Technische und organisatorische Maßnahmen zur Datensicherheit

Bei OWLweb sind nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO getroffen worden:

Inhaltsverzeichnis

1. Vertraulichkeit

Zutrittskontrolle

Das OWLweb (Einzelunternehmung, Thomas Dubbert) Büro befindet sich in einem Bürohaus in Höxter.

Die Zugänge zum Bürohaus und auch zum OWLweb Büroraum sind bei Nacht verschlossen und Video-Überwacht. Zugang zu den Büros haben nur der Vermieter und die Mieter. Es kommt ein elektronisches Schließsystem zum Einsatz, das vom Vermieter verwaltet wird. Jeder Mieter erhielt dazu einen ausgehändigten Transponder-Schlüssel (Karte) um das elektronische Zutrittsrecht zu erhalten.

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

Der Eingang zum OWLweb Büroraum ist mit einer Videoüberwachung gesichert. Diese kann manuell aktiviert und deaktiviert werden. Unabhängig davon wird Videoüberwachung bei Bewegung nach Büroschluss automatisch aktiviert.

Zugangskontrolle

Für die Zugangskontrolle sind nachfolgende Maßnahmen von OWLweb getroffen worden:

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu sind entsprechende Benutzerberechtigungen eingerichtet

worden. Da es sich um ein Einzelbüro (Thomas Dubbert) handelt, besitzt nur diese Person hier Zugang.

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

Remote-Zugriffe auf IT-Systeme OWLwebs erfolgen stets über verschlüsselte Verbindungen.

Auf den Servern OWLwebs 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.

Passwörter werden grundsätzlich verschlüsselt gespeichert.

Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen OWLwebs werden ausschließlich von Administratoren eingerichtet. Wichtige Dokumente und evtl. auch Datensicherungen werden gegenüber Dritten in einem Tresor im Büro gelagert, zudem nur Thomas Dubbert Zugriff hat.

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 Thomas Dubbert.

Es gibt rollen- bzw. Rechte basierte Zugriffskonzepte 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 durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet.

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.

Trennung

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

Pseudonymisierung & Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme im Einsatz.

2. Integrität

Eingabekontrolle

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die von OWLweb im Auftrag verarbeitet werden, wird auf Serversystemen protokolliert.

Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden von OWLweb 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 OWLweb im Zusammenhang mit Kundenprojekten nur nach Hinweis und Einhaltung der Datenschutzrechtlichen Anforderungen gestattet.

Mitarbeiter bei OWLweb werden regelmäßig zu Datenschutzthemen Informiert. Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten vertraglich verpflichtet worden.

3. Verfügbarkeit und Belastbarkeit

Daten auf Serversystemen von OWLweb werden täglich, für jeweils 7 Tage „voll“ gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verbracht (Hosting Provider Domainfactory GmbH, sowie die Hetzner GmbH).

Das Einspielen von Backups wird regelmäßig getestet.

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

Es gibt bei den Hosting Providern einen Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

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

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

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich Thomas Dubbert gemeldet werden. Dieser 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 Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführten Audit durch OWLweb abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses in unregelmäßigen Abständen kontrolliert.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Bei OWLweb 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.

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