AV DSGVO Sage_GmbH_Anhang-03_TOMs
Technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO
für den Sage-Standort Wien

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

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

1.1 Zutrittskontrolle

Der allgemeine Zutritt zum Gebäude erfolgt über ein elektronisches Zutrittskontrollsystem. Besucher müssen sich am Empfang anmelden, Ihre Identität wird überprüft und sie dürfen nur in Begleitung eines Sage Mitarbeiters die Räumlichkeiten betreten.

Der Zutritt zum Serverraum wird über ein elektronisches Zutrittskontrollsystem kontrolliert. Zugang haben nur ausgewählte Mitarbeiter der IT.

Alle Räumlichkeiten sind außerhalb der Arbeitszeiten mittels Alarmanlage gesichert. Alarmbereitschaft eines Wachschutzes ist gegeben.

1.2 Zugangskontrolle

Für die Anmeldung an das Netzwerk ist ein Kennwort mit einer Länge von mindestens 14 Zeichen vorgeschrieben. Dabei sind Zahlen und Sonderzeichen zu verwenden sowie Groß- und Kleinschreibung zu beachten. Für alle Zugriffe in- und außerhalb des VPN wird eine 2-Faktor-Authentifizierung verlangt.

Eine automatische Sperrung des Benutzers erfolgt nach drei falschen Eingaben bei der Benutzeranmeldung. Eine Aktivierung des Bildschirmschoners erfolgt nach 10 Minuten und kann nur wieder über Passworteingabe freigegeben werden.

Die Benutzerauthentifizierung wird mittels eines zentralen Verzeichnisdienstes abgebildet. Grundsätzlich und soweit nicht technisch notwendig, ist ein Zugang zu Auftragsdaten nur mittels personifizierten Accounts zugelassen.

Das System wird durch eine Firewall ständig überwacht. Es gibt eine Antivirus-Software auf Systemebene. Darüber hinaus ist für das Mail-System eine Antivirus-Software je Client sowie Server installiert. Es werden ausschließlich IT-Systeme eingesetzt, die vom Hersteller durch regelmäßige Sicherheitsupdates unterstützt werden.

Logdaten der einzelnen Systeme werden zentral zum Monitoring durchgehend 24/7 durch ein Sage Application & Information Security Team zusammengeführt und ausgewertet.

1.3 Zugriffskontrolle

Die Zugriffskontrolle ist in differenzierten Berechtigungen auf Menü-Ebene eingerichtet. Ein elektronischer Datensafe überwacht den Zugang der Supportmitarbeiter zu Kundendaten und ist nur mittels VPN und MFA möglich. Zugriffe auf Anwendungen werden protokolliert. Zu diesem Zweck werden Logdaten der einzelnen Systeme an einen zentralen Dienst übertragen und stehen dort einem Sage Application & Information Security Team 24/7 zur Verfügung.

1.4 Trennungskontrolle

Soweit eine getrennte Verarbeitung von Datenbeständen erforderlich ist, wurde diese entsprechend eingerichtet. Für Tests oder Entwicklung gibt es eigene Domains.

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Datenbanken der Sage Produkte und unserer internen IT-Systeme sind normalisiert – soweit Business Prozesse es nicht anders erfordern. Das heißt, personenbezogene Daten werden für gewöhnlich in eigenen Datenbanktabellen gespeichert. Sie sind mit Verarbeitungsvorgängen, wie z.B. Tickets,

Abrechnungen, Dokumente etc. über Schlüssel verknüpft. Passwörter werden verschlüsselt gespeichert.

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

2.1 Weitergabekontrolle

Der Transport außerhalb des jeweiligen Netzwerks erfolgt verschlüsselt. Hierzu werden starke Verschlüsselungsalgorithmen eingesetzt. Kundendaten können nur elektronisch direkt in den Datensafe übermittelt werden. Personenbezogene Daten aus dem Datensafe werden nicht weitergegeben. Sie werden mit Abschluss eines Supporttickets automatisch nach einer Frist von 4 Wochen gelöscht.

Alle verbundenen Unternehmen und die einzelnen Standorte der Sage in Zentraleuropa sind über eine Standleitung verbunden. Festplatten von Arbeitsplatzrechnern sowie mobile Datenträger werden mit aktueller Verschlüsselungstechnik geschützt.

