Technische und organisatorische Maßnahmen nach BDSG/DSGVO

Maßnahmen zur Umsetzung der Anforderungen des Bundesdatenschutzgesetzes und der DSGVO

1. Vorwort

Die Einhaltung datenschutzrechtlicher Vorschriften liegt uns sehr am Herzen. Wir sind kontinuierlich bestrebt, geeignete Maßnahmen zu implementieren, um dies zu gewährleisten.

Sofern keine gesetzlichen Normen entgegenstehen, verfolgen wir das Prinzip der Datensparsamkeit und beachten bei der Erhebung, Speicherung, Verarbeitung, Veränderung oder Übermittlung personenbezogener Daten die Zulässigkeitsvoraussetzungen und Interessensabwägungen des § 28 BDSG. Bei der Planung und Konzeption informations-technischer Sicherungseinrichtungen orientieren wir uns an den Empfehlungen des BSI.

Bei der Beschreibung organisatorischer Maßnahmen, kennzeichnen die Begriffe „dürfen“ und „können“ optionale Mitarbeiterverhaltensweisen. Begriffe wie „sollen“ oder „sind aufgefordert“ kennzeichnen empfohlene Mitarbeiterverhaltensweisen, von denen nur nach einer Interessensabwägung abgewichen werden darf. Begriffe wie „müssen“ oder „dürfen nicht“ stellen verbindliche Anweisungen an unsere Mitarbeiter dar.

Das vorliegende Dokument beschreibt den aktuellen Zustand der implementierten technischen und organisatorischen Maßnahmen sowie interne Verhaltensrichtlinien und Mitarbeiteranweisungen. Technische Details entsprechen einem garantierten Mindestschutzumfang. Ein höheres Schutzniveau kann umgesetzt/implementiert sein, aus Sicherheitsgründen jedoch der Geheimhaltung unterliegen.

2. Zugangs- und Zutrittskontrolle

Wir unterhalten keine öffentlich zugänglichen Räume oder Ladenflächen.

Der Zutritt von betriebsfremden Personen (z.B. Gäste) ist nur in Begleitung eines autorisierten Mitarbeiters gestattet.

Der Aufenthalt externer Dienstleister in unseren Räumlichkeiten ist nicht unbeaufsichtigt gestattet.

In den Büro- und Präsentationsräumen existieren keinerlei öffentlich zugängliche Netzwerkanschlüsse. WLAN Verbindungen sind mit 16-stelligen Zugangspasswörtern abgesichert und nur autorisierten Mitarbeitern bekannt.

3. Datenträgerkontrolle

Die Nutzung mobiler Datenträger wie externe Festplatten, USB-Sticks und Speicherkarten jeglicher Art sind für den Transport und die Aufbewahrung personenbezogener Daten, wie in Abschnitt 7 beschrieben, untersagt.

Ausgemusterte Datenträger werden formatiert und so dies aufgrund eines Hardwaredefekts des Datenträgers nicht möglich sein, mechanisch zerstört.

Wie im Abschnitt Verfügbarkeitskontrolle beschrieben, dürfen mobile Datenträger nicht mit Endgeräten verbunden werden. Entsprechend sind keine leicht zu entfernenden Datenträger vorhanden, die gelesen, kopiert, entfernt oder verändert werden könnten.

4. Speicherkontrolle

Die Kenntnisnahme personenbezogener Daten wird über die im Abschnitt Zugriffskontrolle beschriebenen Mechanismen gesteuert und unbefugte Kenntnisnahme verhindert.

Mitarbeiter sind auf den Umgang mit personenbezogenen Daten sensibilisiert und angewiesen, Unterstützungsleistungen gegenüber Dritten abzulehnen oder abzubrechen, wenn es hierdurch zu einer Übermittlung, unbefugten Kenntnisnahme oder sonstigen Verarbeitung personenbezogener Daten kommen sollte. Verantwortliche Dritte sind in diesem Zusammenhang aufgefordert, die Rechtmäßigkeit einer Verarbeitung glaubhaft zu machen, bevor Unterstützungsleistungen erbracht werden, bei denen personenbezogene Daten verarbeitet oder zur Kenntnis genommen werden.

