

DSGVO: Checkliste für die Umsetzung

Hinweis: Alle Angaben ohne Gewähr, es wird keine Haftung übernommen.

Wir stellen Ihnen hier unsere Ausarbeitungen zur DSGVO vor, eine Empfehlung basierend auf unseren Erkenntnissen.

Was bringt uns die DSGVO?

Positiv sehen wir, dass man sich mit der eigenen Organisation im Unternehmen befassen muss. So manche „Leichen“ werden „im Keller“ auftauchen, unnötige Vorgänge werden hervortreten oder es wird sich einfach nur mehr Ordnung einstellen – wenn man die DSGVO umsetzt.

Im ersten Schritt hat die Umsetzung der DSGVO damit zu tun, sich so manche Grundlagen anzueignen und diese im Unternehmen (bei Mitarbeitern) zu verbreiten.

Ein zweiter Schritt hat damit zu tun, das eigene Unternehmen zu analysieren, einiges an Papier wird produziert. Das immer wieder genannte „Verfahrensverzeichnis“ ist ein Bestandteil bzw. ein Werkzeug dazu. So manche kleine Maßnahme wird sicher im Zuge dessen schon umgesetzt.

Erst im dritten Schritt, wenn wirklich alle Abläufe im Unternehmen bewusst gemacht (zu Papier gebracht) wurden, sehen wir das sinnvolle Angehen und Umsetzen von „Technischen und Organisatorischen Maßnahmen (TOMs)“, um wirklich vollständig die DSGVO einhalten zu können.

Der vierte Schritt ist ein periodischer Schritt. Regelmäßig sind wir dazu angehalten, unsere Unternehmen zu prüfen, geänderte Abläufe zu erheben, Verfahrensverzeichnisse anzupassen, usw.

Der angedrohte Strafrahmen von bis zu Euro 20 Mio. ist „eindrucksvoll“. Verhängt werden Strafen von der Datenschutzbehörde, diese kann aus unserer Sicht dadurch strafmildernd beeindruckt werden, indem viel dokumentiert wird, sprich: Papier produziert wird.

Wir gehen davon aus, dass es vielen Unternehmen aus Zeitgründen nicht möglich sein wird, die DSGVO rechtzeitig voll umzusetzen. Zumindest die Papierarbeit müsste jedoch möglich sein. Das Bewusstmachen von Lücken ist der erste und notwendige Schritt, bevor Lücken geschlossen werden können. Wir nehmen an, die EU will mit der DSGVO zumindest das „Bewusstmachen“ erwirken, eine geplante aber zu einem späteren Zeitpunkt erfolgende Umsetzung wird nicht das große Problem sein. Das ist unsere Sicht der Dinge...

1. Schritt: Beginnen Sie mit einem Ordner

Machen Sie den ersten Schritt, ein sog. „Datenschutzmanagementsystem“ (DSMS). Ein herkömmlicher Papier-Ordner, beschriftet mit „DSGVO“. Hier legen Sie alle Dokumente ab, die mit der DSGVO zu tun haben – jede Aktion, die Sie im Sinne von Datenschutz treffen. Jedes Meeting mit Mitarbeitern, Dinge die Sie umgesetzt haben usw. Im Laufe der Zeit werden Sie Dokumente verbessern und aktualisieren, lassen Sie die alten Versionen in dem Ordner. Dies signalisiert der Datenschutzbehörde, dass Sie sich damit beschäftigen und es aktuell halten.

Im Folgenden werden Ihnen beim Durcharbeiten Dinge auffallen. Schreiben Sie es auf eine Liste, um es später abarbeiten zu können.

2. Schritt: Studieren Sie die Grundsätze und geben Sie diese an Ihre Mitarbeiter weiter

Gehen Sie auf www.mmm-software.at/dsgvo.

Wir empfehlen, die Dokumente „Begriffe“ und „Verwendung von Daten“ zu studieren und mit Ihren Mitarbeitern zu besprechen.

3. Schritt: Geldbußen, Schadenersatz, Abmahnungen

Gehen Sie auf www.mmm-software.at/dsgvo.

Wir empfehlen, das Dokument „Geldbußen, Schadenersatz, Abmahnungen“ zu studieren. Machen Sie sich und Ihren Mitarbeitern bewusst, was es kosten kann, sich nicht an die DSGVO zu halten.

4. Schritt: Speicherbegrenzung vs. Aufbewahrungspflicht

Gehen Sie auf www.mmm-software.at/dsgvo.

Wir empfehlen, das Dokument „Aufbewahrungspflicht“ zu studieren.

Es beschreibt die Diskrepanz, personenbezogene Daten einerseits schnellstmöglich löschen, andererseits für die Finanz aufbewahren zu müssen.

5. Schritt: Fahrlehrer

Gehen Sie auf www.mmm-software.at/dsgvo.

Wir empfehlen, das Dokument „Fahrlehrer“ zu studieren.

Machen Sie sich und Ihren Fahrlehrern bewusst, inwieweit auch der „Außendienst“ von der DSGVO betroffen ist und treffen Sie geeignete Maßnahmen.

