AWS BEI PERSONIO

IT-INFRASTRUKTUR UND EINSATZ VON AWS BEI PERSONIO

Personio

Inhaltsverzeichnis

IT-Infrastruktur und Einsatz von AWS bei Personio

Das Wichtigste in Kürze

- **Personio setzt zukünftig auf die Dienstleistungen von Amazon Web Services (AWS) als Hosting Provider**
- **Alle Kundendaten bleiben zukünftig auf Servern in Frankfurt und werden die EU nicht verlassen**
- **AWS erfüllt nicht nur strenge Sicherheits- und Compliance-Anforderungen, sondern ermöglicht die Steigerung der Stabilität und Skalierbarkeit unserer Infrastruktur**
- **Sowohl unser Datenschutzbeauftragter als auch die Landesdatenschutzbehörde haben datenschutzkonforme Nutzung von AWS in Deutschland bestätigt**
- **Alle Daten werden ausschließlich verschlüsselt gespeichert und die Masterschlüssel bei uns generiert, damit weder AWS noch sonstige Drittparteien Zugriff auf Kundendaten erhalten**
- **Personio trifft zusätzliche technische und organisatorische Maßnahmen, um die Sicherheit der Verarbeitung zu gewährleisten**

Einleitung

Im Rahmen der Vorbereitung auf die DSGVO haben wir alle unsere Prozesse, technischen Maßnahmen und Gegebenheiten hinterfragt. Dabei haben wir auch unser Hosting-Konzept im Hinblick auf Datensicherheit, Verfügbarkeit und Skalierbarkeit beleuchtet. Unter Einbeziehung verschiedener Experten (Datenschutzbeauftragter, IT-Sicherheitsberater, Landesdatenschutzbeauftragte etc.) haben wir eine Reihe von Maßnahmen definiert, um langfristig eine unter den genannten Kriterien optimale Lösung für unsere Kunden zu erzielen.

Die wichtigste Veränderung in diesem Kontext ist der Wechsel des Hosting-Providers zu Amazon Web Services (AWS). Diese Entscheidung wurde auf Basis einer ausführlichen Analyse getroffen, in welcher wir diverse Anbieter und Modelle verglichen haben.

Ausschlaggebend für die Entscheidung für AWS waren neben der Erfüllung von strengen Sicherheits- und Compliance-Anforderungen vor allem auch die damit einhergehende Steigerung der Stabilität und Skalierbarkeit unserer Infrastruktur.

Obwohl wir von der Datensicherheit bei AWS überzeugt sind, teilen wir grundsätzlich die rechtlichen und sicherheitsbezogenen Bedenken bei amerikanischen Cloud-Anbietern und haben daher sowohl auf rechtlich-vertraglicher als auch technischer Ebene alle notwendigen Vorkehrungen getroffen, um die bestmögliche Sicherheit aller Ihrer Daten zu gewährleisten.

Dieses Dokument soll sowohl Transparenz über unsere Entscheidungsgrundlage schaffen, als auch einen Einblick in unsere rechtlichen und technischen Maßnahmen geben, mit welchen wir unsere Kundendaten schützen. Es ist vor allem für den Datenschutz- und Informationssicherheitsbeauftragten sowie die Rechtsabteilung Ihres Unternehmens geschrieben.

IT-Infrastruktur und Einsatz von AWS bei Personio

Compliance & Rechtliches

Wir haben AWS anhand eines sorgfältigen Auswahlprozesses unter Berücksichtigung von rechtlichen, organisatorischen und technischen Kriterien ausgewählt. Nach einer intensiven Due Diligence und entsprechenden Verhandlungen freuen wir uns, dass wir mit AWS mit einem Infrastruktur-Partner zusammenarbeiten werden, der neben erstklassigen Produkten und Dienstleistungen auch ein äußerst professionelles Compliance- und Sicherheits-Setup aufweist.

Zertifizierungen zum Nachweis von Informationssicherheit und Datenschutz

Die in der AWS-Region Frankfurt und in den restlichen europäischen Regionen angebotenen und von uns genutzten Dienstleistungen wie RDS (Datenbank), S3 (Speicher für bspw. Dokumente) oder KMS (Schlüsselverwaltung) sowie das Rechenzentrum in Frankfurt verfügen über zahlreiche international anerkannte Zertifizierungen, die von unabhängigen renommierten Beratungsgesellschaften attestiert wurden und die Erfüllung höchster Sicherheitsanforderungen nachweisen.

Die AWS-Region Frankfurt, weitere Regionen und entsprechende Dienstleistungen sind sowohl zur IT-Sicherheit nach der DIN ISO/IEC 27001 als auch zum Schutz personenbezogener Daten in der Cloud nach der DIN ISO/IEC 27018 zertifiziert. Außerdem hat sich AWS nach dem international anerkannten Payment Card Industry Data Security Standard (PCI DSS) zertifizieren lassen. Dieser Standard wird verbindlich von Kreditkartenorganisationen angewandt und gilt als einer der strengsten Sicherheits-Regelwerke weltweit.

