Präambel:

Mit dieser Unternehmens-Leitlinie zum Datenschutz und zur IT-Sicherheit gibt sich **COEmarketing** den verbindlichen Rahmen für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten und den sicheren Betrieb der informationstechnischen Infrastrukturen.

1. Selbstverpflichtung und Leitbild

Die Geschäftsführung und alle Mitarbeiter/innen sind sich ihrer Verantwortung im Umgang mit den eingesetzten informationstechnischen Infrastrukturen bewusst und beachten die einschlägigen Gesetze, vertraglichen Regelungen und die internen Richtlinien.

Die Umsetzung von Datenschutz und IT-Sicherheit hat einen hohen Stellenwert im Unternehmen. Alle notwendigen, geeigneten und angemessenen Maßnahmen werden getroffen, um negative materielle und immaterielle Folgen für Betroffene und das Unternehmen auszuschließen.

COEmarketing schützt die personenbezogenen oder sonstigen vertraulich zu behandelnden Daten seiner Mitarbeiter/innen und Geschäftspartner (Kunden und Lieferanten).

Schutzbedarf besteht nicht nur für personenbezogene Daten, sondern auch für sonstige vertrauliche Betriebs- und Geschäftsgeheimnisse.

2. Prinzipien

Der Umgang mit personenbezogenen Daten ist als Verbot mit Erlaubnisvorbehalt geregelt. Damit ist das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten grundsätzlich verboten. Eine Ausnahme ergibt sich nur, wenn ein Gesetz oder eine andere Rechtsverordnung dies erlaubt oder der Betroffene einwilligt.

Hieraus leiten wir Folgendes ab: Für alle Arbeitsvorgänge ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten soweit möglich zu vermeiden (**Prinzip der Datenvermeidung**).

Es werden **nur die Daten verarbeitet, die für die Aufgabenerfüllung erforderlich sind**. D. h., die Daten werden nur für Zwecke verarbeitet, für die sie erhoben worden sind. Ausnahmetatbestände sind gesondert zu regeln. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist (**Prinzip der Datensparsamkeit).** Eine Datenübermittlung von personenbezogenen Daten an Dritte - eventuell auch ins Ausland - ist zu unterlassen, wenn bei der empfangenden Stelle oder in dem jeweiligen Staat kein angemessenes Datenschutzniveau vorhanden ist oder beispielsweise über besondere Vertragsklauseln nicht hergestellt werden kann.

Soweit bei Arbeitsvorgängen die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nicht vermieden werden kann, wird im Rahmen des technisch Vertretbaren jeweils der Arbeitsvorgang, bei dem so wenig personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden müssen, gewählt **(Prinzip der Erforderlichkeit**).

Eine Verwendung von personenbezogenen Daten für einen anderen als den vorab **festgelegten Zweck** ist ausgeschlossen; es sei denn, es liegt eine **Einwilligung des Betroffenen** vor oder ein Gesetz bzw. eine Rechtsvorschrift erlaubt oder ordnet dies an (**Prinzip der Zweckbindung).**

Bei allen Arbeitsvorgängen werden die jeweiligen **gesetzlichen Löschfristen** beachtet. Werden personenbezogene Daten nicht mehr benötigt, werden sie auch ohne Ausschöpfung der Löschfristen vorzeitig gelöscht (**Prinzip der Datensparsamkeit**).

Die unberechtigte Einsichtnahme oder Weitergabe von Daten ist nicht zulässig. Um den Anforderungen an den Schutz sensibler Daten zu entsprechen, werden die Daten und informationstechnischen Infrastrukturen in ihrer Vertraulichkeit gesichert.

Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern („Privacy by design").

3. Verpflichtung aller Mitarbeiter/innen

Die Gewährleistung von Datenschutz und Datensicherheit ist Aufgabe und Verpflichtung für jede/n einzelne/n Mitarbeiter/in.

Die Mitarbeiter/innen sind bei der Erhebung, Verarbeitung und Nutzung von Daten verpflichtet, diese Leitlinie und die daraus abgeleiteten Standards und Richtlinien zu beachten. Dies gilt nicht nur für die Nutzung mit dem PC, dem Laptop und dem Smartphone und/oder sonstigen elektronischen Medien, sondern auch für sonstige Dokumente - auch die Dokumente in Papierform.

4. Festlegung von Verantwortlichkeiten

Die Führungskräfte sind für die Einhaltung eines angemessenen Sicherheitsstandards im Datenschutz und in der Datensicherheit verantwortlich.

Alle Führungskräfte sind dafür verantwortlich, die bestehenden Sicherheitsstandards in ihrem Fach- bzw. Geschäftsbereich umzusetzen und aufrecht zu erhalten. Hierfür sind die organisatorischen, personellen und technischen Voraussetzungen zu realisieren.

5. Rechte der Betroffenen

Betroffene haben das Recht auf Auskunft über die bei **COEmarketing** über ihre Person gespeicherten personenbezogenen Daten.

Betroffene haben einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen. Betroffene haben auch den Anspruch auf die Löschung ihrer personenbezogenen Daten.

6. Unrechtmäßige Kenntniserlangung von Daten („Datenpanne")

Sollten Unternehmensdaten unrechtmäßig Dritten offenbart worden sein, ist darüber unverzüglich der Datenschutzbeauftragte zu informieren. Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhaltes zu umfassen, insbesondere die empfangene Stelle/Person/Firma, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

7. Umsetzung

Die Umsetzung des Datenschutzes und der IT-Sicherheit in den Arbeitsabläufen erfordert angemessene technische und organisatorische Maßnahmen. Diese Maßnahmen werden in weiterführenden Dokumenten festgelegt und laufend aktuell gehalten.

8. Geltungsbereich

Diese Leitlinie gilt für **COEmarketing** und deren Mitarbeiter/innen.

9. Geltungsdauer

Diese Unternehmens-Leitlinie tritt mit Beschluss der Geschäftsführung vom 30. April 2018 in Kraft. Sie gilt, bis sie außer Kraft gesetzt oder durch eine jüngere Fassung ersetzt wird.

Coesfeld, 30/4/2018

COEmarketing GmbH (Geschäftsführung)