HiOrg Server GmbH

Dr.-Schier-Straße 9
D-66386 St. Ingbert

Tel.: 06894-894905-0
Fax: 06894-894905-9

support@hiorg-server.de
http://www.hiorg-server.de

Gesellschafter/GF:
Christoph Blechschmitt

AmtsG Saarbrücken
HRB 19209

Datum: 13.02.2020

Konzept Datensicherheit & Datenschutz bei HiOrg-Server

Angesichts der Sensibilität der Daten, die in unserem System gespeichert und bearbeitet werden, ist eine kritische Auseinandersetzung mit den Themen „Datensicherheit“ und „Datenschutz“ aus der Perspektive des Nutzers/Auftraggebers nicht nur sinnvoll, sondern zwingend erforderlich im Rahmen der Auswahl und Eignungsprüfung potentieller Dienstleister bei einer Auftragsdatenverarbeitung.

Die Relevanz dieser Themen ist uns als Anbieter durchaus bewusst, daher legen wir selbst großen Wert auf den sorgfältigen Umgang mit den uns anvertrauten Daten, und die korrekte und nachhaltige Behandlung von Datenschutz und -Sicherheit bei den von uns angebotenen Diensten. Da wir auf beiden Gebieten tatsächlich vorbildlich aufgestellt sind, scheuen wir auch keinerlei Detailfragen, sondern erörtern diese Themen gerne und offen.

I. Datensicherheit

Die Priorität unseres Unternehmens ist die Bereitstellung eines stabilen und fehlerfreien Systems, welches im Optimalfall dauerhaft erreichbar und nutzbar ist. Daher wird HiOrg-Server ausschließlich bei ausgewählten Premium-Hostern betrieben. Sämtliche von uns administrierten Server befinden sich auf dem Gebiet der Bundesrepublik Deutschland, es werden zur Speicherung oder Verarbeitung der Kundendaten keine Systeme oder Dienste ausländischer Anbieter genutzt.

Die hochverfügbaren Server-Systeme für das Produktivsystem des HiOrg-Servers befinden sich im Rechenzentrum der KeySystems DataCenter GmbH in St. Ingbert, welches zum Frühjahr 2011 als TÜV-geprüftes Rechenzentrum in Betrieb genommen wurde, und mit der Sicherheitsstufe TIER-III zertifiziert ist. Es ist ausgestattet mit mehreren getrennten Internet- und Strom-Anbindungen, Notstrom-Generator mit Treibstoff-Vorrat für mehrere Tage, vollautomatischer Brand-Früherkennungs- und Löschanlage, mehrstufiger Zugangskontrolle und Alarmanlage. Sämtliche zum Serverbetrieb notwendigen Systeme (Strom, Netzwerk, Klimatisierung) werden mehrfach redundant vorgehalten mit automatischer Umschaltung im Fehlerfall, es handelt sich also um eine vollständige „n+1-Redundanz“ ohne „single-point-of-failure“.

In diesem Rechenzentrum betreiben wir mehrere (derzeit 10) eigenständige Server, deren Aufgaben aus Sicherheits- und Performancegründen klar getrennt sind. Das gesamte Serversystem wird mittels vmWare vCloud komplett virtualisiert, auf der Basis von zahlreichen einzelnen physischen Maschinen, welche gemeinsam den

Ressourcen-Pool für Rechenleistung und Speicherkapazität bilden. Sowohl auf physischer, als auch (nochmals) auf logischer Ebene werden sämtliche Daten per RAID-System redundant gespeichert, so dass ein Datenverlust durch das Versagen eines technischen Gerätes ausgeschlossen ist. Sämtliche Festplatten werden als verschlüsselte LV betrieben.

In einem zweiten Rechenzentrum der Fa. netcup in Nürnberg betreiben wir vier weitere Server. Hier steht u.a. unser “Hot-Standby”-Server. Auf diesen wird der gesamte Datenbestand des HiOrg-Servers nahezu “live” mit nur wenigen Sekunden Verzug gespiegelt, somit könnte dieser jederzeit kurzfristig die Aufgaben des HiOrg-Servers übernehmen (Geo-Redundanz). Von diesem Rechenzentrum aus betreiben wir auch ein umfangreiches, automatisiertes Echtzeit-Monitoring-System, welches zahlreiche Parameter aller von uns betriebenen Server in engen Abständen überwacht und bei ersten Anzeichen einer möglichen Fehlfunktion frühzeitig und über verschiedene Kanäle unseren Bereitschaftsdienst alarmiert.

