Titel:	DSGVO – Anpassungsempfehlung zur Umsetzung	
Thema:	Technische und organisatorische Maßnahmen, sowie Handlungsempfehlungen zur selbständigen Erfassung der internen Datenverwendungsprozesse und/oder Korrektur des Verzeichnisses der Verarbeitungstätigkeiten	
Version / Datum	1.0	21.05.2018
Verfasser & CO:	DI Harald SCHENNER	
Zielgruppe:	Wirtschaftskammer Steiermark, FG 709	Versicherungsmakler

Inhaltsverzeichnis

1 PRÄAMBEL 4

1.1 STATUS 4
1.2 INHALTE 4

2 GRUNDLAGEN DER DSGVO 6

2.1 RECHTMÄßIGKEIT DER VERARBEITUNG 6
2.2 TRANSPARENZ 7
2.3 ZWECKBINDUNG 9
2.4 DATENMINIMIERUNG 9
2.5 SPEICHERBEGRENZUNG 9
2.6 DATENSICHERHEIT 9

3 VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN 11

3.1 STAMMDATEN 11
3.2 STATUS 11
3.3 LOGBUCH 11
3.4 VERARBEITUNGSTÄTIGKEIT 12
3.4.1 Rechtmäßigkeit 12
3.4.2 Datenerhebung 12
3.4.3 Betroffene Personengruppe 12
3.4.4 Verwendete Datenarten 13
3.4.5 Datenweitergabe an externe Empfänger 13
3.4.6 Drittstaaten-Empfänger 13
3.4.7 Übermittlungssystem Eingang/Ausgang 13
3.4.8 Mittel der Verarbeitung 13
3.4.9 Zweck der Verarbeitung 13
3.4.10 Zugriffsberechtigungen 14
3.5 ANWENDUNGEN 14
3.6 ORGANISATORISCHE MAßNAHMEN 14
3.7 TECHNISCHE MAßNAHMEN 14

4 WESENTLICHE UMSETZUNGSMAßNAHMEN 15

4.1 AUFBEWAHRUNGSFRISTEN 15
4.2 VERTRÄGE MIT AUFTRAGSVERARBEITER UND MITARBEITER 15
4.3 SCHULUNGEN 15
4.3.1 Clear-Desk 15
4.3.2 Informationspflichten und Einwilligungen 16
4.3.3 Verschwiegenheit 16
4.3.4 Passwort-Verwaltung 16
4.4 ALLGEMEINER UMGANG MIT DATENSYSTEMEN 16
4.4.1 Website 16
4.4.2 Foto-Berichterstattung 16

4.4.3 eMail-Versand *17*
4.4.4 Daten- und Aktentransporte *17*
4.4.5 Aushang im Betrieb *17*

5 LEITFADEN 18

5.1 DIE 10 STUFEN ZUR UMSETZUNG 18
5.2 DIE 8 WS ZUR DSGVO 19

6 DISCLAIMER UND VERWENDUNGSHINWEISE 20

1 Präambel

Das gegenständliche Dokument enthält grundlegende Handlungs- Umsetzungs- und Korrekturempfehlungen in technischem und organisatorischem Hinblick bezüglich Umsetzung der Vorgaben der DSGVO (Datenschutzgrundverordnung) und des DSG (idF. Datenschutz-Anpassungsgesetz 2018). Das Dokument stellt keine Rechtsberatung, sondern die Sichtweise der Unternehmensberatung zur Thematik dar.

Zu Beginn werden die wesentlichen Artikel der DSGVO zitiert, um die Grundlage für eigene Entscheidungen zu liefern.

1.1 Status

Ein Muster-Verzeichnis der Verarbeitungstätigkeiten wurde mit mehreren Muster-Betrieben erstellt. Dabei wurden die wesentlichen Verarbeitungstätigkeiten erfasst und dokumentiert. Weiters wurden generelle technische und organisatorische Maßnahmen erfasst und dokumentiert.

