Folgende Maßnahmen werden durch enytime.green GmbH getroffen:

(1) Transparenz

Der Grundsatz der Transparenz ist in Art. 5 Abs. 1 lit. a DSGVO festgeschrieben. Er findet sich als tragender Grundsatz des Datenschutzrechts in zahlreichen Regelungen der DSGVO. Insbesondere die Informations- und Auskunftspflichten tragen ihm Rechnung.

Maßnahmen zur Gewährleistung der Transparenz sind:

Dokumentation von Verfahren insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT Systeme, Betriebsabläufe, Verfahrensbeschreibungen, Zusammenspiel mit anderen Verfahren	teilweise
Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verfahren	nein
Dokumentation der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen	ja

Dokumentation von Einwilligungen und Widersprüchen	ja
Protokollierung von Zugriffen und Änderungen	ja
Nachweis der Quellen von Daten (Authentizität)	teilweise
Versionierung	ja

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts	ja
Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept	teilweise

Ergänzungen zur Transparenz:

Die Dokumentation und Prozessgestaltung für die Betroffenenrechte befindet sich gerade in der Umstellung. Die gesetzlichen Vorgaben werden eingehalten, allerdings ist die Dokumentation noch nicht ganz vollständig.

(2) Datenminimierung

Das Gewährleistungsziel Datenminimierung findet sich unmittelbar begrifflich im Verordnungstext wieder: In Art. 5 Abs. 1 lit. c und lit. e DSGVO steht, dass Personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen.

Das Gewährleistungsziel Datenminimierung wird beispielsweise erreicht

durch:

- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen
- Implementierung automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren
- Regelungen zur Kontrolle von Prozessen zur Änderung von Verfahren

Datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung (Art. 25 Abs. 2 DSGVO)

Privacy by design / Privacy by default

Technische Maßnahmen		**Organisatorische Maßnahmen**	
Beschränkung der Angaben und weiteren Verwendung auf das notwendige Maß	ja	Transparente Datenverarbeitung (Funktion, Überwachung durch den Betroffenen)	ja
Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	teilweise	Regelungen zur Datenminimierung, Datensparsamkeit und Erforderlichkeit	ja
Automatisierte Löschfunktionen für nicht mehr benötigte Daten / Lifecycle-Management	teilweise	Einhaltung von Branchenstandards	ja

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

Durch den Betroffenen auswählbare Sicherheitseinstellungen (z.B. Sicherung in der Cloud oder lokale Ablage)	ja	Minimierung von Pflichtfeldern	ja
Automatisierte Erinnerungsfunktion zur Überprüfung erteilter Einwilligungen	nein	Deutliche Kennzeichnung von freiwilligen Angaben	ja
Verwendung von Opt-In-Lösungen	ja		

Ergänzungen Datenminimierung:

Dort, wo keine Automatismen greifen, kann manuell eingegriffen werden.

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

Die Verpflichtung zur Wahrung der Vertraulichkeit ergibt sich insbesondere aus Art. 5 Abs. 1 lit. f DSGVO, aus Art. 32 Abs. 1 lit. b DSGVO sowie Art. 38 Abs. 5 DSGVO (Geheimhaltungspflicht des Datenschutzbeauftragten) bzw. Art. 28 Abs. 3 lit. b DSGVO (Geheimhaltungspflicht des Auftragsverarbeiters). Es gewährleistet den Schutz vor unbefugter und unrechtmäßiger Verarbeitung. Eine Verletzung der Vertraulichkeit stellt in der Regel eine Datenverarbeitung ohne Rechtsgrundlage dar.

Maßnahmen zur Gewährleistung der Vertraulichkeit sind beispielsweise:

- Festlegung eines Rechte- und Rollen-Konzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle
- Implementierung eines sicheren Authentisierungsverfahrens
- Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zu-gelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen
- Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle, spezifizierte, für das Verfahren ausgestattete Umgebungen (Gebäude, Räume)
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen etc.)
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept)
- Schutz vor äußeren Einflüssen (Spionage, Hacking)

a) Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

Technische Maßnahmen		**Organisatorische Maßnahmen**	
Alarmanlage	ja	Schlüsselregelung / Liste	ja

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

Automatisches Zugangskontrollsystem	ja	Empfang / Rezeption / Pförtner	ja
Biometrische Zugangssperren	ja	Besucherbuch / Protokoll der Besucher	ja
Chipkarten / Transpondersysteme	ja	Mitarbeiter- / Besucherausweise	ja
Manuelles Schließsystem	ja	Besucher in Begleitung durch Mitarbeiter	ja

