EU Data Act & IoT-Daten im Unternehmen

In vielen Unternehmen schlummern riesige Datenmengen – insbesondere aus vernetzten Maschinen, Fahrzeugen, Sensoren und anderen IoT-Systemen. Diese Daten bergen ein enormes Potenzial: Sie ermöglichen effizientere Prozesse, neue Geschäftsmodelle und datengetriebene Entscheidungen – vom vorausschauenden Maschinenservice über optimierte Logistik bis hin zu smarten Services für Kunden. Mit dem EU-Data Act werden nun klare Spielregeln geschaffen, wer diese Daten in welchem Umfang nutzen darf und unter welchen Bedingungen sie zwischen Unternehmen, Nutzern und Drittanbietern geteilt werden können. Dabei geht es nicht nur um technische Fragen, sondern vor allem um rechtliche Rahmenbedingungen, Transparenz und faire Verträge.

Gleichzeitig steigen die Anforderungen an Datenschutz, Informationssicherheit und Compliance. IoT-Daten sind häufig eng mit personenbezogenen oder geschäftskritischen Informationen verknüpft, sodass eine klare Datenklassifikation, definierte Rollen und Verantwortlichkeiten sowie ein belastbares Governance-System unerlässlich sind. Unternehmen müssen wissen, welche Daten sie verarbeiten, wem diese gehören, auf welcher Grundlage sie genutzt werden dürfen und wie Risiken – etwa durch Cyberangriffe, Fehlkonfigurationen oder unsichere Schnittstellen – beherrscht werden.

Data-Act-Konformität prüfen und herstellen

Für eine erste Information und zur Selbsteinschätzung haben wir zum Thema *Data Act & IoT-Daten im Unternehmen* eine Datenschutzzeitung erstellt, die Sie gerne bei uns anfordern können. Alternativ bieten wir Ihnen sehr gerne einen unverbindlichen und für Sie

kostenfreien Beratungstermin

an. In diesem gehen wir auf alle rechtlichen Vorgaben ein, skizzieren erste Schritte und sorgen dafür, dass auch Sie rechtssicher agieren, wenn es um den Umgang mit IoT-Daten und die Anforderungen des EU Data Act geht.

Antwort

Ja, wir hätten gerne eine Beratung zum Thema Datenschutz im Allgemeinen oder im Speziellen zum Thema *EU Data Act & IoT-Daten im Unternehmen*.

	Ja	Nein
Wir hätten gerne eine Beratung zum Thema *EU Data Act & IoT-Daten im Unternehmen*.	☐	☐
Bitte senden Sie uns Ihre Datenschutzzeitung zum Thema *EU Data Act & IoT-Daten im Unternehmen* kostenfrei zu.	☐	☐
Wir haben bereits einen betrieblichen oder externen Datenschutzbeauftragten.	☐	☐

Firma, Organisation

Straße

PLZ | Ort

Ansprechpartner

Telefon

E-Mail

Bitte senden Sie diese unverbindliche Anfrage an:

CS Hard- & Software Consulting GmbH
Saarbrücker Straße 72
66386 St. Ingbert

Tel.: 06894 38797 - 0
Fax: 06894 38797 - 99

Web: www.compusaar.de
E-Mail: info@compusaar.de

Datenschutz für Unternemen

EU Data Act & IoT-Daten im Unternehmen

EU Data Act: neue Regeln für IoT-Daten

Der EU-Data Act legt einheitliche Spielregeln dafür fest, wie Daten – insbesondere aus IoT-Geräten und vernetzten Systemen – genutzt und geteilt werden dürfen. Er richtet sich vor allem auf Produkt- und Nutzungsdaten, die bei der Verwendung von Maschinen, Fahrzeugen, Anlagen oder smarten Geräten entstehen. Ziel ist es, bisher ungenutzte Datenpotenziale endlich wirtschaftlich nutzbar zu machen, Innovation zu fördern und gleichzeitig faire Wettbewerbsbedingungen zu schaffen – etwa durch standardisierte Verträge und klare Fristen für Datenzugänge.

Was ändert sich für Unternehmen?

Nutzer von vernetzten Produkten erhalten mehr Rechte auf Zugang zu „ihren" Nutzungsdaten und können diese auch Dritten zur Verfügung stellen, etwa für Service-, Analyse- oder Optimierungsangebote. Hersteller und Anbieter müssen diese Zugriffsrechte bereits bei der Entwicklung ihrer Produkte („by Design") berücksichtigen, Datenzugänge technisch ermöglichen und vertraglich klar regeln, welche Daten zu welchen Zwecken verarbeitet werden dürfen. Das betrifft nicht nur IoT-Geräte, sondern auch angebundene Plattformen, Cloud-Dienste und faire Konditionen bei der Datenfreigabe.

