savient.

Bis am 25. Mai 2018 müssen die betrieblichen Prozesse der EU-DatenschutzGrundVerOrdnung (DSGVO, engl. GDPR) angepasst werden.
Unter bestimmten Umständen sind auch Schweizer Unternehmen dazu verpflichtet.

Was ist im Detail zu tun? Die nachfolgende Liste zeigt es. Zu erstellende Papiere, Dokumentationen etc. sind "fett" geschrieben.
Zusätzlich finden Sie nachfolgend eine einfache Vorlage für Ihre TOMs (Technische & Organisatorische Massnahmen)

Sie dürfen diese Unterlagen gerne benutzen. Wenn Sie Fragen haben, stehen wir gerne zur Verfügung.

RA lic.iur. Marc Fischer

savient.
Industriestrasse 52
6300 Zug
+41 41 711 02 02

DSGVO-Grundlage	Aufgabe	Verantwortl.	Stand	Bemerkungen
DSGVO	Information der Führungskräfte über die bevorstehenden Änderungen			
Art. 30 Abs. 1	Relevante Verfahren zusammentragen			
Art. 30 Abs. 1	Benennung Verarbeitungsverantwortliche & Stellvertreter			
Art. 30 Abs. 1	Erstellung **Verarbeitungsverzeichnis** durch den Verarbeitungsverantwortlichen			
Art. 30 Abs. 1	Relevante **TOMs** (Technische und Organisatorische Massnahmen) für Verarbeitung zusammentragen			
Art. 30 Abs. 2	Auftragsverarbeiter über ihre Pflicht zur Verzeichnisführung unterrichten			
Art. 30 Abs. 2	Auftragsverarbeiter zur Übermittlung ihrer Verzeichnisse auffordern			
Art. 32 Abs. 1 Pkt. A	**Dokumentation Verschlüsselung** personenbezogene Daten			
Art. 32 Abs. 1 Pkt. B	**Dokumentation Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste mit dauerhaften Verfahren**			

Art. 32 Abs. 1 Pkt. C	**Dokumentation Backup**, sowie rasche Wiederherstellbarkeit			
Art. 32 Abs. 1 Pkt. D	**Dokumentation der regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs**			
Art. 32 Abs. 2	Analyse und Beurteilung des angemessenen Schutzniveaus der einzelnen Datenverarbeitungen (Vertraulichkeit, Integrität, Verfügbarkeit, regelmässige Überprüfung)			
Art. 32 Abs. 4	Nachweisführung, dass Mitarbeiter, die personenbezogene Daten verarbeiten, dies jeweils nur auf und nach Anweisung des Datenverarbeitungsverantwortlichen tun			
Art. 33	Einrichten eines Meldeweges und von Meldekriterien von Datenschutzverletzungen bei der Aufsichtsbehörde			
Art. 34	Planung des Vorgehens zur Meldung von Datenschutzverstössen an die Betroffenen			
Art. 35 Abs. 1 & 3	Schriftliche Beurteilung aller Verfahren, ob eine Folgeabschätzung notwendig ist			
Art. 35 Abs. 7	Durchführung der Folgeabschätzungen			
Art. 36 Abs. 1	Evtl. Konsultation der Aufsichtsbehörde zur Genehmigung der risikoreichen Datenverarbeitung basierend auf der Folgeabschätzung			
Art. 13 Abs. 1	Zusammenstellung einer Übersicht der datenerhebenden Dokumente und digitalen Erhebungen			
Art. 13 Abs. 1	Texte zur Erfüllung der Informationspflichten für die Erhebungen erstellen			
Art. 13 Abs. 2	Planung der Bereitstellung der in Abs. 2 genannten Informationen für alle Betroffenen			
Art. 14	Prüfung, ob Daten existieren, die nicht vom Betroffenen erhoben wurden			
Art. 14	Texte zur Erfüllung der Informationspflichten für den Datenbesitz erstellen			
Art. 24 Abs. 1	Nachweisführung der Umsetzung der TOMs durch den jeweiligen Datenverarbeitungs-Verantwortlichen			
Art. 24 Abs. 1	Verfahren zur regelmässigen Nachweisführung der Umsetzung der TOMs durch den jeweiligen Datenverarbeitungs-Verantwortlichen			
Art 24 Abs. 2	Erstellung einer **Datenschutzrichtlinie** zum Nachweis gegenüber der Aufsichtsbehörde			
Art 24 Abs. 2	**Dokumentation der regelmässigen Kontrolle der Einhaltung der Datenschutzrichtlinie zum Nachweis gegenüber der Aufsichtsbehörde**			
Art. 25	**Dokumentation von Privacy by Default und Design** durch den Datenverarbeitungs-Verantwortlichen			
Art. 4 Abs. 1 i.V.m. Erwägungsgrund 30	IP-Adresse und Cookies müssen als personenbezogene Daten behandelt werden. Anpassung der Datenverarbeitung.			
Art. 7 & 8	Anpassung der Einwilligungstexte und der Form der Einwilligung			
Art. 6 Abs. 1 Pkt. F	Nachweis der berechtigten Interessen für die Datenverarbeitung, die deren rechtliche Grundlage bildet			