Außerdem ist AWS das erste Unternehmen, das sich die Sicherheit ihrer Cloud-Umgebung vom Bundesamt für Sicherheit in der Informationstechnik (BSI) auf Basis des Anforderungskatalogs Cloud Computing (Cloud Computing Compliance Controls Catalogue, C5) hat bescheinigen lassen. Damit gilt AWS als Vorreiter für Cloud-Sicherheit in Deutschland. Eine Übersicht über alle Compliance Programme und Zertifizierungen von AWS finden Sie hier.

Im Rahmen des Auswahlprozesses unseres neuen Hosting-Providers haben wir intensiv mit unserem Datenschutzbeauftragten der Bitkom Servicegesellschaft mbH sowie der hiesigen Landesdatenschutzbehörde zusammengearbeitet.

Beide haben uns die datenschutzkonforme Nutzung von AWS in Deutschland bestätigt, solange eine entsprechende Vereinbarung zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO geschlossen ist. Dies haben wir in den Verhandlungen mit AWS entsprechend vereinbart.

Selbstverständlich ist AWS auch DSGVO konform. Nähere Informationen finden Sie hier.

Beschränkung des Server-Standortes auf den EU-Raum

Um sicherzustellen, dass die Daten nicht unbefugt genutzt oder weitergegeben werden können, haben wir zudem vertraglich die Nutzung der Dienste explizit auf den EU-/ EWR-Raum beschränkt und die Zugriffsmöglichkeiten entsprechend geregelt. Dies gilt auch für den Fall der Wartung. Ausgenommen ist hiervon selbstverständlich, wenn Sie den Transfer außerhalb der EU wünschen, bspw. für unsere Kunden im europäischen Ausland oder Ihre

außereuropäischen Niederlassungen.

Uns sind die Vorbehalte einiger Datenschutzexperten in Bezug auf die mögliche Weitergabe von Daten auf Basis der Anfrage der US-Regierung bewusst. Wir beobachten dabei entsprechende Entwicklungen der US-Gesetzgebung wie den Cloud Act ebenso wie EU-Bestrebungen zum Datenaustausch von elektronischem Beweismaterial in Strafangelegenheiten und begrüßen grundsätzlich die Absicht, Rechtssicherheit zu schaffen. Es bleibt festzuhalten, dass es eine anlasslose Herausgabe von Daten weder von uns noch AWS geben wird, da dies weder im unternehmerischen Interesse der beiden Unternehmen noch unserer Kunden ist. Es wäre dennoch falsch, zu verschweigen, dass es gesetzliche Grundlagen gibt, auf den AWS oder wir zur Herausgabe verpflichtet sind, insbesondere im Falle der Verfolgung einer Straftat. Dieses Risiko besteht jedoch ebenso innerhalb von Deutschland sowie in anderen Mitgliedstaaten der EU.

Um selbst in dem unwahrscheinlichen Fall eines Herausgabeanspruchs einer Regierung die Daten sowie bei „Angriffen von außen" die Daten unserer Kunden zu schützen, haben wir mit AWS gemeinsam ein umfangreiches Datenschutz- und IT-Sicherheitskonzept entwickelt. Nach dem „Shared Responsibility Model" setzen wir dabei zum einen auf die umfangreichen Sicherheitsmechanismen von AWS („Security of the Cloud") und werden zudem unsere eigenen Sicherheitsmaßnahmen zusätzlich anwenden („Security in the Cloud"). Mehr Informationen zu dem „Shared Responsibility Model" von AWS finden Sie hier, weitere Informationen zu den technischen und organisatorischen Maßnahmen von AWS sind hier aufgeführt.

Ein wesentliches Kernelement unserer Sicherheitsmaßnahmen ist dabei die auch in der DSGVO geforderte Verschlüsselung. Dabei setzen wir auf Verschlüsselungsalgorithmen nach dem Stand der Technik (siehe Abschnitt „Verschlüsselung"), nach Möglichkeit auf AES-256, welches selbst in den USA für Dokumente der höchsten Geheimhaltungsstufe zugelassen ist und als nicht zu entschlüsseln gilt. Je nach Rechenleistung und der Art des Angriffs kann es daher mehr als zehn Jahre dauern, die Daten zu entschlüsseln.

Im Bewusstsein, dass es hierzu in der Datenschutz-Welt unterschiedliche Ansichten gibt, hat sich die Artikel-29-Datenschutzgruppe, einem Zusammenschluss der nationalen, europäischen Datenschutzbeauftragten in ihrem Working Paper 136 zum Begriff „personenbezogene Daten" zum Personenbezug bei verschlüsselten Daten positioniert: Danach gelten die Daten nicht mehr als personenbezogen, wenn „die Reidentifizierung explizit ausgeschlossen ist und diesbezüglich geeignete technische Maßnahmen getroffen wurden" (Artikel 29-Gruppe WP 136, S. 21 ff.). Dies stellen wir im Rahmen unseres Sicherheitskonzepts für AWS und andere Dritte sicher.

Technische und weitere organisatorische Maßnahmen

Im Folgenden möchten wir näher auf unser Datenschutz- und IT-Sicherheitskonzept im Zusammenhang mit dem Einsatz von AWS eingehen. Sofern Sie Fragen hierzu haben, wenden Sie sich bitte direkt an security@personio.de. Unser Datenschutz- und Informationssicherheits-Team steht Ihnen gerne zur Verfügung.