Zusammenspiel mit DSGVO & NIS2

Der Data Act ersetzt keine bestehenden Regelwerke, sondern ergänzt sie. Für personenbezogene Daten gelten weiterhin die Anforderungen der DSGVO, für kritische Infrastrukturen und Systeme zusätzlich die Vorgaben aus NIS2. Unternehmen müssen daher prüfen, wie Datenzugangs- und Nutzungsrechte nach Data Act mit Datenschutz, Informationssicherheit und bestehenden Verträgen zusammenpassen. Wer hier rechtzeitig nachsteuert, reduziert Haftungsrisiken und kann Datennutzung, Compliance und Sicherheit in ein stimmiges Gesamtkonzept bringen.

IoT-Daten managen und sichern

Arten, Nutzung und Risiken

IoT-Daten fallen überall an, wo Geräte vernetzt sind: in Produktion (Maschinensensoren, Zustandsdaten), Logistik (Positionsdaten) oder Verwaltung (Energieverbrauch). Sie ermöglichen Predictive Maintenance, Prozessoptimierung und neue Services, sind aber oft mit personenbezogenen oder geschäftskritischen Infos verknüpft. Risiken reichen von Cyberangriffen über Fehlkonfigurationen bis zu unkontrollierter Weitergabe – hier hilft eine klare Datenklassifikation (öffentlich, vertraulich, personenbezogen).

Datensouveränität und DSFA

Datenklassifikation bildet die Basis für Souveränität: Wer besitzt welche Daten, zu welchen Zwecken und unter welchen Bedingungen? Eine Datenschutz- Folgenabschätzung (DSFA) ist bei hohem Risiko Pflicht – Schritt für Schritt analysieren, Vorlagen nutzen, in Governance einbetten. So definieren Unternehmen Schutzbedarfe, Zugriffsrechte und ethische Standards, vermeiden Überschneidungen mit DSGVO und schaffen Transparenz für Audits.

Technische Sicherheitsmaßnahmen

Stand der Technik umfasst Verschlüsselung (Ende-zu-Ende, TLS), Zero Trust, Monitoring und Edge/Cloud-Hybride. Incident Response, Business Continuity und Zertifizierungen sichern den Betrieb. „Security by Design" gilt für Hardware, Software und Gerätelebenszyklus – von Inbetriebnahme bis Decommissioning.

Umsetzung, Monitoring und Ausblick

Drittanbieter und Schnittstellen

Auftragsverarbeitung, APIs und Plattformen brauchen klare Verträge, Due Diligence und Sicherheitskonzepte. Data Sharing regeln, Risiken minimieren – etwa durch Audit-Rechte und API-Härtung. So bleibt die Wertschöpfungskette datenschutzkonform.

Organisation und Awareness

Klare Rollen (Management, Datenschutzbeauftragte, IT), Schulungen und Kommunikation schaffen Kultur. Kennzahlen tracken Compliance, Protokollierung erleichtert Nachweise und Berichtspflichten.

Handlungsempfehlungen

Synergien mit NIS2, KI-VO nutzen, Checkliste für Führungskräfte einsetzen.

Fordern Sie unsere neue Datenschutzzeitung an!

Falls Sie mehr über den EU Data Act und die neuen Regeln für den Umgang mit IoT-Daten erfahren möchten, dann können Sie gerne unsere aktuelle Datenschutzzeitung anfordern. Mit dieser erhalten Sie weiterführende Informationen, erste Orientierungshilfen und Einblick in die Verzahnung mit DSGVO und NIS2. Zudem erhalten Sie weiterführende Informationen zu Datenschutz-Folgenabschätzungen und technischen Sicherheitsmaßnahmen und Zugriff auf eine Checkliste für Führungskräfte, die Ihnen als Einstieg dient, um den eigenen Status einzuschätzen und nächste Schritte zu planen.

Wir helfen sehr gerne!

Nutzen Sie die Chance und vereinbaren Sie mit uns einen für Sie kostenfreien Beratungstermin. In diesem erarbeiten wir gemeinsam Lösungen und Handlungsempfehlungen, mit denen auch auch Sie rechtssicher agieren, wenn es um den Umgang mit IoT-Daten und den Anforderungen des EU Data Act geht.