3d-berlin wayfinding

Information

DSGVO-Maßnahmen

Abstrakt

Beschreibung der Maßnahmen der 3d-berlin vr solutions GmbH zum Datenschutz (DSGVO).

Revision

Version	Änderungen	Beschreibung	Autor	Datum
Issue A	-	Erstausgabe	Adrian Zentner	18.03.2020

Zusammenfassung

1 Zusammenfassung

1.1 Kurzdarstellung

1.1.1 3d-berlin GmbH

3d-berlin vr solutions GmbH entstand 2010 um den promovierten Virtual Reality-Spezialisten Dr. Björn Clausen und Dipl.-Ing. Adrian Zentner als Ausgründung der Freien Universität Berlin. 3d-berlin ist mit dem interaktiven und patentierten Gebäudeinformations- und Wegeleitsystem ‚Guide3D' sowie ‚easyGuide' auf die Indoor-Navigation spezialisiert.

1.1.2 Guide3D & easyGuide

Mit den Produkten 'Guide3D' und 'easyGuide' bietet 3d-berlin plattformunabhängige 3D- und 2D-Gebäudeleitsysteme für multiple Ausgabegeräte.

1.2 Gegenstand

Beschreibung der Maßnahmen der 3d-berlin vr solutions GmbH zum Datenschutz (DSGVO).

2 Abkürzungen und Definitionen

2.1 Abkürzungen

Abkürzung	**Bedeutung**
DSGVO	Datenschutz-Grundverordnung
SAAS	Software as a Service
SLA	Service Level Agreement

2.2 Definitionen

Begriff	**Bedeutung**
Anbieter	3d-berlin vr solutions GmbH Geisbergstraße 16 10777 Berlin Deutschland USt-IdNr.: DE 273158896
Anwender / Benutzer	Ein Nutzer des Wegeleitsystems

3 Verweise

Verweis	**Titel**	**Referenz**	**Ausgabe**

OFF_SLA	Service Level Agreement Guide3D & easyGuide product line (www.g3d.me/to/sla-de)	S-SLA-003-DE16	B

4 Technisch-organisatorische Maßnahmen

4.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

4.1.1 Zutrittskontrolle (physisch)

- Schlüssel-Organisation:
  Mitarbeiter erhalten nur nach Bedarf Schlüssel zu verschiedenen Bereichen (Büroräume, Serverraum, Briefkasten, etc.). Der Erhalt von Schlüsseln wird zentral organisiert, die Ausgabe erfolgt nur gegen Unterschrift.
- Schlüssel-Verwahrung:
  Schützenswerte Zentralschlüssel werden durch die Geschäftsführung verwahrt. Die Schlüssel sind mit neutralen Zeichen markiert, ihr jeweiliger Nutzen nicht erkenntlich.
- Unfallverhütung:
  Rauch- und Brandmelder sind in allen Räumen installiert.
- Einbruchschutz:
  Beide Zugangstüren sind mit einer doppelten Sicherung (u.a. Panzerriegelschloss) ausgestattet. Fenster sind entweder vergittert oder mit Rollläden ausgestattet, welche außerhalb der Geschäftszeiten heruntergelassen werden. Im gleichen Objekt (Stand März 2020) ist ein Geschäftsführer in unmittelbarer Nachbarschaft wohnhaft.

4.1.2 Trennungskontrolle

Daten (insbesondere personenbezogen) werden nur auf dedizierten zweckgebundenen Servern mit entsprechenden Zugriffsrechten verarbeitet.

Die vom Anbieter gehosteten SaaS-Anwendungen werden von der Host Europe GmbH (www.hosteurope.com) auf einem dedizierten Server gehostet. Host Europe ist Europas größter privater Datenhosting-Anbieter und ist gemäß ISO 27001 zertifiziert. Die Rechenzentren befinden sich in Köln/Deutschland sowie Straßburg/Frankreich.

Weitere Informationen:
- www.hosteurope.de/en/Host-Europe/Sicherheit bzgl. Sicherheitsangelegenheiten und
- www.hosteurope.de/en/AGB für generelle Leistungsdefinitionen

4.1.3 Pseudonymisierung

Zugangsdaten (insbesondere Passwörter) werden als SHA-Hash (Einwegfunktion) abgespeichert und können somit nicht abgegriffen werden.

