leitnerleitner
wirtschaftsprüfer steuerberater

WKO DER HANDEL

Toolset DSGVO der WKO Bundessparte Handel

Mit 25. Mai 2018 treten die Anforderungen nach der Datenschutzgrundverordnung (DSGVO) in Kraft. Mit diesem Datum müssen zum einen Anforderungen ua an die Dokumentation umgesetzt sein und zum anderen müssen ab diesem Zeitpunkt die organisatorischen Maßnahmen getroffen sein um die Mitarbeiter und Mitarbeiterinnen entsprechend zu schulen und mit dem Thema Datenschutz im laufenden Betrieb umgehen zu können.

Die Umsetzung dieser Anforderungen bedeutet für die meisten Unternehmen einen beträchtlichen Aufwand, wobei die Grundanforderungen für typische Unternehmen einer Branche sehr ähnlich sind.

Um einem typischen österreichischen Handelsunternehmen einen Weg zur Umsetzung dieser Maßnahmen aufzuzeigen hat die Bundessektion Handel der Wirtschaftkammer gemeinsam mit der Firma LeitnerLeitner ein Vorgehensmodell entwickelt. Dies soll die Mitgliedsunternehmen bei der Umsetzung der Maßnahmen unterstützen. Dieses Modell und die unterstützenden Dokumente werden den Mitgliedsunternehmen der Bundessparte Handel unter der Bezeichnung „Toolset DSGVO" zur Verfügung gestellt.

Nachfolgend werden nun die einzelnen Schritte dieses Vorgehensmodells und die dazu verfügbaren Dokumente erläutert.

Bei der Umsetzung im Unternehmen ist aber folgendes zu beachten:

- Das Toolset DSGVO der WKO Bundessparte Handel ist als ein Standardmodell zur Unterstützung bei der Umsetzung im Handel gedacht, muss aber an die jeweilige Branche und das Unternehmen individuell angepasst werden.
- Es ist nur das Datenschutzrecht umfasst, alle anderen Rechtsvorschriften werden darin nicht berücksichtigt bzw gelten wie bisher.
- Die Erstellung erfolgte im Jänner 2018. Etwaige Entwicklungen und Klarstellungen nach diesem Termin sind nicht berücksichtigt.
- Die Umsetzung im Unternehmen muss als Projekt definiert sein und die nötige Unterstützung des Managements/Unternehmers haben.
- Die enthaltenen Musterdokumente dienen der beispielsweisen Umsetzung der Regelungen der DSGVO in Bezug auf das jeweilige Thema. Diese Dokumente sind auf die Bedürfnisse und Gegebenheiten des jeweiligen Unternehmens individuell anzupassen bzw zu ergänzen.
- Die Verantwortung für die gesetzeskonforme Umsetzung der Anforderungen zum Thema Datenschutz liegt beim Unternehmen.

Datenschutz neu – Chance und Risiko für Unternehmen

Die Anforderungen nach der Datenschutzgrundverordnung stellen nicht zuletzt wegen der doch empfindlichen Strafen und dem möglichen Schadenersatz für Betroffene ein Risiko für Unternehmen dar.

Durch die gänzliche Neueinführung der Bestimmungen gibt es noch keine Erfahrungen mit den Behörden, aber es gibt auch noch keine Erfahrungen bei den Behörden.

Durch unbestimmte Rechtsbegriffe wie zB „Geldbußen müssen wirksam, verhältnismäßig und abschreckend sein" wird sich der tatsächliche Umgang mit den Themen erst nach den ersten Entscheidungen und Gerichtsverfahren zeigen.

Für Unternehmen, die sich an die Regeln des Datenschutzes halten gibt es aber auch neue Chancen. Kunden wollen immer häufiger über ihre eigenen Daten bestimmen und überlegen genau, wem sie welche vertraulichen Daten übergeben.

Nicht zuletzt kann jeder von uns auch einmal „auf der anderen Seite stehen". Und dann ist jeder über die Einhaltung der entsprechenden Datenschutzregeln froh.

