Testat Datenschutzmanagement 2024

(inkl. Technische und organisatorischen Maßnahmen Art. 25, 32 DS-GVO)

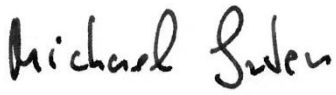
BSP-SECURITY

Die HENRICHSEN4easy GmbH (Weißgerbergasse 6, D-94315 Straubing) hat das im nachfolgenden beschriebenen Datenschutzmanagement inkl. der technischen und organisatorischen Maßnahmen (Art. 25, 32 DS-GVO) wirksam umgesetzt.

Dies wird von mir im Rahmen von Datenschutz-Audits als bestellter externer Datenschutzbeauftragter überprüft und überwacht.

Für weitere Fragen stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen



Michael Gruber
Externer Datenschutzbeauftragter
BSP-SECURITY

BvD e.V.
Datenschutzbeauftragter nach Verbandskriterien verpflichtet
Nr.: 100152

Datenschutzkonzept

1 Zielsetzung

Absicht und Pflicht der Unternehmensleitung des Unternehmens ist es alle gesetzlichen Regelungen, die den Datenschutz betreffen einzuhalten und das Persönlichkeitsrecht zu schützen. Dies betrifft Bewerber und Mitarbeiter sowie auch Kunden, Lieferanten und Geschäftspartner. Darüber hinaus ist das Ziel der Unternehmensleitung, die Daten des Unternehmens und der anvertrauten Kundendaten zu schützen. Alle Mitarbeiter der sind durch Richtlinien diesen Zielen verpflichtet. Die Führungskräfte stellen die Einhaltung dieser Richtlinie in ihrem Bereich sicher.
Die Informationssicherheitsmaßnahmen orientieren sich an den Anforderungen der EU-Datenschutz-Grundverordnung (DS-GVO) und des Bundesdatenschutzgesetzes (BDSG).

2 IT-Sicherheitsrichtlinien

Es existiert ein umfangreiches verbindliches Regelwerk für den Umgang mit Daten und IT-Systemen. Folgende Punkte werden hier u. a. gesondert geregelt:

- Netzwerkinfrastruktur (intern, extern, LAN, WAN, WLAN)
- Kennwortrichtlinie
- Berechtigungsmanagement
- E-Mail- und Internetnutzung
- Benutzung von Software
- Umgang mit Firmen- und Kundendaten
- Externer Zugang / VPN-Nutzung
- …

Jeder Mitarbeiter wird bei der Einstellung schriftlich auf die Einhaltung der IT-Sicherheits-richtlinien verpflichtet.

3 Datenschutzbeauftragter

Für das Unternehmen ist

Herr Michael Gruber
BSP-SECURITY
Thundorferstr. 10
D-93047 Regensburg
E-Mail: michael.gruber@bsp-security.de

als externer Datenschutzbeauftragter (eDSB) schriftlich benannt worden. Der Datenschutzbeauftragte nimmt alle ihm nach der DS-GVO und BDSG obliegenden Aufgaben wahr. Der eDSB wurde der zuständigen Datenschutz Aufsichtsbehörde gemäß Art. 37 DS-GVO gemeldet.

4 Verpflichtung auf Vertraulichkeit

Alle Mitarbeiter werden bei der Einstellung durch eine Vereinbarung auf den Datenschutz gemäß Art. 28 Abs. 3 lit. b, Art. 39 Abs. 1 lit. a DS-GVO und auf § 3 TDDDG (Fernmeldegeheimnis) verpflichtet. Zusätzlich werden die Mitarbeiter auf Berufsgeheimnisse und auf die neben dem BDSG geltenden Landes- und Kirchen-Datenschutzgesetze hingewiesen

Die Mitarbeiter werden durch Anweisungen, Hinweise und Schulungen auf die Anforderungen des Datenschutzes sensibilisiert und geschult.

5 Auftragsverarbeitung nach Art. 28 DS-GVO

Nach Beauftragung verarbeitet, erhebt oder nutzt das Unternehmen personenbezogene Daten im Auftrag des Auftraggebers im Sinne des Art. 28 DS-GVO. Der Gegenstand des Auftragsverhältnisses umfasst die Bearbeitung personenbezogener Daten gemäß dem geschlossenen Hauptvertrag. Die Vereinbarung zur Auftragsverarbeitung nach Art. 28 DS-GVO regelt den Schutz personenbezogener Daten bei der Datenverarbeitung im Auftrag.

