LAPID SERVICE GMBH

Datenschutz- und Datensicherheitskonzept

Version 1.35
Stand 12. Februar 2025

Inhaltsübersicht

Historie

Version	Datum	Änderung	Autor
1.0	27.02.08	Erstfassung	Dirk Fox
1.1	06.03.08	Kleine Korrekturen und Ergänzungen	Uwe Latsch
1.2	11.08.08	Aktualisierung der Grafik	Uwe Latsch
1.3	10.06.10	Gliederung nach Anlage zum § 9 BDSG	Dirk Fox
1.4	07.02.11	Neuer Hosting-Subunternehmer	Dirk Fox
1.5	12.11.12	Neuer Hosting-Subunternehmer	Dirk Fox
1.6	21.11.13	Aktualisiertes Notfallkonzept	Dirk Fox
1.7	19.05.14	Tabellarische Übersicht der Angaben für Verfahrensregister in Anhang	Dirk Fox
1.8	28.07.14	Anpassung Grafik, kleine Präzisierungen	Dirk Fox
1.9	29.09.14	Korrektur Maßnahmenzuordnung	Dirk Fox
1.10	08.05.15	Ergänzungen (Zugangskontrolle)	Dirk Fox
1.11	20.11.15	Ergänzung (regelmäßige Audits)	Dirk Fox
1.12	18.07.16	Ergänzung (Driver App)	Dirk Fox
1.13	02.12.16	Kleine Korrektur	Dirk Fox
1.14	20.02.17	Aufnahme Subunternehmer DEKRA	Dirk Fox
1.15	03.08.17	Anpassungen an DSGVO	Dirk Fox
1.16	04.10.17	Aufnahme UVV-Fahrerunterweisung (Viwis, DEKRA Media)	Dirk Fox
1.17	20.10.17	Vereinheitlichung Löschfristen, Sperrzeiten	Dirk Fox
1.18	13.11.17	Ergänzung Löschfrist	Dirk Fox
1.19	11.12.17	Ergänzung Löschungen	Dirk Fox
1.20	26.03.18	Ergänzung Zugang Fahrerportal	Dirk Fox
1.21	27.04.18	Ergänzung Sicherheitsziel Robustheit	Dirk Fox
1.22	27.04.18	Entfernung der letzten BDSG-Verweise	Kai Rosenthal
1.23	06.11.18	Ergänzungen Schutzmaßnahmen	Dirk Fox
1.24	31.08.19	Ergänzung Abschnitt Pseudonymisierung	Dirk Fox
1.25	11.10.19	Begriffsänderung Datengeheimnis > Vertraulichkeit	Kai Rosenthal
1.26	06.02.20	Design, Anpassung Verarbeitungsbeschreibung	Kai Rosenthal
1.27	03.08.20	Aufnahme API	Kai Rosenthal
1.28	09.11.21	Ergänzung: weitere Unterweisungen	Dirk Fox
1.29	28.01.22	Kleine editorische Änderungen	Kai Rosenthal
1.30	18.08.22	Neuer Hosting-Subunternehmer, Löschkonzept	Kai Rosenthal, Dirk Fox
1.31	23.11.22	Kleine editorische Änderungen	Kai Rosenthal
1.32	12.08.23	Hinzufügung KI, kleine editorische Änderungen	Kai Rosenthal
1.33	14.12.23	Anpassung Schlüssellängen, Entfernung SMS-Kommunikation / Prüfstationen	Kai Rosenthal
1.34	22.03.24	Beschreibung Login Portal / DriverApp	Kai Rosenthal
1.35	12.02.25	Hinzufügen Fahrzeugverwaltung	Kai Rosenthal

Abkürzungen

AES	Advanced Encryption Standard (Verschlüsselungs-Standard)
API	Application Programming Interface (Programmier-Schnittstelle)
ArbSchG	Arbeitsschutzgesetz
BDSG	Bundesdatenschutzgesetz
DMZ	Demilitarisierte Zone
DSGVO	Datenschutz-Grundverordnung der EU
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
IaaS	Infrastructure as a Service
ID	Identification Number (hier: Nummer des LapID Prüfsiegels)
IP	Internet Protocol
KI	Künstliche Intelligenz
KMS	Key Managment System
ISO	International Organization for Standardization
QR-Code	Quick Response Code
RAID	Redundant Array of Independent Disks
RSA	Rivest Shamir Adleman (asym. Verschlüsselungsverfahren)
SMS	Short Message Service
SSL	Secure Socket Layer Protocol
SSO	Single Sign On
StVG	Straßenverkehrsgesetz
TLS	Transport Layer Security Protocol
UAN	Unterauftragnehmer
UVV	Unfallverhütungsvorschriften
VPN	Virtual Private Network
WPA2	Wi-Fi Protected Access 2
ZIP	Daten-Kompressionsformat

1 Beschreibung der Verarbeitung

Die LapID Service GmbH (kurz: LapID) bietet Unternehmen Fuhrpark- und Compliance-Dienstleistungen an, mit deren Hilfe das Unternehmen seinen gesetzlichen Verpflichtungen zur Führerscheinkontrolle und Mitarbeiterunterweisung nachkommen kann.
Zur Identifikation der zu überprüfenden Personen (Mitarbeiter, Fahrer, zu Unterweisende) sowie zur Dokumentation der durchgeführten Überprüfungen und Unterweisungen ist hierbei die Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten der Personen erforderlich.

Das sind im Einzelnen je Unternehmen:

- Der Name der **betroffenen Person** (optional das Geburtsdatum oder die Personalnummer zur eindeutigen Identifikation) und die **E-Mail-Adresse resp. die Mobilfunknummer**
- **Name und E-Mail-Adresse** eines zugeordneten **Empfängers für Überfälligkeitsbenachrichtigungen**

Darüber hinaus werden die im Folgenden erläuterten weiteren Daten (abhängig von der durchzuführenden Überprüfung) erhoben und verarbeitet.

