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

SMEA IT Services GmbH
Industriestraße 14
18069 Rostock

Tel.: +49 (0)381 / 383839-0
Fax: +49 (0)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

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 und allen Räumlichkeiten im Gebäude ist durch eine General-Hauptschließanlage gesichert. Einzelne Bereiche sind durch zusätzliche elektronische Zutrittskontrollen geschützt. Mitarbeiter bekommen mit Aufnahme ihrer Tätigkeit bei SMEA IT Schlüssel und Sicherheitstoken, die ihnen nur den Zutritt zu den für sie freigegebenen Bereichen ermöglichen. Der Entzug dieser Gebäudezutrittsberechtigung ist geregelt.

Der Zutritt und Aufenthalt von Besuchern zu den Büros der Mitarbeiter erfolgt nur in Begleitung von Firmenpersonal. Besucher haben keinen Zutritt zu Technikräumen (Rechenzentrum, Werkstatt).

3.3 Zugangskontrolle

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

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

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 vorgeschrieben und eingerichtet.

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.

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) kann auf Wunsch des Kommunikationspartners geschützt erfolgen. Speicherung, 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.

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.

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

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. Dazu wurden Datensicherungsverfahren eingerichtet. Sicherungsdaten werden räumlich getrennt von den Produktivsystemen gespeichert. Die SMEA IT hat Anlagen für die unterbrechungsfreie Stromversorgung installiert sowie Schutzmaßnahmen eingerichtet, die Angriffe durch unbefugte Dritte verhindern (Virenschutz, Firewall, Spyware Detection, Paketfilter, DMZ, etc.).

Alle SMEA Dienste, 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.

Die Daten jedes Servers werden durch ein zentralisiertes Backup-System gesichert. Datenträger für die Datenrückgewinnung im Notfall werden aufbewahrt.

Wenn Updates für Systeme oder Anwendungen angekündigt werden, werden sie so schnell wie möglich ausgewertet und nach Freigabe installiert. Die Installation sicherheitstechnischer Updates wird priorisiert.

Auf allen für die Verarbeitung personenbezogener Daten verwendeten Rechnern sind Virenscanner installiert und aktiviert. Gespeicherte und verarbeitete Dateien (E-Mails, Downloads, Dokumente, etc.) werden durch den Echtzeitschutz auf Virenbefall gescannt. Updates für die Sicherheitssysteme und weitere im Einsatz befindliche Software werden automatisiert verteilt.

An den Übergängen zum Internet werden Inhalts- bzw. Schadsoftwarefilter eingesetzt. Die genutzten Onlinedienste (z.B. das Mailsystem und die Speicherorte für Dokumente) werden durch verschiedene, mehrstufige Schutzmechanismen der Anbieter gesichert.

Bei den eingesetzten Firewalls werden nur benötigte Protokolle und Anschlüsse zugelassen. Änderungen an der Firewall und dem Regelwerk können nur Mitarbeiter der IT-Abteilung durchführen. Auch auf Endgeräten sind Firewalls installiert.

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