Technische und organisatorische Massnahmen nach DSGVO

Demian Holderegger
3. April 2018 11:03

Folgen

1. Pseudoanonymisierung

Beim Tracking auf unserer Webseite setzen wir Anonymisierung und Pseudoanonymisierung ein um die Privatsphäre unserer Besucher zu schützen.

2. Verschlüsselung

Verschlüsselung ist ein zentrales Element in unserem Sicherheitskonzept. Verschlüsselung verweigert Unberechtigten den Zugriff auf personenbezogene Daten. Eine Verschlüsselung erschwert auch die unberechtigte Veränderung von Daten.

Die Verbindung vom Kunden zum Webling Server ist grundsätzlich verschlüsselt. Es ist jedoch auch möglich, auf Webling über eine unverschlüsselte Verbindung zuzugreifen.

Backups werden verschlüsselt abgelegt und übertragen.

Personenbezogene Daten der Kunden werden ausserhalb des Rechenzentrums nur verschlüsselt oder auf verschlüsselten Datenträgern gespeichert. Einzige Ausnahme ist eine temporäre Kopie der Daten einzelner Kunden für Supportaufgaben. Die temporären Kopien werden nach Erledigung der Aufgaben wieder gelöscht.

3. Vertraulichkeit

Der Auftraggeber bestimmt durch Erstellen von Benutzeraccounts selbst, wer Zugriff auf die personenbezogenen Daten hat.
Die Mitarbeiter können eine temporäre Kopie der Daten einzelner Kunden für Supportaufgaben anlegen. Die temporären Kopien werden wie die produktiven Daten gespeichert und geschützt. Die temporären Kopien werden nach Erledigung der Aufgaben wieder gelöscht. Die Mitarbeiter, die eine temporäre Kopie anlegen können, unterzeichnen eine Geheimhaltungsvereinbarung. Der Auftraggeber kann diese Funktion jederzeit deaktivieren.

4. Integrität

Nur angemeldete Benutzer können in Webling Daten eingeben, verändern oder löschen. Die Aktionen werden protokolliert, diese Protokolle können vom Auftraggeber grösstenteils in Webling eingesehen werden.

5. Verfügbarkeit

Wir setzen auf verschiedene Massnahmen um die Verfügbarkeit der Daten in Webling zu gewährleisten:

- Redundante Server
- Die Server sind in einem Rechenzentrum mit Brandschutzanlagen, unterbrechungsfreier Stromversorgung, redundanter Netzwerkanbindung und weiteren Vorkehrungen, die einen unterbrechungsfreien Betrieb gewährleisten.
- Die Server selbst sind mit redundanten Festplatten ausgerüstet, darüber hinaus steht ein Backupserver bereit.

6. Belastbarkeit der Systeme

Um die Belastbarkeit der Systeme zu gewährleisten, setzen wir auf eine gut ausgebaute Serverinfrastruktur

Zuletzt aufgerufene Beiträge

Datenschutz

Zusatzvereinbarung zur Datenverarbeitung (DSGVO)

Datenschutz & Datensicherheit

Verwandte Beiträge

Datenschutz

Zusatzvereinbarung zur Datenverarbeitung (DSGVO)

Zusatzvereinbarung zur Auftragsdatenverarbeitung

Unterauftragnehmer

Changelog - Was ist neu?

und ein umfangreiches Monitoring um Trends und Lastspitzen zu erkennen und rechtzeitig darauf zu reagieren.

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Wir machen täglich Backups an einen entfernten Ort und haben Notfallpläne für die Wiederherstellung der Daten nach einem Zwischenfall.

8. Verfahren regelmässiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen

Wir führen regelmässige Überprüfungen der Risikoanalyse und der technischen und organisatorischen Massnahmen nach ISO 27001 durch.