Einleitung

Mit diesem Dokument möchten wir Kunden helfen, die digibase für die Verarbeitung Ihrer Geschäftspost nutzen möchten. Es soll ein besseres Verständnis zu folgenden Themen geben:

- Wie sind Datenschutz und Datensicherheit bei Heilmann Software, dem Betreiber von digibase verankert
- wie stehen die einzelnen “Akteure” (Kunde, digibase, Rechenzentrum) zueinander und welche Verantwortung kommt ihnen jeweils zu

Datenschutz & Datensicherheit bei Heilmann Software

digibase ist ein Produkt von Heilmann Software Gesellschaft für Informationstechnologie mbH.

Wir haben über 20 Jahre Erfahrung in der Entwicklung von Systemen, mit denen behördliche Daten sicher verwaltet und gespeichert werden. Die bei diesen hochsensiblen Daten ungleich höheren Anforderungen an Datenschutz und Datensicherheit haben wir bei der Entwicklung unserer Systeme von vornherein umgesetzt.

Die Umsetzung und Erweiterung von Datenschutz und Datensicherheit ist für uns absoluter Schwerpunkt bei der Entwicklung unserer Produkte.

Unsere TÜV-Zertifikate und Qualitätssicherung

Das Zeitalter der Digitalisierung schreitet mächtig voran. Wer dabei Prozesse wie „die Zukunft der Post“, Digitalisierung von Kunden- und Geschäftsbeziehungen oder Auftragsdatenverarbeitung mitgestalten möchte, muss sich bei Verbrauchern unweigerlich ein enormes Maß an Vertrauen erarbeiten.

Deshalb halten wir es für unerlässlich, sich von einer unabhängigen, externen Instanz eine Bestätigung bezüglich Informationssicherheit und Qualitätsmanagement einzuholen – schon allein deshalb, um eine mögliche „Betriebsblindheit“ zu überwinden.

Mit den strengen Vorgaben der Richtlinie DIN ISO 27001 und der Richtlinie DIN ISO 9001 konnten wir Informationssicherheit und Qualitätsmanagement in unserer Organisationsstruktur grundlegend verankern. Alle Prozessabläufe sind nach diesen Maßgaben geprüft und zertifiziert.

Unsere Funktion als Auftragsverarbeiter

Die Rechte an den Daten bleiben zu jeder Zeit bei dem digibase Nutzer. Zur Einhaltung der gesetzlichen Regelungen ist eine Vereinbarung zum Datenschutz und zur Datensicherheit gem. Art. 28 Datenschutz-Grundverordnung (DSGVO) zwischen dem Auftraggeber (digibase Nutzer) und uns als Auftragnehmer notwendig. Nach unseren AGB wird diese Vereinbarung automatisch bei Beauftragung durch den Auftraggeber und Annahme durch uns wirksam und ist Bestandteil des Vertrages.

Datenschutzbeauftragter

Unser Datenschutzbeauftragter André Fripon beantwortet gerne alle Fragen zum Thema Datenschutz und Datensicherheit.

André Fripon

Telefon: 0711 21393-500

E-Mail: afripon@heilmannsoftware.de

Mitarbeiter bei Heilmann Software

Alle Mitarbeiter bei Heilmann Software werden auf die DSGVO, § 53 BDSG (neu) sowie ggf. § 88 TKG und ggf. § 35 SGB I nachweislich verpflichtet.

Technische und organisatorische Maßnahmen

Unsere technischen und organisatorischen Maßnahmen finden Sie im Anhang dieses Dokuments.

Auftragsverarbeiter von digibase (Heilmann Software)

Amazon Web Services

digibase wird auf den Servern von Amazon Web Services (AWS) in Frankfurt gehostet. AWS ist eine sichere Plattform für Cloud-Services, die Rechenleistung, Datenbankspeicherung, Bereitstellen von Inhalten und weitere Funktionen bietet. Alle Dokumente und Metadaten unserer Nutzer werden verschlüsselt in einem AWS Rechenzentrum in Deutschland gespeichert und nur für die von den Nutzern gewünschten Services verwendet.

