© **FM Forum Business Solutions GmbH**
A-1200 Wien, Dresdner Straße 45
E-Mail: kundenservice@forum-media.at

Wesentliche DSGVO-compliance-Punkte (Checkliste)

Struktur und Verantwortlichkeit im Unternehmen

Nr	Bezeichnung	Erfüllt
1	Gibt es das Bewusstsein im Unternehmen, dass Datenschutz auch Management-Verantwortung ist, zB durch:	
	Vorhandensein einer Datenschutzleitlinie/-richtlinie	☐
	Gibt es einen klaren Auftrag vom Management sich innerhalb der Organisation mit Datenschutz auseinanderzusetzen?	☐
	Beschreibung der Datenschutzziele und -risken	☐
	Regelung der Verantwortlichkeiten und Überarbeitung der Stellenbeschreibungen	☐
	Vorhandensein eines Datenschutzhandbuchs	☐
2	Verfügt Ihr Unternehmen über einen betrieblichen Datenschutzbeauftragten bzw über einen betrieblichen Datenschutzkoordinator?	☐
3	Verfügt Ihr Unternehmen über einen externen Datenschutzbeauftragten?	☐

Übersicht über Verarbeitung

Nr	Bezeichnung	Erfüllt
1	In welchen Verarbeitungstätigkeiten werden welche personenbezogenen Daten nach Art 5 Abs 1 DSGVO verarbeitet? ▪ … ▪ … Welche sensiblen Daten (besondere personenbezogene Daten [Art 9]) und Daten über strafrechtliche Verurteilungen und Strafdaten (Art 10) werden verarbeitet? ▪ … ▪ … Mit welchen Systemen werden welche personenbezogenen Daten verarbeitet? ▪ …	

	…	
2	Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem Art 30 DSGVO in Zusammenarbeit mit den internen zuständigen Mitarbeitern erstellt?	☐
3	Wurde im Verarbeitungsverzeichnis pro personenbezogener Verarbeitungstätigkeit ua auf den Zweck, Datenkategorie, Betroffene, Empfänger, Löschfristen, … eingegangen?	☐

Einbindung Externer

Nr	Bezeichnung	Erfüllt
1	Haben Sie externe Dienstleister zur Auslagerung von Arbeitsschritten (Auftragsverarbeiter) eingebunden?	☐
	Gibt es eine zentrale Auflistung über die Auftragsverarbeiter?	☐
	Haben Sie mit allen eine schriftliche Vereinbarung für die Auftragsverarbeitung, dh sind mit den Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art 28 Abs 3 abgeschlossen?	☐
	Weist der Auftragsverarbeiter die erforderliche Zuverlässigkeit auf und wurde diese überprüft (Recht auf Audit, ISO 27001, ISAE3402 Report)? Wurden die technischen und organisatorischen Maßnahmen überprüft?	☐

Transparenz, Informationspflicht und Sicherstellung der Betroffenenrechte

Nr	Bezeichnung	Erfüllt
1	Haben Sie Ihre Texte und Dokumente zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art 13 DSGVO bzw Art 14 DSGVO angepasst bzw wurden diese neu erstellt?	☐
	Haben Sie Prozesse eingerichtet, um vor der Verarbeitung der personenbezogenen Daten den betroffenen Personen die nötigen Informationen gem Art 13 DSGVO bzw Art 14 DSGVO zukommen zu lassen?	☐
2	Haben Sie insbes folgende Informationen neu aufgenommen, sofern nicht bereits vorher enthalten:	☐
	Kontaktdaten des Datenschutzbeauftragten (wenn dieser bestellt wurde)	☐
	Den Zweck und die Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten	☐
	Falls Sie die Verarbeitung mit Ihren berechtigten Interessen oder berechtigten Interessen eines Dritten begründen: die berechtigten Interessen, die verfolgt werden (insbesondere eine genaue Ausformulierung des berechtigten Interesses)	☐
	Falls Sie Daten in Drittländer übermitteln: die von Ihnen zum Einsatz gebrachten geeigneten Garantien zum Schutz der Daten (zB Standarddatenschutzklauseln)	☐
	Dauer der Speicherung; sofern nicht möglich, die Kriterien für die Festlegung dieser Dauer	☐
		☐