IT-Infrastruktur und Einsatz von AWS bei Personio

Verschlüsselung

Um sicherzustellen, dass Amazon bei der Nutzung der AWS-Cloud durch die Personio GmbH keinen Zugang auf die Kundendaten erhält, werden alle Kundendaten ausschließlich verschlüsselt gespeichert.

Dabei kommt das Key Management System der Amazon Web Services (AWS KMS) zum Einsatz. Die verwendeten Schlüssel werden ausschließlich von einem Master Key (Customer Master Key - CMK) abgeleitet, der nicht in der AWS-Cloud generiert wird und nur verschlüsselt im AWS KMS abgelegt wird. Dadurch hat Amazon keinen Zugriff auf die davon abgeleiteten Keys sowie auf die CMK von Personio selbst. Somit kann AWS die in der Cloud gespeicherten Daten nicht entschlüsseln.

Die Verwendung von AWS KMS bei der Personio GmbH - Grundlagen

AWS Key Management Service (AWS KMS) ist ein Managed Service, der die Erstellung und Kontrolle der Verschlüsselungsschlüssel für die Datenverschlüsselung vereinfacht. Die Masterschlüssel in AWS KMS sind durch FIPS 140-2 validirte kryptographische Module geschützt.

Folgende Features werden von AWS KMS grundsätzlich unterstützt:

- Anlegen, Beschreiben und Auflisten des Hauptschlüssels
- Aktivieren und Deaktivieren von Hauptschlüsseln
- Erstellen und Anzeigen von Berechtigungen und Zugriffskontrollrichtlinien für den Master Key (Customer Master Key - CMK)
- Aktivieren und Deaktivieren der automatischen Rotation des kryptographischen Materials in einem Master Key
- Importieren von kryptographischem Material in einen AWS KMS Master Key
- Markieren von Hauptschlüsseln für eine leichte Identifizierung, Kategorisierung und für Tracking
- Löschen von Master Keys zum Abschließen des Lebenszyklusses von Schlüsseln

Die folgenden kryptographischen Funktionen werden von AWS KMS unterstützt:

- Verschlüsseln, Entschlüsseln und Neu-Verschlüsseln von Daten
- Generieren von Schlüsseln zur Verschlüsselung von Daten (Data Encryption Keys)
- Generieren von Zufallszahlen für kryptographische Applikationen

Vertraulichkeit

Personio schränkt aufgrund ihrer Sicherheitsvorgaben diese Features jedoch ein. Die Zufallszahlen, die vom AWS KMS generiert werden, können nicht als vertrauenswürdig betrachtet werden, da die verwendete Hardware sowie die genutzten Algorithmen zur Generierung der Zufallszahlen nicht offengelegt werden. Die Sicherheit

von Schlüsselmaterial und somit der mit diesem erzeugten Verschlüsselungen ist jedoch maßgeblich von den Zufallskomponenten abhängig, die zur Generierung der Schlüssel verwendet werden. Eine nicht ausreichende Zufälligkeit oder gar das Abfangen und Aufzeichnen der Zufallskomponenten ermöglicht Seitenkanal-Angriffe auf die Verschlüsselung und damit das Aufbrechen der Verschlüsselung.

Aus diesem Grund wird der Master Key niemals auf Servern oder sonstigen Rechnern von AWS generiert.

Die Generierung erfolgt mittels OpenSSL - einer quelloffenen Verschlüsselungsbibliothek mit zugehörigen Programmen - auf Rechnern der Personio GmbH, üblicherweise auf den Arbeitsrechnern des zuständigen und fachkundigen technischen Personals, und folgt dem entsprechenden Stand der Technik. Das so erstellte Schlüsselmaterial wird ausschließlich verschlüsselt in das AWS KMS übertragen. So wird sichergestellt, dass auch Mitarbeiter von AWS keinen Zugriff auf verschlüsselte Daten, die die Personio GmbH im Rahmen ihrer Auftragsverarbeitung speichert oder verarbeitet, erlangen können.

Monitoring

AWS KMS ermöglicht es, jeden Zugriff auf die darin gespeicherten Keys detailliert zu überwachen. Jeder Zugriff wird aufgezeichnet. Dadurch kann die Personio GmbH sicherstellen, dass es keine unautorisierten Zugriffe auf die zur Verschlüsselung der Daten verwendeten Schlüssel gibt. Die Zugriffe auf die Schlüsselverwaltung werden automatisiert und in regelmäßigen Abständen sowie bei Verdacht auf einen Sicherheitsvorfall manuell vom IT Security Manager oder durch von ihm beauftragtes Personal der Personio GmbH auf Unregelmäßigkeiten überprüft.

Weiterhin ermöglicht AWS KMS, den Austausch von Schlüsseln zu überwachen sowie eindeutig den Personen, die den Austausch veranlasst haben, zuzuordnen.