5. Benutzerkontrolle

Die Benutzerkontrolle wird über die im Abschnitt Zugriffskontrolle beschriebenen Mechanismen durchgesetzt, unabhängig davon, ob es sich um einen Zugriff per Datenfernübertragung oder standortlokal handelt.

6. Zugriffskontrolle

Für die Zugriffssteuerung setzen wir ein differenziertes Berechtigungskonzept ein, das auf der Mitgliedschaft einzelner Mitarbeiter in verschiedenen Berechtigungsgruppen beruht (Role-Based Access Control (RBAC); TecArt Benutzer und Gruppen). Die Standardrechte unterliegen hierbei maximalen Einschränkungen und werden nur bei Bedarf erweitert. Die Entscheidung über Vergabe und Entzug von Rechten obliegt der Geschäftsführung. Sofern Mitarbeiter das Unternehmen verlassen, werden unverzüglich alle Rechte entzogen – der zugehörige TecArt Benutzer wird gesperrt.

Bei der Implementierung neuer Datenverarbeitungssysteme wird darauf geachtet, dass diese das zentralisierte Berechtigungskonzept unmittelbar für die jeweiligen Systemrechte umsetzen und Zugriffe protokolliert werden.

Für die TecArt Benutzer-Authentifizierung werden individuelle Benutzerpasswörter mit mindestens neun Zeichen verwendet, die Groß-/Kleinbuchstaben und Zahlen enthalten müssen. Die Verwendung

von Sonderzeichen ist optional. Mitarbeiter sind aufgefordert, ihre individuellen Benutzerpasswörter nicht mehrfach zu verwenden. Für Windows-Anmeldungen darf Windows Hello (Anmeldung mittels biometrischer Merkmale, wie Fingerabdruck, Gesichts- oder Iriserkennung) verwendet werden.

Für mobile Geräte und Arbeitsplatz-PCs (Client-Systeme) zugelassene Hersteller sind: HP, Samsung, Microsoft, Apple. Die Geräte müssen über ein Trusted Platform Module (TPM) zur Speicherung sensibler Schlüssel und Gewährleistung der Systemintegrität verfügen. Alle Windows Systeme müssen UEFI Secure Boot verwenden.

Client-Systeme sollen bei der Inbetriebnahme neu installiert werden. Hierfür soll ein Basis-Image verwendet werden. Ziel ist ein sauberes System ohne Backdoors.

Client-Systeme müssen bei Verlassen des Arbeitsplatzes gesperrt werden. Eine automatische Sperrung muss zudem nach längerer Inaktivität erfolgen.

Die Anbindung unseres internen Netzwerks (vertrauenswürdiges Netz) an öffentliche Netzwerke (nicht-vertrauenswürdige Netze) erfolgt durch WAN-VPN-Router mit Paketfilter der Hersteller AVM, Deutsche Telekom AG und XXX. Unsere Serversysteme werden durch eine Sophos UTM Firewall abgesichert.

Die Basis der Firewall-Regelwerke sieht zunächst ein vollständiges Blockieren der gesamten Netzwerkkommunikation vor. Notwendige Kommunikation wird explizit und nur auf Weisung der Geschäftsleitung freigegeben. Hierbei muss auf eine möglichst genaue Spezifikation der Kommunikationseigenschaften geachtet werden. Gewährende Firewall-Regeln sollen auf die zu erwartenden Nutzungszeiten eingeschränkt werden.

Kundennetze, mobile Mitarbeiter und HomeOffices werden – nach Möglichkeit - per VPN angebunden. Für die Transportsicherung kommen IPsec oder TLS (SSL-VPN) zum Einsatz. Für die Anbindung von Kundennetzen soll PFS sowie zertifikatsbasierte Authentifizierung, vor dem Einsatz von Preshared-Keys, verwendet werden. Beim Einsatz von Preshared-Keys gelten die Richtlinien für die Erstellung von Zugangsdaten für Fremdsysteme sinngemäß für die Erstellung des Preshared-Key. Konkrete Verschlüsselungsalgorithmen und Hashfunktionen werden unter Abwägung eines zu erreichenden Sicherheitslevels und des benötigten Rechenaufwands ausgewählt.