	Bestehen der Rechte betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch aufgrund besonderer Situation der betroffenen Person sowie auf Datenportabilität	
	Recht auf Beschwerde bei der Aufsichtsbehörde	☐
	Sofern Verarbeitung auf Einwilligung beruht: das Recht zum jederzeitigen Widerruf der Einwilligung	☐
	Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich	☐
	Sofern einschlägig: die Vornahme einer automatisierten Entscheidungsfindung einschließlich Profiling sowie Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der Verarbeitung für die betroffene Person	☐
3	Haben Sie Ihre Werbe-Einwilligungserklärungen (für Kunden, Interessenten usw) an die Anforderungen von Art 7 und 13 DSGVO angepasst? Hinweis: Insbesondere erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung!	☐
4	Wurden Prozesse eingerichtet, um Anträge von betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch zeitnah und vollständig erfüllen zu können (Art 12 Abs 1)?	☐
5	Wurden Prozesse eingerichtet, um die Überprüfung der Identität der betroffenen Person sicherzustellen?	☐
6	Ist es möglich, durch die Systeme eine Kopie aller personenbezogenen Daten eines Betroffenen zu erstellen?	☐
7	Wurden Prozesse eingerichtet, damit die Betroffenenrechte fristgerecht abgehandelt werden können?	☐
8	Ist bekannt an wen sich betroffene Personen für die Ausübung ihrer Betroffenenrechte wenden können?	☐
9	Ist ein Verfahren eingerichtet, um Anträge auf Datenübertragbarkeit betroffener Personen erfüllen zu können (Art 20 DSGVO)?	☐

Verantwortlichkeit, Umgang mit Risiken

Nr	Bezeichnung	Erfüllt
1	Gibt es für jede personenbezogene Verarbeitungstätigkeit Angaben, mit der Sie die Rechtmäßigkeit ihrer Verarbeitung nachweisen können (zB bezüglich Zweck, Kategorien, Daten, Empfänger, Löschfristen gem Art 5 Abs 2 DSGVO)?	☐
2	Entsprechen die Einwilligungen, auf die Sie eine Verarbeitung stützen, den Voraussetzungen der Art 7, Art 8?	☐
3	Können Sie das Vorliegen der Einwilligung nachweisen (zB durch ein Double Opt-in Verfahren)?	☐
4	Haben Sie ein Datenschutzmanagementsystem installiert, um sicherzustellen und den Nachweis erbringen zu können, dass Ihre Verarbeitung gem der DSGVO erfolgt (Art 24 Abs 1 DSGVO):	

	Dokumentation der Einwilligungserklärungen	☐
	Dokumentation des Verarbeitungsverzeichnis	☐
	Dokumentation der abgeschlossenen Vereinbarung für die Auftragsverarbeitung	☐
	Dokumentation der ergriffenen technischen und organisatorischen Maßnahmen	☐
	Dokumentation der Risikoabschätzung	☐
	Dokumentation der Interessensabwägungen (berechtigtes Interesse)	☐
	Dokumentation der Verträge zur Verarbeitung der Daten im Auftrag	☐
	Dokumentation der innerbetrieblichen Prozesse und Kontrolle dieser	☐
	Dokumentation der Weisungen an den Verantwortlichen oder dem Auftragsverarbeiter unterstellte Personen	☐
	Dokumentation von Verletzungen des Schutzes personenbezogener Daten	☐
	Dokumentation der Verpflichtung der Mitarbeiter zur Vertraulichkeit	☐
5	Ist sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Unternehmen berücksichtigt werden (Privacy by Design – Art 25)?	☐
6	Ist sichergestellt, dass datenschutzrechtliche Belange bei jeder Änderung oder neuen Implementierung von Softwaresystemen in Ihrem Unternehmen berücksichtigt werden?	☐
7	Wie ist Privacy by Design/Privacy by Default implementiert? ▫ … ▫ …	
8	Haben Sie Ihre bestehenden Prozesse zur Überprüfung der Sicherheit der Verarbeitung auf die neuen Anforderungen des Art 32 angepasst?	☐
	Haben Sie insbesondere bestehende Checklisten zur Auswahl von technischen und organisatorischen Maßnahmen durch eine risikoorientierte Betrachtungsweise auf Basis von Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten ersetzt?	☐
	Wurde ein geeignetes Managementsystem zur regelmäßigen Überprüfung, Bewertung und Verbesserung der Security-Maßnahmen umgesetzt?	☐
	Wurden Schutzmaßnahmen wie Pseudonymisierung und der Einsatz von kryptographischen Verfahren zum Schutz vor unbefugten oder unrechtmäßigen Verarbeitungen sowohl bezüglich externer als auch interner „Angreifer“ umgesetzt?	☐
9	Haben Sie sich auf die evtl Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung (Art 35; Privacy Impact Assessment; kurz PIA) vorbereitet?	☐
	Haben Sie eine geeignete Methode zur Bestimmung der Frage, ob eine Datenschutz-Folgenabschätzung durchzuführen ist, in Ihrem Unternehmen eingeführt?	☐

	Haben Sie eine geeignete Risikomethode zur Durchführung einer Datenschutz-Folgenabschätzung in Ihrem Unternehmen eingeführt? Haben Sie sich für einen Prozess der Datenschutz-Folgenabschätzung entschieden; haben Sie diesen schon einmal getestet?	☐