4.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

4.2.1 Weitergabekontrolle

- Kontoverwaltung
  - Alle Zugangsdaten werden zentral von der Geschäftsführung über ein Passwortmanager (Keepass) verwaltet.
  - Zu jedem Konto werden auch die Zugangsberechtigungen in Keepass eingerichtet, woraus individualisiert Passwort-Datenbanken für jeden einzelnen Mitarbeiter nachdem Need-to-know-Prinzip erstellt werden.
  - Passwörter werden durch den integrierten Passwortmanager erzeugt und somit nicht doppelt vergeben.
- Netzwerk:
  - Als IT-Unternehmen ist generell ein hoher Wissenstand in Bezug auf Netzwerksicherheit gegeben. Zusätzlich wird auch externe Fachberatung eingesetzt, um den Sicherheits-Standard zu halten bzw. zu verbessern.
  - Zentrale Rechteverwaltung für Benutzer über „QNAP" für individuelle Verzeichnisse (Beispiel Finanzen).
  - Sicherung der WLAN-Kommunikation derart, dass über WiFi nur auf das Internet, nicht aber das Firmennetzwerk zugegriffen werden kann. Das WiFi-Netzwerk wird nur bei Bedarf Besuchern bereitgestellt, in den Arbeitsprozessen kommen grundsätzlich nur kabelbasierte Verbindungen zum Einsatz.
  - Firewallregeln zum Schutz des Firmennetzwerkes gegen unerwünschte Zugriffe von oder Datenfluss nach außen.
  - "Kill-Switch" des Firmennetzwerkes über den pfSense-Router für den Notfall gegen die Verbreitung von Malware (z.B. Ransomware).
- Fernzugriff
  - Fernzugriff für "Home-Office" Mitarbeiter über Teamviewer nur nach NICHT automatischen Teamviewer-Client Start.
  - Fernzugriff per OpenVPN-Fernzugriff für "Home-Office"-Mitarbeiter mit personalisierten und zeitlich beschränkten Zertifikaten.

4.2.2 Eingabekontrolle

- Die private Nutzung von Arbeitsplatz-Rechnern ist ausdrücklich im Unternehmen untersagt.
- Arbeitsplatz-Rechner verlangen eine Passworteingabe nach kurzer Abwesenheit (= Screensaver)
- Mitarbeiter haben keine Administrator-Rechte für ihre Rechner.
- Jeder Mitarbeiter hat ein individuelles Passwort für sein Windows-Konto.
- Windows-Updates werden automatisch installiert, auch wenn es sich nicht um ein Administrator-Konto handelt.
- Auf jedem Windows-Rechner läuft ein Firewall- und AntiVirus-Programm, welches automatisch aktuell gehalten wird.
- Für jeden Windows-Rechner wird automatisch ein Report generiert, welcher die installierte Software mit Versionsnummer auflistet.

4.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

4.3.1 Verfügbarkeitskontrolle

- Updates

  - Firmware-Updates für bedeutende Hardware (z.B. QNAP, pfSense, Telefonanlage) und bei Bedarf andere Hardware (Drucker, Swichtes, WLAN-Router) wird bei Bedarf durchgeführt.
- Backups
  - Periodische wöchentliche Backups von bedeutenden Workstations und (virtuellen) Servern (vor Ort und remote) sowie die externe Sicherung auf physikalisch mobilen Datenträgern.
- E-Mail-Kommunikation
  - Sicherung der E-Mail-Kommunikation in Form von Backups, Antivirenschutz und Spamfilter. Mails mit gefährdenden Dateianhängen werden automatsich vorab gefiltert.
- Hosting
  - Durch die Host Europe GmbH kann der Auftragnehmer die folgenden Leistungen des Core-Netzwerks garantieren:
    - Verfügbarkeit von 99%
    - Latenz von 20 Millisekunden
    - Bandbreite von 100 Mbit/s bei Höchstbelastung

4.3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Workstation-Backups können innerhalb von 24 Stunden wiederhergestellt werden. E-Mail Backups innerhalb von 12 Stunden durch den Hosting-Provider (Host-Europe).

4.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.4.1 Datenschutz-Management

4.4.2 Incident-Response-Management

Bei Zwischenfällen wird je nach Schwere (siehe SLA) unterschiedlich schnell reagiert.

4.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Die Firmen-Webseite bietet eine „One-Click"-Option, um nur essenzielle Cookies zu akzeptieren.

4.4.4 Auftragskontrolle

Es werden keinerlei personengebundene Daten durch den Anbieter an Dritt-Unternehmen weitergeben.