Schlüsselrotation

Alle Schlüssel werden regelmäßig rotiert. Dabei werden die bisher verwendeten Schlüssel invalidiert und die Daten mit den neu erstellten Schlüsseln neu verschlüsselt.

Die invalidierten Schlüssel werden aus dem AWS KMS entfernt und in ein Archiv überführt, wo sie zur Verfügung gehalten werden, um bei Bedarf Backups zu entschlüsseln. Gibt es keine Backups mehr, die Daten enthalten, die mit den jeweiligen Schlüsseln verschlüsselt wurden, werden die invalidierten Schlüssel aus dem Archiv entfernt. Jeder Zugriff auf das Schlüssel-Archiv wird aufgezeichnet und mittels eines Angriffserkennungssystems an das zuständige Personal notifiziert.

Im Rahmen einer regelmäßigen Sicherheitsprüfung wird sichergestellt, dass die Maßnahmen zur Schlüsselrotation ordnungsgemäß greifen und alte Schlüssel ordnungsgemäß entfernt wurden.

IT-Infrastruktur und Einsatz von AWS bei Personio

Speicherung und Nutzung des unverschlüsselten Schlüssel-Materials

Unverschlüsseltes Schlüssel-Material wird nur so lange unverschlüsselt aufbewahrt, wie es für die Erstellung eines CMK notwendig ist. Zu Zwecken der Archivierung und Nachvollziehbarkeit der Integrität der daraus erstellten Schlüssel wird das Schlüsselmaterial in einem Versionsverwaltungssystem (Git) unter Verwendung von Git-Crypt abgelegt. Git-Crypt verwendet Verschlüsselung mittels Pretty Good Privacy (PGP), um den Zugriff auf diese Daten einzuschränken. Der Zugriff auf das so archivierte Schlüsselmaterial ist ausschließlich für Mitarbeiter des Infrastructure & Engineering-Teams möglich. Verlässt ein Mitarbeiter das Team durch Ausscheiden aus dem Unternehmen oder durch den Wechsel in eine andere Abteilung, wird sein PGP-Schlüssel umgehend aus dem Git-Repository entfernt und der Zugriff auf das Schlüsselmaterial so unterbunden.

Datenbank-Verschlüsselung („Data at rest")

Alle von Personio eingesetzten Datenbanken verwenden eine sogenannte Verschlüsselung „at rest". Dies bedeutet, dass die Daten aus der Datenbank nur gelesen werden können, wenn eine ordnungsgemäße Authentifizierung am jeweiligen Datenbank-System stattfindet. Die Dateien, in denen die Daten abgelegt sind, werden verschlüsselt gespeichert, sodass sie nur von Datenbank-Systemen gelesen werden können, die über den passenden Key für die Entschlüsselung verfügen. Selbiges gilt für etwaige Seitenkanäle der Datenbank-Systeme wie Binlogs. Die Schlüssel werden, wie oben beschrieben, im AWS KMS verwaltet.

Verschlüsselung von Speichermedien

Personio speichert einige Daten direkt als Dateien ohne Verwendung eines Datenbank-Systems. Dies sind insbesondere Dokumente und sonstige Uploads der Kunden sowie Logdaten, die jedoch ggf. mit Datenbank-Inhalten über IDs oder Bezeichner assoziiert werden. Um sicherzustellen, dass kein unautorisierter Zugang zu diesen Daten erfolgen kann, werden die Speichermedien (AWS-Dienste EBS und S3) verschlüsselt.

Für S3 kommt SSE-KMS zum Einsatz, wodurch die volle Kontrolle über den Master-Key bei Personio bleibt. Die Verwendung von SSE-S3 ist untersagt, wenn auf den Speichermedien Kundendaten oder sonstige sensible Daten abgelegt werden.

Für EBS-Volumes werden die von Personio im AWS KMS bereitgestellten CMK verwendet. Diese Master Keys werden auch verwendet, um Snapshots, die aus den Volumes abgeleitet werden, zu verschlüsseln (bspw. Backups). Welcher CMK zum Einsatz kommt, hängt vom Verwendungszweck des Systems und seinem jeweiligen Netzwerk, in dem es sich befindet, ab. Siehe dazu auch „Datentrennung im Rahmen der Verschlüsselung".

Sonstige Datenverschlüsselung

Zusätzlich werden schützenswerte Daten, die nicht auf der Datenbank oder auch Speichermedien abgelegt werden, applikationsseitig verschlüsselt (bspw. Caches).

Transportverschlüsselung („Data in transit")

Die Systeme der Personio GmbH verwenden eine Transportverschlüsselung immer dann, wenn Daten über ein unsicheres oder öffentliches Netzwerk (bspw. außerhalb der Virtual Private Cloud) übertragen werden müssen.

IT-Infrastruktur und Einsatz von AWS bei Personio

Welche Transportverschlüsselung verwendet wird, ist unter anderem abhängig von der vom Client-System angeforderten Verschlüsselung. Personio stellt für die Abwärtskompatibilität auch einige Transportverschlüsselungsalgorithmen zur Verfügung, die als nicht mehr sicher eingestuft werden. Innerhalb des Unternehmens werden jedoch ausschließlich sichere Transportverschlüsselungen verwendet. Der Kunde ist dafür verantwortlich, sicherzustellen, dass sein Client-System die entsprechende Transportverschlüsselung nach dem Stand der Technik unterstützt und entsprechend präferiert.

