

# Datenschutz-Richtlinien der SEMPRIA GmbH, Grafenberger Allee 277-287, 40237 Düsseldorf, <https://www.sempria.de/>

## **1 Vorbemerkung**

Vor dem Hintergrund der Datenschutz-Grundverordnung (DSGVO) wurde der Datenschutz der SEMPRIA GmbH (im Folgenden kurz: Firma) in diesem Dokument zusammengefasst. Seit Gründung der Firma waren die Datenschutz-Richtlinien so strikt, dass keine Verschärfungen zum Erfüllen des DSGVO nötig waren.

## **2 Anfallende personenbezogene Daten**

In der Firma fallen personenbezogene Daten der folgenden Personengruppen an. Es werden maximal folgende Daten gespeichert, sofern diese benötigt werden: Name, postalische Adresse, Telefonnummer, E-Mail-Adresse, Website, Bankverbindung, Notizen zu Kommunikationen.

### **2.1 Kunden**

Für die Abrechnung von Vertragsleistungen und die Erfüllung von Verträgen werden Kundendaten in Papierform und auf Firmen-Rechnern im Hause gespeichert. Falls externe Speicherung erforderlich wird, werden Kundendaten nach dem Stand der Kunst ausreichend verschlüsselt.

### **2.2 Interessenten**

Mögliche Kunden werden in einem CRM-System gepflegt. Dieses wird auf Firmen-Rechnern im Hause betrieben. Sofern externer Zugriff möglich ist, wird dieser nach dem Stand der Kunst ausreichend verschlüsselt.

### **2.3 Mitarbeiter**

Daten zu Mitarbeitern befinden sich nur in Arbeitsverträgen, Zusätzen zu Arbeitsverträgen und in Personalakten. Diese werden in Papierform und elektronisch gespeichert. Sie befinden sich in der Firma und - soweit für die Buchhaltung nötig - beim Steuerberater/Buchhalter der Firma.

### **2.4 Lieferanten**

Lieferanten-Daten werden nur in Papierform abgelegt. Es handelt sich dabei ausschließlich um vom Lieferanten selbst zugesendete Dokumente wie Rechnungen und Lieferscheine.

### **2.5 Weitere Personengruppen**

Daten von weiteren Personengruppen werden in der Firma nicht gesammelt.

### **3 Behandlung von personenbezogenen Daten**

Personenbezogene Daten spielen in keinem Produkt der Firma eine wirtschaftliche Rolle. Sie werden sparsam erhoben und verarbeitet, wie sie für den Betrieb der Firma nötig sind. Jeder Mitarbeiter erhält nur Zugang zu personenbezogenen Daten, soweit es für die Erfüllung der ihm übertragenen Aufgaben sinnvoll ist.

In Verträgen und AGB der Firma findet sich stets ein Datenschutz-Abschnitt, der besonders den Umfang der anfallenden personenbezogenen Daten und das Löschen von personenbezogenen und weiteren Daten nach Vertragsende behandelt. Im Regelfall werden personenbezogene Daten spätestens 90 Tage nach Vertragsende gelöscht oder vollständig anonymisiert. Falls kein Vertrag besteht, können Betroffene per Mail an [info@sempria.de](mailto:info@sempria.de) Daten löschen lassen. Ebenso kann per Mail an [info@sempria.de](mailto:info@sempria.de) angefordert werden, welche Daten über den Betroffenen momentan gespeichert sind. Anfragen an [info@sempria.de](mailto:info@sempria.de) werden innerhalb von 30 Tagen bearbeitet.

### **4 Nutzung von Diensten Dritter mit Relevanz für personenbezogene Daten**

Die Nutzung von Diensten Dritter, die personenbezogene Daten erheben, ist in der Firma grundsätzlich verboten. Das gilt besonders für Google Analytics und ähnliche Dienste. Ausnahmen müssen in das vorliegende Dokument aufgenommen werden mit einer Darlegung, wie der Datenschutz durch den Dritten aussieht und wie dieser Datenschutz mit dem vorliegenden Dokument im Einklang steht.

### **5 Sicherheit der IT**

Es bestehen strikte Richtlinien zu den in der Firma erlaubten Betriebssystemen. Außerdem wird eine sicherheitsorientierte Aktualisierung (Sicherheits-Updates) und Absicherung aller Rechner der Firma in definierten, regelmäßigen Abständen technisch und organisatorisch umgesetzt.

### **6 Datenschutzbeauftragter**

Aufgrund der Größe des Unternehmens und der Art der personenbezogenen Daten ist kein Datenschutzbeauftragter für die Firma vorgeschrieben.

### **7 Umsetzung der Datenschutz-Richtlinien in der Firma**

Alle Mitarbeiter (auch Teilzeitkräfte) werden über die aktuelle Fassung dieses Dokuments informiert. Sie werden darauf hingewiesen, dass die Verletzung der Datenschutz-Richtlinien zu arbeitsrechtlichen Konsequenzen führen kann. Außerdem verpflichten sie sich, Verletzungen und Zweifelsfälle direkt und kurzfristig der Geschäftsführung zu melden. Sie bestätigen dies durch Unterschrift.

Düsseldorf, 2018-05-16