Sowohl die Konfigurationen aller unserer Server, der gesamte Dokumentenspeicher, als auch die Datenbank mit allen Nutzdaten unserer Kunden, werden mindestens einmal täglich auf einem speziell dafür konfigurierten Backup-Server der Fa. Strato in Berlin gesichert. Diese Backups halten wir für vier Wochen vor, ältere Versionen werden automatisch gelöscht.

Der Zugriff auf sämtliche im HiOrg-Server gespeicherten sensiblen Daten ist nach dem Login mittels persönlicher Zugangsdaten jedes einzelnen Nutzers, ausschließlich über eine gesicherte Verbindung (TLS / SSL) möglich. Das hierzu verwendete Zertifikat mit 4096-bit RSA-Verschlüsselung wurde mittels sha256-Algorithmus signiert. Von unserem Server werden ausschließlich aktuelle, hochwertige Verschlüsselungstechniken angeboten (AES_256_GCM_SHA384, sowie Perfect Forward Secrecy, kurz: PFS), welche von einem modernen Browser automatisch genutzt werden.

II. Datenschutz

Wir sind uns der Sensibilität Ihrer mit HiOrg-Server verwalteten persönlichen und unternehmerischen Daten durchaus bewusst, und sorgen daher mit großem Aufwand für die Sicherheit und den Schutz aller uns anvertrauten Daten.

Genau wie jedes andere in Deutschland tätige Unternehmen, sind wir natürlich an das (zu Recht sehr strenge bzw. an den Rechten der „Betroffenen“ orientierte) Bundesdatenschutzgesetz (BDSG) sowie an die Regelungen der EU-weit gültigen Datenschutz-Grundverordnung (DS-GVO) gebunden, und nehmen diese auch im täglichen Umgang sehr ernst.

Alle bei HiOrg-Server gespeicherten Daten werden streng nach dem BDSG und DS-GVO behandelt und somit nicht zur Werbung genutzt oder an Dritte weitergegeben.

Auf die gesamte Datenbank der realen Kundendaten haben nur drei Mitarbeiter der HiOrg Server GmbH Vollzugriff, die Entwickler arbeiten im Regelfall nur mit einer Testdatenbank und fiktiven Daten. Trotzdem müssen alle unsere Mitarbeiter zu Beginn ihrer Tätigkeit eine Schulung und Unterweisung zum Datenschutz inkl. Prüfung durchlaufen.

Jeder im HiOrg-Server registrierte Benutzer kann die zu seiner Person gespeicherten Daten einsehen. Die Anzeige persönlicher Daten (z.B. Geburtsdatum, Kontonummer, …) auf der von anderen Mitgliedern ohne Leitungsfunktion einsehbaren Mitgliederliste kann von jedem Nutzer wahlweise einzeln unterdrückt werden.

Nach der unverbindlichen Testphase schließen wir mit allen Kunden einen Nutzungsvertrag ab, welcher klar die Zuständigkeiten auch in Bezug auf Datenschutzfragen und damit verbundene Pflichten regelt. Erst nach Abschluss dieses Vertrages und einer AVV (s.u.) dürfen reale Daten im HiOrg-Server hinterlegt werden.

Weiterhin sind Sie als verantwortlicher Auftraggeber durch das BDSG und die DS-GVO dazu verpflichtet, mit uns als Dienstleister eine sog. „Vereinbarung zur Auftragsverarbeitung (AVV)“ abzuschließen. Der Inhalt dieser Vereinbarung wird vom Gesetzgeber sehr konkret vorgegeben, und gestaltet sich durchaus komplex.