Um bis Mai 2018 die entsprechenden Maßnahmen umgesetzt zu haben ist es unabdingbar ein Vorgehensmodell zu haben. Rein aus den Bestimmungen der DSGVO wird die Umsetzung sehr schwierig.

Unternehmensstrategie zum Datenschutz am Beginn

Bevor an die Umsetzung mit einem Vorgehensmodell gedacht wird muss jedes Unternehmen für sich eine Strategie überlegen wie mit dem Thema Datenschutz umgegangen werden soll.

Dies ist von Unternehmen zu Unternehmen unterschiedlich. Auf der einen Seite stehen Unternehmen, die Daten nur zur reinen Verwaltung verarbeiten wollen, auf der anderen Seite Händler, die mit aufwändigen Auswertungen aus Onlineshops Kundenprofile für zielgruppenspezifisches Marketing generieren. Die meisten Handelsunternehmen werden irgendwo dazwischen angesiedelt sein.
In der Strategie muss festgelegt werden, wie ein Unternehmen mit Daten umgeht. Dies bestimmt auch wesentlich den zukünftigen Aufwand mit den Regelungen der DSGVO.

Ein wesentlicher Hinweis zur Strategie:

Alle Daten, die nicht gespeichert werden, müssen auch datenschutzrechtlich nicht behandelt werden. Das Sammeln von Daten „auf Vorrat" sollte daher eingestellt werden.

Entwicklung eines Vorgehensmodells zur Vorbereitung auf die DSGVO

Es sind ab 1.2.2018 nicht mehr ganz 4 Monate, bis die Regelungen der DSGVO wirksam werden. Um die Umsetzung strukturiert angehen zu können, ist ein Vorgehensmodell notwendig. Dieses Vorgehensmodell umfasst mehrere Schritte, die meist in einem Projekt abgearbeitet werden.

Toolset DSGVO

In der Folge wird das von der Bundessektion Handel gemeinsam mit LeitnerLeitner entwickelte Beispielvorgehensmodell für den Handel vorgestellt, die einzelnen Schritt beschrieben und die Musterdokumente erläutert.

Übersicht über die Arbeitsschritte

- ¬ Management sensibilisieren
- ¬ Projekt aufsetzen
- ¬ Datenschutzorganisation im Unternehmen definieren
- ¬ Informationen über Prozesse erheben und Verzeichnis der Verarbeitungstätigkeiten erstellen
- ¬ Rechtmäßigkeit der Verarbeitung prüfen
- ¬ Rechtskonformität der Auftragsverarbeitung sicherstellen
- ¬ Technisch organisatorische Maßnahmen beurteilen/anpassen
- ¬ Datenschutz-Folgeabschätzungen durchführen
- ¬ Unternehmensrichtlinien und Schulungen
- ¬ Datenschutz im laufenden Betrieb

Wichtig ist, dass alle Schritte, die zum Datenschutz unternommen werden, dokumentiert werden, da diese im Anlassfall der Behörde nachzuweisen sind!

1. *Management sensibilisieren*

Am Beginn muss die Unternehmensführung und das Management für das Thema Datenschutz und die neuen Anforderungen nach Datenschutzgrundverordnung sensibilisiert werden. Dafür können Seminare und Veranstaltungen der Wirtschaftskammer oder anderer Seminaranbieter besucht werden oder es kann einschlägige Fachliteratur gelesen werden. Ziel ist, dass das Management die Grundbegriffe des neuen Datenschutzrechts kennt und erkennt, dass im Unternehmen Schritte zur Umsetzung erfolgen müssen.

- Dokument im Toolset: D_00a Einführungspräsentation

Um in Ihrem Unternehmen das Management zu sensibilisieren ist im Toolset eine Präsentation mit den wichtigsten Inhalten zum Thema Datenschutz und einem Mustervorgehensmodell enthalten. Diese Präsentation sollte gemeinsam mit dem Management durchgegangen werden. Die Präsentation wurde im Mai 2018 aktualisiert um die Veränderungen seit Ersterstellung zu berücksichtigen.

