Technische und organisatorische Maßnahmen

der [Name des Unternehmens]

1. Zutrittskontrolle

*Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu wahren.*

[stichpunktartig die getroffenen Maßnahmen auflisten]

1. Zugangs- und Zugriffskontrolle

*Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können sowie, dass die berechtigten Personen ausschließlich innerhalb ihrer Berechtigung am Datenverarbeitungssystem arbeiten.*

1. Eingabekontrolle

*Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*

1. Auftragskontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.*

1. Datentrennungskontrolle

*Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*

1. Weitergabekontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*

1. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

*Privacy by Design bedeutet übersetzt „Datenschutz durch Technikgestaltung“. Ziel soll es sein, dass bereits bei der Entwicklung von Verarbeitungsvorgängen geeignete technische Maßnahmen implementiert werden, um die geplanten Verarbeitungsvorgänge datenschutzkonform zu gestalten.*

*Privacy by Default bedeutet übersetzt „Datenschutz durch datenschutzfreundliche Voreinstellungen“. Das heißt, bereits die Werkeinstellungen eines Programms/ einer Software sollen datenschutzfreundlich ausgestaltet sein. Hierdurch sollen vor allem die Daten der Nutzer geschützt werden.*

1. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.*

1. Organisationskontrolle

*Hierbei handelt es sich um Maßnahmen, die sicherstellen, dass die Mitarbeiter über die Anforderungen des Datenschutzes informiert sowie sensibilisiert sind und dass sie auf die Einhaltung des Datenschutzes verpflichtet werden. Außerdem fallen unter den Punkt der Organisation übergreifende Konzepte, in denen die Unternehmensleitung festlegt, wie es den Datenschutz im Unternehmen handhaben will.*

1. Wirksamkeitskontrolle

*Alle Handlungen, die zu einem Nachweis führen, dass die eingesetzten Maßnahmen regelmäßig überprüft werden und tatsächlich funktionieren.*