Um Ihnen den aufwändigen Prozess des Vertragsentwurfs oder der Konkretisierung eines vorliegenden Muster-/Rahmenvertrages zu ersparen, haben wir gemeinsam mit mehreren Landes- und Kirchen-Datenschutzbeauftragten verschiedener Dachverbände, sowie dem für uns zuständigen unabhängigen Datenschutzzentrum des Saarlandes eine AV-Vereinbarung nach DS-GVO entworfen und konkretisiert, so dass Sie diese Vorlage bedenkenlos ohne weitere Anpassungen oder teure Prüfungen einsetzen können.

Die dort als Anlage enthaltene „Dokumentation der technischen und organisatorischen Maßnahmen“ beschreibt nochmals ganz konkret und im Detail alle relevanten Regelungen zum Schutz und Umgang mit personenbezogenen Daten in unserem Betrieb sowie beim Rechenzentrum.

III. Umsetzung konkreter Anforderungen

1. Grundsatz der Datenminimierung

Bei HiOrg-Server werden grundsätzlich nur die Daten erfasst, welche auch (z.B. an anderen Stellen im System) zur Entscheidungsfindung für das System oder den Disponenten als Nutzer notwendig sind. Bei den System-Einstellungen kann der Administrator über diese Grundeinstellung hinaus weitere Datenfelder aktivieren oder deaktivieren, wenn dies für den konkreten Arbeitsablauf in seiner Gliederung passend ist.

2. Pseudonymisierung

In der technisch zugrunde liegenden Datenbank sind sämtliche mit einer konkreten Person verknüpften zusätzlichen Daten (z.B. Ausbildungen, Helferstunden, Teilnahme an Veranstaltungen, zugeordnetes Material u.ä.) bereits pseudonymisiert gespeichert, also nur über die zufällig erzeugte Nutzer-ID referenziert. Um die Daten bei Bedarf vollständig zu pseudonymisieren, muss der Admin lediglich den Namen (sowie ggf. auch Adress- und Kontaktdaten) eines Nutzers in dessen Stammdaten löschen oder pseudonymisieren.

3. Rollen- und Berechtigungskonzept

Durch die zahlreichen, vom Admin einzeln zuweisbaren Benutzer-Rechte und die einzeln zuweisbare Rolle „Mitglied Leitungsteam“ verfügt HiOrg-Server bereits über ein umfangreiches Berechtigungs- und Rollenkonzept. Darüber hinaus kann durch die Zuordnung von Gruppen zu jedem Mitglied der Datenzugriff in einer weiteren Dimension individuell angepasst werden.

4. Zugriffskontrolle

Der Zugriff ist nur nach Anmeldung und Authentisierung des einzelnen Nutzers möglich. Vom Admin können Richtlinien zur geforderten Komplexität der Passwörter und ggf. Ablauffristen festgelegt werden. Die Server befinden sich in gesicherten Rechenzentren, so dass der physikalische Zugriff nur autorisierten Personen möglich ist.

5. Eingabekontrolle

Jeder Login und alle Datenänderungen werden protokolliert, so dass der Admin jederzeit die Ordnungsmäßigkeit der Verarbeitung personenbezogener Daten prüfen kann. Er erhält im Protokoll „Log: Aktivität“ und „Log: Mitglieder“ Auskunft darüber, wer wann welche personenbezogenen Daten in welcher Weise eingegeben, geändert oder gelöscht hat. Auch misslungene Login-Versuche werden protokolliert.

6. Protokollauswertungen

Die unter 5. genannten Protokolldaten sind nur Administratoren zugänglich, und können nicht nachträglich verändert werden. Eine regelmäßige Prüfung dieser Logs kann u.a. durch die Einrichtung eines „RSS-Feed“ erleichtert werden. Die Auswertung der Server-Logs geschieht regelmäßig durch den CSO der HiOrg Server GmbH.

7. Archivierung und Löschung

Um nicht mehr benötigte Daten einfacher löschen zu können, ist im HiOrg-Server eine spezielle Löschfunktion vorgesehen (Menü: „System – Datenpflege – Alte Daten löschen“). Hier kann der Admin anhand einer selbst gewählten Datumsgrenze zunächst ermitteln, welche Datensätze (Anzahl und Typ) betroffen sind, und diese dann in einem zweiten Schritt samt aller Referenzen endgültig löschen.

