

Technische und organisatorische Maßnahmen zur Datensicherheit

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

1. Vertraulichkeit

Zutrittskontrolle

Die Büroräume von Batix befinden sich im Firmengebäude in der Saalstraße 16, 07318 Saalfeld / Saale.

Das komplette Gebäude ist während und außerhalb der Geschäftszeiten durch ein Zutrittskontrollsystem gesichert. Publikumsverkehr ist nicht möglich. Alle systemseitigen Öffnungsvorgänge werden in einem Audit-Log protokolliert. Zur Sicherung des Gebäudes und der Geschäftsräume werden Sicherheitsschlösser eingesetzt.

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. Ein schlüsselloser Zugang ist nur über das elektronische Zutrittskontrollsystem möglich, dessen Nutzung vollständig protokolliert wird.

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 dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

Der Zugang zur lokalen Netzwerktechnik ist durch ein separates Schließsystem gesichert und wird nur in Ausnahmefällen ermöglicht, z. B. durch autorisierte Vertragspartner nach Terminvereinbarung, die sich vor Ort ausweisen müssen. Vertretungsberechtigte benötigen hierzu eine schriftliche Bestätigung des Vertragspartners.

Zusatz: Zutrittskontrolle bei Managed Services / Hosting

Sofern vertraglich nichts anderes vereinbart ist, erfolgt der Betrieb von Kundenanwendungen in einem Rechenzentrum unseres Partners Hetzner (Hetzner Online GmbH) mit Sitz in Gunzenhausen.

Seitens Hetzner wird ein elektronisches Zutrittskontrollsystem mit Protokollierung eingesetzt. Zusätzlich wird der gesamte Datacenterpark mittels eines Hochsicherheitszauns abgesichert. Innerhalb des Rechenzentrums gewährleisten Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude und eine 24/7 personelle Besetzung der Rechenzentren, sowie Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen die Zugangskontrolle. Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters.

Zugangskontrolle

Für die Zugangskontrolle sind nachfolgende Maßnahmen von Batix 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 Antrag kann auch über die Personalabteilung gestellt werden.

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, Ziffern und Sonderzeichen bestehen muss.

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

Auf den Servern von Batix 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 (dediziertes Internet-Gateway mit Firewall, eingehend und ausgehend).

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

Passwörter werden grundsätzlich verschlüsselt gespeichert.

Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen von Batix 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. Der Antrag kann auch bei der Personalabteilung gestellt werden.

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 Mitarbeiter haben also nur auf die Daten Zugriff, die sie für Ihre Arbeit benötigen.

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.

Im Falle von drahtlosen Zugriffen wird ein getrenntes Gäste-WLAN eingesetzt, Ethernet-Zugriffe werden Gästen nicht gestattet.

Trennung

Alle von Batix 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 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 Batix im Auftrag verarbeitet werden, wird grundsätzlich protokolliert.

Alle Benutzerkonten werden zentral erstellt und verwaltet. Jeder Batix-Mitarbeiter erhält persönliche Zugänge, die ihm eindeutig zugeordnet werden können. Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden von Batix erfolgt, darf jeweils nur in dem Umfang, wie 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 Verschlüsselung erfolgt hierbei über SSL-Verschlüsselung, eine VPN-Verbindung, oder die individuelle Verschlüsselung der übertragenen Daten.

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

Mitarbeiter von Batix werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind i. S. d. Art. 32 Abs. 4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen. Die Tatsache der Verpflichtung ist zum Zweck eines jederzeitigen Nachweises in der Personalakte dokumentiert.

Zusatz: Weitergabekontrolle bei Managed Services / Hosting

Sofern vertraglich nichts anderes vereinbart ist, erfolgt der Betrieb von Kundenanwendungen in einem Rechenzentrum unseres Partners Hetzner (Hetzner Online GmbH) mit Sitz in Gunzenhausen.

Seitens Hetzner sind alle Mitarbeiter i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen. Hetzner sichert eine datenschutzgerechte Löschung der Daten nach Auftragsbeendigung zu. Ebenso stellt Hetzner Möglichkeiten zur verschlüsselten Datenübertragung zur Verfügung.

