Whitepaper: Datenschutz und Datensicherheit bei der my-vpa GmbH

Inhaltsverzeichnis:

my-vpa GmbH
Kleine Spitzengasse 2-4
50676 Köln
www.my-vpa.com
Geschäftsführung: Ingmar Bornholz

Einleitung

In der heutigen Zeit ist der Schutz von persönlichen Daten und Informationen wichtiger denn je. Bei der my-vpa GmbH nehmen wir Datenschutz und Datensicherheit sehr ernst und haben eine Reihe von technischen und organisatorischen Maßnahmen implementiert, um die Integrität und Vertraulichkeit der Daten unserer Kunden zu gewährleisten. In diesem Whitepaper präsentieren wir die verschiedenen Schutzmaßnahmen und erläutern, wie unsere Plattform technisch abgesichert ist.

2. Datenschutz und Datensicherheit bei my-vpa

2.1. Gesetzliche Grundlagen und Standards

Die my-vpa GmbH hält sich an alle relevanten Datenschutzgesetze und -standards, insbesondere die EU-Datenschutz-Grundverordnung (DSGVO) und das Bundesdatenschutzgesetz (BDSG).

2.2. Verantwortung für den Datenschutz

Die my-vpa GmbH hat einen Datenschutzbeauftragten ernannt, der für die Einhaltung der Datenschutzbestimmungen und die Umsetzung der Datenschutzstrategie verantwortlich ist. Sie erreichen den Datenschutz unter datenschutz@my-vpa.com

3. Technische Maßnahmen

3.1. Server- und Netzwerksicherheit

Unsere Serverinfrastruktur basiert auf Amazon Web Services (AWS), einem der weltweit führenden Cloud-Anbieter. AWS bietet eine Vielzahl von Sicherheitsfunktionen, wie zum Beispiel physische Sicherheitsmaßnahmen, Netzwerksegmentierung und Firewalls. Darüber hinaus nutzen wir Kubernetes-Cluster, um unsere Anwendungen hochverfügbar und skalierbar zu gestalten. Kubernetes ermöglicht uns, Ressourcen effizient zu verwalten, Lastverteilung durchzuführen und die Anwendungen bei Bedarf automatisch zu skalieren.

3.2. Verschlüsselung und Authentifizierung

Alle Datenübertragungen zwischen unseren Kunden und der my-vpa Plattform werden mittels SSL/TLS-Verschlüsselung geschützt. Für die Authentifizierung und Autorisierung setzen wir auf Keycloak Single Sign-On (SSO), eine moderne und sichere Lösung zur zentralisierten Verwaltung von Benutzerkonten und Zugriffsrechten. Keycloak unterstützt starke

Authentifizierungsverfahren wie Zwei-Faktor-Authentifizierung und ermöglicht es uns, Passwörter effizient und sicher zu verwalten.

3.3. Datensicherung und Wiederherstellung

Wir führen regelmäßige Backups unserer Daten durch, um im Falle von Datenverlust oder technischen Problemen eine schnelle Wiederherstellung zu gewährleisten. Die Backups werden sowohl lokal als auch in geografisch getrennten Rechenzentren gespeichert, um das Risiko von Datenverlust durch Naturkatastrophen oder andere unvorhergesehene Ereignisse zu minimieren.

3.4. Sicherheitsüberprüfungen und Updates

Wir halten unsere Systeme stets auf dem neuesten Stand, indem wir regelmäßige Sicherheitsüberprüfungen durchführen und Sicherheitsupdates zeitnah installieren. Dadurch stellen wir sicher, dass potenzielle Sicherheitslücken schnell geschlossen werden und unsere Plattform gegen bekannte Bedrohungen geschützt ist.

4. Organisatorische Maßnahmen

4.1. Zugriffskontrolle und Berechtigungen

Der Zugang zu unseren Systemen und Daten ist auf Mitarbeiter mit einer entsprechenden Berechtigung beschränkt. Wir verwenden rollenbasierte Zugriffskontrollen, um sicherzustellen, dass Mitarbeiter nur auf die Daten und Ressourcen zugreifen können, die für ihre jeweilige Rolle erforderlich sind.