Sicherheitsschlösser	ja	Sorgfalt bei Auswahl des Wachpersonals	ja
Schließsystem mit Codesperre	teilweise	Sorgfalt bei Auswahl Reinigungsdienste	ja
Absicherung der Gebäudeschächte	ja		
Türen mit Knauf Außenseite	ja		
Klingelanlage mit Kamera	ja		
Videoüberwachung der Eingänge	ja		

Ergänzungen Zutrittskontrolle:

Die gesamte Serverstruktur befindet sich im Rechenzentrum Hetzner, Nürnberg (D). Insofern werden hier keine Angaben zur Zutrittskontrolle gemacht. Das RZ ist ISO 27001 zertifiziert und die Maßnahmen dort wurden im Rahmen des AV-Vertrages geprüft. https://www.hetzner.com/de/unternehmen/zertifizierung

b) Zugangskontrolle: Keine unbefugte Systembenutzung

Technische Maßnahmen		**Organisatorische Maßnahmen**	
Login mit Benutzername + Passwort	ja	Verwalten von Benutzerberechtigungen	ja
Login mit biometrischen Daten	ja	Erstellen von Benutzerprofilen	ja
Anti-Viren-Software Server	nicht relevant	Zentrale Passwortvergabe	nein
Anti-Virus-Software Clients	ja	Richtlinie „Sicheres Passwort“	ja
Anti-Virus-Software mobile Geräte	teilweise	Richtlinie „Löschen / Vernichten“	teilweise
Firewall	ja	Richtlinie „Clean desk“	nein
Intrusion Detection Systeme	teilweise	Allg. Richtlinie Datenschutz und / oder Sicherheit	ja
Mobile Device Management	nein	Mobile Device Policy	ja
Einsatz VPN bei Remote-Zugriffen	teilweise	Anleitung „Manuelle Desktopsperre“	ja
Verschlüsselung von Datenträgern	ja		

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

Verschlüsselung Smartphones	ja		
Gehäuseverriegelung	nein		
BIOS Schutz (separates Passwort)	ja		
Sperre externer Schnittstellen (USB)	nein		
Automatische Desktopsperre			
Verschlüsselung von Notebooks / Tablet			

Ergänzungen Zugangskontrolle:

c) Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

Technische Maßnahmen		**Organisatorische Maßnahmen**	
Aktenschredder (mind. Stufe 3, cross cut)	teilweise	Einsatz Berechtigungskonzepte	ja
Externer Aktenvernichter (DIN 66399)	ja	Minimale Anzahl an Administratoren	ja
Physische Löschung von Datenträgern	nicht relevant	Datenschutztresor	nein
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	teilweise	Verwaltung Benutzerrechte durch Administratoren	ja

Ergänzungen Zugriffskontrolle:

d) Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

Technische Maßnahmen		**Organisatorische Maßnahmen**	
Trennung von Produktiv- und Testumgebung	ja	Steuerung über Berechtigungskonzept	ja
Physikalische Trennung (Systeme / Datenban-ken / Datenträger)	ja	Festlegung von Datenbankrechten	ja

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

Mandantenfähigkeit relevanter Anwendungen	ja	Datensätze sind mit Zweckattributen versehen	nein

Ergänzungen Trennungskontrolle:

e) 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 Maßnahmen		**Organisatorische Maßnahmen**	
Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	nein	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren	ja
Kürzung von Datensätzen um identifizierende Merkmale (z.B. der IP-Adresse)	ja	Anweisungen / Regelungen zur möglichst frühzeitigen Verfremdung von Datensätzen	nein

Verfremdung von identifizierenden Merkmalen durch Eigen- oder Fremdsoftware	nein	Erstellung von Verfremdungskonzepten	teilweise
Löschung von identifizierenden Merkmalen vor Übermittlung	teilweise	Festlegung von Verfremdungsregeln	nein
Ausschluss der (Re-)Identifizierung von Merkmalen durch Berichtigungen	nein	Dokumentation von Einsatzbereichen der Verfremdungsregeln / -konzepte	nein

Ergänzungen Pseudonymisierung:

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

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

Das Gewährleistungsziel der Integrität ist in Art. 5 Abs. 1 lit. f DSGVO als Grundsatz für die Verarbeitung von Daten und in Art. 32 Abs. 1 lit. b DSGVO als Voraussetzung für die Sicherheit einer Datenverarbeitung genannt. Es soll unbefugte Veränderungen und Entfernungen auszuschließen.