- **HTTPS**

  Das Webinterface sowie die API der Personio-Applikation sind ausschließlich über HTTPS-Verbindungen erreichbar. Es wird empfohlen, für den Zugriff Client-Systeme zu verwenden, die mindestens TLS 1.2 unterstützen.

  Folgende Transport-Verschlüsselungen **werden derzeit als unsicher betrachtet**, werden jedoch von Personio für die Abwärtskompatibilität mit älteren und/oder sogenannten mobilen Browsern auf Seiten der Kunden vorerst weiterhin unterstützt:

  - TLS 1.2
    - » TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
    - » TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
    - » TLS_RSA_WITH_AES_128_GCM_SHA256
    - » TLS_RSA_WITH_AES_256_GCM_SHA384
    - » TLS_RSA_WITH_AES_128_CBC_SHA256
    - » TLS_RSA_WITH_AES_256_CBC_SHA256
    - » TLS_RSA_WITH_AES_128_CBC_SHA
    - » TLS_RSA_WITH_AES_256_CBC_SHA
    - » TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS 1.1
    - » TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
    - » TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
    - » TLS_RSA_WITH_AES_128_CBC_SHA
    - » TLS_RSA_WITH_AES_256_CBC_SHA
    - » TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS 1.0
    - » TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
    - » TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
    - » TLS_RSA_WITH_AES_128_CBC_SHA
    - » TLS_RSA_WITH_AES_256_CBC_SHA
    - » TLS_RSA_WITH_3DES_EDE_CBC_SHA

- **Administrative Zugänge**

  Zugriffe auf die Systeme der Personio GmbH für administrative Zwecke erfolgen ausschließlich über VPN-Verbindungen oder über SSH, um eine sichere Transportverschlüsselung zu ermöglichen. Kommt SSH zum Einsatz wird von den Servern der Personio GmbH ausschließlich SSHv2 unterstützt. Die Verwendung von SSHv1 ist im Unternehmen untersagt und alle Server werden durch die zuständigen technischen Mitarbeiter entsprechend konfiguriert.

Datentrennung im Rahmen der Verschlüsselung

So wie Personio darauf achtet, dass die Daten zwischen verschiedenen Netzwerken strikt getrennt werden (Development, Staging, Testing und Production), werden auch die für die verschiedenen Netzwerke verwendeten Verschlüsselungsschlüssel strikt getrennt. Ein Schlüssel wird ausschließlich in dem Netzwerk verwendet, für das er erstellt wurde. Eine Überführung von Schlüsseln in ein anderes Netzwerk ist nicht gestattet und wird durch technische Maßnahmen unterbunden. Regelmäßige Sicherheitsprüfungen stellen sicher, dass die getroffenen technischen Maßnahmen nicht durch manuelle Eingriffe umgangen werden.

Weiterhin wird sichergestellt, dass ein Schlüssel immer genau einem Zweck zugeordnet ist. So darf z. B. auf Infrastruktur-Level ein Schlüssel, der für Storage-Verschlüsselung verwendet wird, nicht gleichzeitig für die Datenbank-Verschlüsselung eingesetzt werden.

Verantwortlichkeiten im Bereich des Datenschutzes

Personio teilt sich seine Verantwortlichkeiten im Bereich Datenschutz mit AWS. Dabei fallen AWS folgende Assets zu:

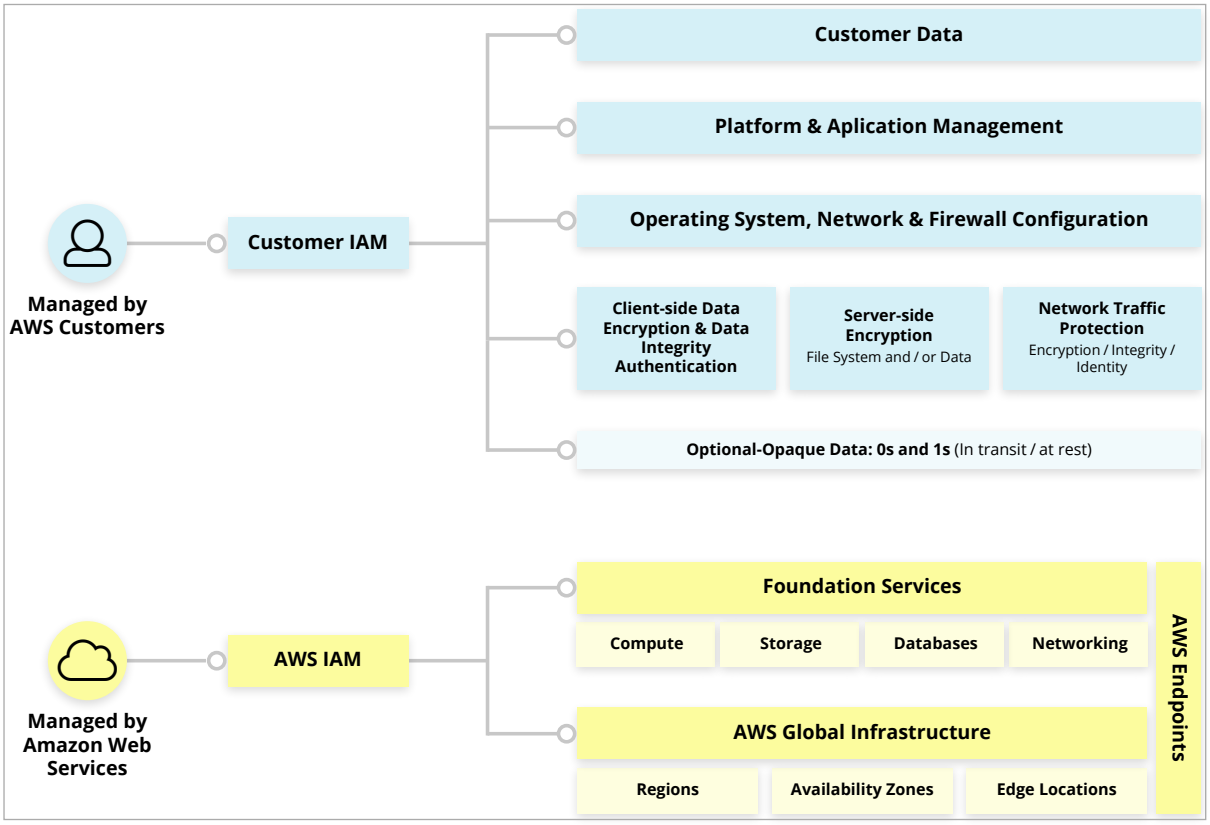
- Anlagen (Rechenzentren, Klimatisierung u. ä.)
- Physische Sicherheit der Hardware
- Netzwerk-Infrastruktur (Router, Switches, Kabel etc.)
- Virtualisierungsinfrastruktur
- Betriebssysteme und Software im Fall von SaaS-Diensten

Folgende Assets fallen in die Verantwortlichkeit von Personio, wenn sie im Rahmen von IaaS genutzt werden:

- Amazon Machine Images (AMI)
- Betriebssysteme
- Applikationen und Programmbibliotheken
- Daten im Transit
- Ruhende/ Gespeicherte Daten
- Datenspeicher

IT-Infrastruktur und Einsatz von AWS bei Personio

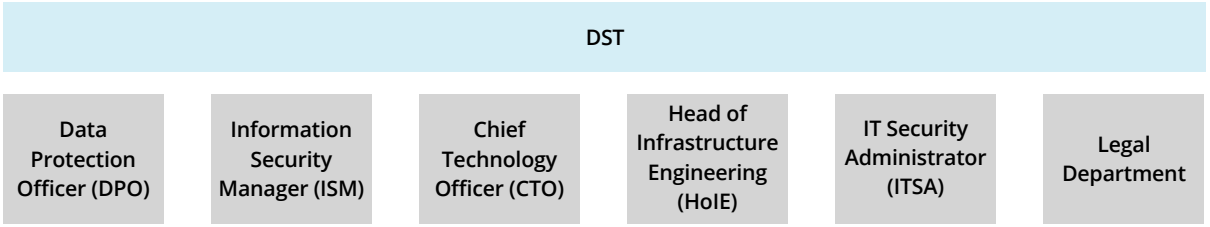
- Anmeldeinformationen
- Policies und Konfigurationen



Quelle: AWS

Personio hat für alle Themen, die den Datenschutz sowie die Datensicherheit betreffen, ein Datenschutz- und Informationssicherheits-Team (DST) gebildet, das aus folgenden Personen besteht:

- Datenschutzbeauftragter (DSB)
- Information Security Manager (ISM)
- Chief Technology Officer (CTO)
- Leiter der Infrastruktur Abteilung (HoIE)
- IT System Administrator (ITSA)
- Rechtsabteilung



IT-Infrastruktur und Einsatz von AWS bei Personio

Zugriffskontrolle

Personio nutzt verschiedene Level der Zugriffskontrolle für seine Systeme und Services bei AWS. Diese werden mittels dem Identity and Access Management (IAM) von AWS verwaltet, das eine feine Granulation der Zugriffe auf verschiedene Dienste innerhalb der AWS-Cloud ermöglicht sowie Zugriffe auf die Dienste aufzeichnet. Oberstes Prinzip bei der Rechtevergabe ist für Personio „Need-to-Know". In der Praxis bedeutet dies, dass Mitarbeiter nur auf die Funktionen Zugriff erhalten, die sie zur Ausübung ihrer Tätigkeiten benötigen. Übergeordnete Rechte sind ausschließlich dem technischen Management (CTO, HoIE etc.) bzw. dem ISM vorbehalten und erfolgen nach dem Vier-Augen-Prinzip. Sie verfügen über die Zugangsdaten der AWS-Accounts und sind gegenüber dem DST rechenschaftspflichtig. Alle anderen Mitarbeiter von Personio bekommen prinzipiell maximal IAM-Accounts, die auf jene Rechte beschränkt sind, die sie für ihre Arbeit benötigen. Der ISM überprüft in regelmäßigen Audits, ob die vergebenen Zugriffsrechte dem Need-to-Know-Prinzip entsprechen.