1.1 Automatische Führerscheinkontrollen

LapID bietet Unternehmen mit Fuhrparks oder Dienstwagen eine automatische Führerscheinkontrolle, mit der das Unternehmen dem gesetzlichen Erfordernis[1] einer regelmäßigen Kontrolle der Fahrerlaubnis aller Fahrer genügen kann. Die automatisierte Durchführung der Kontrollen erfolgt i.d.R. zweimal jährlich und wird zu Nachweiszwecken dokumentiert und archiviert.

Die Kontrolle der Fahrerlaubnis erfolgt durch Übermittlung einer an Prüfstationen elektronisch auslesbaren ID (Prüfsiegel), die auf den Führerschein aufgeklebt wird und nicht unbeschädigt wieder abgelöst werden kann. Alternativ kann der Führerschein auch zur Überprüfung durch LapID fotografiert werden (Driver App); in diesem Fall erfolgt die Prüfung durch Inaugenscheinnahme der Führerscheinfotos. Die Durchführung der visuellen Prüfung und das Prüfergebnis werden mit Zeitstempel dokumentiert.

Zur Dokumentation der durchgeführten Kontrollen ist die Erhebung, Speicherung und Verarbeitung von weiteren personenbezogenen Daten der Fahrer erforderlich, die von der automatischen Führerscheinkontrolle erfasst werden sollen.

[1] In Deutschland: § 21 Abs. 2 StVG in Verbindung mit der allgemeinen Sorgfaltspflicht des Unternehmers. In der Literatur wird bei Fuhrparks und Dienstwagen von der Pflicht des Fahrzeughalters zur mindestens jährlichen Überprüfung der Fahrerlaubnis ausgegangen.

Das sind im Einzelnen:

- **Angaben zur Fahrerlaubnis** der Fahrer (Nummer, ausstellende Behörde, Fahrzeugklassen, Ausstellungsdatum, Ablaufdatum; ID des LapID Prüfsiegels)
- **Durchgeführte Überprüfungen** (mit Zeitstempel) und **Erinnerungen/Alarme** (SMS/E-Mail)
- Führerschein-Fotos (temporär, bei Verwendung der optionalen Driver App)

Die Fahrer können ferner über ein Fahrer-Portal oder die App die Termine der nächsten Unterweisung einsehen.

1.2 Unterweisungen

Darüber hinaus bietet das LapID System die Möglichkeit, regelmäßige Fahrerunterweisungen durchzuführen, in Deutschland z. B. gemäß der Unfallverhütungsvorschrift (UVV) der Berufsgenossenschaften (wie Nutzung von Dienstwagen, Ladungssicherung oder Unterweisung Flurförderfahrzeuge), nach der Gefahrstoff- und Biostoffverordnung (GefStoffV/BioStoffV) sowie weitere Unterweisungen nach Arbeitsschutzgesetz (ArbSchG) und Arbeitsstättenverordnung (wie Brandschutz, Bildschirmarbeit, Home-Office, Corona-Schutz), oder zu IT-Sicherheit und Datenschutz (DSGVO).

Zu diesem Zweck werden zusätzlich die folgenden personenbezogenen Daten verarbeitet:

- **Durchgeführte Unterweisungen** (Zeitpunkt, Ergebnis)
- Die in diesem Zusammenhang versandten **Erinnerungen und Alarme** (SMS/E-Mail)
- Temporär bis zum Abschluss der jeweiligen Unterweisung der Zwischenstand (im Falle einer Unterbrechung der Unterweisung)

Das Herunterladen der Zertifikate zur Bestätigung der durchgeführten Unterweisungen erfolgt durch die zu unterweisenden Personen über ein Fahrer-Portal, über das auch die Termine der nächsten Unterweisung eingesehen werden können.

1.3 Fahrzeugverwaltung

Schließlich bietet das LapID System die Möglichkeit, fuhrparkbezogene Verwaltungsprozesse (Abfrage km-Stände, HU-Nachweise, Reifenwechsel, etc.) durch einen Prozess abbilden zu können.
Hierbei richtet der Fuhrparkverantwortliche einen Prozess ein, indem er eine Abfrage (Eingabe eines Wertes, Hochladen einer Datei) definiert und eine Frist (oder eine Wiederholfrequenz) setzt. Das LapID System wird dann Aufforderungen an den Fahrer/Mitarbeiter senden, und bei Nichterfüllung Eskalationen einleiten.
Zu diesem Zweck werden zusätzlich die folgenden personenbezogenen Daten verarbeitet:

- **Durchgeführte Aufgaben** (Zeitpunkt, Ergebnis)
- Die in diesem Zusammenhang versandten **Erinnerungen und Alarme** (SMS/E-Mail)
- Ggf. (sofern sie personenbezogene Daten enthalten) die für Aufgaben erhobenen Dokumente und Eingaben

