Löschkonzept gemäß DSGVO

für das Kontrollsystem

DriversCheck

DriversCheck GmbH
Lichtstraße 43c | D-50825 Köln
Handelsregisternummer: HRB 95707 | Registergericht: Amtsgericht Köln
Geschäftsführer: Paul Becht, Marc Vogler, Dr. Florian Weiß
info@drivers-check.de

Revision: 21. Januar 2026

I. Inhaltsverzeichnis

1. Datenumfang

Für die Nutzung der App *DriversCheck* zur Durchführung der elektronischen Führerscheinkontrolle werden die folgenden personenbezogenen Daten verarbeitet:

- Anrede
- Vorname
- Nachname
- E-Mail-Adresse
- Passwort
- PIN
- ID des *DriversCheck*-Siegels bei Siegelprüfung
- Führerscheinnummer bei siegelloser Kontrolle
- Zeitstempel und Art der durchgeführten Kontrollvorgänge

Die Daten werden im gemäß DIN ISO/IEC 27001 zertifizierten Rechenzentrum der Hetzner Online GmbH in Deutschland am Standort Nürnberg gespeichert.

2. Löschklasse

Bei den gespeicherten Daten handelt es sich um personenbezogene Daten der Schutzklasse 1, Sicherheitsstufe 3 für sensible Daten.

3. Löschregeln

Kontrolldaten *(Zeitstempel und Art der durchgeführten Kontrollvorgänge)* werden nach drei Jahren ab dem Zeitpunkt der Protokollierung in *DriversCheck* durch einen automatisierten Prozess gelöscht. Gleiches gilt für Nutzerdatensätze und alle damit referenzierten Daten, für Nutzer welche in *DriversCheck* länger als drei Jahre inaktiv sind.

Die Angemessenheit der Speicherdauer für inaktive Nutzer ist mit der Nachweispflicht des Fahrzeughalters zur Durchführung der gesetzlich vorgeschriebenen Führerscheinkontrolle zu begründen.

Beispiel: Ein Nutzer wird deaktiviert und innerhalb von drei Jahren nach dem Zeitpunkt der Deaktivierung nicht mehr reaktiviert. Das hat zur Folge, dass alle den Nutzer betreffenden Daten unwiderruflich und vollständig gelöscht werden. Ab diesem Zeitpunkt besteht für den Fahrzeughalter keine Möglichkeit des Nachweises über die erfolgte Führerscheinkontrolle.

4. Sonderfall

Ein Sonderfall liegt vor, wenn ein Betroffener sich auf *Art. 17 DSGVO* bezieht und von seinem Recht auf Löschung seiner personenbezogenen Daten als Betroffener Gebrauch macht.

In diesem Fall unterrichtet die DriversCheck GmbH (*im Folgenden „DriversCheck“ genannt)* umgehend den Auftraggeber *(in der Regel Arbeitgeber des Dienstwagenfahrers)* über die durch den Betroffenen angeforderte Löschung der personenbezogenen Daten.

Der Auftraggeber stimmt den Fall mit dem Betroffenen ab und unterrichtet DriversCheck über die vorzunehmenden Schritte. Ist eine Löschung der personenbezogenen Daten gewünscht, werden diese unverzüglich und vollständig durch DriversCheck gelöscht.

Der Weg der Löschfreigabe über den Arbeitgeber ist damit zu begründen, dass der Arbeitgeber seiner Nachweispflicht zur gesetzlich erforderlichen Führerscheinkontrolle nachzukommen hat und ein Ausscheiden des Betroffenen aus dem automatischen Kontrollprozess zur Kenntnis nehmen muss. Auf diese Weise erhält der Auftraggeber die Möglichkeit angemessen zu reagieren, in- dem er zum Beispiel dem Betroffenen die Fahrzeugnutzung untersagt.

5. Löschprozess

Automatische Löschläufe finden im wöchentlichen Turnus statt. Personenbezogene Daten, welche außerhalb der Aufbewahrungsfrist von drei Jahren liegen, werden somit automatisiert gelöscht. Die Löschvorgänge werden unter Angabe der User-ID des Betroffenen und des Löschzeitpunktes protokolliert.

Bei Fehlerfällen erfolgt eine Protokollierung und automatische Benachrichtigung der operativen Mitarbeiter von DriversCheck. Die Fehlerursache wird lokalisiert und behoben. Die Löschung wird für den Fehlerfall eingeleitet und protokolliert.