1.2 Inhalte

Folgende Unterlagen erhalten Sie in diesem Paket:

01_Begleitdokument_Allg.pdf	Begleitdokument & Grundlagen DSGVO
02_VdV_709_VersMak_fin.xlsx	Verzeichnis der Verarbeitungstätigkeiten (VdV) Muster der Dokumentation
03_Datenschutzrichtlinie.docx	Muster zur Informationspflicht nach Art. 13 zur Vervollständigung und rechtl. Prüfung
04_TOM-Check.pdf	Checkliste der techn. & organ. Maßnahmen IST-/SOLL-Zustandes
05_dsgvo-canvas.pdf	Vorlage zur Schnellerfassung einer Verarbeitungstätigkeit
05a_App-A_Datenarten.pdf	Info zu den Datenarten und sensiblen Daten
05b_App-B_Datensicherheit.pdf	Maßnahmen zur Datenschutz-Verbesserung
05c_Verarbeitungstaetigkeit_v2.docx	Vorlage zur umfassenden Erfassung einer Verarbeitungstätigkeit inkl. Erklärungen
06a_Geheimhaltungsverpflichtung_vorlage_ma.docx	Geheimhaltungsverpflichtung für Mitarbeiter

06b_Geheimhaltungsverpflichtung_vorlage_firma.docx
Geheimhaltungsverpflichtung für externe Firmen

07_ChecklisteTKG.pdf Checkliste Telekommunikationsgesetz

08_Auftragsverarbeitervertrag_it.docx
Auftragsverarbeitungsvertrag mit IT-Dienstleistungsunternehmen

09_muster-auftragsverarbeiter.docx genereller Auftragsverarbeitungsvertrag

Einwilligungen:

10a_muster-einwilligung_fotonutzungMA.docx

10b_Musterformular_Erlaubnis_Evidenzhaltung_Bewerberdaten.docx

Diverse Muster-Schreiben:

11a_MusterformularAntwortAuskunftsbegehren.doc

11b_MusterformularAntwortAuskunftsbegehrenUnbekannt.doc

12a_Musterformular_Antwortschreiben_Loeschbegehren.docx

12b_Musterformular_BestaetigungDatenloeschung.docx

2 Grundlagen der DSGVO

Gemäß Art. 5 DSGVO muss die Verarbeitung personenbezogener Daten den folgenden Grundsätzen entsprechen: ***Rechtmäßigkeit – Transparenz – Treu und Glauben, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Datensicherheit (Integrität und Vertraulichkeit), Rechenschaftspflicht***.

2.1 Rechtmäßigkeit der Verarbeitung

Als Verarbeitung gilt vereinfacht nicht nur das Erheben und erstmalige Speichern der Daten, sondern auch die Dauer der Speicherung, das Auslesen und das Vernichten von Daten. Es ist wesentlich, die Rechtmäßigkeit der Verarbeitung zu prüfen!

Art. 6 DSGVO:

1. Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur **Durchführung vorvertraglicher Maßnahmen** erforderlich, die auf Antrag der betroffenen Person erfolgen;

c) die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um **lebenswichtige Interessen der betroffenen Person** oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die **Wahrnehmung einer Aufgabe** erforderlich, die im **öffentlichen Interesse** liegt oder in **Ausübung öffentlicher Gewalt** erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen,

insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

In den meisten Fällen wird die Rechtmäßigkeit auf lit. b oder lit. c beruhen. Auch, was die Aufbewahrungspflichten und somit die Mindestspeicherung der entsprechenden Daten anbelangt (Aufbewahrungspflicht gem. Bundesabgabenordnung [Steuerrecht] 7 Jahre für Buchhaltungsunterlagen, in denen auch Kundendaten vorliegen werden). Zudem können Sie auch eine Begründung für die Verarbeitung nach lit. f anführen, die Sie gegen die Rechte der Betroffenen abwägen müssen. Greifen Sie hierbei auf einen Rechtsbeistand zurück, der Ihnen bei dieser Abwägung behilflich sein kann.

Eine Liste der Aufbewahrungspflichten finden Sie auf der Webseite der Wirtschaftskammer Österreich unter:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html
(Stand 21.05.2018)

2.2 Transparenz

Gemäß der zu wahrenden Transparenz haben Sie Ihre betroffenen Personen (Kunden, Mitarbeiter, Bewerber, Praktikanten, Lieferanten, ...) darüber zu informieren, welche Daten Sie zu welchem Zweck und unter welcher Rechtsgrundlage verarbeiten und wem (welchen Empfängern) diese Daten offengelegt (weitergegeben) werden.

