Technische und organisatorische Maßnahmen

für die App zur Durchführung der elektronischen Führerscheinkontrolle

DriversCheck

DriversCheck GmbH
Lichtstr. 43i | D-50825 Köln
Handelsregisternummer: HRB 95707 | Registergericht: Amtsgericht Köln
Geschäftsführer: Markus Schunk, Marc Vogler
info@drivers-check.de

Revision: 02. Mai 2023

I. Inhaltsverzeichnis

II. Abkürzungsverzeichnis

DSGVO	Datenschutz-Grundverordnung
HTTP	Hypertext Transfer Protocol
RAID	Redundant Array of Independent Disks
REST	Representational State Transfer
SSH	Secure Shell
TLS	Transport Layer Security
TOM	Technische und organisatorische Maßnahmen

1. Systemstruktur

Die Grobarchitektur des elektronischen Führerscheinkontrollsystems lässt sich als klassische, mobile und verteilte Applikation beschreiben. Dabei können hinsichtlich der Systemkomponenten der Service-Anbieter einerseits und die Service-Konsumenten andererseits unterschieden werden.

Der Service-Anbieter wird durch unser Rechenzentrum repräsentiert, welches durch eine Firewall vor Angriffen geschützt ist. Sowohl die serviceorientierte Applikationslogik als auch die persistente Datenhaltung werden durch das Rechenzentrum realisiert. Schließlich werden die durch das Rechenzentrum angebotenen Dienste durch Service-Konsumenten in Anspruch genommen.

Als Service-Konsumenten agieren Smartphone- und Web-Applikationen. Die Kommunikation zwischen Serviceanbieter und -Konsumenten findet über *HTTP*-basierte *RESTful* Webservices statt. Zur sicheren Kommunikation authentifizieren sich Service-Konsumenten mittels *Digest Access Authentication* beim Dienstanbieter. Darüber hinaus wird die Datenübertragung mittels *TLS* verschlüsselt. Wartungs- und Entwicklungsaufgaben werden über eine verschlüsselte *SSH*-Verbindung durchgeführt.

Für den Serverbetrieb wurde die *Hetzner Online GmbH* beauftragt. Das hochmoderne Rechenzentrum mit Zertifizierung gemäß DIN ISO/IEC 27001 befindet sich in Deutschland am Standort Nürnberg.

2. Technische und organisatorische Maßnahmen

Die folgenden technischen und organisatorischen Maßnahmen werden für das elektronische Führerscheinkontrollsystem DriversCheck, in Anlehnung an die DSGVO, verbindlich festgelegt.

2.1 Vertraulichkeit

(gemäß Art. 32 Abs. 1 b) DSGVO)

2.1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

2.1.1.1 Rechenzentrum am Standort Nürnberg

- personenbezogene Zutrittsüberwachung
- elektronisches Schließsystem
- Videokameras zur 24/7 Überwachung
- 24/7- Sicherheitsdienst
- Alarmsicherung
- Zutritt nur nach Vier-Augen-Prinzip
- redundante Speicherung der Zutrittsprotokolle
- Hochsicherheitszaun um den gesamten Datacenterpark

2.1.1.2 Client-Arbeitsplätze am Standort Frechen

- ständig besetzter Empfangsbereich
- Führung eines Besucherbuches
- elektronisches Schließsystem für Bürogebäude
- protokollierte Schlüsselausgabe
- Alarmsicherung
- 24/7- Sicherheitsdienst

2.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- persönliche Zugangsdaten bestehend aus Nutzername und sicherem Passwort
- Rechtekonzept mit separatem Administrationsrecht
- Passwortregeln mit Einhaltungszwang *(Mindestlänge von 8 Zeichen, Groß- und Kleinbuchstaben, Ziffern sowie mind. ein Sonderzeichen)*
- automatische Bildschirmsperre nach 5 Minuten Inaktivität an Client-Arbeitsplätzen
- automatische Session-Terminierung nach 24 Minuten Inaktivität für Web-Applikationen
- Firewall mit regelmäßigen Updates
- Festplattenverschlüsselung für Notebooks
- Wartungs- und Entwicklungsaufgaben über verschlüsselte SSH-Verbindungen