4.2. Schulung und Sensibilisierung der Mitarbeiter

Alle Mitarbeiter der my-vpa GmbH erhalten regelmäßige Schulungen und Informationen zum Thema Datenschutz und Datensicherheit. Dies gewährleistet, dass jeder Mitarbeiter die notwendigen Kenntnisse und Fähigkeiten besitzt, um die Datenschutzbestimmungen einzuhalten und die Datensicherheit zu gewährleisten.

4.3. Datenverarbeitungsverträge und Drittunternehmen

Wir arbeiten nur mit vertrauenswürdigen Drittunternehmen zusammen und schließen mit diesen Datenverarbeitungsverträge ab, um sicherzustellen, dass auch sie die Datenschutzbestimmungen einhalten und ein angemessenes Schutzniveau für die Daten bieten.

4.4. Datenschutz-Folgenabschätzung und Risikomanagement

Wir führen regelmäßig Datenschutz-Folgenabschätzungen durch, um potenzielle Risiken für die Datensicherheit zu identifizieren und geeignete Gegenmaßnahmen zu ergreifen.

Eine Zusammenfassung der technischen und organisatorischen Maßnahmen (ToM) inkl. der Auftragsdatenverarbeitungsvereinbarungen (AVV) finden Sie auch hier zum Download.

5. Die technische Absicherung der my-vpa Plattform

.1. Anwendungssicherheit und Code-Überprüfung

Unser Entwicklerteam verwendet bewährte Sicherheitspraktiken, um die Sicherheit unserer auf AWS gehosteten Plattform zu gewährleisten. Dazu gehören die Nutzung von AWS-Sicherheitsfunktionen, Code-Überprüfungen, automatisierte Tests und regelmäßige Sicherheitsaudits. Darüber hinaus werden Sicherheitslücken, die während der Entwicklungsphase identifiziert werden, priorisiert und schnell behoben. Die Nutzung von Kubernetes-Clustern trägt weiterhin zur Sicherheit und Stabilität unserer Plattform bei.

5.2. Sicherheitsmonitoring und Incident Response

Wir überwachen unsere Systeme kontinuierlich, um Anzeichen von Sicherheitsvorfällen oder verdächtigen Aktivitäten frühzeitig zu erkennen. Im Falle eines Sicherheitsvorfalls haben wir ein Incident Response Team, das umgehend Maßnahmen ergreift, um die Bedrohung abzuwehren und die Auswirkungen zu minimieren.

6. Fazit

Die my-vpa GmbH ist sich der Bedeutung von Datenschutz und Datensicherheit bewusst und hat umfassende technische und organisatorische Maßnahmen implementiert, um die Integrität, Vertraulichkeit und Verfügbarkeit der Daten unserer Kunden zu gewährleisten. Durch die kontinuierliche Überwachung unserer Systeme, regelmäßige Sicherheitsüberprüfungen und Schulungen unserer Mitarbeiter stellen wir sicher, dass unsere Plattform technisch abgesichert ist und den aktuellen Datenschutzbestimmungen entspricht.

7. Anhang

7.1. Glossar

- DSGVO: Datenschutz-Grundverordnung
- BDSG: Bundesdatenschutzgesetz
- SSL/TLS: Secure Sockets Layer/Transport Layer Security
- Zwei-Faktor-Authentifizierung: Authentifizierungsverfahren, das zwei unabhängige Komponenten zur Verifizierung der Identität eines Benutzers verwendet

7.2. Weiterführende Links und Ressourcen

- Datenschutz-Grundverordnung (DSGVO): https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Bundesdatenschutzgesetz (BDSG): https://www.gesetze-im-internet.de/bdsg_2018/
- Informationen zur Zwei-Faktor-Authentifizierung: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Zugangssicherung/ZweiFaktorAuthentifizierung/zweifaktorauthentifizierung_node.html

Dieses Whitepaper dient als Übersicht über die Datenschutz- und Datensicherheitsmaßnahmen der my-vpa GmbH und soll einen Einblick in die verschiedenen Schutzmaßnahmen und die technische Absicherung unserer Plattform bieten. Wir hoffen, dass es Ihnen dabei hilft, Vertrauen in unsere Dienstleistungen und unsere Verpflichtung zum Schutz Ihrer Daten zu gewinnen. Bei weiteren Fragen oder Anliegen stehen wir Ihnen gerne zur Verfügung.

my-vpa GmbH, März 2023