Art. 28 Abs. 1	Nachweis der sorgfältigen Auswahl für alle Auftragsverarbeiter erstellen			
Art. 28 Abs. 3	**Verträge und Kontrollen mit den Auftragsverarbeitern** an die geforderten Inhalte von Abs. 3 anpassen			
Art. 28 Abs. 4 i.V.m. Abs. 1	**Nachweise der Vertragsabschlüsse mit Subauftragnehmern** von den Auftragnehmern einfordern			
Art. 39 Abs. 1 Pkt. B	Sensibilisierung der Mitarbeiter			
Art. 39 Abs. 1 Pkt. B	Schulung der Mitarbeiter über die neuen Inhalte			
	Anpassung bereits vorhandener Betriebsvereinbarungen und Arbeitsanweisungen			

Dokumentation

Technische und organisatorische Massnahmen (TOM) für Verantwortliche

Der Verantwortliche bestätigt Massnahmen zur Einhaltung der Anforderungen an die Sicherheit der Datenverarbeitung ergriffen zu haben (Art. 32 DSGVO).

Dies sind folgende:

1. Vertraulichkeit

1.1 Zutrittskontrolle
Bauliche, technische oder organisatorische Massnahmen also z.B. Türsicherung, Sicherung des Serverraums etc.

1.2 Zugangskontrolle
Art und Stärke der Zugangsmedien sowie Aufbewahrung und Vernichtung von Informationen und Informationsträger, also z.B. Kennwortschutz etc.

1.3 Zugangskontrolle
Art und Stärke der Zugangsmedien sowie Aufbewahrung und Vernichtung von Informationen und Informationsträger, also z.B. Kennwortschutz etc.

1.4 Trennungskontrolle
Trennung der Verarbeitung, Beachtung der Zweckbindung z. B. bei Einwilligung zur Speicherung im Rahmen des Mandats, keine Verwendung für Werbung etc.

1.5 Pseudonymisierung
z.B. Daten sind ohne weitere getrennt gespeicherte Informationen nicht mehr einer natürlichen Person zuordenbar.

2. Integrität

2.1 Weitergabekontrolle
Alle Sicherheitsvorkehrungen bei der Datenübertragung und beim Datentransport z.B. Verschlüsselungsmassnahmen etc.

2.2 Eingabekontrolle
Nachvollziehbarkeit der Datenzugriffe oder Veränderungen z. B. durch Protokollierung

2.3 Auftragskontrolle
Massnahmen bei der Auftragsdatenverarbeitung oder beim Outsourcing von Aufgaben innerhalb der Datenverarbeitung, z.B. Verarbeitung nach Art. 28 DSGVO, sorgfältige Auswahl der Vertragspartner etc.

3. Verfügbarkeit und Belastbarkeit

3.1 Backupverfahren
Datensicherungskonzept, Wiederherstellung etc.

3.2 Business Continuity Management
Massnahmen, um in Notfallsituationen oder Störfällen angemessen, zeitnah reagierung zu können, um die Wahrung und Verfügbarkeit der Informationen sicherzustellen

4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

4.1 Auftragskontrolle
Regelmässige Kontrolle der Auftragnehmer

4.2 Mitarbeiterschulung
Darlegung der Schulung der Mitarbeiter in Fragen des Datenschutzes und der Geheimhaltung, z. B. auch CleanDesk etc.

4.3 Prüfung Prozesse und Systeme sowie evtl. Zertifizierung
Regelmässige Überprüfung aller Prozesse und Systeme auf Qualität und Sicherheit

Es liegen folgende Dokumentationen zu sonstigen Massnahmen vor (Datenschutzschulungen, Zertifikate etc.)

……
Datum der Dokumentation

……
Unterschrift Verantwortlicher