DER SCHENNER
Consulting & Training

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	30.03.2018
Verfasser & CO:	DI Harald SCHENNER	DI Gerald KORTSCHAK
Zielgruppe:	FG Buch & Medienwirtschaft WK STMK	

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

Inhaltsverzeichnis

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

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.

1.1 Status

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

1.2 Grundlagen der DSGVO

Transparenz, Datenminimierung, Speicherminimierung, Datensicherheit

Achten Sie generell darauf, sämtliche Daten nur für die notwendige Dauer zu speichern. Speziell Daten mit möglichen Folgen für die Betroffenen oder Dritte müssen entsprechend geschützt und auf die notwendige Speicherdauer reduziert werden.

Dies betrifft vor allem:

- Personaldaten, Bewerberdaten
- Sensible Aufzeichnungen von Kunden, Anamnese-Daten, Befunde, Diagnosen

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

2 Umgang mit den Unterlagen

Das Muster-Verzeichnis der Verarbeitungstätigkeiten ist bereits auf einen Betrieb der Branche abgestimmt. Etwaige zusätzliche Dienstleistungen, die Sie als Betrieb anbieten – und nicht im Verzeichnis angeführt sind – sind individuell zu ergänzen, bzw. 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!

2.1 Inhalt des Verzeichnisses

Das Verzeichnis der Verarbeitungstätigkeiten (VdV als Excel) beinhaltet folgende Karteireiter mit den entsprechenden Informationen, die geprüft, ergänzt oder überhaupt erst ausgefüllt werden müssen:

2.1.1 Stammdaten

Geben Sie hier Ihre Kontaktdaten ein.

2.1.2 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 Rückspielung eines Backups noch einmal vornehmen zu können.

2.1.3 Verarbeitungen

Hier befindet sich die Dokumentation der Verarbeitungstätigkeiten. Es ist unterteilt in interne (Mitarbeiter, Bewerber, ...) Aufgaben und Tätigkeiten, sowie in externe (gegenüber den Angehörigen, der Behörde) Aufgaben unterteilt.

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

entsprechend angekreuzt (das „x“ in der Zelle bedeutet, dass die entsprechende Spalte für die entsprechende Zeile zutrifft).

2.1.4 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.

2.1.5 Behörden-Anwendungen

Listen Sie hier jene Anwendungen auf, die Ihnen seitens der Behörde mit dem Auftrag der expliziten und exklusiven Nutzung zur Verfügung gestellt werden (Einreichungen für Protokolle, Urkunden, Abrechnungen bei Sozialversicherungsträgern, ...).

2.1.6 Organisatorische Maßnahmen intern / extern

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

2.1.7 Technische Maßnahmen

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

2.1.8 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!

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

3 Allgemeine Informationen zur DSGVO

Nachfolgend sind die wichtigsten Punkte der technischen und organisatorischen Maßnahmen angeführt. Achten Sie jedoch auch auf die Registerkarten „Organisatorische Maßnahmen intern / extern“ und „Technische Maßnahmen“ im Excel-Muster.

3.1 Rechtmäßigkeit der Datenverarbeitung

Prüfen Sie die Rechtmäßigkeit der Datenverarbeitung nach den nachfolgend für Sie wesentlichen Kriterien. Zumindest eine davon muss erfüllt sein:

- Notwendig zur Vertragserfüllung oder vorvertraglicher Maßnahmen (Angebot, Bewerbung, ...)
- Gesetzlich vorgeschrieben (Lohnverrechnung, Rechnungslegung)
- Wahrnehmung einer Aufgabe im öffentlichen Interesse, oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde
- Schutz der lebenswichtigen Interessen der betroffenen Person oder einer anderen natürlichen Person
- Zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen)
- Einwilligung der betroffenen Person liegt vor

Jedenfalls ist die betroffene Person immer über die Verwendung ihrer Daten zu unterrichten (zu informieren). Mindestgehalt dieser Information ist, welche Daten konkret zu welchem Zwecke verarbeitet und weitergegeben werden (Muster liegt bei).

3.2 Weitergabe von Daten an Dritte

Bei Weitergabe der Daten an Dritte ist jedenfalls auch die Rechtmäßigkeit zu überprüfen. Achten Sie dabei auch unbedingt an die „Datenminimierung“, sodass nur unbedingt notwendige Daten weitergegeben werden. Holen Sie sich die Zustimmung ein, um Daten von

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

beteiligten Personen (Lieferanten, Subunternehmen, Kooperationspartnern, ...) an die Kunden weitergeben zu dürfen! Gegebenenfalls benötigen Sie die Einwilligung Ihrer Kunden zur Datenweitergabe der Kundendaten an einen Dritten (Weitergabe an Lieferanten, Subunternehmen, Kooperationspartner, ...).

3.3 Aufbewahrungsfristen

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

3.4 Verträge mit Auftragsverarbeiter und Mitarbeiter

Vereinbaren Sie entsprechende Auftragsverarbeiterverträge mit Ihren externen Dienstleistern! Dies umfasst neben den IT-Dienstleistern (mit Wartungsverträgen / lfd Betreuung) und Software-Anbietern auch eventuell extern beauftragte Reinigungsfirmen (da diese zu allen Bereichen Ihres Unternehmens entsprechende Zutrittsberechtigungen genießen und somit in Daten einsehen können). 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.

Bewahren Sie alle Verträge, Geheimhaltungsvereinbarungen und Einwilligungen für den Fall einer Beweisführung auf!