Das Unternehmen wird den Auftraggeber bei der Wahrung der datenschutzrechtlichen Verpflichtungen, insbesondere im Hinblick auf die Benachrichtigung, Auskunftserteilung, Berichtigung, Sperrung und Löschung im Rahmen seiner Möglichkeiten unterstützen.

Bei einer eventuell notwendigen Beauftragung von Subunternehmern werden die gleichen Datenschutzpflichten auferlegt werden, die in Kunden AV-Verträgen festgelegt sind. Es wird sichergestellt, dass die geeigneten technischen und organisatorischen Maßnahmen vom Subunternehmer so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des Datenschutzrechts erfolgt.

6 Datenschutzdokumentation

Die nachfolgenden Datenschutzdokumente wurden von mir erstellt und bei Bedarf aktualisiert:

- Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO)
- Technische und organisatorischen Maßnahmen (Art. 32 DS-GVO)

7 Datenschutzaudit

Ich prüfe regelmäßig im Rahmen von Datenschutzaudits die Umsetzung und Wirksamkeit der gesetzlichen erforderlichen Maßnahmen zum Datenschutz und zur Informationssicherheit. Dies erfolgt unter Zuhilfenahme einer DS-GVO Checkliste des Bayerischen Landesamts für Datenschutz. Die Ergebnisse des Audits und eventuell notwendige Korrekturmaßnahmen werden in Form eines Datenschutzaudit-Berichtes von mir erstellt und der Geschäftsführung zur Nachbearbeitung vorgelegt.

8 Technische und organisatorische Maßnahmen (Art. 25, 32 DS-GVO)

Nach Art. 5 Abs, 2 DS-GVO ist die verantwortliche Stelle für die Einhaltung des Absatzes 1, Art. 5, DS-GVO verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“). Im Art. 32 DS-GVO ist definiert, dass der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu treffen hat, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Um die technischen und organisatorischen Maßnahmen bewerten zu können sind die nachfolgenden Fragen zu beantworten, bzw. die zu den einzelnen Punkten getroffen Maßnahmen zu benennen.

In den Art. 25, 28 und 32 DS-GVO ist festgelegt, dass der Auftraggeber und der Auftragnehmer geeignete technische und organisatorische Maßnahmen zu treffen haben, um ein dem Risiko angemessenes Schutzniveau der personenbezogenen Daten zu gewährleisten.

Die nachfolgend aufgeführten technischen und organisatorischen Maßnahmen sind im Unternehmen umgesetzt.

8.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

8.1.1 Zutrittskontrolle
Kein unbefugter Zutritt ins Gebäude und zu Datenverarbeitungsanlagen

☒ Zentrales Schließsystem (Sicherheitsschlösser)
☒ Sicherheitsschlösser
☒ Schlüsselverwaltung / Schlüsselbuch
☒ Zutritt Serverräume ist speziell abgesichert
☐ Empfang
☐ Videoüberwachung
☒ Abholung am Empfang, persönliche Besucherführung
☐ Wachdienst außerhalb der Arbeitszeit

8.1.2 Zugangskontrolle
Kein unbefugter Zugang zu IT-Systemen

☒ Authentifikation mit Benutzername und Passwort
☒ Virenscanner
☒ Firewall
☒ Mobile Device Management
☒ VPN-Technologie
☒ Datenträgerverschlüsselung
☒ Verschlüsselung mobiler Endgeräte (Smartphone, Laptop…)
☒ Komplexe Kennwortregeln
☒ Sperrung des Bildschirms nach Inaktivität des Benutzers
☒ Passwortsafe mit Berechtigungsgruppen
☒ Jährliche Überprüfung VPN und AD

☒ Automatische Sperrung des AD-Kontos von inaktiven Benutzern

8.1.3 Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen personenbezogener Daten

☒ Aktenvernichtung nach DIN 66399
☒ Ordnungsgemäße Datenträgervernichtung nach DIN 66399
☒ Protokollierung der Datenvernichtung
☒ Berechtigungskonzept
☒ Autorisierungsprozess für Berechtigungen
☒ Protokollierung bei Änderungen von Berechtigungen
☒ Komplexe Kennwortregeln
☒ Sichere Aufbewahrung von Datenträgern
☒ Sichere Aufbewahrung von Papierunterlagen
☒ Sichtschutzfolien für Laptops, Tablets
☒ Mobile Device Management:

8.1.4 Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

☒ Verarbeitung auf getrennten IT-Systemen (Produktion, Test, Entwicklung)
☒ Verwendung von Testdaten
☒ Berechtigungskonzept
☒ Festgelegte Datenbankrechte
☒ Logische Mandantentrennung