Kundennetze werden als nicht-vertrauenswürdige Netze betrachtet und entsprechend behandelt.

7. Weitergabekontrolle, Transportkontrolle und Übertragungskontrolle

Systeme, die zur Übertragung personenbezogener oder vertraulicher Daten eingesetzt werden, müssen mindestens eine Transportverschlüsselung einsetzen. Die damit zwingend einhergehenden Fehlererkennungs- und -korrekturverfahren sichern die Integrität der zu übermittelnden Daten. Mitarbeiter sollen Übertragungsweisen bevorzugen, die eine Ende-zu-Ende-Verschlüsselung unterstützen (z.B. Bereitstellung von Daten per Download über unsere Homepage www.unified-solution.de oder Microsoft OneDrive).

Protokolle ohne Transportsicherung dürfen nicht verwendet werden, wenn ein alternatives Protokoll mit Transportsicherung verfügbar ist (z.B für FTP, HTTP).

Für die Sicherung der Emailübertragung (IMAP und SMTP) setzen wir TLS ein. Für die Ende-zu-Ende-Sicherung von Übertragungen per www.unified-solution.de setzen wir HTTPS (SSL) ein. Unsere Identität weisen wir dabei über ein, von einem vertrauenswürdigen Drittanbieter signiertes, RSA-Webserverzertifikat nach. Die Identität des Empfängers wird über die Kenntnis einer Zufallszeichenfolge innerhalb einer bereitgestellten URL sichergestellt. Bei der Bereitstellung soll ein Zeitablauf sowie ein zusätzliches Kennwort vergeben werden.

Für die Übermittlung besonders sensibler oder vertraulicher Daten soll eine persönliche oder telefonische Kontaktaufnahme zur Verifikation der Empfängeridentität und Übermittlung einer Bereitstellungs-URL der zu übermittelnden Daten stattfinden. Bei telefonischer Übermittlung sensibler oder vertraulicher Daten muss die Telefonieverbindung mindestens bis zum Telefonieprovider verschlüsselt erfolgen (SIP-TLS/SRTP). Für verschlüsselte Telefonieverbindungen stehen uns die Provider STARFACE Connect und QSC zur Verfügung, die für ausgehende Gespräche automatisch ausgewählt werden. Für die Übermittlung besonders sensibler oder vertraulicher Daten sind Mitarbeiter außerdem angewiesen, für die per www.unified-solution.de oder Microsoft OneDrive zum Download bereitgestellten Daten, eine Dokumentenverschlüsselung (verschlüsseltes PDF) zu verwenden. Das Dokumentenkennwort soll dabei im Rahmen der persönlichen oder telefonischen Kontaktaufnahme übermittelt werden.

Aufgrund geänderter rechtlicher Rahmenbedingungen (DSGVO-Compliance) wird auf revisionssichere Emailarchivierung verzichtet (da Löschpflichten ansonsten nicht nachgekommen werden kann). Stattdessen werden Dokumenten und Emails über Kategorisierungen/Labels entsprechende Aufbewahrungsrichtlinien (Retention-Policies) zugewiesen, die neben der Sicherstellung der Einhaltung einer Aufbewahrungsdauer auch eine automatische Löschung von Daten vorsehen.

Die Übermittlung von Daten per Email wird protokolliert. Im Falle von aufbewahrungspflichtigen Emails, erfolgt eine revisionssichere Speicherung (Archivierung) der Emails für eine Dauer von 6 respektive 10 Jahren (zur Erfüllung gesetzlicher Anforderungen der GoBD aus HGB und AO). Diese Speicherung/Archivierung wird über Office 365 Retention-Policies umgesetzt.

Die Verwendung mobiler Datenträger (USB-Sticks, CDs/DVDs, mobile Festplatte, etc.) zum Transport personenbezogener Daten ist Mitarbeitern nicht gestattet. Die Annahme fremder mobiler Datenträger und deren Verwendung an unseren Datenverarbeitungssystemen ist Mitarbeitern ebenfalls untersagt.