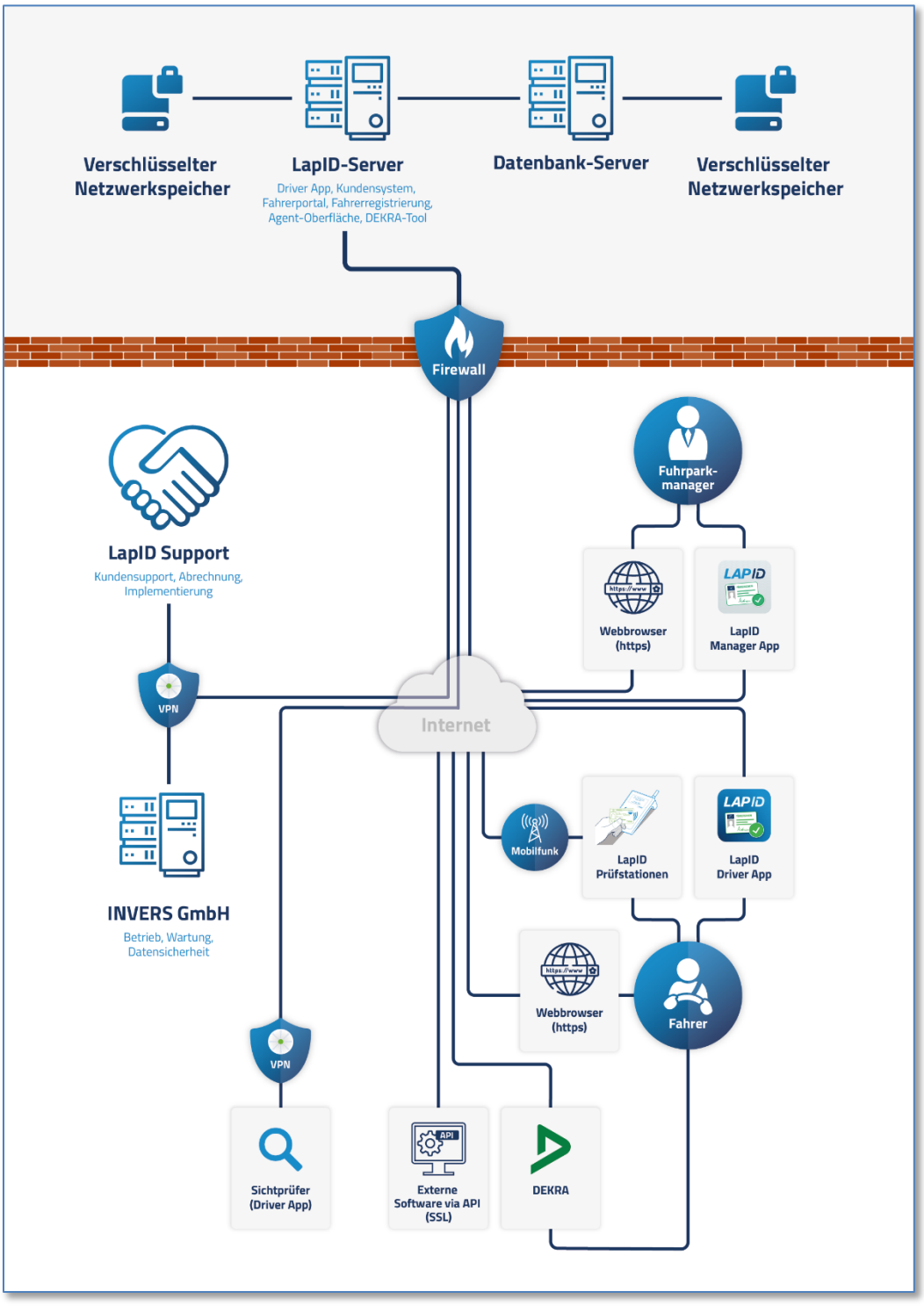

Abbildung 1: Schemabild des LapID Systems

1.4 Technische Umsetzung

Die LapID Datenbank und der LapID Anwendungsserver werden im Rechenzentrum der Firma Telekom Deutschland GmbH (Bonn) als virtuelle Maschine mit verschlüsselten Festplatten betrieben. Das Backup erfolgt über eine VPN-Verbindung mit einem System der Firma INVERS.

Optional kann die Erhebung der Fahrer-Stammdaten auf Kundenwunsch durch die DEKRA SE erfolgen. Hierbei werden die Daten durch Mitarbeiter der DEKRA erhoben, in eine Webschnittstelle der LapID eingegeben, und dem Fuhrparkbetreiber dann als verschlüsselter PDF-Download zur Verfügung gestellt, so dass dieser die Daten in das LapID System eintragen bzw. im LapID System ändern kann.

Die Sichtprüfung der Führerscheine von Nutzern der optionalen Driver App wird vom Dienstleister TMA Telesmart GmbH (Hagen) über eine Web-Schnittstelle unterstützt. Hierbei kommen auch KI-gestützte Verfahren zum Einsatz;

- Die KI wird von LapID selbst betrieben, sie ist Teil der Driver App
- Die KI wird eingesetzt, um, bevor das Foto einem Menschen vorgelegt wird, bereits herauszufiltern, was kein Führerschein ist (Personalausweise, Bankkarten usw.).
- Ferner gibt die KI eine erste Einschätzung, ob Sicherheitsmerkmale vorhanden sind (trifft aber keine Entscheidung). Diese Information wird zusammen mit dem Foto des Führerscheins an die LapID Server geschickt, und nur dorthin.
- Sollte es sich um einen Führerschein handeln, liegen alle Entscheidungen bei einem Menschen.
- Die KI wird niemals mit personenbezogenen Daten unserer Kunden trainiert
- Es erfolgt kein weiterer Datentransfer und kein Profiling

Im Rahmen der Fahrzeugverwaltung erfolgt die Eingabe der angefragten Werte / das Hochladen der geforderten Dokumente durch einen in der Aufforderung versandten Link. Die im Rahmen der Fahrzeugverwaltung hochgeladenen Dokumente liegen verschlüsselt in einem Objektspeicher des Hostings bei der Telekom Deutschland.

Auf entsprechende Weisung des Auftraggebers kann der Zugriff auf die von LapID im Auftrag verarbeiteten Daten für die Nutzung durch ein Fuhrparkmanagementsystem über eine API freigeschaltet werden.

