Version: 1.0 | Stand: 25. Juni 2018

DATENSICHERHEITSKONZEPT (DS-GVO)
SICHERHEITSKONZEPTION - SCHUTZ VON DATEN (TOMS)

Die getroffenen Maßnahmen sollen insbesondere die Einhaltung der europäischen Datenschutz-Grundverordnung (DSGVO) gewährleisten und in der Gesamtheit der Dokumentation den Nachweis der Einhaltung schaffen.

Geeignete technische und organisatorische Maßnahmen um unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ein dem Risiko angemessenes Schutzniveau zu gewährleisten und nachzuweisen.

Zur Erhöhung der Datensicherheit im Unternehmen werden Kontrollmechanismen eingesetzt die insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von Daten gewährleisten sowie unbefugten Zugriff, Kenntnisnahme, Manipulation oder Entfernung von Daten verhindern sollen.

- Schulung, Sensibilisierung und Verpflichtung der Mitarbeiter
- Informationsklassifizierung und Schutzbedarfsfeststellung der Daten bezüglich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit (BSI-Standard)
- Sicherheitsprozesse (top down) und Festlegung der Rollen und Verantwortlichkeiten
- Verpflichtung zur kontinuierlichen Verbesserung des Datenschutzmanagements
- Durchgeführte und regelmäßige Sicherheitsanalyse, Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Zenterprise
Friedrichstrasse 29
53111 Bonn

Verantwortlich
Florin Ziefer
M +49 171 3259 342
florin.ziefer@zenterprise.de

Bank
Commerzbank AG, Bonn
IBAN DE90 3804 0007 0104 1391 00
BIC COBADEFFXXX

Website
https://www.zenterprise.de

VERTRAULICHKEIT (ART. 32 DS-GVO)

Zutrittskontrolle

Zenterprise verwehrt Unbefugten den Zutritt zu Geschäftsräumen durch elektronische und mechanische Zutrittskontrolle u.a. mit Hilfe von Türöffnungssystemen, physischen und umgebungsbezogenen Sicherheitsvorkehrungen.

Die Zutrittskontrolle zum Rechenzentrum geschieht durch:

- Rechenzentrum mit elektronischem Zutrittskontrollsystem mit Protokollierung
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Verwaltung durch elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um das gesamte Rechenzentrum
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) nur in Begleitung
- Dokumentierte Schlüsselvergabe und 24/7 personelle Besetzung der Rechenzentren

Zugangskontrolle

Zenterprise verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Dies geschieht durch:

- Authentifizierung von Systemanwendern durch Benutzer-/Passwortverfahren
- Persönliche Benutzerkonten für Anwender zur Steuerung individueller Berechtigungen
- Passwortrichtlinien für die Erneuerung von Passwörtern von Systemadministratoren und wichtigen Passwörtern sowie Userkonten in nicht-kritischen Systemen und Anwendungen
- Einbindung in die Sicherheitsarchitektur von Entwicklungsumgebungen und Test-Systemen

Zugriffskontrolle

Zenterprise gewährleistet, 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. Dies geschieht durch:

- Rollenbasiertes verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers und Festlegung von Benutzerprofilen
- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden

Trennungskontrolle

Zenterprise gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies geschieht durch:

- Mandantentrennung durch zumindest logische Datentrennung auf Basis von Kunden- bzw. Mandantennummern

INTEGRITÄT (ART. 32 DS-GVO)

Weitergabekontrolle

Zenterprise gewährleistet, dass personenbezogene Daten während 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 Einrichtung zur Datenübertragung vorgesehen ist. Dies geschieht durch:

- Verschlüsselung beim Versand insb. bei schützenswerten personenbezogenen Daten
- Restriktiver Fax-Versand insbesondere beim Versand an fremde Fax-Nummern
- Elektronische Datenträger werden vor einer Versendung angemessen verschlüsselt
- Papierunterlagen werden entweder über geeignete Entsorgungscontainer gesammelt und einem zuverlässigen Entsorgungsunternehmen übergeben, oder zentral gesammelt und durch Zenterprise datenschutzkonform vernichtet.

Eingabekontrolle

Zenterprise gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies geschieht durch:

- Organisatorische Festlegung von Zuständigkeiten und Zugriffsprotokollierungen

Auftragskontrolle

Zenterprise gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Dies geschieht durch:

- Abstimmungen in der Arbeitsorganisation mit dem Auftraggeber
- Das vereinbarte Niveau der Informationssicherheit im Rahmen der Dienstleistungserbringung durch regelmäßige Überprüfung der A aufrechterhalten

VERFÜGBARKEIT & BELASTBARKEIT (ART. 32 DS-GVO)

Verfügbarkeitskontrolle

Zenterprise gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dies geschieht durch:

- Gewährleistung der Belastbarkeit der Systeme und Antiviren-Schutz
- Definition von und besonderer Schutz von Sicherheitszonen (Server, Netzwerk)
- Regelmäßige Anfertigung von Datensicherungen
- Auslagerung Backupmedien an externen Lagerungsort, Verschlüsselung des Backupmediums
- Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Verfahren regelmäßiger Prüfung, Bewertung & Evaluierung (Art. 32; Art. 25 DS-GVO)

- Datenschutz-Management mit Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle – keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B. eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, Auswahl des Dienstleisters, Vorabüberzeugung und Nachkontrollen.