Für Remote-Unterstützung/-Support beim Kunden setzen wir die Software TeamViewer, der TeamViewer GmbH aus Göppingen ein. Übertragungen sind hierbei durch Public-Key-Kryptographie (RSA 2048-Bit; Authentifizierung) und symmetrischer AES 256 Bit-Verschlüsselung (Transportsicherung) geschützt. Details sind einzusehen unter: https://www.teamviewer.com/de/security/ und https://dl.tvcdn.de/docs/de/TeamViewer-Security-Statement-de.pdf.

Mitarbeiter sind im Rahmen ihres Arbeitsvertrags zur Geheimhaltung und auf das Datengeheimnis nach § 5 BDSG verpflichtet. Diese Verpflichtung überdauert das Arbeitsverhältnis und besteht auch nach dessen Beendigung fort.

8. Eingabekontrolle

Die von uns eingesetzten Systeme zur Erhebung, Verarbeitung, Speicherung und Nutzung von Daten bestehen hauptsächlich aus unserem CRM System (TecArt) des Herstellers TecArt GmbH. Die Systeme protokollieren vollumfänglich jede Änderung an Daten sowie administrative Tätigkeiten inklusive des durchführenden Benutzers.

Daten (wie Dokumente, Emails oder allgemein Dateien), die im CRM System abgelegt werden, werden mit Hilfe von Subversion (SVN) versioniert. Eine Veränderung der Daten setzt voraus, dass ein berechtigter Mitarbeiter ein Dokument zur Bearbeitung auscheckt bzw. in einen Bearbeitungsmodus überführt und nach der Bearbeitung eincheckt bzw. die Änderung speichert und den Bearbeitungsmodus dadurch verlässt. Übergänge in den oder aus dem Bearbeitungsmodus werden protokolliert. Außerdem ist gewährleistet, dass ein Dokument zeitgleich nur durch einen Mitarbeiter verändert werden kann – im Bearbeitungsmodus ist das Dokument für andere Mitarbeiter gesperrt.

Die zur Erhebung, Verarbeitung, Speicherung und Nutzung von Daten verwendeten System werden täglich im Rahmen eines Backups gesichert.

9. Auftragskontrolle

Wir setzen derzeit keine externen Auftragnehmer für die Betreuung unserer eigenen Datenverarbeitungsanlagen ein. Alle von uns eingesetzten Dienste und System werden – mit Ausnahme von Microsoft Office 365-Diensten (Exchange Online, OneDrive for Business) – "on premise", auf unseren eigenen Servern an unserem Hauptstandort in Wiesbaden betrieben.

Unser externer Mailserver (Exchange Online) wird von Microsoft am Standort Wien (Österreich) betrieben. Weitere von uns genutzte Microsoft-Dienste, wie OneDrive for Business und SharePoint Online, werden in Rechenzentren in Irland oder den Niederlanden bereitgestellt. Die Datenschutzvereinbarung, Zertifizierungen und Compliance-Informationen befindet sich abrufbar unter:

https://www.microsoft.com/de-de/trustcenter/about/transparency

Nur auf ausdrücklichen Wunsch oder nach Zustimmung durch den Auftraggeber, werden Auftragsdaten zur Erbringung von Servicedienstleistungen (zum Beispiel für Support und Fehleranalysezwecke) an Soft- und Hardwareherstellers eines betroffenen Produkts übermittelt. Übermittelte Log-Dateien und Endkundeninformationen können als Nebenfolge hierbei personenbezogene Daten enthalten, die jedoch für keine anderen Zwecke als die Erbringung der konkreten Servicedienstleistung verwendet werden dürfen. Mit diversen Herstellern haben wir zu diesem Zweck Auftrags(daten)verarbeitungsverträge (AV-Verträge) geschlossen. Im Rahmen der Prüfung der technischen und organisatorischen Maßnahmen (TOM) der Hersteller wurde uns jeweils ein ausreichendes Schutzniveau zugesichert, welches jedoch nicht notwendigerweise dem von uns in diesem Dokument aufgeführten Schutzniveau entsprechen muss.

