Technische und organisatorische Maßnahmen der D&G-Software GmbH

Der Artikel 32 der DSGVO in der Fassung vom 27. April 2016 legt fest, dass nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, technische und organisatorische Maßnahmen (TOMs) zu treffen haben, die erforderlich sind, um die Sicherheit der Verarbeitung der personenbezogenen Daten entsprechend den Vorschriften der DSGVO zu gewährleisten.

Die innerbetriebliche Organisation der D&G-Software GmbH ist so aufgebaut, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. So haben wir ein innerbetriebliches Datenschutz- und Datensicherheitskonzept entwickelt.

In diesem Dokument werden alle Maßnahmen aufgeführt, die von der D&G-Software GmbH getroffen werden, um den Schutz personenbezogener Daten zu gewährleisten. Viele dieser aufgeführten Maßnahmen werden bereits seit Jahren von der D&G-Software GmbH durchgeführt. Dazu gehören

- die AGB, Wartungsverträge und Rahmenbedingungen der D&G-Software GmbH, die sowohl die Aufgaben, den Datenschutz als auch die Weitergabe von Daten an mögliche Dritte regeln,
- die Verpflichtung der Mitarbeiter auf die Vertraulichkeit nach §53 BDSG (neu),
- die Erstellung und Einhaltung der D&G-Compliance Clause (im Rahmen einer Betriebsvereinbarung) über die Nutzung von z.B. eMail oder Internet, dem Mitbringen externer Datenträger etc.,
- sowie die Ernennung eines externen Beauftragten für den Datenschutz.

Darüber hinaus sorgen wir durch regelmäßige, externe Sicherheitsüberprüfungen dafür, dass die einzelnen Maßnahmen nicht nur auf ihre Umsetzung, sondern auch auf mögliche Verbesserungen geprüft werden.

Bitte sprechen Sie uns an, sofern Ihnen Sachverhalte oder Maßnahmen dieser Dokumentation unklar sind.

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

1.1 Zutrittskontrolle

Die D&G-Software GmbH gewährleistet, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Dies geschieht durch folgende Maßnahmen:

- Zutrittskontrollsystem über Transponder (Transponderliste)
- Schlüsselvergabe nur an beschränkten Personenkreis mit Schlüsselliste
- Türsicherung (elektrischer Türöffner und Transponderkontrolle)
- Überwachungseinrichtung durch Alarmanlage und Aufschaltung auf Sicherheitsdienst
- Außerhalb der Arbeitszeiten: Überprüfung des Gebäudes durch Sicherheitsdienst
- Nur ein zentraler Zugang zu den Unternehmensräumen
- Zugangstür ständig geschlossen, Zutritt zu den Unternehmensräumen nur nach Klingeln und Öffnen eines Mitarbeiters
- Durchführung externer Sicherheitsaudits
- Großteil der IT-Landschaft ist in einem etablierten externen Rechenzentrum mit Sitz in Deutschland ausgelagert, welches ISO27001-zertifiziert ist

1.2 Zugangskontrolle

Die D&G-Software GmbH gewährleistet, dass das Eindringen Unbefugter in die DV-Systeme durch folgende Maßnahmen verhindert wird:

- Kennwortverfahren (u.a. Komplexitätsanforderungen (3 aus 4), Mindestlänge (10 Zeichen), regelmäßiger Wechsel des Kennworts mit Historienverwaltung)
- Automatische Sperrung des Logins bei 3-maliger Fehleingabe des Kennworts
- Einrichtung eines Benutzerstammsatzes pro User
- Passwortschutz der Datenträger
- Protokollierung der Nutzung
- Bei Bedarf verschlüsseltes WLAN für den internen Gebrauch, zusätzlich entkoppeltes für Gäste in DMZ
- Ausgefeiltes Firewall-Konzept
- Verwendung von zeitgesteuerter Bildschirmsperre mit Passwortschutz
- Durchführung externer Sicherheitsaudits

1.3 Zugriffskontrolle

Die D&G-Software GmbH gewährleistet durch folgende Maßnahmen, 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.

- Festlegung und Kontrolle der Zugriffsbefugnisse, differenziert nach Daten, Programmen und Zugriffsarten (Berechtigungskonzept)
- Zeitnahes Einspielen der notwendigen Sicherheitsupdates
- Ständige Aktualisierung des Virenschutzes
- Auswertungen über Zugriffe
- Durchführung externer Sicherheitsaudits
- Sichere Verwaltung und Verwahrung von Datenträgern/-beständen
- Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network) für eingeschränkten Mitarbeiterkreis
- Gesicherter Zugriff über Proxy
- Vernichtung sensibler Unterlagen oder Datenträger durch Entsorgungs-Fachbetrieb, Nachweis über Vernichtung durch Datenvernichtungsprotokoll
- Sperrung sämtlicher USB-Ports (mit Ausnahme von peripheren Geräten wie Drucker oder Tastatur) zur Verhinderung des Anschlusses externer Festplatten, Memory-Sticks oder sonstiger Hardware, die ein Speichern oder Kopieren von Daten zulässt
- Sperrung von CD-/DVD-Laufwerken mit Schreibmöglichkeiten
- Verbot der Verwendung privater Datenträger oder Eingabegeräte (Betriebsvereinbarung)

1.4 Trennungskontrolle

Die D&G-Software GmbH gewährleistet durch folgende Maßnahmen, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden:

- "Interne Mandantenfähigkeit" des D&G-Versandhaus-Systems VS/4
- Trennung der Datensätze durch Speicherung in physikalisch getrennten Datenbanken
- Funktionstrennung zwischen Produktion und Test
- Anonymisierung der Daten bei Datenübernahme (z.B. durch Löschung von eMail-Kundendaten)