Über diese Schnittstelle sind die folgenden Zugriffe auf das LapID System möglich:

- Anlegen, Lesen, Ändern und Löschen einer Person
- Anlegen, Lesen, Ändern und Löschen eines Empfängers für Überfälligkeitsbenachrichtigungen
- Optional: Anlegen, Lesen, Ändern und Löschen einer durchgeführten manuellen Führerscheinkontrolle
- Optional: Anlegen, Lesen, Ändern und Löschen des Termins einer Unterweisung

2 Organisatorische und technische Schutzmaßnahmen

Das Dienstleistungsangebot der Firma LapID unterliegt den Bestimmungen der Datenschutz-Grundverordnung (DSGVO). Das vorliegende Datenschutz- und Datensicherheitskonzept beschreibt die zum Schutz der von LapID verarbeiteten personenbezogenen Daten umgesetzten Maßnahmen.

Von LapID wurden die im Folgenden dargestellten organisatorischen und technischen Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten vor unbefugter Kenntnisnahme (Vertraulichkeit), Verfälschung (Integrität) und Verlust (Verfügbarkeit) sowie Belastbarkeit gemäß Art. 32 DSGVO ergriffen. Diese Maßnahmen werden jährlich einem Datenschutz-Audit unterzogen.

Schutzziel (DSGVO)	Zutrittskontrolle	Zugangskontrolle	Zugriffskontrolle	Weitergabekontrolle	Eingabekontrolle	Auftragskontrolle	Verfügbarkeit, Notfallkonzept	Getrennte Verarbeitung
Vertraulichkeit	X	X	X	X		X		X
Integrität				X	X	X		X
Verfügbarkeit						X	X	
Belastbarkeit							X	

2.1 Zutrittskontrolle

Der Gebäudezugang zur Firma LapID ist nur mit Schlüssel und Zugangskarte möglich und durch eine Alarmanlage gesichert. Der Zutritt zu den Räumen, in denen das Backup-System betrieben wird und die Backup-Bänder im Tresor gelagert werden, ist durch eine Schlüsselregelung auf ausgewählte und auf Vertraulichkeit verpflichtete Personen beschränkt. Im Falle der Beendigung des Anstellungsverhältnisses bei LapID werden die Zutrittsberechtigungen sofort entzogen.

Putzpersonal und andere Externe können den Serverraum nur in Begleitung und unter Aufsicht berechtigter Personen betreten. Der Zutritt zum Rechenzentrum des Hosting-Dienstleisters (Telekom Deutschland GmbH) ist durch technische und organisatorische Maßnahmen geschützt; der Dienstleister ist nach ISO 27001 zertifiziert.

2.2 Zugangskontrolle

Auf die Daten der LapID Datenbank wird über eine Web-Administrationsschnittstelle (Frontend) zugegriffen. Durch Mindestanforderungen an die Authentifizierung gemäß dem jeweils aktuellen Stand der Technik werden unbefugte Zugriffe verhindert. Es werden ausschließlich personalisierte Accounts vergeben. Die Passwörter für die Accounts des Auftraggebers haben eine erzwungene Mindestlänge von 8 Zeichen und müssen mindestens jeweils ein Zeichen aus den Bereichen Großbuchstaben/Kleinbuchstaben/Sonderzeichen/Zahl enthalten. Für die Wartungsaccounts des Auftragnehmers gelten eine Passwort-Mindestlänge von 10 Zeichen und dieselben Komplexitätsanforderungen. Nach einer Inaktivität von 15 Minuten (Auftraggeber) bzw. 30 Minuten (Wartungsaccount) wird die Session automatisch beendet. Nach drei Login-Fehlversuchen wird der Account gesperrt.

Die Mitarbeiter des Auftraggebers erhalten zur Durchführung einer Kontrolle oder Unterweisung einen Zugang zum LapID Portal oder der App. Die Authentifizierung erfolgt durch Nutzername und Passwort oder über einen Deep Link (z.B. QR Code) in der Aufforderungs-E-Mail an den Mitarbeiter. Ein Single Sign On (SSO) via Microsoft Entra ID oder eine ActiveDirectory-Anbindung ist möglich.

Die gehosteten LapID Server werden durch eine Firewall und regelmäßige Software-Updates vor Schwachstellen und unberechtigten Zugriffen geschützt. Die virtuellen Maschinen von LapID werden mit verschlüsselten Festplatten betrieben. Hierbei wird der Verschlüsselungsalgorithmus AES-256 verwendet. Die Schlüssel werden von einem KMS der Firma Telekom Deutschland GmbH verwaltet. Die LapID Service GmbH verwendet eigene Keys für die Verschlüsslung der Daten (vgl. Prinzip "Bring Your Own Key"). Durch die Speicherung in einem Hardware-Sicherheitsmodul ist sichergestellt, dass Dritte nicht an die Keys gelangen können.

Sofern Wartungszugriffe von Rechnern der LapID über einen WLAN-Zugang erfolgen, sind diese mit einer WPA2-Verschlüsselung und einem WPA Enterprise-Zugang über eine RADIUS-Authentifizierung gesichert. Im LapID Netzwerk sind ausschließlich firmeneigene Systeme von LapID zugelassen, die durchgängig mit einem aktuellen Virenscanner ausgestattet sind. Es werden regelmäßig Software-Updates auf den Systemen eingespielt. Das LapID Netz ist außerdem über eine restriktiv konfigurierte Firewall vor unberechtigten Zugriffen geschützt.

Der Dienstleister INVERS GmbH hat über eine verschlüsselte VPN-Verbindung Zugang zu den Systemen der LapID Service GmbH.

Alle für den Betrieb der LapID Systeme Verantwortlichen wurden auf Vertraulichkeit verpflichtet.

2.3 Zugriffskontrolle

Für den LapID Server liegt ein dokumentiertes Berechtigungskonzept vor, das die Zahl der Zugriffsberechtigten auf das Erforderliche beschränkt.