2. *Projekt aufsetzen*

Um die Maßnahmen zum Datenschutz im Unternehmen strukturiert umsetzen zu können, ist es unbedingt notwendig, ein Projekt aufzusetzen. Dafür wird, unabhängig davon wie viele Mitarbeiter oder Mitarbeiterinnen beteiligt sind, ein Projektplan benötigt. Dieser soll alle notwendigen Schritte, deren Zeitplanung und Verantwortungen enthalten. Denn nur so kann sichergestellt werden, dass die Umsetzung zeitgerecht und zielgerichtet erfolgt.

- Dokument im Toolset: D_02a Beispielprojektplan

Im Toolset ist ein Beispielprojektplan enthalten, der die notwendigen Schritte des Vorgehensmodells enthält. Ebenso können dort auch organisatorische Punkte wie Verantwortungen und Zeitrahmen definiert werden. Auf vorhandene Beispieldokumente wird auch hingewiesen.

Dieser Beispielprojektplan ist um die im jeweiligen Unternehmen notwendigen Schritte zu ergänzen und dient dann als Grundlage für das nachfolgend im Unternehmen durchzuführende Projekt.

3. *Datenschutzorganisation im Unternehmen definieren*

Am Beginn des Projekts muss definiert werden, wer im Unternehmen für Datenschutz zuständig ist. Diese Tätigkeiten werden meist in 2 Positionen dargestellt:

Der Datenschutzmanager/Die Datenschutzmanagerin ist normalerweise für die Umsetzung der Anforderungen zuständig und dann im laufenden Betrieb für den Umgang mit Anfragen von Betroffenen, usw. Diese Position kann auch die Geschäftsführung innehaben.

Der Datenschutzbeauftragte ist eine Position, deren Aufgaben in der DSGVO definiert ist. Diese Position hat eine eher beratende Rolle im Thema Datenschutz und soll va Kontrollen ausüben. Diese Position ist mit einer Geschäftsführungsposition oder IT-Funktion wegen der Selbstkontrolle unvereinbar.

Ein Datenschutzbeauftragter ist nur in gewissen Fällen verpflichtend zu bestellen, kann aber freiwillig bestellt werden. In einem typischen Handelsunternehmen

wird es eher keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten geben. Auch kann diese Funktion ausgelagert werden.

Des Weiteren sollte man sich bereits im Vorfeld überlegen, wer im Anlassfall zum Thema Datenschutz Hilfestellung geben kann. Daher sollte ev der Kontakt zum Firmenanwalt, zum Datenschutzverantwortlichen des Dienstleisters etc hier hinterlegt werden.

Im Toolset sind zur Datenschutzorganisation folgende Dokumente enthalten:

- D_03a Übersicht Datenschutzorganisation

Dieses Dokument soll eine Übersicht über die Verantwortungen im Unternehmen zum Thema Datenschutz geben. Auch sollen hier wichtige Personen/Stellen wie Rechtsanwaltskanzlei, Datenschutzverantwortliche bei Dienstleistern etc enthalten sein.

- D_03b Positionsbeschreibung Datenschutz Manager/Verantwortlicher
- D_03c Positionsbeschreibung Datenschutzbeauftragter (nach DSGVO)
- D_03d Entscheidungsbaum, ob ein Datenschutzbeauftragter benötigt wird

Anhand des Entscheidungsbaums kann leicht festgestellt werden, ob ein Datenschutzbeauftragter im Unternehmen benötigt wird oder nicht. In Zweifelsfragen sind stets Spezialisten zu befragen.

4. *Information über Prozesse erheben / Verzeichnis der Verarbeitungstätigkeiten*

In diesem Schritt müssen im Unternehmen alle Prozesse identifiziert werden, in denen Daten verarbeitet werden. Dann muss ein Verzeichnis der Verarbeitungstätigkeiten angelegt werden. Dies muss auch enthalten, an wen allenfalls Daten weitergegeben werden.

