Die Datenschutzgrundverordnung – Ein Überblick der wichtigsten Neuerungen

Die Datenschutzgrundverordnung (DS-GVO) tritt am 25.05.2018 in Kraft. Sie hat massive Auswirkungen auf die Tätigkeiten der Fahrschulen. Alle Beteiligten, Inhaber sowie Mitarbeiter sind von den Regelungen betroffen. Um Ihnen einen ersten Überblick zu verschaffen, haben wir Ihnen eine Erläuterung rund um das Thema angehängt. Wir werden Ihnen in Kürze weitere Informationen bzw. Handlungshilfen zukommen lassen.

Was regelt die DS-GVO?
Beim Datenschutz geht es um den Schutz personenbezogener Daten. Er beinhaltet alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, wie Name, Geburtsdatum oder IP-Adresse.

Was sind die Grundsätze der DS-GVO?
Art. 5 beinhaltet die Grundsätze, die bei einer Verarbeitung personenbezogener Daten zu beachten sind:

- Verbot mit Erlaubnisvorbehalt
Da die Verarbeitung personenbezogener Daten in das verfassungsrechtlich geschützte Persönlichkeitsrecht eingreift, ist eine Datenverarbeitung grundsätzlich verboten. Nur, wenn sie z. B. gesetzlich erlaubt oder auf der Einwilligung der betroffenen Person beruht, ist sie erlaubt.

- Rechtmäßigkeit
Die Verarbeitung ist dann rechtmäßig, wenn sie auf einer entsprechenden Grundlage beruht (Rechtsgrundlage, Einwilligung usw.) und der Zweck der Verarbeitung von der Rechtsgrundlage bzw. der Einwilligung umfasst ist.

- Transparenz
Die betroffene Person muss wissen, wer welche Daten für welchen Zweck verarbeitet. Daher gibt es umfangreiche Betroffenenrechte (z. B. Informationspflichten, Auskunftsrechte, Recht auf Berichtigung der Daten, Widerspruchsrecht).

- Zweckbindung
Die Daten dürfen nur für die genannten Zwecke verarbeitet werden. Ausnahmen sind vorgesehen für sog. kompatible Zwecke, also Zweckänderungen, die aber mit dem ursprünglichen Zweck eng zusammenhängen.

- Datenminimierung
Es dürfen nur die personenbezogenen Daten verarbeitet werden, die für die Zweckerreichung notwendig sind.

- Richtigkeit
Die Daten müssen richtig sein, anderenfalls müssen sie berichtigt oder gelöscht werden.

- Speicherbegrenzung
Die Datensparsamkeit ist hierbei zu beachten, also die Frage, wann Daten nicht mehr benötigt und daher gelöscht werden können. Zudem sind alle Möglichkeiten zur Anonymisierung von Daten zu nutzen.

- Integrität und Vertraulichkeit
Die DS-GVO verknüpft sehr stark den Datenschutz mit der Technik. Die IT-Verfahren müssen somit schon von Anfang an darauf ausgerichtet sein, möglichst wenig personenbezogene Daten verarbeiten zu können.

- Rechenschaftspflicht – Massive Erhöhung des Bußgeldrahmens
Das ist der wichtigste Aspekt der Grundsätze! Die verantwortliche Stelle, also das Unternehmen oder die Institution sind verantwortlich für den Datenschutz und seine Beachtung. Dazu ist ein Datenschutzmanagement notwendig – natürlich abhängig von der Größe des Unternehmens, der personenbezogenen Daten, die verarbeitet werden und der Menge und der Qualität der Daten. Zumindest muss aber auch in kleineren und mittleren Unternehmen ein Mindestmaß an Dokumentation vorhanden sein, um die Einhaltung des Datenschutzes nachweisen zu können. Denn

die Verletzung der Datenschutzpflichten zieht empfindliche Bußgelder nach sich: Bis zu 20 Mio. Euro oder 4 % des weltweiten Umsatzes können von den Aufsichtsbehörden verhängt werden.