Art. 13 DSGVO:

1. Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den **Namen und die Kontaktdaten des Verantwortlichen** sowie gegebenenfalls seines Vertreters;

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

c) **die Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage für die Verarbeitung**;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die **berechtigten Interessen**, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

e) gegebenenfalls die **Empfänger oder Kategorien von Empfängern** der personenbezogenen Daten und

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen **Daten an ein Drittland oder eine internationale Organisation zu übermitteln**, sowie das **Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses** der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

2. Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die **Dauer**, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) das **Bestehen eines Rechts auf Auskunft** seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf **Berichtigung oder Löschung** oder auf **Einschränkung** der Verarbeitung oder eines **Widerspruchsrechts** gegen die Verarbeitung sowie des Rechts auf **Datenübertragbarkeit**;

c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

f) das **Bestehen einer automatisierten Entscheidungsfindung** einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

3. Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

4. Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

2.3 Zweckbindung

Die Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden.

2.4 Datenminimierung

Verarbeiten Sie nur Daten, die dem Zweck angemessen und erheblich sowie auf das für den Zweck notwendige Maß beschränkt sind. Unterlassen Sie die Verarbeitung von Daten, die Sie nicht unbedingt für den Zweck der Verarbeitung benötigen!

2.5 Speicherbegrenzung

Die personenbezogenen Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Die Rechtmäßigkeit der Datenspeicherung ergibt sich für Ihre Branche meist aus lit b (Vertragserfüllung), lit c (rechtliche Verpflichtung), lit f (berechtigtes Interesse des Verantwortlichen) oder schlussendlich aus lit a (Einwilligung) – beachten Sie dazu den Punkt 2.1 (Rechtmäßigkeit der Verarbeitung). Beachten Sie dazu auch unbedingt die Aufbewahrungspflichten, denen Sie aus anderen gesetzlichen Bestimmungen unterliegen.

2.6 Datensicherheit

Alle Daten, insbesondere Daten mit möglichen Folgen für die Betroffenen oder Dritte (speziell sensible Daten der besonderen Datenkategorie nach Art. 9 und strafrechtliche Daten nach Art. 10 DSGVO sowie Daten, die den

sozialen Status der betroffenen Person herabsetzen könnten), müssen entsprechend geschützt werden.

Dies betrifft nicht nur, aber vor allem:

- Personaldaten, Bewerberdaten
- Sensible Aufzeichnungen von Kunden
    - Gesundheitsdaten (Gesundheitsfragen, Diagnosen, Befunde, Arztrechnungen, ...)
    - Vollmachten
    - Darstellung wirtschaftlicher Verhältnisse (Haushaltsrechnung, Vermögenswerte, Belastungen, etwaige Exekutionen bei Gehaltsnachweisen, ...)

Die minimalen Anforderungen bzw. Ihre Erhebung des IST-Zustandes finden Sie in beiliegenden Dokumenten.

3 Verzeichnis der Verarbeitungstätigkeiten

Das Muster-Verzeichnis der Verarbeitungstätigkeiten (02_VdV_709_VersMak_fin.xlsx) ist bereits auf Basis von Betriebsinterviews und System-Analysen mehrerer Musterbetriebe erstellt worden. Etwaige zusätzliche/abweichende Dienstleistungen, die Sie als Betrieb anbieten – und nicht im Verzeichnis angeführt sind – sind individuell zu ergänzen, bzw. entsprechend die Abweichungen zu korrigieren.

Generell müssen Sie das Verzeichnis sichten und auf Korrektheit und Vollständigkeit prüfen. Die Vorlage dient als Muster (inkl. der wesentlichen Verarbeitungstätigkeiten der Branche). **Erst durch diese Prüfung und Ergänzung können Sie den Bestimmungen der DSGVO entsprechen!**

Weiters können Sie mittels TOM-Check (04_TOM-Check.docx) den bestehenden IST-Zustand der technischen und organisatorischen Maßnahmen (TOMs) Ihres Betriebes erfassen und mit dem Mindest-SOLL-Zustand vergleichen.

