Konzept der technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO

SMEA IT Services GmbH
Industriestraße 14
18069 Rostock

Tel.: +49 381 383839-0
Fax: +49 381 383839-39
Mail: info@smea-it.de

Änderungshistorie

Version	Datum	Autor
2018-03	03.04.2018	Torsten Prehn – Geschäftsführung Marcel Erntges – Datenschutzbeauftragter
2018-04	26.04.2018	Torsten Prehn – Geschäftsführung
2018-05	05.05.2018	Torsten Prehn – Geschäftsführung
2018-05	26.05.2018	Torsten Prehn – Geschäftsführung
2019-07	19.07.2019	Torsten Prehn – Geschäftsführung
2021-02	19.02.2021	Torsten Prehn – Geschäftsführung
2021-12	10.12.2021	Torsten Prehn – Geschäftsführung

SMEA IT Services GmbH, Industriestraße 14, 18069 Rostock - HR-B: 9320 Amtsgericht Rostock | USt.ID: DE226089681
Geschäftsführer: Christian Bartsch, Torsten Prehn – Fon 0381/3838390, Fax 0381/3838390 – service@smea-it.de

1. Gegenstand und Geltungsbereich

Dieses Konzept dokumentiert die Einrichtungen und die Organisation zum Datenschutz bei der SMEA IT Services GmbH (nachfolgend „SMEA IT“ genannt). Als Leitfaden dient die Anlage zu Art. 32 Datenschutzgrundverordnung (DS-GVO). Dieses Konzept kann als Nachweis für getroffene Sicherheitsmaßnahmen für Auftraggeber bei Verträgen zur Datenverarbeitung im Auftrag oder weitere interessierte Dritte dienen.

2. Ansprechpartner

Geschäftsführer
Torsten Prehn, tprehn@smea-it.de

Datenschutzbeauftragter
Herr Marcel Erntges, dsb@smea-it.de

3. Sicherheitsmaßnahmen

3.1 Allgemeines

Die SMEA IT hat einen Datenschutzbeauftragten bestellt. Der Datenschutzbeauftragte wirkt auf die Einhaltung des Datenschutzes hin. Mitarbeiter sind auf die Verschwiegenheit und die Wahrung des Datengeheimnisses verpflichtet worden. Der Datenschutzbeauftragte berät die Geschäftsführung und die Mitarbeiter hinsichtlich des Datenschutzes und führt Kontrollen auf die Einhaltung des Datenschutzes im Unternehmen durch.

3.2 Zutrittskontrolle

Die SMEA IT trägt dafür Sorge, dass Unbefugte keinen Zugang zu Datenverarbeitungsgeräten des Unternehmens (Server, Arbeitsplatzrechner, Monitore, Drucker, etc.) erlangen können und Räume, in denen Daten verarbeitet werden, nicht betreten können.

Der Zutritt zum Gebäude am Hauptsitz der SMEA IT und den darin genutzten Räumlichkeiten ist durch eine General-Sicherheitsschließanlage gesichert, die sich unter Kontrolle der SMEA IT befindet. An anderen Standorten genutzte Räumlichkeiten verfügen mindestens über Sicherheitsschließsysteme mit einzeln identifizierbaren Schlüsseln oder Zugangstoken. Besonders sicherheitsrelevante Bereiche, wie z.B. Rechenzentren, sind mit zusätzlichen elektronischen Zutrittskontrollen und Alarmaufschaltung versehen. Mitarbeiter erhalten mit Aufnahme ihrer Tätigkeit bei der SMEA IT Schlüssel und Sicherheitstoken, die ihnen nur den Zutritt zu den für sie freigegebenen Bereichen ermöglichen. Der Entzug dieser Zutrittsberechtigung ist geregelt. Ausgabe und Einzug der Schlüssel und Token werden dokumentiert.

Besucher werden während ihres Aufenthalts in Räumen der SMEA IT von Firmenpersonal begleitet. Besucher haben keinen Zutritt zu technischen Betriebsräumen, Werkstätten und Lagern.

SMEA IT Services GmbH, Industriestraße 14, 18069 Rostock - HR-B: 9320 Amtsgericht Rostock | USt.ID: DE226089681
Geschäftsführer: Christian Bartsch, Torsten Prehn – Fon 0381/3838390, Fax 0381/3838390 – service@smea-it.de

3.3 Zugangskontrolle

Die SMEA IT hat verschiedene Maßnahmen zur Zugangskontrolle implementiert, um zu verhindern, dass Unbefugte Datenverarbeitungsanlagen des Unternehmens nutzen können oder unberechtigt auf Daten des Unternehmens zugreifen können.

