Umsetzung DSGVO – Stichtag 25. Mai 2018
Kurz-Checkliste für Versicherungsvermittler zur Ersteinschätzung

Empfindliche Strafen – nach DSGVO bis zu € 20 Mio. lassen sich durch einige einfache Maßnahmen verhindern.

Kundeneinwilligung
Liegen von allen Kunden eine Einwilligungserklärung bzw. eine Datenschutzerklärung vor? **O** ja **O** nein

Wenn nein: Erhebung, Verarbeitung und Speicherung von personenbezogenen Daten **nicht** erlaubt!

Datenschutzbeauftragter
Verarbeiten mehr als 9 Mitarbeiter personenbezogene Daten? **O** ja **O** nein

---

Verarbeiten Sie Gesundheitsdaten in erheblichem Umfang? (speziell bei Lebens- und Krankenversicherungen) **O** ja **O** nein

---

Wenn ja: in einer Position. Sie müssen einen Datenschutzbeauftragten (intern oder extern) bestellen.

Externe Verarbeitung von personenbezogenen Daten
Erfasst, verarbeitet oder speichert ein Externer für Sie personenbezogene Daten? **O** ja **O** nein

Wenn ja: Sie benötigen einen DSGVO konformen Vertrag zur Auftragsverarbeitung.

Verarbeitungsverzeichnis
Haben Sie ein Verzeichnis der Verfahren in Ihrem Unternehmen zur Dokumentation (Erhebung, Verarbeitung, Speicherung) von personenbezogenen Daten? **O** ja **O** nein

Wenn nein: DSGVO und BDSG sehen für kleinere Unternehmen keine grundsätzliche Pflicht vor – jedoch kann dies von der Aufsichtsbehörde verlangt werden.
Empfehlung: Führen Sie in jedem Fall ein Verarbeitungsverzeichnis.

Recht auf Vergessenwerden
Haben Sie ein Verfahren zur Löschung von nicht mehr benötigten personenbezogenen Kundendaten? **O** ja **O** nein

Wenn nein: Hier müssen Sie ein Verfahren implementieren, um dieses sicher zu stellen. Achtung aber – gesetzliche Aufbewahrungspflichten beachten/ Daten zur Beweissicherung müssen weiterhin aufbewahrt werden.

Recht auf Datenmitnahme

Der Kunde hat ein Recht, seine Daten zu einem anderen Anbieter mit zu nehmen. Haben Sie ein Verfahren? **O** ja **O** nein

Wenn nein: Sie müssen ein Verfahren haben, damit Sie auf Verlangen des Kunden diese Daten elektronisch zur Verfügung stellen können. Achtung. Identitätsprüfung! DSGVO spricht vom Entgegenwirken der Anbieterabhängigkeit.

Meldepflichten gegenüber Aufsichtsbehörden

Haben Sie ein Verfahren, welches sicherstellt, dass bei Schutzverletzungen der personenbezogenen Daten (z.B. Datenverlust durch Diebstahl, Datenhacking) die Aufsichtsbehörde und der Betroffene innerhalb von 72 Stundeninformiert wird. **O** ja **O** nein

Wenn nein: Implementieren Sie ein entsprechendes Verfahren zum Erkennen und Melden. Nach DSGVO sind Sie hierzu verpflichtet

Haben Sie eine Arbeitsanweisung zum Thema Datenschutz

Wenn Sie Mitarbeiter beschäftigen, sollten Sie Regeln zum Datenschutz in Ihrem Unternehmen festschreiben und diese zur Pflicht machen. **O** ja **O** nein

Wenn nein: Arbeiten Sie eine verbindliche Arbeitsanweisung aus, geben Sie diese Ihren Mitarbeitern zur verpflichtenden Einhaltung zur Kenntnis und lassen Sie sich dies durch Unterschrift bestätigen.

Mitarbeiterschulung

Schulen Sie Ihre Mitarbeiter regelmäßig zum Thema Datenschutz? **O** ja **O** nein

Wenn nein: Führen Sie regelmäßig Schulungen durch und dokumentieren Sie diese. So sind Sie auf der sicheren Seite.

Schweigepflichtserklärung

Haben Sie von Ihren Mitarbeitern eine Schweigepflichtserklärung unterzeichnen lassen (Liegt diese in der Personalakte?) **O** ja **O** nein

Wenn nein: Die DSGVO sieht diese im Gegenteil zum BDSG nicht mehr verpflichtend vor. Sie sollten diese trotzdem zu den Akten nehmen. Sie können somit die Einhaltung der DSGVO in Ihrem Unternehmen dokumentieren.