Informationssicherheitsrichtlinie für Lieferanten und Auftragnehmer der Schmalz Gruppe

§ 1 Informationssicherheit

1. Der Auftragnehmer hat angemessene organisatorische und technische Massnahmen nach dem aktuellen Stand der Technik zu treffen, um die Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit des Betriebs des Lieferanten sowie seiner Lieferungen und Leistungen sicherzustellen. Diese Massnahmen sollen branchenüblich sein und ein angemessenes Managementsystem für Informationssicherheit in Übereinstimmung mit Standards wie ISO/IEC 27001 oder IEC 62443 (soweit anwendbar) beinhalten.
   „Betrieb des Lieferanten" bedeutet alle Güter, Prozesse und Systeme (einschliesslich Informationssysteme), Daten (einschliesslich Kundendaten), Mitarbeiter und Standorte, die zeitweise für die Durchführung dieses Vertrages verwendet oder verarbeitet werden.
   Der Auftragnehmer räumt dem Auftraggeber nach angemessener Anmeldung den Zutritt zu seinen Einrichtungen ein, um sich von der Umsetzung geeigneter technischer und organisatorischer Massnahmen zu überzeugen.

2. Auf dem gesamten Betriebsgelände sowie in allen Räumlichkeiten des Auftraggebers ist es untersagt, ohne vorherige schriftliche Zustimmung, Bild- und Tonaufnahmen jeglicher Art zu machen.

3. Sofern Lieferungen oder Leistungen Software, Firmware oder Chipsätze beinhalten:

   wird der Lieferant angemessene, branchenübliche Standards, Prozesse und Methoden in Übereinstimmung mit Standards wie ISO/IEC 27001 oder IEC 62443 (soweit anwendbar) implementieren, um jegliche Schwachstellen, Schadcode und sicherheitsrelevante Ereignisse in den Lieferungen und Leistungen zu verhindern, zu identifizieren, zu bewerten und zu beheben;
   wird der Lieferant für den Zeitraum einer angemessenen Lebensdauer der Lieferungen und Leistungen Reparatur-, Update-, Upgrade- und sonstige Pflegeleistungen anbieten und Patches zur Verfügung stellen, um Schwachstellen zu beheben;
   wird der Lieferant eine Stückliste zur Verfügung stellen, aus der sich alle Softwarekomponenten Dritter ergeben, die in den Lieferungen und Leistungen verwendet werden. Softwarekomponenten Dritter müssen zum Zeitpunkt der Lieferung auf dem aktuellen Stand sein;
   ist der Auftaggeber berechtigt, jedoch nicht verpflichtet, die Lieferungen und Leistungen jederzeit selbst oder durch Dritte auf Schadcode und Schwachstellen zu testen, wobei der Lieferant den Auftraggeber in angemessener Weise unterstützen wird.

4. Der Auftragnehmer wird dem Auftraggeber einen Kontakt für Themen der Informationssicherheit (erreichbar während der Geschäftszeiten) benennen.

5. Der Lieferant wird entsprechende Massnahmen treffen, um seinen Mitarbeiter, Unterlieferanten und Lieferanten, innerhalb eines angemessenen Zeitraums, Verpflichtungen aufzuerlegen, die den Verpflichtungen des allgemeinen Datenschutzes gemäß GdPDU, sowie dieser Richtlinie entsprechen.

§ 2 Geheimhaltung

1. Der Auftragnehmer verpflichtet sich, vertrauliche oder streng vertrauliche Informationen strikt geheim zu halten und diese ausschließlich zum Zweck der Bearbeitung des Auftrags zu verwenden. Dies gilt auch nach Vertragsende und Ausscheiden von Angestellten, Erfüllungsgehilfen oder Subunternehmern.
   Vertrauliche Informationen können insbesondere folgende Informationen und/oder Gegenstände (einzeln oder in ihrer Gesamtheit) sein:

technische Informationen, besonders Produkt-, Entwicklungs- oder Funktionsbeschreibungen, Pflichten- oder Lastenhefte, Skizzen, Grafiken, Zeichnungen und andere technische Dokumente sowie Handbücher, technische Verfahren und Prozesse und anderes Know-how, insbesondere technisches Wissen,
Informationen über bestehende oder künftige Rechtspositionen, insbesondere Nutzungs- und Lizenzrechte, Lizenzsätze, Anmeldungen für Patente und patentfähige Erfindungen, Gebrauchsmuster, Geschmacksmuster oder Markenrechte sowie alle weiteren Rechte,
Informationen über Unternehmensstrategien, Zeitpläne, Ziele, Ideen, geplante Projekte, Vertriebswege sowie kaufmännische Daten, insbesondere Umsätze und Margen,
Informationen, die der Auftragnehmer im Rahmen von Service- oder Reparaturmaßnahmen an einer von dem Auftraggeber gelieferten Maschine oder Komponente über deren Aufbau und Funktionsweise erlangt.
IT-Know-How wie z.B. Ausstattung, Prozesse, Programme und Lizenzen, Entwicklungen, Datenaustausch, Security-Einrichtungen und Security-Maßnahmen.
Alle vom Auftraggeber dem Auftragnehmer zur Verfügung gestellten Vertraulichen Informationen bleiben das alleinige Eigentum des Auftraggebers.