Der Mindest-SOLL-Zustand soll den minimalen – und jedenfalls nicht vollständigen – Stand der Technik darstellen.

Die einzelnen Registerblätter des Excel-Dokuments werden nachfolgend näher erläutert:

3.1 Stammdaten

Geben Sie hier Ihre Kontaktdaten und die Daten des für alle Anfragen bezüglich Datenschutz zuständigen Mitarbeiters (sofern dies nicht durch den Inhaber des Unternehmens wahrgenommen wird) ein.

3.2 Status

Geben Sie den Status des Dokuments an (Erstellung, Aktualisierung, Version, ...).

3.3 Logbuch

Das Logbuch dient dazu, sämtliche Anfragen zu den Betroffenenrechten protokollieren zu können. Dies ist vor allem wichtig, um zum einen die Beweisführung zu sichern, zum anderen etwaige Löschungen von

Datensätzen bei Rückspielen eines Backups noch einmal vornehmen zu können.

Weiters werden hier etwaige Datenschutz-Verstöße protokolliert.

3.4 Verarbeitungstätigkeit

Hier befindet sich die Dokumentation der Verarbeitungstätigkeiten. Es ist unterteilt in die einzelnen Bereiche (interne = Personalverwaltung; externe = Kundenbetreuung, Auftragswesen; Auftragsverarbeitung = im Auftrag des Vertragspartners [Leasing, Versicherung, ...]).

Jede Zeile in der Liste entspricht einer Verarbeitungstätigkeit. Dabei sind die zutreffenden Daten in den nach rechts folgenden Spalten entsprechend angekreuzt:

„x" die entsprechende Spalte trifft (wahrscheinlich) für die Zeile zu

„?" die entsprechende Spalte kann zutreffen

„(x)" trifft unter Umständen (wahrscheinlich) zu

3.4.1 Rechtmäßigkeit

Sehen Sie dazu den Punkt 2.1 (Rechtmäßigkeit der Verarbeitung)

3.4.2 Datenerhebung

Wurden die Daten direkt von der betroffenen Person erhoben, oder haben Sie diese über Dritte übermittelt bekommen. Der Unterschied liegt in der Informationspflicht! Bei direkter Erhebung müssen Sie die Information zugänglich machen, wie Sie die Daten verarbeiten (siehe Punkt 2.2 Transparenz).

Haben Sie die Daten von Dritten erhalten, so haben Sie die Informationspflicht nach Art. 14 DSGVO zu wahren, indem Sie ehestmöglich, spätestens jedoch innerhalb eines Monats die betroffene Person davon in Kenntnis setzen, dass Sie in den Besitz der Daten gelangt sind und von wem Sie diese erhalten haben. Zusätzlich sind die Informationen der unter Punkt 2.2 (Transparenz) genannten Datenschutzrichtlinie zugänglich zu machen.

3.4.3 Betroffene Personengruppe

Hier geben Sie an, welche Personengruppe die von der jeweiligen Verarbeitungstätigkeit betroffene Gruppe ist. Fehlt eine Gruppe, so fügen Sie diese einfach ein (Spalte einfügen).

3.4.4 Verwendete Datenarten

Hier werden die verwendeten Datenarten (inkl. besondere Datenkategorien = sensible Daten = rot gekennzeichnet) angegeben. Generell gilt speziell hier: fehlt Ihnen eine Datenart, so fügen Sie einfach eine Spalte hinzu und geben Sie diese entsprechend ein.

Nähere Informationen zu den Datenarten finden Sie im beiliegenden Dokument „05a_App-A_Datenarten.pdf".

3.4.5 Datenweitergabe an externe Empfänger

Geben Sie hier die Empfänger (Dritte) der Daten an. Geben Sie auch die dafür zugrundeliegende Rechtmäßigkeit an.

3.4.6 Drittstaaten-Empfänger

Werden die Daten außerhalb der EU weitergegeben, so fügen Sie dies in dieser Spalte an.