Dies ist für alle Unternehmen der umfassendste Schritt in der Umsetzung. Das Toolset unterstützt dies durch Beispielvorlagen für die Verfahrenstätigkeiten „Rechnungswesen und Geschäftsabwicklung", „Personalverwaltung" und „Marketing". Weitere Verfahrenstätigkeiten sind aufgezählt.

Die Beispielvorlagen sind entsprechend anzupassen und für weitere Verfahrenstätigkeiten sind ebensolche Verzeichnisse zu erstellen.

Die Toolbox enthält dazu folgende Dokumente:

- D_04a Musterverfahrensdokumentation inkl Prüfung auf Rechtmäßigkeit und allfällige Risikoanalyse hinsichtlich Datenschutzfolgenabschätzung
- D_04 bEine Erläuterung zum Umgang mit Onlineshops

5. *Prüfung der Rechtmäßigkeit*

Da die Verarbeitung von Daten grundsätzlich verboten ist und nur in besonderen Fällen erlaubt ist, ist es notwendig für jede Verarbeitungstätigkeit eine Rechtsgrundlage zu haben. Diese Rechtsgrundlagen sind in der DSGVO definiert.

Werden personenbezogene Daten erhoben haben die betroffenen Personen nach Artikel 13 und Artikel 14 DSGVO darüber informiert zu werden. In diesen Artikeln ist definiert, welche Informationen vom Verantwortlichen bereitgestellt werden müssen. Diese Information kann auch auf der Website in der sog. Datenschutzerklärung veröffentlicht werden.

Diese ist nicht nur bei Online-Shops und Online-Formularen zu verwenden, sondern es kann auch bei Einverständniserklärungen (zB bei Anmeldung zu Newslettern) darauf verwiesen werden.

Die Musterdatenschutzerklärung im Toolset ist auf die jeweiligen Erhebungsmethoden anzupassen.

Das Toolset enthält dazu die folgenden Dokumente:

- D_05a Rechtsgrundlagen nach DSGVO inkl Muster für Rechtsgrundlagen pro Verarbeitungstätigkeit
- D_05b Eine Musterdatenschutzerklärung für ein Unternehmen zur Veröffentlichung auf der Website (Datenschutzmitteilung)
- D_05c Entscheidungsbaum zur Videoüberwachung um diese auf Rechtmäßigkeit zu überprüfen.
- D_05d1 Ein Praxisbeispiel zum Prozess der Sammlung von Interessentendaten
- D_05d2 Einverständniserklärung für die Verarbeitung von Interessentendaten.

6. *Auftragsverarbeitung*

Werden Tätigkeiten wie zum Beispiel IT oder Lohnverrechnung an Dritte ausgelagert muss hinsichtlich Datenschutz mit diesen Auftragsverarbeitern eine Vereinbarung abgeschlossen werden, deren Inhalte in Art. 28 der DSGVO wie folgt definiert sind:

- Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen (inkl Informationspflicht bei abweichender rechtlicher Verpflichtung)
- Vertraulichkeitserklärung/Verschwiegenheitspflicht des Personals
- Sicherstellung von technischen und organisatorischen Datenschutzmaßnahmen
- Zustimmungsrechte oder Informationspflicht mit Einspruchsrecht bei Subauftragsverarbeitern und Überbindung aller eigenen Verpflichtungen
- Verpflichtung zur Unterstützung des Verantwortlichen hinsichtlich Datensicherheit und Betroffenenrechte
- Pflicht zur Datenlöschung/-rückgabe nach Beendigung der Tätigkeit
- Nachweis- und Inspektionsrechte

Der auslagernde Unternehmer als Verantwortlicher hat eine Rechenschaftspflicht über die Einhaltung von geeigneten technischen und organisatorischen Maßnahmen beim Auftragsverarbeiter (Auswahlverschulden).