Auch bei der Löschung eines Benutzers unterstützt der HiOrg-Server den Admin bei der Ermittlung aller Referenzen (z.B. Einteilung als Teilnehmer oder Verantwortlicher einer Veranstaltung) und deren Löschung oder Änderung auf andere Personen.

Für alle Server-Logs bestehen feste Löschfristen (i.d.R. 4 Wochen), die Löschung geschieht automatisiert.

8. Auskunftsrecht des Betroffenen

Um einem Betroffenen sämtliche über seine Person gespeicherten Stammdaten zur Verfügung zu stellen, bietet HiOrg-Server den Ausdruck einer „Karteikarte“ an. Diese kann bei Bedarf (z.B. bei Nutzung zusätzlicher organisationsspezifischer Datenfelder) vom Admin um weitere Variablen ergänzt werden. Auch die Log-Daten können nach einer Benutzerkennung gefiltert werden, um alle relevanten Bewegungsdaten zu einer Person ermitteln und exportieren zu können.

9. Recht auf Einschränkung der Verarbeitung

Wenn ein Benutzer vom Admin als „gesperrt“ oder „versteckt“ markiert wird, so können normale Nutzer dessen Daten im HiOrg-Server nicht mehr abrufen. Sie bleiben trotzdem noch in der Datenbank enthalten und können durch den Admin in einer speziellen Ansicht eingesehen werden, wenn dies notwendig ist. Nach Ablauf einer ggf. vorliegenden Aufbewahrungsfrist können diese Daten (z.B. mit der in Punkt 7 genannten Löschfunktion) vollständig gelöscht werden.

10. Recht auf Datenübertragbarkeit

Neben der in Punkt 8. genannten Druckansicht, ermöglicht HiOrg-Server den maschinenlesbaren Export von Nutzerdaten in das gängige CSV-Format, welches sich zum Austausch strukturierter Daten zwischen verschiedenen elektronischen Systemen etabliert hat.

11. Widerspruchsrecht

Sämtliche persönlichen Daten (z.B. Kontaktdaten, Geburtsdatum, Fahrerlaubnis) können vom Nutzer selbst als „versteckt“ markiert werden, so dass diese von anderen Nutzern nicht eingesehen werden können. Nur Admins und Disponenten können diese Daten nach spezieller Anforderung („versteckte Daten anzeigen“) einsehen. Im Sinne von „Privacy by default“ sind bei Neuanlage eines Nutzers alle persönlichen Daten als „versteckt“ markiert, und müssen vom Nutzer einzeln freigegeben werden. Der Admin kann alternativ bei den Einstellungen festlegen, dass alle Daten grundsätzlich versteckt bleiben, und der Nutzer diese nicht freigeben kann.

Zusätzlich kann jeder Nutzer selbst wählen, zu welchen Anlässen er ggf. Benachrichtigungen per E-Mail oder SMS erhalten möchte.

12. Nachweis durch Zertifizierung

Eine Zertifizierung nach EU-Recht kann nur von Dienstleistern erteilt werden, die zuvor von der Deutschen Akkreditierungsstelle (DAkkS) akkreditiert bzw. der zuständigen Aufsichtsbehörde zugelassen wurden. Derzeit sind (mangels feststehender Kriterien für eine Akkreditierung) noch keine Akkreditierungen erfolgt.

13. IT-Sicherheit

Die vom Gesetzgeber geforderten technischen und organisatorischen Maßnahmen hinsichtlich der IT-Sicherheit werden eingehalten und sind in der „Anlage TOM zur AV-Vereinbarung“ dokumentiert.

14. Datenschutzrechtliche Verpflichtungserklärung

Die Verpflichtung eines Nutzers auf die Wahrung des Datengeheimnisses kann z.B. in einem „benutzerdefinierten Feld der Mitgliederliste“ registriert werden, welches der Admin im Bereich „System – Einstellungen – Mitgliederliste“ anlegen kann. Achten Sie dabei darauf, das Häkchen zu setzen: „Der Inhalt des Felders kann nicht vom Mitglied selbst geändert werden“.