Es werden drei (bzw. vier) Gruppen von Berechtigten unterschieden: Die Fahrzeughalter (Fuhrparkmanager) und die Support-Berechtigten; bei Nutzung der Driver App gibt es zusätzlich die Gruppe der Prüfer. Ferner erhalten die Mitarbeiter des Auftraggebers eine Zugriffsmöglichkeit zur Durchführung der eigenen Führerscheinkontrolle (bei Nutzung der Driver App) oder der Unterweisungen.
Die jeweils eingeräumten Zugriffsrechte sind auf das Erforderliche beschränkt („Need-to-Know"-Prinzip):

- Die Fuhrparkmanager haben Zugriff auf den oder die Fuhrparks ihres Unternehmens. Sie besitzen Schreibberechtigung auf die Stammdaten ihrer Fahrzeugnutzer und Leseberechtigung auf alle ihre Fahrzeugnutzer betreffenden Ereignisse (durchgeführte Kontrollen mit Zeitstempel, verschickte Erinnerungen und Alarme). Sie können neue Fahrzeugnutzer und deren Stammdaten aufnehmen und Fahrzeugnutzer löschen. Über den initial vergebenen Login-Account des Fuhrparkmanagers können von diesem weitere Fuhrparkmanager-Accounts angefordert werden.
- Support-Berechtigung erhalten ausschließlich ausgewählte und schriftlich auf Vertraulichkeit verpflichtete Mitarbeiter der LapID. Diese werden außerdem regelmäßig im Datenschutz geschult. Sie können über die Web-Administrationsschnittstelle Fuhrparkmanager anlegen und zur Erledigung von Support-Anfragen auf alle gespeicherten Daten eines Fuhrparks zugreifen. Über eine nur ihnen zugängliche Schnittstelle können sie bei der Neueinrichtung eines Fuhrparks vorbereitete Stammdatensätze der Fahrzeugnutzer in die Datenbank importieren.
- Sichtprüfer erhalten (bei Verwendung der optionalen Driver App) im Rahmen der Führerscheinprüfung lesenden Zugriff auf die temporär gespeicherten Führerscheinfotos.
- Die Mitarbeiter des Auftraggebers erhalten optional Zugriff auf das LAPID-Portal und eine mobile App, in welchen sie die anstehenden Termine einsehen können. Über das LAPID-Portal können die Unterweisungen durchgeführt werden (bei Nutzung der Unterweisungen). Bei Nutzung der optionalen DriverApp erhalten die Mitarbeiter in dieser die Möglichkeit, die Kontrolle der Führerscheine vorzunehmen.

2.4 Weitergabekontrolle

Der LapID Webserver, auf den der Fuhrparkmanager zugreift, wird in einer durch eine Firewall geschützten DMZ bei der Firma Telekom Deutschland GmbH (Bonn) betrieben.

Bei der elektronischen Übermittlung personenbezogener Daten zum und vom LapID Server sind die Daten durch Verschlüsselung vor unbefugter Kenntnisnahme und Veränderung geschützt. So erfolgt die Übertragung der Daten bei allen Online-Zugriffen auf das LapID System über das SSL-(TLS-)Protokoll.

Für den Import vorbereiteter Stammdatensätze bei der Neueinrichtung einer Fuhrpark-Datenbank durch die Support-Mitarbeiter der LapID in die LapID Datenbank erfolgt die Übertragung dieser initialen Datensätze so, dass ein Zugriff Unberechtigter ausgeschlossen werden kann. Dabei können – nach Absprache – die folgenden Schutzmaßnahmen zum Einsatz kommen:

- ein verschlüsseltes ZIP-File,
- die Ablage auf einem Passwort-geschützten FTP-Server von LapID oder
- die Zusendung als verschlüsselter E-Mail-Anhang.

Die Zwischenspeicherung der Daten durch Mitarbeiter von LapID erfolgt auf einem für diesen Zweck eingerichteten Laufwerk auf dem LapID Server, auf das ausschließlich die Support-Mitarbeiter der LapID Zugriffsrechte besitzen.

Nach dem Import der Datensätze über eine VPN-Verbindung in die LapID Datenbank werden die zwischengespeicherten Daten wirksam gelöscht.

Die Übertragung der Prüfdaten (ID des Prüfsiegels, Zeitstempel) von einer LapID Prüfstation zum LapID Server erfolgt als AES-verschlüsselter Datensatz (128 bit Schlüssellänge) über GPRS. Bei Verwendung der (optionalen) Driver App erfolgt die Übermittlung der Führerschein-Fotos ebenfalls AES-verschlüsselt (zufälliger Session-Key, 256 bit Schlüssellänge, verschlüsselt mit dem öffentlichen, 4096 bit langen RSA-Key des Servers).

Daten des LapID Systems werden nicht an Dritte übermittelt.

2.5 Eingabekontrolle

Die Vergabe von Zugriffsberechtigungen und alle Berechtigungsänderungen werden in der Datenbank revisionssicher dokumentiert. Ebenfalls dokumentiert werden alle Login- und Logout-Vorgänge sowie alle Änderungen an Stammdaten von Fahrzeugnutzern.

Die Protokolleinträge umfassen die User-ID, die IP-Adresse von der der Zugriff erfolgte, einen Zeitstempel und die Angabe der durchgeführten Aktivität. Die Logdaten können vom jeweiligen Nutzer nicht modifiziert werden.

2.6 Auftragskontrolle

Die Infrastruktur für den LapID Server, die LapID Datenbank und den LapID Webserver wird im Auftrag von LapID bei der Firma Telekom Deutschland GmbH bereitgestellt (IaaS). Zur Erfüllung der Anforderungen des Art. 28 DSGVO wurde dazu zwischen LapID und der Telekom Deutschland GmbH ein Vertrag zur Auftragsverarbeitung geschlossen. Die Rechenzentren sind nach ISO 27001 zertifiziert. Die Daten des Datenbank- und Anwendungs-Servers werden verschlüsselt gespeichert. Die Mitarbeiter der Telekom haben keinen Zugriff auf die Datenbank.