2.2 Eingabekontrolle

Alle Netzwerkan- und -abmeldungen sowie sämtliche Transaktionen (z.B. Neuanlagen, Veränderungen, Löschungen) werden protokolliert. Die Protokolle werden hinsichtlich unberechtigter Zugriffe analysiert und nach 6 Monaten gelöscht.

Spezielle Werkzeuge überwachen außerdem unseren gesamten internen und externen Netzwerkverkehr auf ungewöhnliche Aktivitäten und melden diese automatisch, um weitere Nachforschungen anzustoßen.

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

3.1 Verfügbarkeitskontrolle

Es wird ein wöchentliches Backup (Vollsicherung) durchgeführt. Dazu wird zusätzlich täglich inkrementell gesichert. Die Sicherung erfolgt in zwei räumlich getrennten Rechenzentrums-Bereichen auf entsprechenden Storage Systemen.

Es wird ein RAID-Verfahren bei den Festplattensicherungen eingesetzt. Unterbrechungsfreie Stromversorgung (USV) samt Überspannungsschutz ist vorhanden.

Durch den Einsatz der Firewall und der Antivirus-Software für das Mail-System und alle Server, sowie Antivirus-Software je Client wird die Verfügbarkeit technisch bestmöglich sichergestellt.

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

4.1 Datenschutz-Management

Alle Mitarbeiter bei Sage sind auf das Datengeheimnis verpflichtet. Es erfolgt eine regelmäßige Unterweisung der Mitarbeiter im Datenschutz. Ein Datenschutzkonzept und eine IT-Policy wurden erstellt. Zusätzlich existieren Sage-weit geltende Richtlinien zur Informationssicherheit und zum Schutz personenbezogener Daten. OneTrust ist konzernweit für das Management des Datenschutzes im Einsatz.

Ein Datenschutzbeauftragter wurde bestellt: E-Mail: DSGVO@sage.com. Die Organisation kommt ihren Informationspflichten nach Art. 13 und 14 DSGVO nach. Zur Erfüllung von Betroffenenrechten gemäß Kapitel 3 DSGVO existiert ein formalisierter Prozess. Für die eingesetzten IT-Systeme und Prozesse existieren Verarbeitungsverzeichnisse. Die Wirksamkeit unserer technischen und organisatorischen Schutzmaßnahmen wird in Abstimmung mit dem Sage-Konzern regelmäßig überprüft.

4.2 Incident-Response-Management

Firewalls, Spamfilter und Virenscanner werden eingesetzt und regelmäßig aktualisiert. Daneben existieren Systeme zur „Intrusion Detection and Prevention“. Eine Policy regelt den Umgang mit Sicherheitsvorfällen. Es gibt Alarmpläne und eine Dokumentation von Sicherheitsvorfällen und

Datenpannen. Dabei werden Datenschutz, IT-Security sowie Rechtsabteilung stets involviert. In Abstimmung mit dem Datenschutz erfolgen Meldungen gegenüber den Aufsichtsbehörden.

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

Die Prozesse für Softwarepflegeleistungen, die im Zusammenhang mit personenbezogenen Daten stehen, sind klar definiert. Die involvierten Mitarbeiter sind per bindender Arbeitsanweisung entsprechend verpflichtet. Dazu gehört, dass Kundendaten nur über den Datensafe entgegengenommen und verwaltet werden. Die Mitarbeiter sind angehalten nicht mehr personenbezogene Daten zu erheben, als für den jeweiligen Zweck erforderlich sind. Aufzeichnungen von Remote-Sitzungen werden nach 4 Wochen automatisch gelöscht.

4.4 Auftragskontrolle (Outsourcing an Dritte)

Unsere Mitarbeiter kennen den Datenverarbeitungszweck. Sie erhalten Weisungen zum Umgang mit personenbezogenen Daten. Spezielle Unterauftragsverhältnisse (Subunternehmer) werden schriftlich beauftragt und sind bei den jeweiligen Produkten bzw. Services im Anhang Produkte zur AV-Vereinbarung aufgeführt. Zwischen den einzelnen Sage-Gesellschaften bestehen Vereinbarungen zur Auftragsverarbeitung (Controller-to-Controller und Controller-to Processor) auf Basis von EU-Standardvertragsklauseln.