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

3.5 Schulungen

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

3.5.1 Clear-Desktop

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. Dies ist ebenso durch organisatorische Maßnahmen umsetzbar, indem Sie darauf achten, dass keine Dritten Einsicht in Unterlagen bekommen. Beispielsweise Datenblätter umdrehen oder anderweitig die Einsicht verhindern.

3.5.2 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.

3.5.3 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.

3.5.4 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!

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

3.6 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.

3.6.1 Terminkalender

Bewahren Sie Ihren Terminkalender so auf, dass Kunden oder andere externe (nicht zum Betrieb gehörende) Personengruppen darauf keine Einsichtnahme vornehmen können. Suchen Sie dafür eine geeignete Stelle (Lade oder Fach beim Tresen/Empfang, ...) aus, damit Sie in der operativen Arbeit nicht beeinträchtigt werden.

3.6.2 Kundenkartei (Papier)

Verwahren Sie die Kundenkartei ebenfalls nicht für Kunden einsehbar. Befinden sich sensible Daten (Befunde, Diagnosen, Anamnese-Blätter, Gesundheitsinformationen, Allergien, ...) in der Kundenkartei, so ist diese unbedingt versperrt aufzubewahren!

3.6.3 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, ...).

3.6.4 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, ...

3.6.5 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!

3.6.6 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, ...).

3.6.7 Aushang im Betrieb

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

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

4 Leitfaden

Prüfen Sie, ob Sie alle notwendigen Maßnahmen umgesetzt haben.

4.1 Die 10 Stufen zur Umsetzung

To-Do	erledit
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	

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

4.2 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).

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

4.3 Datenschutz-Checkliste

Datenschutzaudit: Checkliste für Unternehmen	Erledigt?	
Organisationskontrolle	Ja	Nein
... Datenschutzbeauftragter vorhanden	❍	❍
... Mitarbeiter zum Datengeheimnis nach verpflichtet?	❍	❍
... Mitarbeiterschulung zum Datenschutz erfolgt?	❍	❍
... Datenschutzkonzept erarbeitet?	❍	❍
Zutrittskontrolle	Ja	Nein
... Zutritt zum Gebäude beschränkt?	❍	❍
... Rechnerräume nur für befugtes Personal zugänglich?	❍	❍
... Server sicher aufgestellt?	❍	❍

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

Datenschutzaudit: Checkliste für Unternehmen		Erledigt?
... Zutritt zu Räumen beschränkt, in denen Datenmaterial verwahrt wird (Akten, Datenträger)?	❍	❍
Zugangskontrolle	Ja	Nein
... Bildschirmsperren eingerichtet?	❍	❍
... Firewall installiert, aktiviert, aktualisiert?	❍	❍
... Software zum Schutz vor Schadsoftware installiert, aktiviert und aktualisiert?	❍	❍
... Benutzeridentifikation/Authentifizierung eingerichtet?	❍	❍
... sichere Passwörter?	❍	❍
Zugriffskontrolle	Ja	Nein
... Konzept für Zugriffsberechtigungen liegt vor?	❍	❍

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

Datenschutzaudit: Checkliste für Unternehmen		Erledigt?
... unterschiedliche Zugriffsrechte eingeteilt?	❍	❍
... Verletzungen werden protokolliert?	❍	❍
... Datenträger/Datenblätter werden sicher entsorgt?	❍	❍
... Kopierschutz/Bearbeitungsschutz eingerichtet?	❍	❍
Weitergabekontrolle	Ja	Nein
... Datenverschlüsselung eingerichtet und aktiv?	❍	❍
... regelmäßige Wartung und Prüfung der Datenverarbeitungssysteme?	❍	❍
... veraltetes Equipment sicher entsorgt?	❍	❍
... Beschränkung bei Nutzung von privatem Equipment?	❍	❍

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

Datenschutzaudit: Checkliste für Unternehmen	Erledigt?	
Eingabekontrolle	Ja	Nein
... Protokollierung von Erhebungen, Änderungen und Löschung?	❍	❍
... Protokollierung von Verwaltungsakten?	❍	❍
Auftragskontrolle	Ja	Nein
... Auftragsannahme sicher?	❍	❍
... Konfliktmanagement bei Verstößen/Verdachtsfällen installiert?	❍	❍
... Mechanismen zur Selbstkontrolle auf Seiten des Auftragnehmers vorhanden?	❍	❍
Verfügbarkeitskontrolle	Ja	Nein
.... Daten gegen unbeabsichtigte Löschung oder Vernichtung abgesichert?	❍	❍

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

Datenschutzaudit: Checkliste für Unternehmen		Erledigt?
... Sicherungskopien vorhanden?	❍	❍
... Sicherung vor Schadsoftware vorhanden?	❍	❍
Trennungsgebot	Ja	Nein
... gemeinsam erhobene Daten getrennt voneinander verarbeitbar?	❍	❍
... personenbezogene Daten einzelner Betroffener getrennt verfügbar?	❍	❍

sevian7 IT development GmbH
Triesterstrasse 136
8020 Graz
www.sevian7.com / office@sevian7.com

5 DISCLAIMER und Verwendungshinweise

Die Autoren weisen 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.

Sie erreichen die Autoren unter der gemeinsamen Projektseite www.dsgvo2018.at.

Die Autoren sind zertifizierte Datenschutz-Experten, zertifizierte IT-Security-Experten und zertifizierte Unternehmensberater. Beide unterrichten auf Fachhochschulen und sind Trainer bei Wifi, Incite und weiteren Bildungsträgern.

CERTIFIED DATA & IT SECURITY EXPERT CMC CERTIFIED DIGITAL CONSULTANT

WIR NEHMEN **WISSEN** IN BETRIEB.