Bei einer Weisung durch den Auftraggeber zur Löschung außerhalb der Löschfrist, wird die Löschung von einem autorisierten Mitarbeiter von DriversCheck manuell vorgenommen. Der Löschvorgang wird anhand der Mitarbeiterkennung, der User-ID des Betroffenen und des Löschzeitpunktes aufgezeichnet.

6. Löschen und Vernichten von Datenträgern

Für das sichere Entfernen von Daten werden Datenträger physisch zerstört. Die Vernichtung erfolgt primär durch Durchbohren des Datenträgers, sodass die speichernden Komponenten (z. B. Magnetscheiben, Speicherchips, Leiterbahnen und Controller) irreversibel beschädigt werden und eine Wiederherstellung nicht mehr möglich ist.

USB-Speicher, die weiterhin in Verwendung sind, werden formatiert; sollen USB-Speicher entsorgt werden, erfolgt ebenfalls die Zerstörung durch Durchbohren.

Die Vernichtung wird dokumentiert (Datenträgertyp, Seriennummer soweit vorhanden, Datum, verantwortliche Person/Beauftragte/r).

6.1 Papierdokumente

Datenschutzrechtliche (personenbezogene) Daten werden nicht auf Papierdokumente übertragen. Papierdokumente, welche zu vernichten sind, werden generell mit einem Aktenvernichter P4 auf Partikelgröße zerkleinert.

6.2 Festplatten (magnetische HDD)

Der Datenträger wird durch Durchbohren zerstört. Dabei wird die Festplatte ausgebaut und so bearbeitet, dass die Magnetscheiben (Platter) sicher getroffen und dauerhaft deformiert/zerstört werden.

Das Durchbohren erfolgt durch das Festplattengehäuse an mehreren Stellen, damit nicht nur Elektronik, sondern insbesondere der Scheibenstapel beschädigt wird. Anschließend wird die Festplatte, als vernichtet gekennzeichnet und für die Entsorgung (z. B. Elektroschrott/Recyclingprozess) bereitgestellt.

Die Durchführung wird protokolliert (Gerät/Seriennummer, Datum, verantwortliche Person/ Beauftragte/r).

6.3 Festplatten mit Halbleiterspeicher

Der Datenträger wird physisch vernichtet (Durchbohren). Das Durchbohren erfolgt so, dass die Speicherbausteine (Flash-/Speicherchips) und die

relevante Elektronik (Controller/Platinenbereiche) sicher beschädigt werden.

Bei Geräten/Datenträgern mit mehreren Speicherbereichen ist darauf zu achten, dass die Bohrungen die tatsächlichen Speicherchips treffen (nicht nur Gehäuseabdeckung). Danach wird der Datenträger als vernichtet gekennzeichnet und ordnungsgemäß entsorgt.

Die Durchführung wird protokolliert (Gerät/Seriennummer, Datum, verantwortliche Person/ Beauftragte/r).

6.4 Flüchtige Halbleiterspeicher (SRAM, DRAM)

Zum Löschen wird die Stromversorgung ausgeschaltet. Wenn vorhanden, muss vorher die Pufferbatterie entfernt werden.

Soll das Speichermodul zusätzlich vernichtet werden, erfolgt die Zerstörung durch Durchbohren des Moduls an einer Stelle, die Leiterbahnen und Bauteile (insbesondere die Speicherchips) beschädigt, sodass eine Nutzung bzw. Rekonstruktion ausgeschlossen ist. Anschließend wird das Modul als vernichtet gekennzeichnet und entsorgt.

6.5 Löschen von Daten remote

Das Remote-Löschen von Daten auf Laptops erfolgt zentral über Microsoft Intune. Sobald ein Gerät zur Aussonderung vorgesehen ist oder ein Sicherheitsvorfall dies erfordert, wird die Anmeldung am Gerät gesperrt, um eine weitere Nutzung und Datenveränderung zu verhindern. Anschließend wird das Gerät aus der Domäne entfernt, sodass keine Unternehmensanmeldung und keine Domänenrichtlinien mehr greifen. Danach werden die Daten auf dem Laptop remote gelöscht (Windows-seitige Lösch-/Zurücksetzfunktionen, ausgelöst und überwacht über Microsoft Intune. Die Durchführung wird protokolliert (Gerät/Hostname, Seriennummer soweit vorhanden, Datum/Uhrzeit, verantwortliche Person, Ergebnis/Status).