2.1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- differenziertes Berechtigungskonzept mit den Rollen Fah*rer*, *Kontrolleur*, *Fuhrparkmanager* und *Administrator*
- persönliche Zugangsdaten bestehend aus Nutzername und sicherem Passwort
- Rechtevergabe nach dem „Need-to-Know“-Prinzip
- Zugriffsprotokoll
- Trennung von Produktiv- und Testsystem

2.1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- vollständige logische Mandantentrennung
- differenziertes Berechtigungskonzept in Abhängigkeit der Funktion im Unternehmen

2.1.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- Trennung von Produktiv- und Testsystem
- Festplattenverschlüsselung im Rechenzentrum

2.2 Integrität

(gemäß Art. 32 Abs. 1 b) DSGVO)

2.2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Über-tragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Daten werden ausschließlich verschlüsselt übertragen
- Zugriffsschutz bei mobilen Endgeräten via PIN

2.2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- protokollierter Datenzugriff
- protokollierte Datenmodifikation

2.3 Verfügbarkeit und Belastbarkeit

(gemäß Art. 32 Abs. 1 b) DSGVO)

2.3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

2.3.1.1 Stromversorgung Rechenzentrum

- AC: 230V, 16A
- redundante USV-Anlagen
- Batterie-Betrieb: ca. 15 Minuten
- Netzersatzanlage
- Notstromdiesel für autonomen Betrieb
- Stromversorgung erfolgt über Doppelboden

2.3.1.2 Klimatisierung Rechenzentrum

- energieeffiziente direkte freie Kühlung Redundanz N+2
- Kaltgang-Einhausungen
- Unterboden-Klimaanlage
- überdurchschnittlich hoher Doppelboden
- Temperaturüberwachung der Raumluft
- Temperaturüberwachung in Server-/Verteilerschränken

2.3.1.3 Brandschutz Rechenzentrum

- modernes Brandfrüherkennungssystem mit direkter Verbindung zur örtlichen Feuerwehr
- spezielle Tür- und Schließsysteme

2.3.1.4 Sonstiges

- tägliche automatische Sicherung des kompletten Servers
- verschlüsselte Sicherung in separatem Brandabschnitt
- RAID-System mit permanenter Überwachung
- Hot-Plug zum Austausch von defekten RAID-Festplatten ohne Ausfall
- Monatlicher Test der Backup-Widerherstellung
- zügige Wiederherstellbarkeit des laufenden Betriebes ist möglich gemäß *Art. 32 Abs. 1 c) DSGVO*
- Virenschutz, Spamfilter und Firewall

2.4 Verfahren zur Überprüfung, Bewertung und Evaluierung

(gemäß Art. 32 Abs. 1 b); Art. 32 Abs. 1 DSGVO)

2.4.1 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Datenschutzbeauftragter ist bestellt
- Datenschutzschulung von Mitarbeitern
- schriftliche Verpflichtung von Mitarbeitern auf Datengeheimnis
- AV-Vereinbarung mit Hetzner Online GmbH
- Regemäßige Prüfung der TOM-Dokumentation von Hetzner Online GmbH

2.4.2 Datenschutz-Management

Zentrale Verwaltung, Nachvollziehbarkeit und Protokollierung des aktuellen Datenschutzniveaus im Unternehmen.

- interne Datenschutzaudits
- strukturierte Protokollierung von Ergebnissen

2.4.3 Incident-Response-Management

Umfasst den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT/Datenschutz-Bereichen berücksichtigen.

- DDoS-Schutz
- Automatische Systemüberwachung mit Reporting im Falle von erkannten Sicherheitsvorfällen
- Meldewege und Prozesse sind bekannt

2.4.4. Datenschutzfreundliche Voreinstellungen

Einstellungen von Soft- und Hardware vor Nutzung und Herausgabe an Benutzer bzw. Kunden.

- Beachtung bei der App-Entwicklung
- Beachtung bei der Konfiguration von Hard- und Softwaresystemen