Zugriff auf Backend-Systeme erfolgt ausschließlich über VPN. Eine öffentliche Freigabe von Backend-Systemen ist untersagt.

Nur Mitarbeiter des Infrastructure Engineering Teams von Personio erhalten Zugriff auf Systemebene der von Personio betriebenen Systeme. Dieser Direktzugriff wird ausschließlich für Fehleranalysen genutzt.

Durch Verschlüsselung der Daten stellt Personio sicher, dass Mitarbeiter von AWS keinen Zugriff auf Kundendaten erlangen können. Siehe dazu auch den Abschnitt „Verschlüsselung".

Firewalling und Security Groups

AWS stellt mittels Security Groups eine Paketfilter-Firewall bereit, die den Zugriff auf Dienste einer Server-Instanz (EC2) oder auf SaaS-Dienste einschränkt. Personio nutzt diese um sicherzustellen, dass Dienste, die innerhalb der AWS-Umgebung laufen, nur für die Netzwerke erreichbar sind, für welche die Notwendigkeit dafür besteht. Das bedeutet, dass der Zugriff auf Netzwerk-Ports verschiedener Dienste soweit eingeschränkt wird, dass ein Zugriff nur noch durch jene anderen Dienste möglich ist, die den Zugriff zwingend benötigen.

Die Security Groups werden unter anderem auch für die Netzwerk-Trennung verwendet. Siehe dazu Abschnitt „Netzwerktrennung".

Zusätzlich steht auf AWS EC2-Instanzen, die für die Personio eigene Software verwendet werden, die Linux-Firewall „iptables" zur Verfügung, die eine zusätzliche Granulation der Filterregeln ermöglicht. Diese wird zum Beispiel im Rahmen des Kubernetes-Clusters von Personio verwendet.

Verfügbarkeitszonen und Geolocation

Personio speichert Daten ausschließlich in AWS-Rechenzentren in Deutschland (Frankfurt). Durch vertragliche Vereinbarungen ist sichergestellt, dass AWS keine Daten von Personio an andere Locations transferiert, auch nicht für Wartungszwecke (siehe dazu auch den Abschnitt „Compliance & Rechtliches"). In Frankfurt stehen 3

IT-Infrastruktur und Einsatz von AWS bei Personio

Verfügbarkeitszonen zur Verfügung. Alle Frontend- und Backend-Systeme, die von Personio betrieben werden, sind redundant ausgelegt und werden auf diese drei Zonen verteilt. So ist sichergestellt, dass selbst beim Ausfall einer Verfügbarkeitszone der Betrieb der Personio-Applikation uneingeschränkt möglich ist.

Jede Verfügbarkeitszone ist an mehrere Internet Service Provider angeschlossen und wird durch mehrere Stromkreise versorgt. Sie sind durch High-Speed-Links miteinander verbunden, so dass die Applikationen, die auf mehrere Zonen verteilt sind, LAN-Verbindungen nutzen können, um zwischen den Zonen zu kommunizieren. Dies ermöglicht eine optimale Performance alle Systeme, die von der Personio-Applikation genutzt werden.

Netzwerktrennung

Personio stellt eine Trennung von Netzwerken, die für unterschiedliche Zwecke verwendet werden, in der AWS-Umgebung dadurch sicher, dass sowohl unterschiedliche AWS-Master-Accounts als auch unterschiedliche VPC (Virtual Private Clouds) verwendet werden. Eine Übertragung von Daten zwischen verschiedenen VPC wird durch die oben beschriebenen Security Groups unterbunden.

Intrusion Detection/ Malware Detection/ Logging von sicherheitsrelevanten Ereignissen

Personio verwendet ein Host-Based Intrusion Detection System (HIDS). Es besteht aus den Agents, die auf den jeweiligen EC2-Instanzen laufen, sowie einem zentralen Master, der die Verfügbarkeit der Agents überwacht und der von den Agents über Anomalien informiert wird.

Das HIDS überwacht:

- Logdateien auf ungewöhnliche oder unbekannte Einträge
- Änderungen an Systemdateien (File Integrity Monitoring) sowie AWS-eigene Konfigurationen
- Sämtliche Login-Versuche sowie Rechte-Änderungen innerhalb der Systeme
- Änderungen im Device-Filesystem und den geladenen Kernel-Modulen, um den Anschluss unautorisierter Hardware zu erkennen
- Netzwerk-Traffic
    - » Bekannte Exploits und Rootkits
    - » Spoofing
- Alle Änderungen am HIDS selbst inkl. Restarts oder Ausfall von Agents
- Durch IAM-Benutzer ausgelöste API-Events innerhalb der AWS-Account-Umgebungen
- Ungenutzte Dienste oder Benutzer auf den jeweiligen Systemen
- Änderungen bei genutzten (Netzwerk-)Ports

IT-Infrastruktur und Einsatz von AWS bei Personio

Werden sicherheitsrelevante Anomalien auf einem System erkannt, werden diese automatisch den zuständigen Mitarbeitern bei Personio mitgeteilt, die daraufhin eine manuelle Prüfung der Anomalie vornehmen. Besonders kritische Anomalien wie z. B. bei der Erkennung eines Rootkits werden automatisch unterbunden. Weiterhin unterstützt das HIDS ein Security Policy Enforcement, das den Anforderungen von PCI DSS 3.0 entspricht. Dieses wird genutzt, um sichere Konfigurationen der laufenden Dienste zu erzwingen sowie mögliche Sicherheitsrisiken (beispielsweise nicht genutzte Systemzugänge) zu erkennen.