§ 3 Meldepflichten

1. Informationssicherheitsvorfälle sind umgehend an den Projektansprechpartner und an die eMail Adresse Informationssicherheit@schmalz.de zu melden. Es werden das Schadenereignis, Sofortmassnahmen, Ursachen und Langfristmassnahmen gemeldet. Der Ansprechpartner initiiert anschließend ohne ungerechtfertigte Verzögerung den Prozess zum Umgang mit Informationssicherheitsereignissen. Mögliche Ereignisse können beispielsweise sein:
   - unwirksame Sicherheitsmaßnahmen,
   - Verdacht auf Datenverlust, - diebstahl
   - Verstöße gegen die erwartete Vertraulichkeit
   - Fehlfunktionen von Software, die die Informationssicherheit beeinträchtigen

   Der Auftragnehmer räumt dem Auftraggeber Zutritt zu seinen Einrichtungen ein, um sich von der Umsetzung geeigneter technischer und organisatorischer Massnahmen zur Vermeidung von derartigen Ereignissen, sowie zur Schadensbegrenzung im Falle des Eintretens eines derartigen Ereignisses, zu überzeugen.

§ 4 Datenschutz

1. Jede Partei ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz, insbesondere die EU-Datenschutzgrundverordnung (DSGVO) bei der Ausführung der Vereinbarung zu beachten und die Einhaltung dieser Bestimmungen ihren Mitarbeitern aufzuerlegen.

2. Jede Partei verarbeitet etwa erhaltene personenbezogene Daten der anderen Partei (z.B. Namen und Kontaktdaten der jeweiligen Ansprechpartner) ausschließlich zur Erfüllung dieser Vereinbarung und wird diese durch technische Sicherheitsmaßnahmen (Art. 32 DSGVO) schützen, die an den aktuellen Stand der Technik angepasst sind. Jede Partei ist verpflichtet, die personenbezogenen Daten der anderen Partei zu löschen, sobald deren Verarbeitung nicht mehr erforderlich ist. Etwaige gesetzliche Aufbewahrungspflichten bleiben hiervon unberührt.

3. Sollte eine Partei im Rahmen der Vertragsdurchführung für die andere Partei personenbezogene Daten im Auftrag verarbeiten, werden die Parteien hierüber eine Vereinbarung über die Auftragsverarbeitung nach Art. 28 DSGVO schließen. Eine zusätzliche Verarbeitung für eigene Zwecke, auch in anonymisierter Form, ist ausgeschlossen.

Anlage 1
Meldeformular für Informationssicherheitsereignisse / -vorfälle

1. Allgemeine Angaben zum Vorfall

Lieferanten Name: Name/Kontaktdaten des Einreichers:
Thema des Vorfalls:
Datum: Uhrzeit:
Zeitpunkt des Vorfalls, betroffener Zeitraum:
Datenverarbeitungsverfahren:
Verantwortlicher Fachbereich:
Verantwortlicher Bearbeiter für den Vorfall:

Beschreibung Vorfall

Betroffene Systeme/Objekte
Wie hat sich der Vorfall ereignet?
Welche Folgen wurden festgestellt?

Reaktionen und Zustand des Systems

Ursachen für den Vorfall
Reaktionen/Maßnahmen auf den Vorfall (Quickfix und Langfristmassnahme zur Vermeidung des erneuten Auftretens)
Aktueller Zustand des Systems

2. Angaben zum Vorfall

2.1 Art des Vorfalls:
(Vorfälle sind z.B. Verlust der Vertraulichkeit, Datendiebstahl, Zerstörung oder Verfälschung der Daten, Übermittlung an unbefugte Stellen etc.)
2.2 Kategorien von Informationen / personenbezogenen Daten:
2.3 Wahrscheinliche Folgen/Risiken der Verletzung des Schutzes der Informationen *(Hier sind die möglichen Risiken und Folgen für die Betroffenen anzugeben.)*

3. **Eingeleitete Maßnahmen zur Behebung**

3.1 Eingerichtete Maßnahmen (Hier sind die Maßnahmen zu beschreiben, die eingeleitet worden sind.)

3.2 Weitere beabsichtigte Maßnahmen
(Hier sind die Maßnahmen zu beschreiben, deren Einrichtung aufgrund des Vorfalls zusätzlich geplant ist.)