3.4.7 Übermittlungssystem Eingang/Ausgang

Das Übermittlungssystem ist genau zu evaluieren: werden sensible Daten (rote Datenarten) in entsprechender sicherer Art und Weise übertragen/übermittelt? Ein eMail gilt nicht als sicheres Übertragungsmedium, es sei denn, es ist verschlüsselt. Alternativ kann auch der Dateianhang verschlüsselt werden.

3.4.8 Mittel der Verarbeitung

Die Mittel der Verarbeitung sind unter diesem Spaltenblock anzugeben. Auch hier gilt: Fügen Sie hinzu, was Ihnen fehlt!

Die Liste der Verarbeitungs-Mittel oder Verarbeitungssysteme ergibt auch eine schöne Übersicht, mit welchen Ihrer Software-Anbieter Sie eventuell einen Auftragsverarbeitungsvertrag benötigen (immer dann, wenn der Anbieter entweder direkten Zugriff auf die Daten Ihrer betroffenen Personen hat oder diese direkt verarbeitet).

3.4.9 Zweck der Verarbeitung

Geben Sie hier den Zweck der Verarbeitung an. Aus dem Punkt 2.3 (Zweckbindung) wissen Sie, dass der Zweck entsprechend definiert sein muss und gem. Informationspflicht an die betroffenen Personen kommuniziert werden muss.

3.4.10 Zugriffsberechtigungen

Dokumentieren Sie, wer in Ihrem Unternehmen auf welche Datensysteme Zugriff hat – denken Sie hierbei nicht nur an die Berechtigungsrollen der EDV (fragen Sie dazu Ihren IT-Dienstleister), sondern auch um die Zugänge zu analogen Datenhaltungssysteme (Personalordner, Auftragsordner).

Allgemein gilt: nur wer die Daten zur Bearbeitung im Unternehmen tatsächlich benötigt, soll entsprechenden Zugang erhalten!

3.5 Anwendungen

Listen Sie genau die verwendeten Anwendungen und Software-Programme auf. Mit allen Dienstleistern, die Zugang auf Ihre Systeme oder Daten haben (Cloud-Anbieter, Branchen-Software-Lösung, IT-System, ...) sind entsprechende Auftragsverarbeiter-Verträge zu schließen. Ein Muster der WKÖ liegt bei.

3.6 Organisatorische Maßnahmen

Bitte gehen Sie jeden Punkt der organisatorischen Maßnahmen durch und prüfen Sie, ob diese in Ihrem Unternehmen bereits umgesetzt sind.

Zudem nehmen Sie die Checkliste 04_TOM-Check.pdf zur Hand und gehen Sie alle Bereiche zur Feststellung Ihres Status Quo durch.

3.7 Technische Maßnahmen

Bitte gehen Sie jeden Punkt der technischen Maßnahmen durch und prüfen Sie, ob diese in Ihrem Unternehmen bereits umgesetzt sind.

Zudem nehmen Sie die Checkliste 04_TOM-Check.pdf zur Hand und gehen Sie alle Bereiche zur Feststellung Ihres Status Quo durch.

4 Wesentliche Umsetzungsmaßnahmen

Nachfolgend sind die wichtigsten Punkte der technischen und organisatorischen Maßnahmen angeführt.

4.1 Aufbewahrungsfristen

Beachten Sie grundlegend die Aufbewahrungsfristen, die seitens des Gesetzgebers vorgegeben werden – insbesonders in Hinblick auf Rechnungen, Lohnverrechnungsunterlagen, Protokolle, Meldungen, Gutachten udgl.

4.2 Verträge mit Auftragsverarbeiter und Mitarbeiter

Vereinbaren Sie entsprechende Auftragsverarbeiterverträge mit Ihren externen Dienstleistern! Dies umfasst neben den IT-Dienstleistern und Software-Anbietern auch jedenfalls extern beauftragte Reinigungsfirmen (da diese zu allen Bereichen Ihres Unternehmens entsprechende Zutrittsberechtigungen genießen). Denken Sie in diesem Zusammenhang vor allem auch auf Ihre Büro-Datenablage, sodass sensible Daten vor Einsichtnahme verschlossen bleiben.

