Datensicherheitskonzept

Technische und organisatorische Maßnahmen (TOM)
i.S.d Art. 32 DSGVO

Datenschutzmaßnahmen

Präambel

Die im Folgenden beschriebenen t*echnischen und organisatorischen Maßnahmen (TOM)* sind die Datensicherheitsmaßnahmen, die von O.OPEN getroffen wurden um zu gewährleisten, dass die Sicherheits-. und Schutzanforderungen i.S.d. *Art. 32 DSGVO* erfüllt sind.

I Vertraulichkeit

Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

Rechner und Systeme in den Räumlichkeiten des Auftraggebers

- Die Verantwortung der Zutrittskontrolle obliegt dem Auftraggeber.

Rechner und Systeme in Rechenzentren – Hosting von Internet Services

- elektronisches Zutrittskontrollsystem.
- dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden.
- Videoüberwachung an den Ein- und Ausgängen.

EDV-Systeme O.OPEN

- O.OPEN verwendet für die Administration von Rechnern und Services stationäre Desktop-PCs wie auch mobile Laptops. Die Desktop PCs befinden sich in einem Büroraum des Inhabers von O.OPEN, Christoph Kuchenbuch, in dessen Privatwohnung. Alle Betriebssysteme und die darin installierte Software, die zur Administration von Systemen eingesetzt werden, befinden sich auf verschlüsselten Partitionen. Das gilt sowohl für die betrieblichen Laptops wie Desktop-PCs.

Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

Rechner und Systeme in den Räumlichkeiten des Auftraggebers

- Personalisierte Accounts.
- SSH-Verbindung ausschließlich im Key Verfahren.
- Passwortgeschützte Benutzerkonten.
- VPN Verbindung, Legitimierung durch passwortgeschütztes Zertifikat.
- Absicherung durch eine Firewall.
- Grundsätzlich keine initialen Verbindungen aus dem öffentlichen Internet in nichtöffentliche Netzwerke. Ausnahmen sind administrative Zugänge, und die Bereitstellung von Services die vom Auftraggeber explizit autorisiert sind.

Rechner und Systeme in Rechenzentren – Hosting von Internet Services

- Personalisierte Accounts.
- SSH-Verbindung ausschließlich im Key Verfahren.
- Passwortgeschützte Benutzerkonten.
- Absicherung durch eine Firewall.

EDV-Systeme des Auftragnehmers

- Der Zugang zu den EDV-Systemen von O.OPEN ist nur mit personalisierten, passwortgeschützten Accounts möglich.

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

Rechner und Systeme in den Räumlichkeiten des Auftraggebers

- Alle Mitarbeiter sind auf das Datengeheimnis nach *§ 53 BDSG* verpflichtet.
- Regelmäßige Sicherheitsupdates nach dem Stand der Technik.
- Prinzip der minimalen Rechte.

Rechner und Systeme in Rechenzentren – Hosting von Internet Services

- Alle Mitarbeiter sind auf das Datengeheimnis nach *§ 53 BDSG* verpflichtet.
- Regelmäßige Sicherheitsupdates nach dem Stand der Technik.
- Prinzip der minimalen Rechte.
- FTP-Accounts voneinander isoliert (chrootet).

Trennungskontrolle

Maßnahmen des Auftragnehmers, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Rechner und Systeme in den Räumlichkeiten des Auftraggeber

- Die Verantwortung der Trennungskontrolle obliegt dem Auftraggeber.

Rechner und Systeme in Rechenzentren – Hosting von Internet Service

- Daten sind auf File- und Datenbankebene logisch und/oder physikalisch voneinander getrennt.
- Tägliche Sicherung aller relevanten Daten.
- Die Datensicherung erfolgt auf physikalisch und örtlich voneinander getrennten Systemen.

EDV-Systeme des Auftragnehmers

- In der EDV-Umgebung des Auftragnehmers befinden sich neben den Kontaktdaten des Auftraggebers keine personenbezogenen Daten.

Pseudomisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technichen und organisatorischen Maßnahmen unterliegen.

- De Verantwortung der Pseudomisierung obliegt dem Auftraggeber.