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

2.1 Weitergabekontrolle

Die D&G-Software GmbH gewährleistet durch folgende Maßnahmen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern 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:

- Protokollierung sämtlicher eingegangener und ausgegangener Datenträger (Archivierung) nebst eindeutiger Kennzeichnung
- Transportsicherung bei Versand mit Nachweiskontrolle
- Datenvernichtung entsprechend datenschutzrechtlicher Vorgaben
- Aufbewahrung in gesichertem Bereich

2.2 Eingabekontrolle

Die D&G-Software GmbH gewährleistet durch folgende Maßnahmen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Protokollierungs-Technik durch Festhalten in Datenbank und Protokollauswertung der jeweiligen Benutzer (eindeutige Benutzer-OPID)
- Eindeutige Datenerfassungsanweisung (Handlungsanweisungen)
- Protokollierung im Ticketsystem

3. Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO)

3.1 Verfügbarkeitskontrolle

Die D&G-Software GmbH gewährleistet durch folgende Maßnahmen, dass die Daten gegen zufällige Zerstörung oder Verlust geschützt werden:

- Definiertes Backup-Verfahren
- Verfügbarkeitsgewährleistung durch RAID-Verfahren und redundante Speichersysteme
- Unterbrechungsfreie Stromversorgung (USV)
- Gesicherter und klimatisierter Serverraum (redundant)
- Räumlich- und mediumgetrennte Aufbewahrung
- Virenschutz / Firewall
- Rauchmeldeanlage
- CO_2-Feuerlöscher
- Notfallplan
- Großteil der Systeme steht in einem ISO 27001-zertifizierten Rechenzentrum in Deutschland.

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

4.1 Auftragskontrolle

Die D&G-Software GmbH gewährleistet durch folgende Maßnahmen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Unterzeichnetes Auftragsformular bei Einzelanforderung und Hauptvertrag nebst Wartungsvertrag)
- Verpflichtung des Personals der D&G-Software GmbH sowie von der D&G-Software GmbH beauftragter Unternehmen (Dienstleistungsunternehmen, Steuerberater, Wirtschaftsprüfer, Sicherheitsunternehmen und weitere) auf das Datengeheimnis § 53 BDSG (neu)
- Dokumentierte Rückgabe der ggf. überlassenen Datenträger und Löschung von Restdaten

4.2 Datenschutz-Management

Es ist ein Datenschutz-Managementsystem implementiert, mit dessen Hilfe die Nachweispflichten der DSGVO und des BDSG (neu) umgesetzt werden:

- Rechtsgrundlagen der Verarbeitung, Art.6 DSGVO
- Erteilung der Einwilligung, Art.7 DSGVO
- Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person, Art.12 DSGVO
- Einhaltung der Informationspflichten, Art.13 DSGVO
- Datenschutz durch Technik, Art.25 DSGVO
- Auskunftsrecht der betroffenen Person, Art.15 DSGVO
- Recht auf Berichtigung, Art.16 DSGVO
- Recht auf Löschung, Art.17 DSGVO
- Umsetzung der Speicherbegrenzung, Art.5 DSGVO
- Umsetzung der Sicherheit der Verarbeitung, Art.32 DSGVO
- Auflistung aller Auftragsverarbeiter, Art.30 Abs.2 DSGVO
- Umgang mit Datenschutzverletzungen, Art.33 DSGVO
- Darstellung der Meldepflicht an Aufsichtsbehörden, Art.33 DSGVO
- Verwendung von Werkzeug Zertifizierung, Art.42 DSGVO
- Risikobewertung / Datenschutzfolgenabschätzung, Art.35 DSGVO
- Dokumentation von Audits
- Dokumentation von Awareness-Maßnahmen

4.3 Incident-Response-Management

Ein organisatorischer und technischer Prozess zum Umgang mit Sicherheitsvorfällen (incidents) ist definiert und implementiert. Hierüber werden auch eine einheitliche Reaktion sowie ein prozessualisierter Umgang mit erkannten und vermuteten Sicherheitsvorfällen/Störungen sichergestellt. Ebenfalls erfolgt im Rahmen dessen, eine einheitliche Nachbereitung und Kontrolle im Sinne eines kontinuierlichen Verbesserungsprozesses.

4.4 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Um dem Datenschutz gerecht zu werden, werden bereits seit vielen Jahren Maßnahmen im VS/4 ergriffen, so dass der DSGVO bspw. mit folgenden Funktionen, bzw. Maßnahmen nachgekommen wird:

- Kombination aus "Windows Remote App" & Server-Manager: Zur Absicherung des Datenzugriffs.
- Benutzerverwaltung und Berechtigungen: Zugriffsverwaltung für verschiedene Abteilungen und Nutzer durch individuelle Rechte und Beschränkungen möglich.
- Verzeichnis-Strukturen/Reorganisation: Getrenntes Eingabe-/Ausgabe-Verzeichnis.
- Reorganisations- und Löschmechanismen für temporäre Datentabellen und Verarbeitungskopien.
- Selektionsverwaltung VS/4-Selektion: Sicherung der Adressnummer als Referenz für mögliche Exportverfahren ohne doppeltes/mehrfaches Speichern von Adressdaten.
- Kommunikationssperren: datenschutzfreundliche Voreinstellung, so dass bspw. die Vermietungs-, Telefon-, Newsletter-Sperre von vornherein aktiviert sind.
- Adressen anonymisieren: Möglichkeit der Anonymisierung von Interessentendaten ohne Bewegungen.