Ein entsprechendes Vertragsmuster der Wirtschaftskammer Österreich liegt bei.

Vereinbaren Sie geeignete Verschwiegenheitsverpflichtungen mit Ihren Mitarbeitern, damit auch diese sich um geeignete Schutzmechanismen kümmern und in die Verantwortung in Hinblick auf den Datenschutz eingebunden werden.

Eine entsprechende Vorlage der Wirtschaftskammer Österreich liegt bei.

4.3 Schulungen

Schulen Sie Ihre Mitarbeiter im Umgang mit den Datenschutz-Vorgaben. Darin sollten vor allem nachfolgende Inhalte besprochen werden:

4.3.1 Clear-Desk

Die Schreibtische der Mitarbeiter, die direkt mit Kunden in Kontakt kommen, sollten keine offen einsehbare Unterlagen aufliegen haben. Die Bildschirme der Mitarbeiter sollen nicht von Kunden einsehbar sein, speziell zu jenen Zeiten, in denen Fremddaten (also von anderen Kunden oder anderen betroffenen Personen) verarbeitet oder angezeigt werden.

4.3.2 Informationspflichten und Einwilligungen

Schulen Sie Ihre Mitarbeiter, wann eine Informationspflicht vorgeschrieben ist und wie diese durchzuführen ist. Schulen Sie Ihre Mitarbeiter auch, wann sie eine Einverständniserklärung von den Kunden einholen müssen.

4.3.3 Verschwiegenheit

Schulen Sie Ihre Mitarbeiter, was genau unter die Verschwiegenheit fällt, welche Informationen über Telefon oder eMail weitergegeben werden dürfen und welche Daten beim Versand über eMail verschlüsselt werden müssen. Lassen Sie Verträge bzw. Vereinbarungen dazu unterzeichnen.

4.3.4 Passwort-Verwaltung

Schulen Sie Ihre Mitarbeiter im Umgang mit Ihren Passwörtern bzw. Benutzer-Zugängen. Diese dürfen nicht einsehbar gelagert werden. Achten Sie vor allem darauf, dass die Passwörter nicht an den PCs oder Bildschirmen oder auf dem Schreibtisch öffentlich zugänglich sind!

4.4 Allgemeiner Umgang mit Datensystemen

Prüfen Sie Ihre Aktenverwahrung insbesonders in Hinblick auf notwendige Zugriffskontrollen. Verwahren Sie sensible Daten in versperrbaren Aktenschränken.

Vernichten Sie zusätzliche Papier-Kopien sämtlicher operativ verwendeter Daten, wenn Sie diese Daten zur operativen Bearbeitung nicht mehr benötigen! Die Originale sichern Sie gemäß etwaiger Aufbewahrungspflichten.

Als Aktenvernichter gilt für sensible Daten aus aktueller Sicht ein so genannter „Kreuzschnitt-Aktenvernichter", der das Papier nicht nur in Streifen, sondern in kleine Schnipsel zerteilt.

4.4.1 Website

Werden Mitarbeiter auf der eigenen Website angeführt (Namen, Kontaktdaten, Foto), so ist die Einwilligung des Mitarbeiters einzuholen!

Ebenfalls gilt dies, wenn Sie diese Daten auf anderen Portalen hinterlegen oder an anderer Stelle veröffentlichen (Social-Media, ...).

4.4.2 Foto-Berichterstattung

Achten Sie bei jedwelcher Bilderfassung (Fotos von Mitarbeiter, von Kunden, ...) unbedingt darauf, dass Sie die Einwilligung der auf den Bildern gezeigten

Personen einholen, um das Bild zu speichern und vor allem, wenn Sie dieses veröffentlichen werden/wollen!

Dies gilt gleichermaßen auch für den Aushang im Betrieb, Presseaussendungen, Social-Media-Plattformen, ...

