Elmos
ESG Richtlinien

Abschnitt:	Governance
Kapitel:	Informationssicherheit
Richtlinie:	Informationssicherheit und Datenschutz
Geltungsbereich:	Elmos Konzern
Unterstützte UN SD Ziele:	
Adressierte GRI Standards:	2-27, 418

Einführung: Elmos verfügt über ein Compliance Management System (CMS). Das Elmos CMS stellt einen konzernweit verbindlichen Handlungsrahmen für alle Beschäftigten zum Zweck der Einhaltung von geltenden Gesetzen, regulatorischen Vorschriften und der über- bzw. innerbetrieblichen Regelwerke in allen Geschäftsbereichen dar. Auch die Themenbereiche Informationssicherheit und Datenschutz sind im Elmos CMS abgedeckt.

Informationssicherheit: Informationen zählen zum wertvollsten Kapital in einem Unternehmen. Daher gilt es sämtliche Informationen – analog wie digital – zu schützen. Elmos stellt sicher, dass nur autorisierte Personen Zugriff auf diese schützenswerten Informationen haben und ein unbefugter bzw. unkontrollierbarer Zugriff bzw. Weitergabe nicht erfolgen kann. Dabei orientieren wir uns an den drei wichtigsten Zielen der Informationssicherheit C – I – A (Confidentiality – Vertraulichkeit, Integrity – Integrität, Availability – Verfügbarkeit) und haben ein entsprechendes Informationssicherheitsmanagementsystem (ISMS) etabliert.

TISAX (Trusted Information Security Assessment Exchange) ist ein von der ISO 27001 abgeleiteter Standard, der den Austausch von Prüfergebnissen gemäß dem Automobilbranchen-spezifischen Standard VDA-ISA regelt. Themen sind beispielsweise die Klassifizierung von Informationen, die Geheimhaltung von Informationen (hierunter fällt auch geistiges Eigentum), die Sicherheitszonen, unser Sicherheitspersonal oder auch das Thema Cybersicherheit. Elmos hat ein Assessment nach TISAX Level 3 erfolgreich bestanden. Als innovatives Unternehmen führen wir zudem regelmäßig Gespräche mit potenziellen Geschäftspartnern. Auch dabei legen wir höchsten Wert auf Informationssicherheit und Datenschutz. Daher schließen wir jährlich zahlreiche Verträge zur Auftragsdatenverarbeitung sowie Geheimhaltungsvereinbarungen ab.

Datenschutz: Das Verbot der Verarbeitung von personenbezogenen Daten ist als Grundprinzip in der Datenschutz-Grundverordnung (DSGVO) festgelegt. Auch Elmos verpflichtet sich zur Einhaltung der DSGVO und stimmt einer Datenverarbeitung bzw. Datennutzung von personenbezogenen Daten nur dann zu, wenn sie entweder vom Gesetz erlaubt oder von den Betroffenen bewilligt wird.

Selbstverständlich wahrt Elmos sämtliche Betroffenenrechte. Entsprechende Prozessbeschreibungen zur Datenauskunft und/oder Datenlöschung sind beispielsweise in unserer Datenschutzrichtlinie festgehalten. Diese stellt das unternehmensweit geltende Regelwerk zur Umsetzung des Datenschutzes gemäß DSGVO dar. Sie bildet somit die Verhaltensrichtlinie für die Verarbeitung von personenbezogenen Daten für sämtliche Elmos Mitarbeitende. Die Datenschutzrichtlinie ist auf unserer Webseite sowie im firmeneigenen Intranet zu finden. Im Intranet findet sich zudem ein FAQ[1] zum Thema Datenschutz und DSGVO.

[1] Frequently Asked Questions / Häufig gestellte Fragen

Verantwortlichkeiten: Die Gesamtverantwortung liegt beim Vorstand. Die Verantwortung für den Themenbereich Informationssicherheit liegt bei unserem Informationssicherheitsbeauftragten. Die Verantwortung für den Themenbereich Datenschutz liegt bei unserem Datenschutzbeauftragten. Dieser führt beispielweise das von der DSGVO vorgeschriebene Verzeichnis von Verarbeitungstätigkeiten in Bezug auf personenbezogene Daten. Sowohl der Informationssicherheitsbeauftragte als auch der Datenschutzbeauftragte berichten regelmäßig und nach Bedarf, mindestens jedoch einmal pro Jahr, an Vorstand und Aufsichtsrat zum Themenfeld IT Sicherheit. Zudem kann es sein, dass bei ausgewählten Fragestellungen mit Datenschutzbezug unser Betriebsrat (aufgrund seines Mitbestimmungsrechtes) oder auch unsere IT-Abteilung (beispielsweise bei Soft- und Hardwareintegration) mit einbezogen werden.

Bei Sicherheitsvorfällen, welche die Elmos IT betreffen, ist unverzüglich auch das Computer Emergency Response Team (CERT) zu informieren, welches umgehend die nächsten Schritte definiert und einleitet. Sollte es zu einer Datenpanne gekommen sein, besteht eine interne Meldepflicht. Entsprechende Meldungen können über ein Formular im Intranet getätigt werden. Der Datenschutzbeauftragte prüft den Vorfall und leitet ggf. notwendige Maßnahmen ein.

Schulungen: Alle Beschäftigten müssen einmal im Jahr sowohl an einer Pflichtschulung zum Thema „Cyber Security“ als auch einer Pflichtschulung zum Thema „Informationssicherheitsmanagementsystem“ teilnehmen. Zusätzlich müssen alle Mitarbeitenden alle zwei Jahre an einer Pflichtschulung zum Thema „Datenschutz“ teilnehmen. Im Rahmen der Schulungen sind Präsentationen durchzuarbeiten und Wirksamkeitsüberprüfungen zu bestehen. Inhalte sind neben Begriffsdefinitionen und gesetzlichen Rahmenwerken wie der DSGVO auch Fallbeispiele zur Cybersicherheit und Anweisungen zum mobilen Arbeiten sowie der Umgang mit Videokonferenzen. In Ergänzung zu den Pflichtschulungen führt Elmos mehrmals im Jahr unternehmensweite Phishing Tests zur Sensibilisierung der Mitarbeitenden durch.

ESG Richtlinien	Compliance Management System (CMS) Qualitäts- und Krisenmanagement Unternehmensethik und Anti-Korruption
ESG KPIs	Durchschnittliche Schulungsstunden
Zertifikate	Qualitätsmanagementsystem-Zertifikat IATF 16949:2016
Begleitende Dokumente	Code of Conduct für Lieferanten und Geschäftspartner Verhaltenskodex für Mitarbeiterinnen und Mitarbeiter
Weitere Dokumente	Datenschutzerklärung