Bekenntnis zu Grundsätzen und Verhaltensregeln nach Art. 40 DSGVO und deren Umsetzung

Die Firma Johann Heinen GmbH & Co. KG, Berliner Str. 188, 51377 Leverkusen

bekennt sich zu den allgemeinen Prinzipien der Verarbeitung personenbezogener Daten nach der EU-Datenschutzgrundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) wie folgt und stellt deren Umsetzung sicher. Diese Grundsätze und Verhaltensregeln nach Art. 40 DSGVO werden im Rahmen der Verhältnismäßigkeit anerkannt und umgesetzt.

Prinzipien der Verarbeitung von personenbezogenen Daten. Dazu zählen nach Art. 5 Abs. 1 DSGVO:

- → **Rechtmäßigkeit und Transparenz:** Ohne eine Ermächtigungs- bzw. Rechtsgrundlage dürfen keine personenbezogenen Daten erhoben und benutzt werden. Das Verbot mit Erlaubnisvorbehalt regelt, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich verboten ist, es sei denn, es gibt eine Erlaubnis. Diese kann entstehen aus: Gesetzen, z.B. aus dem BDSG, TMG, DSGVO oder der Einwilligung der betroffenen Person
- → **Zweckbindung:** Daten werden nur zu dem Zweck verarbeiten, für den sie erhoben wurden. Die personenbezogenen Daten, für die eine Ermächtigungsgrundlage vorhanden ist, dürfen nur zu dem Zweck verwendet werden, für den ebendiese Ermächtigung erteilt wurde. Werden die Daten noch **für einen anderen Zweck** als für den der ersten Erhebung weiterverarbeitet, ist der Betroffene darüber zu informieren.
- → **Datenminimierung bzw. -sparsamkeit:** Die Datenverarbeitung muss auf das notwendigste Maß beschränkt werden. Es dürfen nur die und so viele Daten erhoben und verarbeitet werden, wie tatsächlich benötigt. Eine „Datenerhebung auf Vorrat" ist verboten (Art. 5 Abs. 1c DSGVO).
- → **Richtigkeit von Daten:** Daten müssen inhaltlich und sachlich richtig und aktuell gehalten sein. Bei falschen und unsachlichen Daten hat der Betroffene sofortigen Anspruch auf Berichtigung bzw. Löschung unzutreffender Daten.
- → **Speicherbegrenzung:** Eine Speicherung mit Personenbezug erfolgt höchstens so lange, wie es für die Verarbeitungszwecke erforderlich ist. Die Datenspeicherung ist auf den Zeitraum der Verarbeitung beschränkt und unbegrenzte Datenspeicherung muss vermieden werden.
- → **Integrität, Vertraulichkeit, Verfügbarkeit:** Die personenbezogenen Daten müssen mit geeigneten technisch-organisatorischen Maßnahmen angemessen gesichert werden, insbesondere gegen unbefugte oder unrechtmäßige Verarbeitung, zufälligen Verlust, zufällige Zerstörung, Schädigung, Manipulation oder Fälschung.
- → **Rechenschaftspflicht:** Die Einhaltung dieser Grundsätze muss nachgewiesen werden.

Eine Vielzahl von Vorschriften konkretisiert diese allgemeinen Grundsätze.
Im Hinblick auf die rechtliche Zulässigkeit der Datenverarbeitung betrifft das u.a. folgende Punkte:

- → **„Privacy by Design"** und **„Privacy by Default"** (Art. 25 DSGVO): Datenschutz muss bereits im Vorfeld ein Teil von Entwicklungsprozessen im Unternehmen sein und darf nicht erst nachträglich berücksichtig werden. Datenschutz ist schon beim Planen z.B. neuer Techniken oder neuer Verfahren und Verarbeitungen durch datenschutzfreundliche Grundeinstellungen zu berücksichtigen.

  „Privacy by Design" bedeutet, dass Datenschutzmaßnahmen nach dem Stand der Technik bereits in die konzeptionelle Entwicklung von Produkten und Verfahren einbezogen werden müssen.