Welche neuen Vorgaben der DS-GVO müssen die Unternehmen beachten?

Datenschutzbeauftragter:
Unternehmen müssen zukünftig nach Art. 37 DS-GVO einen betrieblichen Datenschutzbeauftragten (DSB) benennen, wenn ihre Kerntätigkeit bzw. die ihres Auftragsverarbeiters:

- aus Verarbeitungsvorgängen besteht, die nach Art, Umfang und/oder Zweck eine systematische Überwachung erfordern
- die Verarbeitung besonders sensibler Daten nach Art. 9 DS-GVO und Art. 10 DS-GVO betrifft.

Zusätzlich **erweitert in Deutschland** der § 38 DSAnpUG-EU die Gründe für die Benennung eines DSB. Eine Erforderlichkeit zur Bestellung eines DSB besteht danach auch dann, wenn:

- i.d.R. mindestens 10 Personen ständig mit der Datenverarbeitung beschäftigt
- Verarbeitungen vornimmt, die der Datenfolgenabschätzung (s.u.) unterliegen (besonders relevant bei Gesundheitsdaten)
- personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet.

Bezüglich der Bestellung eines DSB ist **sowohl die Möglichkeit einer externen als auch internen Lösung** gegeben. Wichtig ist in allen Fällen, dass der DSB entsprechend qualifiziert ist. Arbeitsrechtlich hat die interne Bestellung eines DSB zur Folge, dass dieser ohne wichtigen Grund (außerordentliche Kündigung nach § 626 BGB) nicht mehr abberufen oder gekündigt werden kann (§ 38 i.V.m. § 6 Abs. 4 DSAnpUG-EU).

Die Art. 38 DS-GVO und Art. 39 DS-GVO enthalten die wichtigsten inhaltlichen Regelungen für die Arbeit des DSB. Er hat folgende Aufgaben wahrzunehmen:

- Kooperation mit der Aufsichtsbehörde
- Überwachung der Einhaltung der rechtlichen Vorgaben sowie des Umgangs des Verantwortlichen (bzw. Auftragsverarbeiters) sowie die Schulung der relevanten Mitarbeiter
- Unterrichtung des Verantwortlichen (bzw. Auftragsverarbeiters)
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung gem. Art. 35 DS-GVO

Datenschutz in technischer und organisatorischer Hinsicht:
Die Art. 24 DS-GVO und Art. 25 DS-GVO geben den Verantwortlichen (Unternehmen) vor, dass sie geeignete technische und organisatorische Maßnahmen treffen müssen, um den Datenschutz und die Datensicherheit zu gewährleisten. Zu beachten bleiben diesbezüglich vor allem die Grundsätze der Datensparsamkeit (so wenige Daten wie möglich) und der Pseudonymisierung, welche so schnell wie möglich durchgeführt werden sollte. Bezüglich der zur Datenverarbeitung genutzten Hard- und Software gilt die Vorgabe, dass diese so eingestellt werden soll, dass nur diejenigen Daten erhoben werden, welche für den Zweck der Verarbeitung notwendig sind.

Datenschutzfolgeabschätzung:
Im Rahmen des Art. 35 DS-GVO wird das neue Instrument der Datenschutzfolgenabschätzung eingeführt. Sie ist durchzuführen, wenn ein Datenverarbeitungsverfahren voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen birgt. Die Durchführung der Datenschutzfolgeabschätzung erfolgt in drei Schritten:

(1) Zunächst ist zu prüfen, ob ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht.

(2) Besteht ein Risiko nach (1), ist anschließend eine Bewertung vorzunehmen, ob geplante Abhilfemaßnahmen und Sicherheitsvorkehrungen ausreichen, um den Datenschutz zu gewährleisten. Zusätzlich muss ein Nachweis erfolgen, dass die DS-GVO eingehalten und die Interessen
der Betroffenen beachtet wurden.