Warum wir uns für Amazon entschieden haben

Amazon AWS ist führender Anbieter, speziell im Hinblick auf Skalierbarkeit, Datenschutz und Datensicherheit. Dies stellt eine hohe Verfügbarkeit unserer Dienste bei gleichzeitig hohem Sicherheitsstandard sicher.

Wir erbringen Services für hunderttausende Einrichtungen, einschließlich Großunternehmen, Bildungseinrichtungen und Regierungsorganisationen, in über 190 Ländern. Unser Kundenstamm umfasst große regionale und multinationale Finanzdienstleister und Dienstleister aus dem Gesundheitswesen und wir bekommen einige ihrer sensibelsten Informationen anvertraut.

Quelle: aws.amazon.com/de/

Grundlage für die Auswahl eines geeigneten Rechenzentrums war, die Vorgaben aus den BSI Standards 100-1 und 100-2 sowie die Vorgaben zur IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten erfüllen zu können. Nur so konnte (u.a.) die Zertifizierung im Rahmen der DIN 27001 problemlos umgesetzt werden.

Die Wahl fiel deshalb auf das AWS Rechenzentrum in Frankfurt (Region). Damit werden sowohl höchste Sicherheitsanforderungen erfüllt als auch keine Daten außerhalb von Deutschland gespeichert.

Europäische Datenschutzaufsichtsbehörde

AWS ist einer der bedeutendsten Anbieter von Cloud Computing-Diensten und hat seine Datenschutzvereinbarungen durch die europäischen Datenschutzaufsichtsbehörden unter Federführung der Luxemburger Aufsichtsbehörde (CNPD) prüfen lassen.

Am 6. März 2015 wurde die um die Standardvertragsklauseln ergänzte Auftragsdatenverarbeitungsvereinbarung von der als "Artikel-29-Datenschutzgruppe" bezeichneten Gruppe der nationalen Datenschutzbehörden der EU-Mitgliedstaaten genehmigt. Diese Genehmigung bedeutet, dass jeder AWS-Kunde, der die Standardvertragsklauseln benötigt, sich jetzt darauf verlassen kann, dass die AWS Auftragsdatenverarbeitungsvereinbarung ausreichende vertragliche Verpflichtungen enthält, um internationale Datenströme in Übereinstimmung mit der Richtlinie zu ermöglichen. Ausführliche Informationen zu der Genehmigung der Artikel-29-Datenschutzgruppe erhalten Sie auf folgender Seite der luxemburgischen Datenschutzbehörde:

http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html

---

Bundesamt für Sicherheit in der Informationstechnik (BSI)

AWS hat als erster Cloud-Service-Anbieter ein Testat nach den Anforderungen des Anforderungskatalogs Cloud Computing (Cloud Computing Compliance Controls Catalogue, C5) des Bundesamts für Sicherheit in der Informationstechnik (BSI) erhalten.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI):
https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Erstes_Testat_nach_Cloud-Anforderungen_12122016.html

Ein Novum im Vergleich zu anderen Sicherheitsstandards sind die sogenannten Umfeldparameter. Sie geben Auskunft über Datenlokation, Diensterbringung, Gerichtsstandort, Zertifizierungen und Ermittlungs- und Offenbarungspflichten gegenüber staatlichen Stellen und enthalten eine Systembeschreibung. Die so geschaffene Transparenz erlaubt es potentiellen Cloud-Kunden zu entscheiden, ob gesetzliche Vorschriften (wie z. B. Datenschutz), die eigenen Richtlinien oder auch die Gefährdungslage bezüglich Wirtschaftsspionage die Nutzung des jeweiligen Cloud-Dienstes als geeignet erscheinen lassen.
Quelle:
https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html

---

Datenschutz & Datensicherheit bei Amazon AWS

Während Amazon für die Sicherheit der Cloud (Anlagen, Hardware, Netzwerk etc.) verantwortlich ist, sind wir (Heilmann Software) für die Sicherheit in der Cloud verantwortlich. Das bedeutet, dass wir verantwortlich für die Verwaltung und Konfiguration des Gast-Betriebssystems (einschließlich Updates und Security Patches), der zugehörigen Anwendungssoftware, der Firewall und Verschlüsselung der Daten sind.