Die Zugänge zu den Firmennetzwerken der SMEA IT werden an allen Standorten durch Firewalls nach intern und extern geschützt. Nur zugelassene, überprüfte Geräte können eine Verbindung mit den internen Netzwerken herstellen.

Bei der Anmeldung an Systemen müssen sich die Anwender persönlich authentifizieren. Alle Mitarbeiter wurden über die geltenden Anforderungen an sichere Anmeldeverfahren in Kenntnis gesetzt und sind darüber informiert, wie IT-Geräte bei Verlassen des Arbeitsplatzes zu sichern sind.

Für die Anmeldung an Onlinediensten ist zusätzlich eine mehrstufige Authentifizierung (MFA) vorgeschrieben und eingerichtet. Soweit technisch möglich, wird MFA über zentrale Richtlinien erzwungen.

Für alle Rechner im Büro-Netzwerk der SMEA IT wird eine Anmeldesperre bei Inaktivität erzwungen. Für mobile IT-Geräte werden Konformitätsrichtlinien erzwungen, die u.a. Zugangspassworte, Gerätesperre bei Inaktivität und Geräteverschlüsselung beinhalten.

3.4 Zugriffskontrolle

Die SMEA IT gewährleistet, dass ausschließlich Personen Zugriff auf Daten erlangen, die mit der Erfüllung der damit verbundenen Aufgabe beschäftigt sind. Hierzu sind entsprechende Zugriffsberechtigungsmaßnahmen (Profile, Gruppen, Rollen etc.) eingerichtet.

Der Zugriff zu Informationen, die auf Systemen der SMEA IT abgelegt sind, wird ausschließlich auf “Need-to-know-Basis” gewährt. Bei der Anmeldung an den Datenverarbeitungssystemen der SMEA IT wird dem Benutzer ein definiertes Profil zugeordnet.

Sofern eine Softwareapplikation die Möglichkeit zur Rollen- und Rechtevergabe bietet, werden diese Möglichkeiten, auf Grundlage der im vorhergehenden Absatz geschilderten Grundsätze, genutzt.

Die gespeicherten Daten werden, soweit technisch möglich, zusätzlich durch ein Rechtemanagement-/Informationsmanagementsystem geschützt. Daten werden dadurch verschlüsselt und der Zugriffsschutz unabhängig vom Speicherort gewährleistet.

Zugriffe auf Daten und Systeme werden im Rahmen der technischen Möglichkeiten der Systeme protokolliert.

3.5 Weitergabekontrolle

Die SMEA IT gewährleistet im Rahmen der technischen Möglichkeiten und soweit sie administrative Hoheit über die entsprechenden technischen Systeme hat, dass Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Übertragung von personenbezogenen Daten (u.a. per E-Mail) erfolgt besonders geschützt. Bei der Übertragung wird standardmäßig eine Verschlüsselung des Transportwegs versucht, die auf Anforderung auch erzwungen werden kann. Zusätzlich kann auf Wunsch des Kommunikationspartners eine Verschlüsselung der Mailinhalte erfolgen. Die Speicherung, der Versand oder Transport von personenbezogenen Daten auf mobilen Datenträgern (CD, USB-Stick, Speicherkarten etc.) erfolgt nur verschlüsselt. Der externe Zugriff auf Datenverarbeitungsanlagen der SMEA IT erfolgt ausschließlich über sichere verschlüsselte Verbindungen.

SMEA IT Services GmbH, Industriestraße 14, 18069 Rostock - HR-B: 9320 Amtsgericht Rostock | USt.ID: DE226089681
Geschäftsführer: Christian Bartsch, Torsten Prehn – Fon 0381/3838390, Fax 0381/3838390 – service@smea-it.de

3.6 Eingabekontrolle

Wo immer technisch möglich gewährleistet die SMEA IT, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Informationssysteme werden in der Form konfiguriert, dass eine Vorgangsprotokollierung zur Verfügung steht, die das Betriebs-, Sicherheits- und Datenschutzmanagement in ausreichender Weise unterstützt.

Dafür zur Verfügung stehende Protokollierungssysteme wurden aktiviert. Die Protokolle werden regelmäßig ausgewertet.