Maßnahmen zur Gewährleistung der Integrität bzw. zur Feststellung von Integritätsverletzungen sind beispielsweise:

- Einschränkung von Schreib- und Änderungsrechten
- Einsatz von Prüfsummen, elektronische Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts
- dokumentierte Zuweisung von Berechtigungen und Rollen
- Prozesse zur Aufrechterhaltung der Aktualität von Daten
- Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen
- Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durchführen von Tests zur Feststellbarkeit bzw. Feststellung der Ist-Zustände von Prozessen

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

Technische Maßnahmen		**Organisatorische Maßnahmen**	
Email-Verschlüsselung	nein	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen	teilweise
Einsatz von VPN	teilweise	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen	teilweise
Protokollierung der Zugriffe und Abrufe	ja	Weitergabe in anonymisierter oder pseudonymisierter Form	teilweise
Sichere Transportbehälter / Verpackungen	nicht relevant	Sorgfalt bei Auswahl von Transport, Personal und Fahrzeugen	nicht relevant
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	ja	Persönliche Übergabe mit Protokoll	nicht relevant
Nutzung von Signaturverfahren	ja		

Ergänzungen Weitergabekontrolle:

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

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

Technische Maßnahmen		**Organisatorische Maßnahmen**	
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	ja	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können	teilweise

Manuelle oder automatisierte Kontrolle der Protokolle	teilweise	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	ja
		Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	ja
		Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden	ja
		Klare Zuständigkeiten für Löschungen	ja

Ergänzungen Eingabekontrolle:

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

Der Grundsatz der Verfügbarkeit ist in Art. 32 Abs. 1 lit. b und lit. c explizit im Kontext der Sicherheit von Datenverarbeitungen aufgenommen. Es ist zudem in Art. 5 Abs. 1 lit. e DSGVO als Voraussetzung für die Identifizierung der betroffenen Person verankert. Es gewährleistet die Verfügbarkeit der Daten zu dem jeweiligen Zweck, solange dieser noch besteht. Der Grund-satz kommt zum Tragen bei den Informations und Auskunftspflichten (Art. 13 und 15 DSGVO) gegenüber den Betroffenen. Für das Recht auf Datenübertragbarkeit (Art. 20 DSGVO) ist das Gewährleistungsziel der Verfügbarkeit ebenso Grundvoraussetzung.

Maßnahmen zur Gewährleistung der Verfügbarkeit sind beispielsweise:

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt)
- Dokumentation der Syntax der Daten
- Redundanz von Hard- und Software sowie Infrastruktur

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

- Umsetzung von Reparaturstrategien und Ausweichprozessen

Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO):

Schutz gegen zufällige oder mutwillige Zerstörung sowie Verlust und Vorkehrungen, um möglichst schnell die Daten wieder herzustellen

Technische Maßnahmen		**Organisatorische Maßnahmen**	
Feuer- und Rauchmeldeanlagen	nicht relevant	Backup & Recovery-Konzept (ausformuliert)	teilweise
Feuerlöscher Serverraum	nicht relevant	Kontrolle des Sicherungsvorgangs	ja
Serverraumüberwachung Temperatur und Feuchtigkeit	nicht relevant	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse	ja
Serverraum klimatisiert	nicht relevant	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums	ja
USV	nicht relevant	Keine sanitären Anschlüsse im oder oberhalb des Serverraums	nicht relevant
Schutzsteckdosenleisten Serverraum	nicht relevant	Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 200-4)	nicht relevant
Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	nicht relevant	Getrennte Partitionen für Betriebssysteme und Daten	nicht relevant
RAID System / Festplattenspiegelung	nicht relevant	Vertretungsregelungen für abwesende Mitarbeiter	ja
Videoüberwachung Serverraum	nicht relevant		
Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	nicht relevant		

Ergänzungen Verfügbarkeitskontrolle:

Die gesamte Serverstruktur befindet sich im Rechenzentrum Hetzner, Nürnberg (D). Insofern werden hier keine Angaben zur Zutrittskontrolle gemacht. Das RZ ist ISO 27001 zertifiziert und die Maßnahmen dort wurden im Rahmen des AV-Vertrages geprüft.
https://www.hetzner.com/de/unternehmen/zertifizierung

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

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

Datenschutz-Management

Technische Maßnahmen		**Organisatorische Maßnahmen**	
Software-Lösungen für Datenschutz-Management im Einsatz	ja	externer Datenschutzbeauftragter (Name / Firma / Kontaktdaten)	ja
		Kontakt DSB: Frau Christiane Mestel, mc-Technik Dienstleistungs- und Consulting GmbH, Marienthaler Straße 24, 24340 Eckernförde, Tel. 04351-7321-0, E-Mail: datenschutz@mc technik.de	
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	ja	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet	ja
Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	nein	Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich	teilweise
Anderweitiges dokumentiertes Sicherheits-Konzept	nein	Interner / externer Informationssicherheits Beauftragter Name / Firma Kontakt	nein
Sicherheitskonzept:		*Sicherheitsbeauftragter:*	

Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	ja	Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt	ja
Regelmäßige Auditierung / Zertifizierung durch Externe	ja	Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach	ja
Regelmäßiges Berichtswesen an die Geschäftsführung	ja	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden	ja
		Eskalationsverfahren für Notfälle	ja

Ergänzungen Datenschutz-Management:

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen		**Organisatorische Maßnahmen**	
Einsatz von Firewall und regelmäßige Aktualisierung	ja	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)	ja
Einsatz von Spamfilter und regelmäßige Aktualisierung	ja	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen	ja
Einsatz von Virenscanner und regelmäßige Aktualisierung	ja	Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen	ja

Intrusion Detection System (IDS)	nicht relevant	Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem	ja
Intrusion Prevention System (IPS)	nicht relevant	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen	ja

Ergänzungen Incident-Response-Management:

Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Organisatorische Maßnahmen	
Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation	ja
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit	ja

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard Vertragsklauseln	ja
Schriftliche Weisungen an den Auftragnehmer	ja
Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis	ja
Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht	ja
Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer	ja
Regelung zum Einsatz weiterer Sub-Unternehmer	ja

Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags	ja
Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus	ja

Hiermit versichern wir, keine Subunternehmer im Sinne einer Auftragsverarbeitung einzusetzen.	nein

Ergänzungen Auftragsverarbeitung:

(7) Nichtverkettung

Die Verpflichtung, Daten nur für den Zweck zu verarbeiten, zu dem sie erhoben wurden, ist insbesondere den einzelnen Verarbeitungsbefugnissen zu entnehmen, die die Geschäftszwecke, die Forschungszwecke etc. zum Maßstab machen und findet über den Zweckbindungs-grundsatz aus Art. 5 Abs. 1 lit. c DSGVO Eingang in die Grundverordnung. Bei der Datenverarbeitung auf der Grundlage der Einwilligung ergibt sich aus Art. 7 Abs. 4 DSGVO, dass eine Einwilligung unwirksam sein kann, wenn die Daten zu Zweckerfüllung nicht erforderlich sind.

Eine typische Maßnahme der Nichtverkettung ist etwa die Pseudonymisierung und wird beispielsweise in Art. 40 Abs. 2 lit. d DSGVO genannt.

Maßnahmen zur Gewährleistung der Nichtverkettung sind:

Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten	ja
programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten	ja
regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung	ja
Trennung nach Organisations-/Abteilungsgrenzen	nicht relevant

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens	ja
Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle	ja

Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten	nein
geregelte Zweckänderungsverfahren	nicht relevant

(8) Intervenierbarkeit

Die Interventionsrechte der Betroffenen ergeben sich explizit aus den Vorschriften zu Berichtigung, Sperrung, Löschung und zum Widerspruch (Art. 16. 17 DSGVO). Sie können sich außerdem als Ergebnis einer Interessenabwägung im Rahmen eines gesetzlichen Erlaubnistat-bestandes ergeben. Wiederum müssen die verantwortlichen Stellen gem. Art. 5 Abs. 1 lit. d) DSGVO die Voraussetzung für die Gewährung dieser Rechte, sowohl auf organisatorischer als auch, soweit erforderlich, auf technischer Ebene schaffen.

Maßnahmen zur Gewährleistung der Intervenierbarkeit sind:

differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten	ja
Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen	ja
dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes	teilweise
Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem	ja
Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen	ja
Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte	ja
Einrichtung eines Single Point of Contact (SPoC) für Betroffene	ja
operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten	ja

DSGVO - Dokumentation

Maßnahmen zur Gewährleistung der Schutzziele

Ausgefüllt für das Unternehmen durch

Name Ulrich Meyer

Funktion Geschäftsführer

Rufnummer: 01705582554

Email uli.meyer@enytime.green

Ort, Datum Hamburg, 01.01.2025

(9) Bewertung des Schutzniveaus durch den DSB:

Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?

geeignet

Begründung:

Die getroffenen und umgesetzten Maßnahmen reichen unter Berücksichtigung des Schutzniveaus der personenbezogenen Daten und der eingesetzten finanziellen Mittel aus, die verarbeiteten Daten umfangreich zu schützen. Die Firma enytime.green befindet sich noch im Aufbau, dadurch ist die Dokumentation noch nicht vollständig abgeschlossen. Dennoch sind die datenschutzrechtlichen Anforderungen bekannt und werden umgesetzt. Aufgrund der Art der angebotenen Dienstleistungen ist eine sichere technische Umgebung absolut notwendig, was auch einen hohen Schutz der personenbezogenen Daten nach sich zieht. Außerdem arbeitet die enytime.green kontinuierlich an Verbesserungen, um das vorhandene Niveau weiter zu optimieren und dem Stand der Technik zu folgen.