  „Privacy by Default" bedeutet wiederum, dass zum Beispiel die Voreinstellungen bei Geräten oder bei Onlineplattformen standardmäßig die höchste Datenschutzstufe haben sollen.
- → **Datenschutz-Folgenabschätzung** (Art. 35, 36 DSGVO): Der Verantwortliche muss bei einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen vorab eine Analyse der Folgen erstellen. Für die identifizierten Risiken muss er geeignete Maßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren umsetzen.
- → **Übermittlung in Drittländer** (Art. 44 DSGVO): Bei der Datenübermittlung in ein Drittland muss der Verantwortliche (samt Auftragsverarbeiter) Garantien für eine rechtmäßige Verarbeitung bieten.

Maßnahmen zur datenschutzrechtlichen Information und Kommunikation

Die DSGVO fordert vom Verantwortlichen geeignete Maßnahmen zur datenschutzrechtlichen Information und Kommunikation, insbesondere für den „Fall des Falles":

- **Transparenz** (Art. 12 DSGVO): Der Verantwortliche muss Betroffene in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache informieren, und zwar in Bezug auf Name und Kontaktdaten der verantwortlichen Stelle (samt Datenschutzbeauftragtem) sowie Zwecke, ggf. berechtigte Interessen und Empfänger sowie die Drittlandübermittlung.
- **Verletzung** (Art. 33, 34 DSGVO): Verletzungen des Schutzes personenbezogener Daten muss der Verantwortliche an die Aufsichtsbehörde melden. Gegebenenfalls muss er die Betroffenen benachrichtigen.

Technisch-organisatorische Maßnahmen:

Im Rahmen der eigentlichen Verarbeitung personenbezogener Daten muss der Verantwortliche geeignete technisch-organisatorische Maßnahmen u.a. in folgenden Bereichen vorsehen, umsetzen und nachweisen können:

- **Verantwortung** (Art. 24 DSGVO): Der Verantwortliche hat risikobasiert die geeigneten Maßnahmen zum Schutz der von der Verarbeitung betroffenen Daten zu ergreifen. Die Maßnahmen muss er nachweisen und aktuell halten.
- **Auftragsverarbeitung** (Art. 28 DSGVO): Der Verantwortliche darf nur mit Auftragsverarbeitern zusammenarbeiten, die Garantien dafür bieten, dass sie personenbezogene Daten durch geeignete technisch-organisatorische Maßnahmen schützen. Darüber muss ein Vertrag existieren.
- **Datensicherheit** (Art. 32 DSGVO): Der Verantwortliche muss risikobasiert durch geeignete Maßnahmen die klassischen IT-Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit bei der Datenverarbeitung sicherstellen.

Erforderliche interne Maßnahmen

Die DSGVO verlangt vom Verantwortlichen die Umsetzung einer Reihe interner Maßnahmen. Die wichtigsten:

- **Verzeichnis** (Art. 30 DSGVO): Der Verantwortliche muss ein Verzeichnis aller Verarbeitungstätigkeiten führen – ähnlich dem aus dem BDSG bekannten Verfahrensverzeichnis.
- **Dokumentation** (Art. 26, 28, 31, 44 DSGVO): Der Verantwortliche muss neben dem Führen eines Verzeichnisses seiner Dokumentationspflicht nachkommen, z.B. bei Weisungen, Verletzungen oder Garantien im Rahmen der Drittlandübermittlung.
- **Datenschutzbeauftragter** (Art. 37–39 DSGVO): Der Verantwortliche hat unter bestimmten Voraussetzungen einen Datenschutzbeauftragten zu bestellen, dessen Aufgaben v.a. in der Beratung und in der Überwachung des Einhaltens der DSGVO-Vorgaben liegen
- **Recht auf Vergessenwerden** (Art. 17 DSGVO): Die wichtigsten Gründe, wann Sie die Daten löschen müssen:
  - Der Zweck für die Datenverarbeitung ist weggefallen (Art. 17 Buchstabe a)
  - Der Betroffene hat seine Einwilligung widerrufen (Art. 17 Buchstabe b)
  - Die Datenverarbeitung war unrechtmäßig (Art. 17 Buchstabe d)
- **Recht auf Interoperabilität** (Art. 20 DSGVO): Daten von Betroffenen müssen in einem gängigen, maschinenlesbaren Format ausgeben und zu einem anderen Anbieter mit genommen werden können. Beispiele: Wechsel zu anderen sozialen Netzwerken, Banken oder Arbeitgebern.

Leverkusen, Mai 2018
Ort, Datum

Unterschrift Geschäftsleitung