3.7 Auftragskontrolle

Die SMEA IT stellt sicher, dass Auftragnehmer in Fällen von Datenverarbeitung im Auftrag sorgfältig ausgewählt werden.

Die SMEA IT gewährleistet, dass personenbezogene Daten der Auftraggeber nur gemäß deren Weisungen verarbeitet werden. Beschäftigt die SMEA IT einen Unterauftragnehmer, so wird dieser in gleicher Weise zur Erfüllung der Weisungen und zur Einhaltung des Datenschutzes verpflichtet. Die SMEA IT kontrolliert in regelmäßigen Abständen die Einhaltung der vertraglichen Regelungen.

3.8 Verfügbarkeitskontrolle

Die SMEA IT sorgt dafür, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Verschiedene Datensicherungsverfahren wurden konfiguriert und aktiviert. Dazu gehören redundante Speicherung, mehrstufige „Papierkörbe“, Versionierung, Archivierung mit Schutz vor endgültiger Löschung sowie regelmäßiges Backup. Sicherungsdaten werden je nach technischer Möglichkeit räumlich/geografisch getrennt von den Produktivsystemen gespeichert.

Die ausschließliche Speicherung geschäftsrelevanter Daten auf Endgeräten wird durch organisatorische und technische Maßnahmen verhindert (Arbeitsanweisungen, Richtlinien im Devicemanagement). Soweit technisch möglich wird eine Grundverschlüsselung der Datenspeicher aller genutzten Systeme erzwungen. Mobile Endgeräte ohne eine solche Verschlüsselung dürfen nicht in Einsatz gebracht werden.

Erfolgreiche Angriffe durch unbefugte Dritte werden durch ein Bündel sich ergänzender Maßnahmen verhindert, die den Schutz von Daten, Geräten, Anwendungen und Identitäten sicherstellen. Computersysteme verfügen über eine lokale Endpointprotection u.a. vor Malware, Spyware und Zero-Day-Exploits. Der Schutz wird zentral verwaltet, protokolliert und durch aktuelle KI-basierte Technologien unterstützt. Der Zugriff auf Daten wird durch Conditional-Access-Richtlinien, Multifaktorauthentifizierung und Informationprotection-Richtlnien (RMS/IRM) abgesichert.

Sind Updates für Systeme oder Anwendungen verfügbar, werden sie so schnell wie möglich ausgewertet und nach Freigabe automatisiert installiert. Die Installation sicherheitsrelevanter Updates wird priorisiert.

Netzwerke an Bürostandorten der SMEA IT sind durch Firewalls/UTM-Gateways geschützt. An den Übergängen zum Internet werden Inhalts- bzw. Schadsoftwarefilter eingesetzt. Bei den eingesetzten Firewalls werden nur benötigte Protokolle und Anschlüsse zugelassen. Änderungen am Regelwerk können nur Mitarbeiter der internen IT-Abteilung durchführen. Auf Endgeräten wird die Aktivierung der lokalen Firewalls erzwungen und überwacht.

SMEA IT Services GmbH, Industriestraße 14, 18069 Rostock - HR-B: 9320 Amtsgericht Rostock | USt.ID: DE226089681
Geschäftsführer: Christian Bartsch, Torsten Prehn – Fon 0381/3838390, Fax 0381/3838390 – service@smea-it.de

Alle durch die SMEA IT betriebenen zentralen IT Systeme, die für die Weiterführung des Geschäftsbetriebs wichtig sind, werden vor den Auswirkungen durch Stromschwankungen oder Stromausfälle geschützt. Dies erfolgt im Wesentlichen durch den Einsatz unterbrechungsfreier Stromversorgungen. Für selbst betriebene Rechenzentren sind diese mehrstufig ausgelegt.

3.9 Trennungsgebot

Die SMEA IT sorgt dafür, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden. Die Trennung der Daten ist so gestaltet, dass eine „Vermischung“ von Daten für unterschiedliche Verarbeitungszwecke oder anderer Vertragspartner / Auftraggeber nicht möglich ist.

SMEA IT Services GmbH

SMEA IT Services GmbH, Industriestraße 14, 18069 Rostock - HR-B: 9320 Amtsgericht Rostock | USt.ID: DE226089681
Geschäftsführer: Christian Bartsch, Torsten Prehn – Fon 0381/3838390, Fax 0381/3838390 – service@smea-it.de