Die Administration der Server erfolgt über eine verschlüsselte VPN-Verbindung, welche durch die Firma INVERS GmbH (Siegen) bereitgestellt wird. Die Mitarbeiter von INVERS haben keinen Zugriff auf die virtuellen Maschinen bei der Telekom.

Zur Erfüllung der Anforderungen des Art. 28 DSGVO wurde dazu zwischen LapID und der INVERS GmbH ein Vertrag zur Auftragsverarbeitung geschlossen. In diesem Vertrag wurden LapID insbesondere Zutritts- und Kontrollrechte zur Überprüfung des datenschutzkonformen Betriebs der Systeme durch INVERS eingeräumt.

Optional kann die Ersterhebung der Fahrer-Stammdaten durch Mitarbeiter der DEKRA (über eine Web-Oberfläche direkt im LapID System) erfolgen. Dazu wurde zwischen LapID und der DEKRA SE ein Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO geschlossen.

2.7 Verfügbarkeitskontrolle und Notfallkonzept

Alle im LapID System verarbeiteten personenbezogenen Daten werden wirksam vor Zerstörung und Datenverlust geschützt.

Die LapID Prüfstationen speichern bei Ausfall einer Kommunikationsverbindung bis zu 200 Prüfnachrichten; damit kann selbst bei (seltenen) Lastspitzen erfahrungsgemäß ein Ausfallzeitraum von mindestens 48 Stunden ausgeglichen werden.

Als Schutz gegen Ausfall werden die Server bei der Telekom in Magdeburg und Biere als Cluster innerhalb von drei physikalisch getrennte Verfügbarkeitszonen betrieben. Die Telekom setzt in Magdeburg und Biere auf die Twin-Core-Technologie, es handelt sich hierbei um zwei baugleiche Anlagen, die durch ein Hochgeschwindigkeitsnetzwerk miteinander verbunden.

Die betriebenen Dienste führen eine automatisierte Auswahl des primären Servers durch. Bei Ausfall des primären Servers oder einer kompletten Verfügbarkeitszone wird ein sekundärer Knoten zum neunen primären Knoten bestimmt. Sollten zwei Verfügbarkeitszonen ausfallen, ist ein Betrieb innerhalb von einer Verfügbarkeitszone kurzfristig möglich.

Im Normalbetrieb werden von allen eingehenden Daten identische Kopien auf unterschiedlichen Speicherknoten abgelegt. Zusätzlich wird ein tägliches Vollbackup der Datenbank erzeugt, welches in ein weiteres Rechenzentrum der Telekom in die Niederlande übertragen wird. Sollte es zu einem Ausfall aller drei

Verfügbarkeitszonen in Deutschland kommen, wäre auch ein Betrieb der LapID Anwendung in Amsterdam möglich. Darüber hinaus wird die Datenbank täglich nach Siegen gespiegelt.

Der von Telekom gehostete LapID Server protokolliert über den Zeitraum von einer Woche alle eingehenden Prüfnachrichten in einer Logdatei. Bei Ausfall der Datenbank können daher alle seit dem letzten Backup eingegangenen Prüfnachrichten rekonstruiert und erneut eingespielt werden.

Alle über die Web-Schnittstelle vorgenommenen Eingaben im System werden ebenfalls über den Zeitraum von einer Woche protokolliert, sodass die vorgenommenen Änderungen auch im Falle eines Defekts der Datenbank ohne Datenverlust rekonstruierbar sind.

Die (verschlüsselten) Backups in Amsterdam werden in einem verschlüsselten Objektspeicher aufbewahrt. Dabei werden die täglichen Backups sieben Tage, die monatlichen Backups ein Jahr und die Jahresbackups zehn Jahre aufbewahrt. Die Rückspielbarkeit der Tages- und Monatsbackups wird regelmäßig (mindestens einmal jährlich) überprüft und dokumentiert.

2.8 Getrennte Verarbeitung

Auf dem LapID Server werden weder andere Anwendungen betrieben, noch greifen andere Anwendungen als das LapID System auf die LapID Datenbank zu.

Alle im LapID System eingerichteten Zugriffsaccounts (einschließlich der Service-Accounts) wurden mit strikter Mandantentrennung realisiert. So erfolgt der Zugriff jeweils ausschließlich auf einen Fuhrpark bezogen.

Bei Verwendung der (optionalen) Driver App erfolgt die Prüfung der Führerscheinfotos ohne Zugriff auf weitergehende Daten (bspw. Halterinformationen etc.).

Weiterentwicklung und Tests neuer Versionen des LapID Systems werden ausschließlich auf vom Produktivsystem getrennten Entwicklungs- und Testsystemen durchgeführt.

3 Pseudonymisierung

Die LapID Führerscheinprüfung arbeitet weitestmöglich mit pseudonymen Daten. So werden von den LapID Prüfstationen lediglich die Prüfsiegel-IDs übermittelt. Auch die Unterweisungen verwenden lediglich pseudonyme Personen-IDs. Die Zuordnung zu einer Person erfolgt nur in der zentralen Datenbank, die vom Fuhrparkmanager verwaltet wird. Hier können statt Klarnamen ebenfalls Pseudonyme zur Personenidentifikation eingetragen werden. Lediglich bei einer Führerscheinprüfung über die Driver App ist eine Identifikation des Fahrers erforderlich.

4 Auskunftsersuchen

Richtet ein Fahrzeugnutzer ein datenschutzrechtliches Auskunftsersuchen an den Fuhrparkmanager (Fahrzeughalter), kann dieser über einen Menüeintrag auf eine übersichtliche und ausdruckbare Gesamtansicht aller über diesen Fahrzeugnutzer in der LapID Datenbank gespeicherten Daten zugreifen und diese für den Betroffenen ausdrucken.