3. Verfügbarkeit und Belastbarkeit

Daten auf internen Serversystemen von Batix werden mindestens täglich inkrementell und wöchentlich „voll“ gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verbracht. Zusätzlich wird bei allen relevanten Servern eine Festplattenspiegelung eingesetzt.

Alle internen Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Die internen Serversysteme verfügen zudem über eine unterbrechungsfreie Stromversorgung.

Das Einspielen von Backups wird regelmäßig getestet.

Es gibt bei Batix einen Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

[Zusatz: Verfügbarkeitskontrolle bei Managed Services / Hosting](#)

Sofern vertraglich nichts anderes vereinbart ist, erfolgt der Betrieb von Kundenanwendungen in einem Rechenzentrum unseres Partners Hetzner (Hetzner Online GmbH) mit Sitz in Gunzenhausen.

Seitens Hetzner erfolgt der Einsatz unterbrechungsfreier Stromversorgung.

Zusätzlich erfolgt durch Hetzner ein dauerhaft aktiver DDoS-Schutz. DDoS-Attacken (Distributed-Denial-of-Service) gehören mittlerweile leider zum Alltag in der IT. Um die Bandbreite oder die Ressourcen eines Servers zu überlasten, wird dieser mit gefälschten Anfragen überflutet. Dabei werden oftmals massenhaft kompromittierte Rechner eingesetzt (Bot-Netze), um gigantischen Datenverkehr zu erzeugen. Die Folge sind hohe Ladezeiten Ihrer Website oder im schlimmsten Fall sogar der Totalausfall. Damit Ihre Web-Anwendungen, Websites, Server und IT-Infrastruktur gegen diese Gefahren abgesichert sind, setzt Hetzner Online auf eine automatisierte Sicherheitslösung, bei der Angriffsmuster in den meisten Fällen frühzeitig erkannt und abgewehrt werden. Basierend auf den neuen hochwertigen Hardware-Applikationen und der komplexen Filtertechnik sind Sie vor DDoS-Angriffen weitestgehend geschützt

Durch Batix erfolgt im Rahmen der Dienstleistungen ein individuelles Backup- und Recovery-Konzept, das in den jeweiligen Leistungsvereinbarungen mit dem Auftraggeber festgelegt wird.

[4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung](#)

Bei Batix 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.

[Zusatz: Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung bei Managed Services / Hosting](#)

Sofern vertraglich nichts anderes vereinbart ist, erfolgt der Betrieb von Kundenanwendungen in einem Rechenzentrum unseres Partners Hetzner (Hetzner Online GmbH) mit Sitz in Gunzenhausen.

Hetzner Online ist nach DIN ISO/IEC 27001 zertifiziert. Der international anerkannte Standard für Informationssicherheit bescheinigt der Hetzner Online GmbH, dass ein geeignetes Informationssicherheitsmanagementsystem, kurz ISMS, implementiert und adaptiert wurde. Das ISMS findet an den Standorten Nürnberg und Falkenstein bei der Infrastruktur und dem Betrieb der gesamten Datacenterparks Anwendung und wurde durch die FOX Certification geprüft.

Das Zertifikat weist ein adäquates Sicherheitsmanagement, die Sicherheit der Daten, die Vertraulichkeit der Informationen und die Verfügbarkeit der IT-Systeme nach. Es bestätigt zudem, dass die Sicherheitsstandards kontinuierlich verbessert und nachhaltig kontrolliert werden.

Auftragskontrolle

Bei Batix ist ein betrieblicher Datenschutzbeauftragter benannt.

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführter Prüfung durch den Datenschutzbeauftragten von Batix abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

Zusatz: Auftragskontrolle bei Managed Services / Hosting

Sofern vertraglich nichts anderes vereinbart ist, erfolgt der Betrieb von Kundenanwendungen in einem Rechenzentrum unseres Partners Hetzner (Hetzner Online GmbH) mit Sitz in Gunzenhausen.

Die Mitarbeiter von Hetzner werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betriebliche Prozesse.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Bei Batix 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.