Quelle: Amazon Web Services:
Übersicht über die Sicherheitsprozesse, http://aws-de-media.s3.amazonaws.com/images/Region%20Frankfurt/AWS_Security_Whitepaper-german_final.pdf)

Amazon AWS Region Frankfurt

Die digibase Server-Infrastruktur wird in einer Virtual Private Cloud (VPC, Region Frankfurt) gehostet.

AWS-Kunden wählen die AWS-Region(en), in denen ihre Inhalte gehosted werden. Dies erlaubt Kunden mit besonderen Anforderungen an den Ort der Datenverarbeitung, Umgebungen an einem Standort bzw. an Standorten ihrer Wahl einzurichten. Zum Beispiel können sich AWS-Kunden in Europa dafür entscheiden, ihre AWS-Services ausschließlich in Amazon Web Services – EU Datenschutz Whitepaper Oktober 2015 der EU (Deutschland) Region einzusetzen. Wenn der Kunde sich so entscheidet, werden die Inhalte in Deutschland gespeichert, es sei denn, der Kunde wählt eine andere AWS-Region.

Quelle: Amazon AWS: EU Datenschutz Whitepaper
https://d1.awsstatic.com/whitepapers/compliance/De_Whitepapers/AWS_EU_Data_Protection_Whitepaper_DE.pdf

---

Betriebssystem Updates & Patches

Die digibase Server werden mit dem Betriebssystem Ubuntu Linux 16.04 betrieben. Auf allen Servern ist sicherstellt, dass alle Sicherheit-Patches automatisch installiert werden, sobald sie veröffentlicht werden. Zusätzlich werden alle anderen Pakete und Services in regelmäßigen Intervallen geprüft und gegebenenfalls aktualisiert.

HTTPS und SSL-Zertifikate

Alle Inhalte und Interaktionen mit Browsern von End-Benutzern werden ausschließlich über das HTTPS-Protokoll ausgetauscht.

Das verwendete SSL-Zertifikat wird von dem renommierten SSL-Anbieter GeoTrust ausgestellt und wird in regelmäßigen Intervallen erneuert. Im Fall von entdeckten Sicherheitslücken in dem SSL-Protokoll selbst (z.B. “POODLE”-Lücke) werden Anweisungen der Sicherheits-Community schnellstmöglich implementiert und das Zertifikat gegebenenfalls erneuert.

Datenbanken und Dokumente

Alle Datenbanken und Dokumente sind geschützt und gesichert. Durch Redundanz-Modelle und einer ausgereiften Backup-Strategie wird das Risiko des Verlusts oder der Nichtverfügbarkeit von Daten minimalisiert.

AWS hat keinen Einblick in die Inhalte, die der Kunde auf AWS einstellt, und ändert auch nicht die Einstellungen des Kunden.
Quelle: Amazon AWS - EU Datenschutz Whitepaper (Sicherheit in der Cloud)

Als Anbieter einer Selbstbedienungs-Infrastruktur, die vollständig unter der Kontrolle des Kunden ist (einschließlich hinsichtlich des Ob und Wie der „Datenverarbeitung“), bietet AWS lediglich Infrastruktur-Services für Kunden an, die Inhalte auf das AWS-Netzwerk hochladen und dort verarbeiten wollen. In diesem Zusammenhang hat AWS keinen Einblick in oder Kenntnis davon, was Kunden auf das AWS-Netzwerk hochladen, und auch nicht, ob der Inhalt personenbezogene Daten enthält oder nicht. AWS-Kunden haben zudem die Möglichkeit, Verschlüsselung zu verwenden, um die Inhalte für AWS unlesbar zu machen.

Quelle: Amazon AWS - EU Datenschutz Whitepaper (Sicherheit in der Cloud)
https://d1.awsstatic.com/whitepapers/compliance/De_Whitepapers/AWS_EU_Data_Protection_Whitepaper_DE.pdf

---

Beim Speichern der Dokumente verwenden wir eine der stärksten verfügbaren Blockverschlüsselungen, die 256-bit Advanced Encryption Standard (AES-256), um Ihre Daten zu verschlüsseln.

Mitarbeiter und Entwickler von Heilmann Software haben auf die Dokumente nur nach Freigabe des Kunden (zum Beispiel bei 3rd-Level-Supportfällen) Zugriff.