Das Toolset enthält dazu die folgenden Dokumente:

- D_06a Beispiel Auftragsverarbeitungsvertrag

7. *Technisch organisatorische Maßnahmen beurteilen/anpassen*

Die Definition der Technisch Organisatorische Maßnahmen ist in Artikel 32 der DSGVO zu finden. Verantwortliche und Auftragsverarbeiter haben dafür zu sorgen, dass „geeignete technische und organisatorische Maßnahmen" implementiert sind, die sicherstellen, dass „ein angemessenes Schutzniveau zu gewährleistet ist".

Die Maßnahmen sollen sicherstellen, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Sicherheit der Daten und damit der Systeme gegeben ist.

Für den Verantwortlichen sind dabei der Stand der Technik, die Implementierungskosten und das Risiko (Eintrittswahrscheinlichkeit und Schadenshöhe) zu berücksichtigen.

Das Toolset enthält dazu das folgende Dokument:

- D_07a Technisch/Organisatorische Maßnahmen

In der Toolbox ist zu Technisch organisatorischen Maßnahmen ein Dokument enthalten, das die Maßnahmen beschreibt und eine Liste von technischen und organisatorischen Maßnahmen enthält.

Jedes Unternehmen muss nach einer Risikoeinschätzung die geeigneten technisch- organisatorischen Maßnahmen einführen.

8. *Datenschutz Folgenabschätzung (13)*

Eine Datenschutzfolgenabschätzung ist dann durchzuführen, wenn Daten besonderer Kategorien verarbeitet werden und in diesem Zusammenhang ein Risiko für den Betroffenen besteht. Auch ist für Verarbeitungstätigkeiten, die auf der sog „Blacklist" der Datenschutzbehörde stehen, eine Folgenabschätzung durchzuführen.

Die Datenschutzbehörden können auch eine sog „Whitelist" für Tätigkeiten, für die keine eigene Folgenabschätzung notwendig ist, veröffentlichen. Die Österreichische Datenschutzbehörde hat eine Whitelist veröffentlicht. Eine Datenschutz-Folgenabschätzung ist daher nur mehr selten notwendig.

Im ersten Schritt muss eine Risikoabschätzung erfolgen. Sollte als Ergebnis ein Risiko für Betroffene bestehen, ist eine Datenschutzfolgenabschätzung durchzuführen.

Sollte in Ihrem Unternehmen eine Datenschutz-Folgenabschätzung notwendig sein dann ist es aufgrund der Komplexität einer solchen am besten, externe Unterstützung in Anspruch zu nehmen.

Das Toolset enthält dazu ein Beispiel:

- Risikoeinschätzung

Eine Risikoeinschätzung als erster Schritt einer Datenschutz Folgenabschätzung ist bereits im Dokument D_04a der Verfahrensdokumentation enthalten.

9. *Unternehmensrichtlinien und Schulungen*

Um das Thema Datenschutz im Unternehmen bekannt zu machen und die Mitarbeiter und Mitarbeiterinnen zu sensibilisieren, müssen Schulungen abgehalten werden.

Auch muss es im Unternehmen Richtlinien für Mitarbeiter und Mitarbeiterinnen geben, wie mit Daten umzugehen ist und welche Tätigkeiten nicht erlaubt sind.

Um diesen Bereich abzudecken sind im Toolset folgende Musterdokumente enthalten:

- D_09a Allgemeine Datenschutzrichtlinie

Muster für eine allgemeine Richtlinie zum Umgang mit Daten im Unternehmen

- D_09b Richtlinie Umgang mit Daten besonderer Kategorien

Muster für eine Richtlinie für den Umgang mit sensiblen Daten (va für Personaldaten)

- D_09c Richtlinie Umgang mit Datenträgern oder Privatgeräten

Umgang mit externen Datenträgern und Mobiltelefonen. Um im Falle des Verlusts eines Datenträgers oder Mobiltelefons keine personenbezogenen Daten zu verlieren und ev eine Data Breach Notification an die Datenschutbehörde machen zu müssen, sollen keine Daten direkt auf diesen Geräten gespeichert werden. ein Verbot einer solchen Speicherung enthält diese Musterrichtlinie.