(3) Steht als Ergebnis der Bewertung fest, dass entgegen aller Maßnahmen ein hohes Risiko besteht, muss eine Meldung bei der Aufsichtsbehörde erfolgen (siehe Art. 36 DS-GVO). Zuständig ist der Bundesbeauftragte für den Datenschutz (§ 69 Abs.1 DSAnpUG-EU). Unabhängig des Risikos ist bei besonders sensiblen Fällen die Durchführung der Datenschutzfolgeabschätzung zwingend von Art. 35 DS-GVO vorgeschrieben. Es hat eine schriftliche Dokumentation der Datenschutzfolgeabschätzung zu erfolgen. Bei vorhandenem DSB im Unternehmen, ist dieser unbedingt in die Folgenabschätzung einzubeziehen.

Melde- und Informationspflichten bei Datenpannen:
Nach Art. 33 DS-GVO müssen alle Verletzungen des Schutzes personenbezogener Daten gemeldet werden. Die Meldung muss binnen 72 Stunden nach Bekanntwerden der Aufsichtsbehörde (Bundesdatenschutzbeauftragter, § 65 DSAnpUG-EU) gegenüber erfolgen. Die von der Verletzung Betroffenen (z.B. Arbeitnehmer, Kunden) müssen selbst auch informiert werden (Art. 34 DS-GVO).

Auftragsdatenverarbeitung:
Es handelt sich dabei um die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen Auftragsverarbeiter nach den Weisungen des für die Verarbeitung Verantwortlichen auf Grundlage eines schriftlichen Vertrages. Sie ist nach Art. 28 DS-GVO und Art. 29 DS-GVO erlaubt. Als Beispiel ist hier die Bestellung einer externen Stelle zu nennen, welche die Erstellung von Rechnungen wahrnimmt. Die Zulässigkeit besteht jedoch nur dann, wenn der Auftragsverarbeiter hinreichend Garantien für eine ordnungsgemäße Datenverarbeitung gewährleistet (siehe Art. 28 DS-GVO).

Verzeichnis der Verarbeitungstätigkeiten:
Art. 30 DS-GVO ordnet an, dass Verantwortliche und Auftragsdatenverarbeiter ein Verzeichnis über alle Verarbeitungstätigkeiten unter der Angabe der im Artikel genannten Punkte führen müssen. Nach Art. 30 Abs. 5 DS-GVO ist es jedoch möglich, dass Unternehmen mit weniger als 250 Beschäftigten von dieser Pflicht ausgenommen werden können.

Was sollten Unternehmen jetzt beachten?

Angesichts des enorm gestiegenen Strafrahmens sollte das Thema Datenschutz nicht „stiefmütterlich“ in der Ecke liegen gelassen werden. Besonders die Unternehmen, welche nach den oben aufgezeigten Voraussetzungen zur Bestellung eines Datenschutzbeauftragten verpflichtet sind, sollten unbedingt handeln. Vorhandene DSB sollten nachgeschult werden. Ist noch kein DSB vorhanden, muss zeitnah eine externe oder interne Lösung gefunden werden. Besteht ein Betriebsrat, sollte ein konstruktiver Austausch mit diesem zur zukünftigen Umsetzung erfolgen.

Als besonders wichtig ist auch die zukünftige Pflicht zur Datenschutz-Folgeabschätzung zu bewerten. Unternehmen, die mit einem IT-Unternehmen zusammenarbeiten, sollten diese kontaktieren und mit diesen gemeinsam die Umsetzung des DS-GVO Vorgaben vornehmen. Es sollte eine umfassende Risikoanalyse der bisherigen Datenverarbeitung anhand der neuen Gesetzesgrundlage erfolgen. Dies erfolgt am besten in Form eines Abgleichs des aktuellen Ist-Zustandes mit dem künftigen Soll-Zustand.

Nutzen Sie bereits heute schon Auftragsdatenverarbeiter, sollten die bestehenden Verträge inhaltlich überprüft oder ggf. überarbeitet werden. (D.Q.)