Wie unter Weitergabekontrolle, Absatz 8 beschrieben, fallen beim Anbieter TeamViewer GmbH Verkehrsdaten an. Darüber hinaus hätte der Anbieter die Möglichkeit eines Man-in-the-Middle-Angriffs auf TeamViewer-Sitzungen. TeamViewer wurde einer sicherheitstechnischen Prüfung der

FIDUCIA IT AG sowie einem BISG-Gutachten unterzogen. Darüber hinaus ist TeamViewer SOC 2 zertifiziert.

Weitere Kommunikationsverkehrsdaten fallen bei den Anbietern QSC, STARFACE Connect, HFO Telecom, Vodafone, Deutsche Telekom AG, peoplefone, Ecotel, Versatel, Telefónica o2 Germany, und sipgate an. Die Anbieter erbringen öffentlich zugängliche Telekommunikationsdieste und Telefondienste im Sinne des Telekommunikationsgesetzes (TKG) und unterliegen den besonderen Datenschutzanforderungen und dem Fernmeldegeheimnis des TKG.

Zum Zwecke der Buchführung und Erstellung von Jahresabschlüssen und deren Prüfung, ist nicht auszuschließen, dass personenbezogene Daten auf Belegen (Lieferscheine, Rechnungen, etc.) oder aus Fahrtenbüchern (Ansprechpartner eines Termins) an die Steuerberatungskanzlei Benedikt & Benedikt GmbH (Wiesbaden) und die DATEV eG (Nürnberg) übermittelt werden. Die Datenschutzvereinbarung und das Verfahrensverzeichnis der DATEV eG befindet sich abrufbar unter: https://www.datev.de/web/de/m/ueber-datev/datenschutz/.

Mitarbeiter der Benedikt & Benedikt GmbH sind als Berufsgeheimnisträger zu besonderer Sorgfalt und Geheimhaltung verpflichtet. Das Unternehmen hat einen Datenschutzbeauftragten zur Prüfung und ordnungsgemäßen Umsetzung von Anforderungen aus Datenschutzgesetzen bestellt.

10. Verfügbarkeitskontrolle, Wiederherstellbarkeit, Zuverlässigkeit und Datenintegrität

Unsere Datenverarbeitungsanlagen sind vollständig mindestens zweifach-redundant ausgelegt. Jeweils zwei Online-USVs versorgen die redundanten Netzteile eines Servers oder PoE-Switches und sichern diese gegen Überspannung und Stromausfälle ab. Betriebssystemspeicher sind RAID-1 datengespiegelt. Alle weiteren Datenspeicher befinden sich auf RAID-5 Volumes mit einem Hotspare-Laufwerk oder auf RAID-6 Volumes.

Das Virenschutzkonzept sieht eine Perimetersicherung durch die UTM-Firewalls vor und setzt auf den in Windows integrierten Windows Defender. Die Mitarbeiter sind darüber hinaus sensibilisiert und geschult, auf den Umgang mit Daten unbekannter Herkunft, die Verifizierung von Datei-Prüfsummen und die Verwendung von Plattformen wie VirusTotal zur Prüfung fremder Dateien.

Windows-Updates und Updates der Firewall (Firm-/Software, Signaturdateien, etc.) werden regelmäßig durchgeführt. Diverse Quellen für Zero-Day-Exploit-Informationen (Mailinglisten, Twitter, Websites) werden von uns überwacht, um schnellstmöglich auf mögliche Sicherheitslücken reagieren zu können.

11. Umsetzung des Trennungsgebots

Die Daten des Auftraggebers werden physikalisch oder logisch / virtuell von anderen Daten getrennt. Die Datensicherung erfolgt auf physikalisch oder virtuell getrennten Einheiten. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

Mitarbeiter sind in Rechtegruppen unterteilt (z.B. Buchhaltung, Service/Support, Geschäftsführung, etc.), die mit unterschiedlichen Zugriffsrechten unterschiedlichem Funktionsumfang innerhalb einzelner Dienste einhergehen.