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:	Bestattungsunternehmen	

Die IT-Architekten
sevian7
e pluribus unum
>> www.sevian7.com

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

Die IT-Architekten
sevian7
e pluribus unum
>>www.sevian7.com

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

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.

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
- Todesursache des/der Verstorbenen (als Auswirkung auf lebende Angehörige)

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

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

entsprechend angekreuzt (das „x" in der Zelle bedeutet, dass die entsprechende Spalte für die entsprechende Zeile zutrifft). Bitte sehen Sie sich diesen Karteireiter zusammen mit dem Dokument „02_ErfassungVerarbeitungstätigkeit_vorlage.docx" an, da in diesem Dokument weiterführende Erklärungen enthalten sind, wie eine Verarbeitungstätigkeit zu dokumentieren ist.

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, ...).

2.1.6 Informationspflichten

Bei Erhebung der Daten oder nach Erhalt der Daten von Dritten haben Sie die betroffene Person (jene Person, um die es bei den Daten handelt) zu informieren, welche Daten, weshalb (zu welchem Zweck) in welchen Systemen verarbeitet werden. Diese Information ist der betroffenen Person zugänglich zu machen (Veröffentlichung auf der Website und Aushang im Unternehmen).

2.1.7 Organisatorische Maßnahmen intern / extern

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

2.1.8 Technische Maßnahmen

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

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

2.1.9 Individuelle technische und organisatorische Maßnahmen

Erarbeiten Sie mit Ihrem IT-Dienstleister und Ihren Mitarbeitern etwaige Verbesserungen der technischen und organisatorischen Maßnahmen, um ein besseres Sicherheitsniveau herstellen zu können. Vor allem geht es dabei um leistbare und durchführbare Maßnahmen, damit sich im tagtäglichen operativen Umfeld diese Maßnahmen auch einhalten lassen. Reine theoretische Formulierungen, die nicht gelebt werden, sind sinnlos, da diese nicht als zweckdienlich von der Behörde eingestuft werden.

2.1.10 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!

2.1.11 Folgenabschätzung

Achten Sie auf etwaige Folgen, die zwar die Verstorbenen nicht mehr betreffen (Datenschutz ist ein Persönlichkeitsrecht, das mit dem Tode erlischt), sich jedoch auf die Angehörigen auswirken können!

Beispiel Erbkrankheit als Todesursache: Der Sohn verstirbt, im Totenbeschau-Protokoll wird als Todesursache „Erbkrankheit" angegeben. Nach Bekanntwerden (öffentlich) der Todesursache wurden dem Vater sowohl die Lebensversicherung gekündigt (Begründung: falsche Angaben bei den Gesundheitsfragen) als auch der Hausbaukredit fällig gestellt (Begründung: fehlende Versicherungs-Vinkulierung).

2.1.12 Auskunftsbegehren

Vorgefertigter Mustertext für ein Auskunftsbegehren.

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

2.1.13 Löschbegehren

Vorgefertigter Mustertext für ein Löschbegehren.

Achtung: Prüfen Sie die Aufbewahrungspflichten und die Zeitvorhaltungen Ihrer Backup-Systeme, um hier korrekte Angaben machen zu können.

2.1.14 Information zu Datenarten

Information zu den Datenarten, um eine Anleitung zu haben.

2.1.15 Information zu Datensicherheit

Informationen zu Maßnahmen, um die Datensicherheit zu erhöhen. Es liegen konkrete Hilfestellungen in Bezug auf bauliche, organisatorische und technische Maßnahmen vor.

2.1.16 Hilfe zu Löschfristen

Zusatzinformation zur Definition von Regellöschfristen in Abhängigkeit der zu erfüllenden Aufbewahrungsfristen.

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", „Technische Maßnahmen" und „individuelle TOM" 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 (Versicherungsangebot, Bestattungsangebot, ...)
- Gesetzlich vorgeschrieben (Lohnverrechnung, Rechnungslegung)
- 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.

3.2 Weitergabe von Daten an Dritte

Bei Weitergabe der Daten an Dritte ist jedenfalls auch die Rechtmäßigkeit zu überprüfen. Diese kann eventuell von Bundesland zu Bundesland verschieden sein (Bestattungsverordnung ist ein Landesgesetz). Achten Sie dabei auch unbedingt an die „Datenminimierung", sodass nur unbedingt notwendige Daten weitergegeben werden. Holen Sie sich die Zustimmung ein, um Daten von beteiligten Personen (Kirchenmusik, Vorbeter, ...) an die Angehörigen weitergeben zu dürfen!

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

3.3 Aufbewahrungsfristen

Beachten Sie grundlegend die Aufbewahrungsfristen, die seitens des Gesetzgebers (Bestattungsverordnung) vorgegeben werden – insbesonders in Hinblick auf Protokolle, Meldungen, udgl.

3.4 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.

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.

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

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!

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 (wie zB. Hardcopys zu Werkstatt-Auftrag, Sterbefall-Aufnahme, ...), 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 Website

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

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

Ebenfalls gilt dies, wenn Sie diese Daten auf Parte-Portalen (wie Aspetos) hinterlegen oder an anderer Stelle veröffentlichen.

3.6.2 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, ...

3.6.3 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, Beschauprotokolle oder Todesanzeige (vor allem Urkunden mit Todesursache) 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!

3.6.4 Daten- und Aktentransporte

Achten Sie beim Datentransport (digitale Speichermedien oder Aktenordner für Buchhaltung, Steuerberatung, Abgabe an Gemeinden/Standesämter, ...) auf eine sichere Verwahrung sensibler Daten. Ein zugänglich abgelegter Ordner im Fahrzeug eines Mitarbeiters gilt nicht als zuverlässig vor unberechtigtem Zugriff verwahrt. Gehen Sie

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

damit ebenso sorgfältig um, wie Sie auch andere Wertsachen im Fahrzeug verwahren würden (optisch nicht frei einsehbar, versperrt, ...).

3.6.5 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 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.