Virtual Private Cloud (VPC)

Die komplette digibase Server-Infrastruktur wird in einem Virtual Private Cloud (VPC) von AWS gehostet. Der Hauptvorteil des VPCs ist, dass alle Ressourcen auf Netzwerk-Ebene von Ressourcen anderer Kunden isoliert und getrennt sind.

Innerhalb des VPC-Containers sind 2 Subnetze konfiguriert: Ein Öffentliches und ein Privates. Die Server im öffentlichen Subnetz haben öffentliche und Internet-routbare IP-Adressen. Die Server im privaten Subnetz haben keine öffentliche, sondern nur private IP-Adressen. Das bedeutet, dass eine direkte, aus dem Internet initiierte Verbindung mit den Servern im privaten Subnetz nicht möglich ist.

Server Infrastruktur - Sicherheit & Firewall

In AWS sind Firewall-Regeln mit dem Konzept von Security-Groups implementiert. Jedem Server wird eine oder mehrere Security-Groups zugewiesen, in welchen geregelt ist, über welchen Eingangs- und Ausgangs-Port der Server mit anderen Ressourcen kommunizieren kann.

Load-Balancer & VPN

Zugang zum Applikation-Server wird durch AWS Elastic Load Balancer (ELB) gesichert. Er routet und balanciert Web-Requests von den Client-Browsern zu den Applikation-Servern im privaten Subnetz. Zugang zum Applikation-Server wird durch AWS Elastic Load Balancer (ELB) gesichert. Der Load-Balancer liegt im öffentlichen Subnetz und hat 2 offene Ports: HTTP (80) und HTTPS (443). Er routet und balanciert Web-Requests von den Client-Browsern zu den Applikation-Servern im privaten Subnetz.

Zugriffskontrolle

Alle Zugriffe auf digibase (API etc.) werden mit dem AWS Cloudtrail Service protokolliert. Dieser Service nimmt alle Ereignisse auf und protokolliert diese.

AWS CloudTrail erhöht die Transparenz von Benutzer- und Ressourcenaktivitäten durch das Aufzeichnen von AWS Management Console-Aktionen und API-Aufrufen. Sie sehen, welche Benutzer und Konten AWS aufgerufen haben, sowie die IP-Quelladressen und den Zeitpunkt der API-Aufrufe.

Quelle: https://aws.amazon.com/de/cloudtrail/

BC Direct Group GmbH

Die BC Direct Group GmbH ist mit der Produktion der postalischen Briefe beauftragt. Die Zusammenarbeit erfolgt auf Grundlage eines Vertrages nach Art. 28 DSGVO.

Alle Mitarbeiter der BC Direct Group GmbH werden nach DSGVO, PostGesetz und Telekommunikationsgesetz verpflichtet und regelmäßig auf die entsprechenden Inhalte geschult.

Die an die BC Direct Group übermittelten Druckdaten liegen in geschützten Verzeichnissen auf einem lokalen Server. Auf diese Verzeichnisse haben ausschließlich die Prozeduren des SQL-Servers und des Output-Management-Systems Leserechte.

Aufbewahrungsfrist

Die Druckdaten werden im Output-Management-System nach 14 Tagen vollständig gelöscht. Die Aufbewahrungsfrist wird benötigt, um eventuelle Reklamationen nachvollziehen und bearbeiten zu können.

Externes Wartungspersonal

BC Direct Group wartet seine Systeme soweit wie möglich selbst. Externes Wartungspersonal wird nur in seltenen Fällen benötigt und während der Wartungsarbeit persönlich überwacht. Dazu wird der Zugang nur über einen VPN ermöglicht, der nur für die Dauer des Einsatzes geöffnet ist.

Manuelle Bearbeitung

Es findet keine manuelle Bearbeitung von Papierpost statt. Die Produktion der Briefe und die Kuvertierung erfolgen in vollautomatischen Verarbeitungsschritten.

Wird ein Druckauftrag nicht richtig durchgeführt (Beschädigung, mindere Druckqualität etc.) wird der Auftrag vernichtet und automatisiert neu gedruckt und verarbeitet.