Diese Auflistung umfasst neben den Stammdaten alle in der Datenbank gespeicherten Kontaktvorgänge (Erinnerungs-E-Mails/-SMS) sowie die Zeitstempel und Ergebnisse aller innerhalb der vergangenen sechs Jahre durchgeführten Überprüfungen.

Nutzt der Kunde die (optionalen) Unterweisungen, kommen die im Zusammenhang mit der letzten Unterweisung gespeicherten Daten (Datum, Ergebnis, Erinnerungs-E-Mails/-SMS) hinzu.

Anhang A: Löschkonzept

Das Löschkonzept des LapID Systems betrifft vier verschiedene Datenkategorien.

1. Führerscheinfotos

Bei der Nutzung der (optionalen) Driver App werden Führerschein-Fotos erstellt und an den LapID Server übermittelt.

- *Datenkategorie*:
  Fotos der Führerscheine der Fahrer
- *Art der Löschung*:
  Automatisch
- *Löschmethode*:
  Löschung in der Datenbank
- *Beginn der Löschfrist*:
  Zeitpunkt der Aufnahme der Fotos durch die Driver-App
- *Löschfrist*:
  Unmittelbar nach Abschluss der Sichtprüfung und spätestens nach zwei Werktagen.
- *Begründung der Löschfrist*:
  Die Fotos der Führerscheine enthalten personenbezogene Daten mit besonderem Schutzbedarf gem. Art. 9 (1) DSGVO (biometrische Daten, ggf. medizinische Daten). Nach Erfüllung des Verarbeitungszwecks, also nach Abschluss der Sichtprüfung müssen die Daten unverzüglich gelöscht werden.

2. Durchgeführte Kontrollen / Unterweisungen / Aufgaben

Jeder Kontrollvorgang wird im LapID System zusammen mit allen damit in Zusammenhang stehenden Vorgängen gespeichert (durchgeführte Führerscheinkontrollen, durchgeführte Unterweisungen, hierzu versandte Benachrichtigungen).

- *Datenkategorien:*
  - **Daten durchgeführter Kontrollen** (Zeitpunkt, welche Methode, Stichtag)
  - **Daten durchgeführter Unterweisungen** (Zeitpunkt, Stichtag)
  - **Daten durchgeführter Aufgaben** (Zeitpunkt, Stichtag, erhobene Werte)
  - Sich hierauf beziehende **Aufforderungen und Eskalationen** (Versandzeitpunkt, Empfänger, Anzahl Aufforderungen/Eskalationen, Stichtag)
- *Art der Löschung:*
  Automatisch
- *Löschmethode:*
  Löschung in der Datenbank
- *Beginn der Löschfrist:*
  Termin einer Kontrolle oder Unterweisung
- *Löschfrist:*
  Sechs Jahre (taggenau)
- *Begründung der Löschfrist:*
  Drei Jahre für die Nachweisbarkeit gem. § 21 StVG, insbesondere Abs. 3 zuzüglich der Verjährungsfrist von drei Jahren (§ 195 BGB), innerhalb der ein Geschädigter den Ersatz eines Schadens in Anspruch nehmen kann (vgl. auch HWK Ulm).

3. Personendaten

Löscht ein Fuhrparkmanager die Stammdaten einer Person aus dem LapID System, werden alle zu dieser Person gehörigen personenbezogenen Daten zunächst gesperrt (um irrtümliche Löschungen korrigieren zu können) und nach spätestens 12 Monaten wirksam und vollständig aus der LapID Datenbank gelöscht. Bei Unterweisungen werden auch die beim Dienstleister unter Pseudonym gespeicherten Daten der durchgeführten Unterweisungen gelöscht.

- *Datenkategorien:*
  - **Stammdaten der Person** (Name, Kommunikationsdaten, Führerscheindaten)
  - **Daten durchgeführter Kontrollen** (Zeitpunkt, Methode, Stichtag)
  - **Daten durchgeführter Unterweisungen** (Zeitpunkt, Stichtag)
  - **Aufforderungen und Eskalationen** (Versandzeitpunkt, Empfänger, Anzahl Aufforderungen/Eskalationen, Stichtag)
- *Art der Löschung:*
  Automatisch
- *Löschmethode:*
  Löschung in der Datenbank
- *Beginn der Löschfrist:*
  Löschung durch den Fuhrparkmanager
- *Löschfrist:*
  Ein Jahr (taggenau)
- *Begründung der Löschfrist:*
  Da Führerscheinkontrollen meist alle 6 Monate erfolgen, kann es vorkommen, dass eine irrtümliche Löschung erst nach mehr als sechs Monaten auffällt.

4. Hochgeladene Dokumente

Die im Rahmen der Fahrzeugverwaltung übermittelten Dokumente können vom Systembenutzer gespeichert werden, dieses Speichern muss aktiv ausgewählt werden. Die so gespeicherten Dokumente werden 10 Jahre aufbewahrt, und dann automatisch gelöscht.

- *Datenkategorien:*
  - Durch durchgeführte Aufgaben **hochgeladene Dokumente**
- *Art der Löschung:*
  Automatisch
- *Löschmethode:*
  Löschung im Objektspeicher
- *Beginn der Löschfrist:*
  Datum der Speicherung
- *Löschfrist:*
  Zehn Jahre (taggenau)
- *Begründung der Löschfrist:*
  Die gesetzliche Aufbewahrungsfrist für verschiedene Dokumente im Geschäftswesen beträgt zwischen 2 und 10 Jahren. Zur Vereinfachung wurde eine einheitliche Löschfrist gewählt, die aber alle Fälle abdecken muss, daher musste der Wert von 10 Jahren gewählt werden.

