Checkliste für Betriebsvereinbarungen nach der EU-Datenschutzgrundverordnung (gilt ab dem 25.5.2018)

Bestehende und neue Betriebsvereinbarungen müssen im Einklang mit der DSGVO stehen. Widersprechen Regelungen in bestehenden Betriebsvereinbarungen diesen Grundsätzen, so werden sie in diesem Bereich ungültig. Die betroffene Betriebsvereinbarung insgesamt bleibt weiterhin in Geltung (bestehen).

Die folgende Checkliste[1] enthält zentrale Grundsätze der DSGVO, die in der Betriebsvereinbarung wie folgt abzubilden sind:

☑	Es ist eine **Differenzierung nach Datenarten/-kategorien** vorzunehmen (Art 9, 10): Einhaltung der erhöhten Schutzanforderungen für die Verarbeitung besonderer Datenkategorien (ethnische Herkunft, politische Meinung, Religion, sexuelle Orientierung, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten, Daten über Verurteilungen und Straftaten).
☑	**Personenbezogene Daten** müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art 5 Abs 1a). Die Regelungen zum Umgang mit ihren Daten müssen für Arbeitnehmer daher transparent und nachvollziehbar sein.
☑	**Zweckbindung** ist an- und auszuführen: Personenbezogene Daten dürfen nur für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden. Es sind detaillierte Beschreibungen der Zwecke der geplanten Datenverarbeitung aufzunehmen. Diese können die betrieblichen Sozialpartner im Rahmen von Anhängen zur Betriebsvereinbarung ausführen. Eine Verarbeitung zu anderen Zwecken ist grundsätzlich unzulässig. Es ist davon auszugehen, dass zu unbestimmte und allgemeine Aussagen zu den zulässigen Zwecken oder die Angabe von Zweckbündeln von den Gerichten in Zukunft als unzulässig bewertet werden (Art 5 Abs 1 lit b).
☑	**Datenminimierung und Datensparsamkeit:** Die Datenerhebung und -verarbeitung muss auf das für die Zwecke der Datenverarbeitung notwendige Mindestmaß beschränkt sein (Art 5 Abs 1 lit c). Bereits bei Planung und Einführung der IT-Systeme sind Maßnahmen zur Umsetzung der Datenschutzgrundsätze in dem jeweiligen technischen System anzuführen. Dazu sieht die DSGVO die Modelle „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy by Design and by Default)" vor, zB Pseudonymisierung, Konzepte zur Datenminimierung, zum Datenzugriff, zur Datenlöschung (Art 25).
☑	**Datenrichtigkeit und Datenaktualität:** Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein. Personenbezogene Daten, die im Hinblick auf ihre Zwecke unzutreffend sind, sind unverzüglich zu löschen oder zu berichtigen. Regelungen zu Korrekturprozessen, sobald Datenunrichtigkeiten bekannt werden, sind festzulegen (Art 5 Abs 1 lit d).
☑	**Beschränkung der Speicherdauer:** Daten dürfen nur so lange gespeichert werden, wie dies zur Erreichung der mit der Datenverarbeitung verfolgten Zwecke erforderlich ist. Die Speicherdauer bzw. die Kriterien zur Festlegung der Speicherdauer sind anzuführen (Art 5 Abs 1 lit e).
☑	**Einhaltung der Anforderungen an Datensicherheit:** Personenbezogene Daten sind so zu verarbeiten, dass sie vor unbefugter oder unrechtmäßiger Verarbeitung, vor zufälligem Verlust, zufälliger Zerstörung oder Schädigung geschützt sind. Dazu sind geeignete technische und organisatorische Maßnahmen zu treffen (Art 5 Abs 1 lit f).
☑	**Datenübermittlung an Dritte:** Hinweis auf Empfänger von Daten oder Kategorien von Datenempfängern und Hinweis auf Übereinstimmung mit dem berechtigten Zweck; bei Datenübermittlung an Drittländer darf das Schutzniveau für die Betroffenen (geeignete Garantien, durchsetzbare Rechte und wirksame Rechtsbehelfe) nicht

[1] Die folgende Checkliste entstammt dem Buchbeitrag *Angerler/Reven*, DSGVO und nationales Arbeitsrecht, in Knyrim (Hrsg), Datenschutz-Grundverordnung. Das neue Datenschutzrecht in Österreich und der EU (2016).

	untergraben werden. Es ist ein Hinweis auf Maßnahmen zur Sicherung eines angemessenen Datenschutzniveaus erforderlich (Art 44–50).
☑	**Aufklärungs- und Informationspflichten:** Klare und leicht verständliche Informationen zur Datenverarbeitung müssen vorhanden sein, sowie Modalitäten für die effektive Ausübung der Rechte der betroffenen Person. Über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling muss ausdrücklich informiert werden, in diesem Fall sind den Betroffenen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung zu übermitteln (Art 12–14).
☑	**Hinweis auf Betroffenenrechte** (Art 15–20) und deren Ausübung, und zwar das Recht auf Auskunft, auf Berichtigung, auf Löschung von Daten zur eigenen Person sowie das Recht auf Widerspruch, insb. bei Profiling (Art 21–22).
☑	**Sicherstellung rechtmäßiger Auftragsdatenverarbeitung:** Vorhandensein von Garantien, die die Eignung des Auftragsverarbeiters sicherstellen, verordnungskonforme Datenverarbeitungen durchzuführen; Vorhandensein eines (Dienstleister-)Vertrages, der Art, Zweck und Dauer der Verarbeitung sowie Art der personenbezogenen Daten und Kategorien der betroffenen Personen enthält; Berücksichtigung der Betriebsvereinbarung durch den Auftragsdatenverarbeiter (Art 28).
☑	**Ergebnis der Datenschutz-Folgenabschätzung und der Risikoeinschätzung** – wenn erforderlich – prüfen (Sicherheitskonzept), insb bei automatisierten Einzelentscheidungen und Profiling sowie bei Verwendung besonderer Datenkategorien (Art 35).
☑	**Vorab-Konsultationspflicht** bei risikoreichen Datenverarbeitungen – schriftliche Empfehlungen der Aufsichtsbehörde umsetzen (Art 36).