4.4.3 eMail-Versand

Werden personenbezogene Daten per eMail versendet, so ist das geeignete Schutzniveau auf Basis der versendeten Daten zu prüfen. Lohnverrechnungsunterlagen, Krankenstandsbestätigungen, Versicherungsverträge oder andere Verträge, Führerschein- oder Reisepasskopien und dergleichen sollten verschlüsselt (als PDF mit Passwort-Schutz oder in einem ZIP-Archiv mit Passwortschutz) übermittelt werden. Fragen Sie dazu Ihren IT-Dienstleister, welche Programme Sie sehr effizient und praktikabel verwenden können.

Zur Erklärung: Ein normales eMail ist mit einer Postkarte zu vergleichen, die von jedermann eingesehen und gelesen werden kann. Prüfen Sie anhand der Analogie zu einer Postkarte, welche Informationen Sie „einsehbar" oder eben „nicht einsehbar" per eMail versenden sollten!

4.4.4 Daten- und Aktentransporte

Achten Sie beim Datentransport (digitale Speichermedien oder Aktenordner für Buchhaltung, Steuerberatung, Abgabe an Behörden oder Gerichte, ...) auf eine sichere Verwahrung sensibler Daten. Ein zugänglich abgelegter Ordner im Fahrzeug eines Mitarbeiters gilt nicht als zuverlässig vor unberechtigtem Zugriff verwahrt. Gehen Sie damit ebenso sorgfältig um, wie Sie auch andere Wertsachen im Fahrzeug verwahren würden (optisch nicht frei einsehbar, versperrt, ...).

4.4.5 Aushang im Betrieb

Zu Ihrer Erleichterung können Sie Ihrer Informationspflicht auch an geeigneter Stelle mittels öffentlichem Aushang der entsprechenden Information im Betrieb nachkommen.

5 Leitfaden

Prüfen Sie, ob Sie alle notwendigen Maßnahmen umgesetzt haben.

5.1 Die 10 Stufen zur Umsetzung

To-Do	erledigt
Feststellung IST-Zustand	
Bestellung Datenschutzbeauftragter ja/nein	
Dokumentation der Verarbeitungsvorgänge	
Datenschutz-Folgenabschätzung	
Meldung von Verstößen	
Verträge mit Auftragsverarbeitern	
Formulare prüfen und anpassen	
Informationspflichten / Betroffenenrechte	
Sicherheitsmaßnahmen	
Mitarbeiterschulungen	

5.2 Die 8 Ws zur DSGVO

WER	•(wer als Verantwortlicher benannt wird)
WAS	•(welche Daten-Kategorien erfasst werden)
WO	•(Daten gespeichert und verarbeitet werden – betroffene Systeme,)
WARUM	•(was ist der Rechtsgrund, der zur Anwendung kommt)
WOZU	•(Zweck der jeweiligen Datenverarbeitung)
WOHIN	•(wenn Daten weitergegeben werden - an wen werden die Daten übergeben, auch ob innerhalb der EU oder Drittland)
WIE LANGE	•(werden Daten gespeichert – welche Löschfristen kommen zur Anwendung)
WIE SICHER	•(welche Datensicherheitsmaßnahmen werden ergriffen).

6 DISCLAIMER und Verwendungshinweise

Der Autor weist ausdrücklich darauf hin, dass die hier vorliegende Unterlage nach Treu und Glauben angefertigt und im Wesen den Inhalt der aktuellen Gesetzgebung wiedergibt, jedoch keine juristische Beratung durch einen eingetragenen Rechtsanwalt ersetzt.

Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung, ist ausschließlich dem Autor vorbehalten. Kein Teil dieser Unterlage darf in irgendeiner Form (durch Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung des Autors reproduziert oder unter Verwendung elektronischer oder nicht-elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Ausnahme: Die uneingeschränkte Selbst-Nutzung dieser Unterlage ist den Mitgliedsbetrieben der Fachgruppe 709 (Versicherungsmakler und Berater in Versicherungsangelegenheiten) der Wirtschaftskammer Steiermark ausdrücklich erlaubt.

Sie erreichen den Autor unter der www.derSchenner.at oder unter der Projektseite www.dsgvo2018.at.

CERTIFIED DATA & IT SECURITY EXPERT CMC GEPRÜFTER DATENSCHUTZEXPERTE CERTIFIED DIGITAL CONSULTANT

WIR NEHMEN **WISSEN** IN BETRIEB.