6. Schritt: Datenschutzbeauftragter

Gehen Sie auf www.mmm-software.at/dsgvo.

Studieren Sie das Thema „Datenschutzbeauftragter“.

Vermutlich sehen Sie es wie wir, dass Sie als Fahrschule keinen Datenschutzbeauftragten haben müssen. Entschließen Sie sich gerne dennoch dafür, einen Datenschutzbeauftragten zu ernennen. Ein Mitarbeiter könnte einen Kurs samt Prüfung absolvieren, Sie könnten es als Qualitätsmerkmal nach außen nutzen.

7. Schritt: Sensible Daten im Fahrschulwesen: Arztgutachten und Personalwesen

Gehen Sie auf www.mmm-software.at/dsgvo.

Studieren und besprechen Sie das brennende Thema „Arztgutachten“.

Folgen Sie unserer Empfehlung bzw. der DSGVO, halten Sie so viel Abstand wie möglich von Arztgutachten. Treffen Sie eine Entscheidung, wie Sie in Zukunft damit umgehen werden.

Studieren und besprechen Sie das Thema „Personalangelegenheiten“. Finden und löschen Sie jegliche Bewerbungsunterlagen, die Sie von Bewerbern erhalten haben. Ob auf Papier, Mails, anderswo gespeichert, löschen Sie diese, falls diese älter als 6 Monate sind – falls Sie keine Einwilligung zur Evidenzhaltung haben.

8. Schritt: Einwilligungen

Gehen Sie auf www.mmm-software.at/dsgvo.

Studieren und besprechen Sie „Einwilligungen“.

Erstellen Sie für Ihren Ausbildungsauftrag entsprechend passende Einwilligungserklärungen.

9. Schritt: Betroffenenrechte

Gehen Sie auf www.mmm-software.at/dsgvo.

Studieren und besprechen Sie „Betroffenenrechte“.

Der Informationspflicht müssen Sie nachkommen, bevor Sie personenbezogene Daten erheben (in den AGBs der Homepage, auf einem Zettel vor der Anmeldung).

Alle anderen Rechte können von betroffenen Personen jederzeit wahrgenommen werden, bereiten Sie sich vor, die Rechte zu wahren.

10. Schritt: Auftragsverarbeiter

Gehen Sie auf www.mmm-software.at/dsgvo.

Studieren Sie das Thema „Auftragsverarbeiter“. Binden Sie auch gerne Ihre Mitarbeiter ein, zusammen finden sich die Auftragsverarbeiter schneller und vollständiger.

Beachten Sie: Nur, wenn ein Auftragsverarbeiter von Ihnen personenbezogene Daten erhält, müssen Sie einen Vertrag abschließen.

Gehen Sie nun die Schritte „Das ist nun zu tun“ des obigen Dokumentes durch, dort finden Sie auch einen Mustervertrag.

11. Schritt: Datenschutz-Folgenabschätzung

Gehen Sie auf www.mmm-software.at/dsgvo.

Studieren Sie das Thema „Datenschutz-Folgenabschätzung“. Binden Sie auch gerne Ihre Mitarbeiter ein. Finden Sie jegliche Verarbeitungen, die ein „hohes Risiko“ für die Rechte und Freiheiten von betroffenen Personen haben. Vermeiden Sie deren Verarbeitung. Falls Sie diese Verarbeitungen beibehalten möchten, sichern Sie diese so weit als möglich ab und erstellen Sie eine Folgenabschätzung.

12. Schritt: Data Breach (Datenschutzverletzung)

Gehen Sie auf www.mmm-software.at/dsgvo.

Studieren Sie das Thema „Data Breach“. Machen Sie sich und Ihren Mitarbeitern bewusst, was zu tun ist, sollte „es“ passieren.

13. Schritt: Verfahrensverzeichnis

Gehen Sie auf www.mmm-software.at/dsgvo.

Studieren Sie das Thema „Verfahrensverzeichnis“.

Dies wird ein umfangreicher Punkt, der viel Zeit in Anspruch nehmen wird.

Wir empfehlen auf jeden Fall, das Personal einzubinden, und ein Muster zu verwenden.

Ob ein Muster von der WKO allgemein, vom Fachverband, von uns, oder eine Software-Lösung (siehe unsere Empfehlungen) – Hauptsache Sie haben am Ende ein Verfahrensverzeichnis.

14. Schritt: Technische und Organisatorische Maßnahmen

Gehen Sie auf www.mmm-software.at/dsgvo.

Studieren Sie das Thema „Technische und Organisatorische Maßnahmen“.

Arbeiten Sie entsprechende Maßnahmen aus. Manche Maßnahmen können Sie sofort umsetzen, manche werden etwas Umsetzungszeit in Anspruch nehmen. Unsere Beispielliste soll Ihnen bei der Umsetzung helfen, konsultieren Sie dazu auch gerne Ihren IT-Fachmann oder Datenschutz-Experten.

15. Noch ein Durchgang

Sie können auch andere Checklisten studieren, wie z. B.

<https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Checkliste.html>

Unsere Empfehlung ist: beginnen Sie nochmals von vorne, bei jedem weiteren Durchgang werden Dinge klarer und vollständiger.