II Integrität

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Rechner und Systeme in den Räumlichkeiten des Auftraggebers

- Regelmäßige Sicherheitsupdates nach dem Stand der Technik.
- Absicherung durch eine Firewall.

Rechner und Systeme in Rechenzentren – Hosting von Internet Services

- Alle Mitarbeiter sind auf das Datengeheimnis nach *§ 53 BDSG* verpflichtet.
- Regelmäßige Sicherheitsupdates nach dem Stand der Technik.
- Datenschutzgerechte Löschung der Daten nach Weisung des Auftraggebers.
- Möglichkeiten zur verschlüsselten Datenübertragung werden zur Verfügung gestellt.
- Absicherung durch eine Firewall.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Rechner und Systeme in den Räumlichkeiten des Auftraggebers

- Die Verantwortung zur Protokollierung auf den zu administrierenden Systemen obliegt dem Auftraggeber.

Rechner und Systeme in Rechenzentren – Hosting von Internet Services

- Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
- Änderungen der Daten werden automatisch protokolliert.

III Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Maßnahmen des Auftragnehmers, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Rechner und Systeme in den Räumlichkeiten des Auftraggeber

- Die Verantwortung der Verfügbarkeitskontrolle insbesondere der Datensicherung obliegt dem Auftraggeber.

Rechner und Systeme in Rechenzentren – Hosting von Internet Service

- Tägliche Sicherung (Backup) aller relevanten Daten.
- Sachkundiger Einsatz von Schutzprogrammen wie etwa Firewall und SPAM-Filter.
- Festplatten sind im RAID-Verfahren eingebunden, mindestens RAID 1.
- Monitoring aller relevanten Services.

EDV-Systeme des Auftragnehmers

- In der EDV-Umgebung des Auftragnehmers befinden sich neben den Kontaktdaten des Auftraggebers keine perosnenbezogenen Daten.

IV Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz Management

- Alle Mitarbeiter werden im Umgang mit Vertraulichkeit von Daten geschult und sind auf das Datengeheimnis nach *§ 53 BDSG* verpflichtet.
- Den Informationspflichten i.S.d. *Art.13 und 14 DSGVO* wird nachgekommen.
- Die Wirksamkeit der technischen Schutzmaßnahmen werden regelmäßig überprüft und gegebenenfalls angepasst.

Die Voraussetzungen für die Bestellung eines betrieblichen Datenschutzbeauftragten liegen nicht vor

Incident-Response-Management

Unterstützung bei de Reaktion auf Sicherheitsverletzungen

Rechner und Systeme in den Räumlichkeiten des Auftraggebers

- Absicherung der internen Netzwerke durch seperaten Gateway Rechner unter Einsatz einer Firewall.
- Weiterer organisatorischer Maßnahmen werden ggf. in einem schriftlichen Vertrag zur Auftragsdatenverarbeitung gem. *Art. 28 DSGVO* geregelt.

Rechner und Systeme in Rechenzentren – Hosting von Internet Services

- Regelmäßige Sicherheitsupdates von Betriebssystem und installierten Services.
- Absicherung durch eine Firewall
- Je nach auf den Systemen bereitgestelllten Services werden weitere Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) eingesetzt.

Detenschutzfreundliche Voreinstellungen

- Das Prinzip der Datensparsamkeit und Datenminimierung i.S.d. *Art. 5 Abs. 1(c) DSGVO* wird berücksichtigt.
- Datenschutzfreundliche Voreinstellungen i.S.d. *Art 25 Abs.2 DSGVO* bei Softwareentwicklung und Konfiguration von Services werden berücksichtigt.

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

Rechner und Systeme in den Räumlichkeiten des Auftraggebers

- Schriftlicher Vertrag zur Auftragsdatenverarbeitung gem. *Art. 28 DSGVO*

Rechner und Systeme in Rechenzentren – Hosting von Internet Services

- Keine Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Solche Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
- Datenschutzgerechte Löschung der Daten nach Weisung des Auftraggebers.

Ort, Datum

Berlin, den **28.05.2018**

O.OPEN – Christooph Kuchenbuch