



Arbeitsblatt: Checkliste zu den Umsetzungen aus der Europäischen Datenschutz-Grundverordnung (DSGVO)

der

am Standort: _____

I. Struktur und Verantwortlichkeiten

1. Ist das datenschutzrechtliche Bewusstsein im Unternehmen vorhanden?

- | | |
|--|--|
| <input type="checkbox"/> Vorhandensein einer Datenschutzleitlinie | <input type="checkbox"/> Beschreibung der Datenschutzziele |
| <input type="checkbox"/> Regelungen der Verantwortlichen | <input type="checkbox"/> Bewusstsein über Datenschutzrisiken |
| <input type="checkbox"/> Transparenz über Zielkonflikte (z. B. zwischen Marketing und Rechtsabteilung) | |

2. Wurde ein Datenschutzbeauftragter benannt?

- | | |
|--|--|
| <input type="checkbox"/> JA. | <input type="checkbox"/> NEIN, weil _____. |
| <input type="checkbox"/> JA und die Voraussetzungen der Einbeziehung im Unternehmen allgemein bekannt. | <input type="checkbox"/> JA und er wurde der zuständigen Aufsichtsbehörde gemäß Art. 37 Abs. 8 DSGVO gemeldet. |
| <input type="checkbox"/> Transparenz über Zielkonflikte (z. B. zwischen Marketing und Rechtsabteilung) | |

II. Übersicht über die Verarbeitungen

1. Gibt es ein Verzeichnis zu den Verarbeitungstätigkeiten gemäß Art. 30 DSGVO?

- | | |
|-----------------------------|--|
| <input type="checkbox"/> JA | <input type="checkbox"/> NEIN, weil _____. |
|-----------------------------|--|

2. Wie werden die datenschutzrechtlichen Belange bei Beginn oder Änderung eines Prozesses im Unternehmen sichergestellt (z. B. Privacy by Design gemäß Art. 25 DSGVO)?

- JA, durch _____

III. Einbeziehung von Externen

1. Haben Sie externe Dienstleister/Partner (z. B. Subunternehmen) zur Erledigung Ihrer Arbeiten eingebunden?

- | | |
|------------------------------|---|
| <input type="checkbox"/> JA. | <input type="checkbox"/> JA und es gibt eine Übersicht über die eingesetzten Dienstleister. |
|------------------------------|---|

- JA und es wurde mit allen Auftragsverarbeitern eine Auftragsverarbeitungsvereinbarung gemäß Art. 28 Abs. 3 DSGVO abgeschlossen.
- Bewusstsein über Datenschutzrisiken

IV. Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte

1. *Haben Sie datenschutzrechtlichen Dokumentationen bzw. die Informationen an die betroffenen Personen bei Datenerhebung an die Anforderungen des Art. 13,14 DSGVO angepasst?*

- JA, die allgemeine Datenschutzdokumentation wurde angepasst.
- JA, die Informationen an die betroffenen Personen wurden angepasst.
- Nein, weil _____.
- Bewusstsein über Datenschutzrisiken

2. *Haben Sie die folgenden Informationen aufgenommen, sofern nicht vorher schon enthalten?*

- Kontaktdaten Datenschutzbeauftragter
- Bei Datenübermittlungen in Drittländer die zum Einsatz gebrachten geeigneten Garantien zum Schutz der Daten (z.B. Standarddatenschutzklauseln)
- Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten
- Dauer der Speicherung; sofern nicht möglich, die Kriterien für die Festlegung dieser Dauer
- Bei Begründung der Datenverarbeitung mit berechtigten Interessen
- Bestehen der Rechte betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Widerspruch aufgrund besonderer Situation einer betroffenen Person sowie auf Datenportabilität
- Bei Einwilligung das Recht auf jederzeitigen Widerruf
- Recht auf Beschwerde bei der Aufsichtsbehörde
- Grundlage der Datenverarbeitung auf vertraglicher oder gesetzlicher Basis
- Bei einer automatisierten Entscheidungsfindung einschließlich Profiling (involvierte Technologie, Tragweite und Auswirkungen)
- Bei Daten die nicht aus einer Direkterhebung stammen Angabe der Quelle
- Anpassung der Werbeeinwilligungen gemäß Art. 7 und 13 DSGVO (z. B. erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung)

3. *Gibt es eine Vorgehensweise bei Anfragen von Betroffenen (z. B. Auskunft gemäß § 15 DSGVO), um eine zeitnahe und vollständige Erfüllung zu sichern (Art. 12 Abs. 1 DSGVO)?*

- JA, durch _____

4. *Gibt es einen Antrag, um die Datenübertragbarkeit (Art. 20 DSGVO) bei den betroffenen Personen zu erfüllen?*

- JA, durch _____



V. Verantwortlichkeit und Umgang mit Risiken

1. Gibt es für jede Verarbeitungstätigkeit Angaben zum Nachweis der Rechtmäßigkeit der Verarbeitung (z. B. Zweck, Kategorien personenbezogener Daten, Empfängern und/oder Löschfristen (Art. 5 Abs. 2 DS-GVO)?

JA, durch _____

Wurden die vorhandenen Einwilligungen für die Verarbeitung gemäß Art. 7 und/ oder 8 DSGVO überprüft?

JA, durch _____

Können die Einwilligungen nachgewiesen werden?

JA, durch _____

2. Ist ein Datenschutzmanagementsystem im Einsatz zum Nachweis der Verarbeitung gemäß § 24 Abs.1 DSGVO?

JA, durch _____

3. Wurden die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO angepasst?

JA, Checklisten zu den technischen und organisatorischen Maßnahmen wurden angepasst.

JA, es wurden die risikoorientierte Betrachtungsweise auf Basis von Art, Umfang, der Umstand und Zwecke der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten einbezogen.

JA, es wird ein geeignetes Managementsystem zur regelmäßigen Überprüfung, Bewertung und Verbesserung der Sicherheitsmaßnahmen eingesetzt.

JA, es werden Schutzmaßnahmen in Form von Pseudonymisierung und kryptographischen Verfahren zum Schutz vor unbefugten oder unrechtmäßigen Verarbeitungen sowohl bezüglich externer als auch interner „Angreifer“ umgesetzt.

4. Wurde eine Vorgehensweise für Datenschutz-Folgenabschätzungen eingerichtet?

JA, durch _____

Gibt es Vorgaben, wann eine Datenschutz-Folgenabschätzung durchzuführen ist?

JA, durch _____



Gibt es einen geeigneten Prozess, einschließlich einer Risikomethode zur Durchführung einer Datenschutz-Folgenabschätzung?

JA, durch _____

VI. Datenschutzverletzungen

1. Kann sichergestellt werden, dass gemäß Art. 33 DSGVO innerhalb von 72h eine Meldung an die Datenschutzaufsichtsbehörde erfolgen kann?

JA, durch _____

Kann sichergestellt werden, dass Datenschutzverletzungen erkannt werden (Risikoermittlung)?

JA, durch _____

Gibt es einen internen Prozess wie bei Datenschutzverletzungen zu verfahren ist?

JA, durch _____

Gibt es einen Verantwortlichen, wer mit der Aufsichtsbehörde kommuniziert?

JA, durch _____

Verantwortlicher für die Erstellung in Druckbuchstaben

_____, den _____

Unterschrift Verantwortlicher für die Erstellung