5. Gesamte Vertragsdaten

Bei Beendigung des Vertragsverhältnisses zwischen dem Auftraggeber und LapID sind, sofern vertraglich nicht anders geregelt oder durch eine Weisung anders angeordnet, alle personenbezogenen Daten von den Systemen der LapID Service GmbH und denen etwaiger Unterauftragnehmer vollständig zu löschen. Sollten bereits gelöschte Daten aus einem gekündigten Vertragsverhältnis über einen Backup-Vorgang wieder eingespielt werden, werden diese unverzüglich (erneut) gelöscht.

- *Datenkategorien*:
  - **Stammdaten der Systemnutzer**
  - **Stammdaten der Eskalationsempfänger**
  - **Stammdaten der Personen (Fahrer und zu Unterweisende)**
  - **Daten durchgeführter Kontrollen und Unterweisungen**
- *Art der Löschung:*
  Manuell durch Mitarbeiter von LapID, durch den etablierten Prozess bei Kündigung eines Kunden.
- *Löschmethode:*
  Löschung in der Datenbank
- *Beginn der Löschfrist:*
  Datum des Vertragsendes
- *Löschfrist:*
  Unverzüglich nach Vertragsende, sofern keine anderslautende Weisung vorliegt.
- *Begründung der Löschfrist:*
  Mit Vertragsende endet die Auftragsverarbeitung und damit erlischt die Berechtigung von LapID, personenbezogene Daten des Auftraggebers zu verarbeiten. Da die Daten der Personen keinen Aufbewahrungsfristen unterliegen, werden sie bei Vertragsende unverzüglich gelöscht.

Anhang B: Angaben für das Verzeichnis der Verarbeitungstätigkeiten des Auftraggebers nach Art. 30 DSGVO

Bezeichnung der Verarbeitung:	LapID Führerscheinkontrolle und/oder Durchführung und Dokumentation von Unterweisungen und/oder Fahrzeugverwaltung
Verantwortliche Stelle:	*<Bezeichnung inkl. Rechtsform sowie vollständige Anschrift des Auftraggebers>*
Leiter der Verantwortlichen Stelle:	*<Name Geschäftsführer, Vorstand oder Inhaber des Auftraggebers>*
Leiter der Datenverarbeitung:	*<Name des Leiters der Datenverarbeitung beim Auftraggeber>*
Zweckbestimmung:	Optional: Regelmäßige Überprüfung der Fahrerlaubnis aller Fahrer von Fahrzeugen im Eigentum der Verantwortlichen Stelle. Optional: Durchführung und Dokumentation von regelmäßigen Unterweisungen (in Deutschland nach UVV, ArbSchG, GefStoffV/BioStoffV oder DSGVO). Optional: Durchführung fuhrparkbezogener Verwaltungsprozesse (Abfrage km-Stände, HU-Nachweise, Reifenwechsel, etc.)
Rechtsgrundlage:	1. Gesetzliche Verpflichtung (Straftatbestand des Fahrens ohne Fahrerlaubnis, in Deutschland § 21 Abs. 1 StVG; Sorgfaltspflicht des Fahrzeughalters) 2. Ggf. Unfallverhütungsvorschriften der Berufsgenossenschaften, (in Deutschland ArbSchG, ArbStättV, GefStoffV/BioStoffV und DSGVO) 3. Fahrzeug-Überlassungsvereinbarung bzw. wenn nicht vorhanden, berechtigtes Interesse des Fahrzeughalters
Betroffene Personengruppen:	Alle Fahrer von Fahrzeugen im Eigentum der Verantwortlichen Stelle und/oder zu unterweisende Mitarbeiter der Verantwortlichen Stelle und/oder Mitarbeiter der Verantwortlichen Stelle im Rahmen der Fahrzeugverwaltung
Datenkategorien:	1. Name der Person, E-Mail-Adresse resp. Mobilfunknummer (optional: Geburtsdatum, Personalnummer) 2. Name und E-Mail-Adresse von Empfängern der Überfälligkeitsbenachrichtigungen 3. Angaben zur Fahrerlaubnis (Nummer, ausstellende Behörde, Fahrzeugklassen, Ausstellungsdatum, Ablaufdatum; ID des LapID Prüfsiegels) 4. Durchgeführte Überprüfungen (mit Zeitstempel) und Erinnerungen/Alarme (SMS/E-Mail) 5. Fotos des Führerscheins zur Prüfung (nur bei Verwendung der optionalen Driver App) 6. Datum und Ergebnis der durchgeführten Unterweisungen, Zertifikate. Temporäre Zwischenstände (bis Abschluss der jeweiligen Unterweisung) Erinnerungen/Alarme (SMS/E-Mail) (optional)

	7. Durchgeführte Aufgaben im Rahmen der Fahrzeugverwaltung (Zeitpunkt, Ergebnis) sowie die für Aufgaben erhobenen Dokumente und Eingaben. Die in diesem Zusammenhang versandten Erinnerungen und Alarme (SMS/E-Mail).
Empfänger:	LapID als Auftragsverarbeiter, Behörde zum Nachweis der regelmäßigen Überprüfung, Versicherungen im Schadensfall (jeweils nur auf Anforderung)
Regelfristen für die Löschung:	Löschung aller Daten eines Fahrers: spätestens ein Jahr nach Ablauf der Fahrzeug-Überlassungsvereinbarung, soweit keine gesetzliche Aufbewahrungspflicht besteht Löschung der durchgeführten Überprüfungen/Unterweisungen: spätestens sechs Jahre nach der Prüfung Löschung der Führerschein-Fotos nach 48 Stunden.
Datenübermittlung in Drittstaaten:	Nein
Schutzmaßnahmen:	siehe Datenschutz- und Sicherheitskonzept in der aktuellen Fassung
Zugriffsberechtigte:	Auftraggeber: Fuhrparkmanager bzw. HR Auftragnehmer: Support-Berechtigte gemäß Berechtigungskonzept (aktuelle Liste der Personen mit Zugriffsberechtigung auf die LapID Datenbank); bei Verwendung der optionalen Driver App: Sichtprüfer