- D_09d Schulungsunterlage (inkl Bestätigung)

Diese Schulungsunterlage soll Mitarbeitern und Mitarbeiterinnen in Handelsbetrieben (va Verkäufinnen und Verkäufern) ein Grundlagenwissen zum Datenschutz geben. Das Muster muss um die unternehmensspezifischen Details ergänzt werden. Der Besuch der Schulung/der Erhalt der Unterlage muss dokumentiert werden. Die Unterlage wurde im Mai 2018 adaptiert und optischneu gestaltet.

10. Datenschutz im laufenden Betrieb

Ab dem 25.5.2018 gelten die Anforderungen der DSGVO. Ab diesem Zeitpunkt muss die Datenschutzorganisation im Unternehmen funktionieren und alle Beschäftigten müssen mit dem Thema umgehen können. Vor allem muss die Datenschutzorganisation bekannt sein.

Im Toolset DSGVO sind dazu die folgenden Dokumente enthalten:

- D_10a1 Datenschutzanfragen Anweisung MitarbeiterInnen
- D_10a2 Datenschutzanfragen Aushang Musterantwort

Bei Anfragen zum Thema Datenschutz (Löschbegehren, Richtigstellungen, Beschwerden) müssen Beschäftigte richtig reagieren und immer auf die Wichtigkeit des Datenschutzes im Unternehmen hinweisen und auf den Verantwortlichen verweisen. Das Dokument a1 enthält dazu eine Musteranweisung, die um den Namen des Datenschutzverantwortlichen ergänzt werden muss. Das Dokument a2 enthält einen Mustertext, der ev übergeben werden kann bzw am Telefon mitgeteilt werden kann.

Die weiteren Dokumente sind hauptsächlich für den Datenschutzverantwortlichen bestimmt:

- D_10b Prozess Datenschutzanfrage

Dieses Musterdokument beschreibt den Umgang mit einer Datenschutzanfrage und welche Schritte gesetzt werden müssen. Musterantwortschreiben sind in den Dokumenten D_10b1 bis D_10b3 zu finden.

- D_10c Data Breach

Im Falle eines Verlusts von personenbezogenen Daten (Hacking, Verlust von Geräten oder Speichermedien) kann es notwendig sein, dass binnen 72 Stunden nach Bekanntwerden die Behörde verständigt werden muss. Die Anforderungen an so eine Data Breach Notification sind in diesem Dokument zu finden.

- D_10d Prozess Anfragen Datenschutzbehörde

Wie wird mit Anfragen der Datenschutzbehörde umgegangen. Welche externe Hilfe steht zur Verfügung.

- D_10e Logbuch Datenschutz

Das Muster für ein einfaches Logbuch Datenschutz. Dies dient der Dokumentation von Vorgängen zum Datenschutz. Da der Behörde die getätigten Maßnahmen im Bedarfsfall nachgewiesen werden müssen ist es sinnvoll alle Tätigkeiten im Zusammenhang mit Datenschutz (Anfragen von Betroffenen und deren Bearbeitung, Schulungen, Änderungen der Verarbeitungen, etc) laufend zu dokumentieren.

<u>Schlussbemerkung</u>

Trotz dieser Beispielvorgehensweise und den Musterdokumenten muss sich jedes Handelsunternehmen noch mit dem Thema Datenschutz beschäftigen und die Vorgehensweise und die Dokumente an die eigenen Anforderungen anpassen. Mit einer strukturierten Vorgehensweise sollte es aber gelingen, die Anforderungen der DSGVO zu erfüllen.

Stand: Mai 2018

Hinweis:

Dieses Muster dient der beispielsweisen Umsetzung ist auf die Bedürfnisse des jeweiligen Unternehmens individuell anzupassen.

Dieses Muster wurde mit größter Sorgfalt erstellt, für die Richtigkeit, Vollständigkeit, Aktualität oder Qualität des bereitgestellten Musters können wir jedoch keine Gewähr übernehmen. Haftungsansprüche gegen Personen, welche dieses Muster erstellt haben, sind daher ausgeschlossen.