Logging/ Audit Trail

Personio nutzt in seinen AWS-Umgebungen Logging für verschiedene Bereiche. Diese umfassen:

- System-Ereignisse
- Error Logging
- Benutzer-Aktivitäten
- Anmeldungen sowie Anfragen an Datenbank-Systeme
- Sonstige Security-relevanten Ereignisse / Audit Logging

Durch die Verwendung von AWS Cloudtrail hat Personio die Möglichkeit, sämtliche Events innerhalb der genutzten Cloud-Umgebungen aufzuzeichnen und dadurch nicht nur transparente Benutzer- und Ressourcen-Aktivitäten zu schaffen, sondern auch ein hohes Transparenz-Level zur forensischen Analyse möglicher Sicherheitsvorfälle bereitzustellen.

Die Informationen, die durch Cloudtrail gesammelt werden, werden durch das HIDS ausgewertet, um Anomalien zeitnah zu erkennen.

Change Management

Personio verwaltet Konfigurationen von Systemen und Software mittels „Infrastructure as Code“. Der zugehörige Code wird in Repositories einer Versionsverwaltung (Git) abgelegt, um Änderungen zeitlich und inhaltlich nachvollziehbar zu machen.

Bevor Änderungen in die Betriebsumgebung eingespielt werden, werden diese in einer Staging-Umgebung, die identisch zur Betriebsumgebung aufgebaut ist, getestet. Dies gilt sowohl für Konfigurationsänderungen als auch für System- und Software-Updates.

Backups

Personio erstellt tägliche Backups aller Daten, die zum Betrieb der Infrastruktur notwendig sind, sowie aller Daten, die von Kunden in der Personio Applikation eingegeben oder hochgeladen werden.

IT-Infrastruktur und Einsatz von AWS bei Personio

Performance und Auto Scaling

Soweit möglich nutzt Personio die von AWS bereitgestellten Auto-Scaling-Funktionen, um eine bestmögliche Performance zu ermöglichen. Dadurch ist es möglich, vollständig automatisiert Ressourcen zu den Netzwerken zuzuschalten, wenn die vorhandenen Ressourcen nicht mehr ausreichend sind.

Monitoring

Personio nutzt verschiedene Monitoring-Tools, um eine maximale Verfügbarkeit und Performance der Applikation sicherzustellen. Diese überwachen mindestens folgende Parameter:

- Verfügbarkeit
  - » Erreichbarkeit der Applikation
  - » Erreichbarkeit von Backend-Systemen und -Diensten
- Ressourcen
  - » Auslastung von CPUs
  - » Auslastung von Netzwerk-Interfaces
  - » Auslastung von persistenten und flüchtigen Speichern
- Performance
  - » Application Performance Index (Apdex)
  - » Antwortzeiten der Applikation
  - » Antwortzeiten von Backend-Systemen
  - » Abfragezeiten für Datenbankinhalte
- Security
  - » Siehe Abschnitt „Intrusion Detection / Malware Detection / Logging von sicherheitsrelevanten Ereignissen“
  - » Update-Status von Systemen
- Monitoring
  - » Error-Logs
  - » Zugriffslogs

Zusätzlich zu diesem automatisierten Monitoring überwachen Mitarbeiter vom DST einschlägige Online-Medien und Blogs auf das Bekanntwerden von Sicherheitslücken, um zeitnah auf diese reagieren zu können.

IT-Infrastruktur und Einsatz von AWS bei Personio

Security Audits und Penetration Tests

Personio führt in regelmäßigen Abständen sowohl interne als auch externe Sicherheitstests durch. Zudem wird die Sicherheit der Personio-Applikation regelmäßig durch einen externen, unabhängigen Anbieter auf mögliche Schwachstellen überprüft (Ergebnisse des letzten Penetrationstest auf Anfrage sowie des letzten Audits durch die Bitkom auf unserer Datenschutz-Website unter *Downloads*). Weiterhin führt das DST auch interne Audits durch, bei denen nicht nur die technischen, sondern auch die organisatorischen Maßnahmen innerhalb des Unternehmens auf ihre Wirksamkeit hin untersucht werden.

Abschließend möchten wir Sie gerne auf unsere **Datenschutz-Website** personio.de/datenschutz hinweisen, auf der Sie weiterführende Informationen und Dokumente zum Thema einsehen bzw. anfordern können. Sollten dennoch Fragen ungeklärt bleiben, wenden Sie sich gerne an datenschutz@personio.de.

Stand: 14.05.2018

Personio

Das HR-Betriebssystem