Beschreibung der technischen und organisatorischen Maßnahmen

Organisationskontrolle

Organisatorische Maßnahmen zur Sicherstellung der besonderen Anforderungen des Datenschutzes: Organisationskontrolle-Checkliste

---

1. Datensicherungsmaßnahmen - Vertraulichkeit

Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden: Die Geschäftsräume der w3 GmbH befinden sich in der Betriebsstätte in 88250 Weingarten (Büro & Produktion), sowie in 88212 Ravensburg (Produktion Werbetechnik).

Die Zugänge zum Bürohaus und auch zu den Büroräumen der w3 GmbH sind Nachts verschlossen. Zugang zum Bürohaus haben Mitarbeiter, Kunden und Besucher. Es kommt ein Sicherheits-Schließsystem zum Einsatz, das von der Geschäftsführung verwaltet wird.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Besucher erhalten nur zum Empfang Zutritt und dann den Büroräumen. Der Empfang kann die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet.

Jeder Besucher wird von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet.

Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

Zutrittskontrolle-Checkliste

Zugangskontrolle

Für die Zugangskontrolle sind nachfolgende Maßnahmen von der w3 GmbH getroffen worden:

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt

wurde.

Der Benutzer erhält dann einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben und Ziffern bestehen muss.

Passwörter werden alle 90 Tage gewechselt. Ausgenommen hiervon sind Passwörter, die über eine Mindestlänge von 32 Zeichen verfügen. Hier ist ein automatischer Passwortwechsel nicht indiziert.

Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen 3 Passwörter nicht noch einmal verwendet werden können.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

Remote-Zugriffe auf IT-Systeme der w3 GmbH erfolgen stets über verschlüsselte Verbindungen.

Auf den Servern der w3 GmbH ist ein Intrusion-Prevention-System im Einsatz. Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.

Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.

Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen, sofern technisch möglich wird das IT-System ohne Benutzerinteraktion nach 5 Minuten automatisch gesperrt.

Passwörter werden grundsätzlich verschlüsselt gespeichert.

Checkliste TOM Zugangskontrolle

Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen der w3 GmbH werden ausschließlich von Administratoren eingerichtet.

Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind.

Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten.

Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.

Die Vernichtung von Datenträgern und Papier erfolgt nach DIN 66399.

Alle Mitarbeiter bei w3 GmbH sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte der für die Vernichtung zuständigen Person auszuhändigen (Zustandig: Philipp Rehm, Abteilung Druck).

Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

Checkliste TOM Zugriffskontrolle

Trennungskontrolle

Alle von w3 GmbH für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Kunden ist stets gewährleistet.

Siehe Checkliste TOM Trennungskontrolle.

---

2. Integrität

Eingabekontrolle

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die von w3 GmbH im Auftrag verarbeitet werden, wird grundsätzlich protokolliert.

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

Checkliste TOM Eingabekontrolle

Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden von w3 GmbH erfolgt, darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern ist den Beschäftigten bei w3 GmbH im Zusammenhang mit Kundenprojekten untersagt.

Mitarbeiter bei w3 GmbH werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

Checkliste TOM Weitergabekontrolle

---

3. Verfügbarkeit und Belastbarkeit

Daten auf Serversystemen von w3 GmbH werden mindestens täglich inkrementell und wöchentlich „voll“ gesichert. Die Datensicherung wird zusätzlich über Nacht verschlüsselt auf einen physisch getrennten Ort gespiegelt.

Das Einspielen von Backups wird regelmäßig getestet.

Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich ein Brandmelder sowie eine CO2-Löscheinrichtung. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Ein Notfallplan ist hier einzusehen

Checkliste TOM Verfügbarkeitskontrolle

---

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Bei der w3 GmbH ist ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.

Es ist ein Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.

Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen. Auftragskontrolle

Die Verarbeitung der Datenhaltung erfolgt ausschließlich in der Europäischen Union.

Bei der w3 GmbH ist ein externer Datenschutzbeauftragter benannt.

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführten Audit durch den Datenschutzbeauftragten von w3 GmbH abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Bei der w3 GmbH wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces Rechnung getragen wird. So sind z.B. Formularfelder, Bildschirmmasken flexibel gestaltbar. So können Pflichtfelder vorgesehen oder Felder deaktiviert werden.

Die Software der w3 GmbH unterstützt sowohl die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht.

Berechtigungen auf Daten oder Applikationen können flexibel und granular gesetzt werden.

Weitere Informationen

* Mustervereinbarung Auftragsdatenverarbeitung

Quellen u.a.

https://www.datenschutz-wiki.de/Checkliste_Technische_und_organisatorische_Ma%C3%9Fnahmen