8.1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO, Art. 25 Abs. 1 DS-GVO)
Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

☒ Auf Anforderung und bei Umsetzbarkeit erfolgt die Pseudonymisierung personenbezogener Daten

8.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

8.2.1 Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen personenbezogener Daten bei elektronischer Übertragung, Transport oder Speicherung

☒ Verwendung von VPN-Tunneln
☒ E-Mail-Verschlüsselung
☒ Sichere Transportbehälter
☒ Verschlüsselung der mobilen Datenträger
☒ Verschlüsselung von Laptops, Smartphones und Tablets
☒ MDM
☒ Sperrung unbefugter Geräte
☒ Protokollierung der Nutzung
☒ Sicherheitsrichtlinien
☒ Dokumentation der Dauer der Überlassung/ Löschfristen

☒ Gesichertes WLAN (WPA2)
☒ Verwendung gesicherter Protokolle: SFTP
☒ Verwendung gesicherter Protokolle Web-Site: TLS/HTTPS, STARTTLS, PFS
☒ Verwendung gesicherter Protokolle SMTP-Server: STARTTLS, PFS
☒ Datenträger in Multifunktionsdruckern werden datenschutzkonform behandelt

8.2.2 Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

☒ Protokollierung von Eingaben und Veränderungen auf Systemebene
☒ Vergabe von Rechten auf Basis eines Rollenkonzepts
☒ Protokollierung fehlgeschlagener Anmeldeversuche
☒ Protokollierung SMTP-Server
☒ Protokollierung Firewall/VPN-Gateway

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

8.3.1 Verfügbarkeits- und Belastbarkeitskontrolle
Es ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und stets verfügbar sind.

☒ Unterbrechungsfreie Stromversorgung
☒ Feuerlöscheinrichtung
☒ Feuer- und Rauchmeldeanlage
☒ Klimaanlage
☒ Überwachung des Raumklimas (Serverräume)
☒ Schutzsteckdosenleisten
☒ Alarm bei unberechtigtem Zutritt
☒ Datensicherung an einem sicheren, ausgelagerten Ort
☒ Backup- & Recovery-Konzept
☒ Notfallplan
☒ Sicherer Standort der Server (RZ)
☒ Firewall
☒ Virenschutz
☒ Notstromaggregat (RZ)
☒ Prüfen von Sicherheitspatches und -Updates vor Freigabe
☒ Zeitnahes Einspielen von Sicherheitspatches und Updates

8.3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
Personenbezogene Daten können bei aufgetretenen Problemen in kurzer Zeit wieder verlustfrei hergestellt werden.

☒ Notfall Übungen (Recovery Tests)
☒ Sporadisches Zurücksichern von Dateien auf Anfrage

8.4 Regelmäßigen Überprüfung, Bewertung und Evaluierung

8.4.1 Datenschutzmanagement

☒ Benennung eines Datenschutzbeauftragten
☒ Meldung des Datenschutzbeauftragten an die Datenschutzaufsichtsbehörde
☒ Verpflichtung der Mitarbeiter auf den Datenschutz
☒ Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO)
☒ Organisatorische und technische Maßnahmen (Art. 32 DS-GVO)
☒ Risikoanalyse (Art. 32 DS-GVO)
☒ Bei Bedarf: Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)
☒ Datensicherheitsrichtlinien
☒ Schulung und Sensibilisierung der Mitarbeiter
☒ Jährliches Datenschutzaudit

8.4.2 Incident-Response-Management

☒ Prozess Meldung von Sicherheitsvorfällen (Art. 33, 34 DS-GVO) vorhanden
☒ Prozess Betroffenenrechte (Art. 15 – 22, 34 DS-GVO) vorhanden

8.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO)

Standardisierte Voreinstellung bei Anwendungen und IT-Systemen

☒ Verschlüsselung mobiler Endgeräte (Smartphone, Laptop)
☒ E-Mail-Verschlüsselung
☒ WLAN (WPA2)
☒ HTTPS, STARTTLS, PFS, SSL/TLS (Web-Site)
☒ STARTTLS, PFS (SMTP)
☒ SFTP
☒ Verpflichtende Änderung des Passwortes bei Erstbenutzung

8.4.4 Auftragskontrolle (Art. 28 DS-GVO)

☒ Eindeutige Vertragsgestaltung
☒ Strenge Auswahl des Dienstleisters
☒ Schriftliche Weisung an den Auftragnehmer
☒ Verpflichtung der Mitarbeiter auf Vertraulichkeit
☒ Vernichtung der Daten nach der Beendigung des Auftrags
☒ Datenschutz Schulung der Mitarbeiter