Boardroom Questions

DSGVO / Schweizer Datenschutzgesetz
Sind Sie bereit für die neue Datenschutz-Ära?

Die Datenschutz-Grundverordnung (DSGVO) – in der EU jetzt vollständig in Kraft – ist der Beginn einer neuen Ära für den Datenschutz. Was können wir in der Schweiz, die dem Vorstoss der EU in Kürze folgen wird, daraus bereits lernen? Neben dem vorsätzlichen Missbrauch von Daten wurden Unternehmen insbesondere wegen Fahrlässigkeit und unzureichender Cyber-Sicherheitsmassnahmen verurteilt. Wie steht es um Ihre Compliance und welche Strategie verfolgen Sie im Hinblick auf die Zukunft des Datenschutzes in Ihrem Unternehmen?

Für EU-Firmen und Schweizer Unternehmen, die in der Europäischen Union tätig sind, ist der DSGVO-Compliance-Prozess bereits in vollem Gange. Ihre Aufgabe für die kommenden Jahre besteht darin, bereits vorhandene, grundlegende Compliance-Strukturen zu optimieren und auszuweiten.

Die Schweiz gleicht derzeit ihr eigenes Datenschutzgesetz (DSG) an die DSGVO an und es ist nur eine Frage der Zeit, bis Schweizer Unternehmen ähnliche Verpflichtungen – und Herausforderungen – wie ihre Mitstreiter in der EU haben.

Doch auch unabhängig von den rechtlichen Anforderungen untergraben Datenschutzverletzungen das Vertrauen der Verbraucher und sind schädlich für Marke und Reputation – ein weiterer Grund dafür, dass die Verwaltungsräte das Thema Datenschutz fest in ihre Tagesordnung aufnehmen sollten.

Höchste Zeit, der Compliance mehr Priorität einzuräumen und in Sachen Datenschutz weiter voranzukommen.

Warum sollten Sie dieses Thema ernst nehmen?

- In einer Welt, in der Cyber-Angriffe zum Alltag gehören, können Unternehmen es sich nicht mehr leisten, die Risiken von Datenschutzverletzungen zu ignorieren.
- Täter mit zumindest grundlegenden – und nachweisbaren – DSGVO-Compliance-Massnahmen werden von den EU-Behörden in der Regel nachsichtiger behandelt, weshalb es wichtig ist, die einzelnen Schritte der Entwicklungsphase genau zu dokumentieren.
- Das revidierte Datenschutzgesetz der Schweiz wird die gleichen Anforderungen an die Compliance-Struktur stellen wie die DSGVO.
- Die Verwaltungsräte müssen gewährleisten, dass entsprechende Massnahmen effektiv und effizient umgesetzt werden, also auch in der Praxis tatsächlich funktionieren.
- Mögliche Lücken können frühzeitig im Rahmen von Compliance-Prüfungen aufgedeckt werden. Führen die Massnahmen wirklich dazu, dass sämtliche Datenschutzverpflichtungen eingehalten werden?

Welche Fragen sollte sich der Verwaltungsrat stellen?

- Haben wir die erforderlichen DSGVO-Compliance-Massnahmen umgesetzt und sind sie wirksam?
- Falls die DSGVO für uns als Schweizer Firma bisher nicht relevant war, wäre ein DSGVO-Compliance-Programm als Vorbereitung auf das revidierte DSG in der Schweiz sinnvoll?
- Wie sieht unsere Governance-Strategie für die Datenschutz-Compliance aus? Haben wir die Umsetzung und Wirksamkeit unserer Compliance-Strukturen überprüft?
- Wie hoch ist unser Restrisiko?
- Fördern wir durch die Kommunikation unserer Datenschutzmassnahmen nach aussen das Vertrauen unserer Stakeholder?

Welche Fragen sollte der Verwaltungsrat an sein Führungsteam richten?

- Was müssen wir noch tun, um die Compliance sicherzustellen, eine reibungslose Umsetzung der noch laufenden Massnahmen zu gewährleisten und das Restrisiko weiter zu senken?
- Wie sehen unsere Planung und das Budget aus?
- Wie effizient nutzen wir unsere Compliance-Strukturen? Haben wir Automatisierung (sogenannte «Electronic Governance, Risk and Compliance (eGRC)»-Tools) und Möglichkeiten für Outsourcing (z. B. DSB-Dienstleistungen) ausreichend berücksichtigt?
- Wer ist für die Einhaltung des neuen Schweizer DSG verantwortlich?
- Ist die Rahmenstruktur in unser Risk and Compliance Management integriert und gibt es überprüfbare Kontrollen?
- Wie gewährleisten wir den Datenschutz für Dritte, mit denen wir zu tun haben?

Beurteilen	Planen	Umsetzen und automatisieren	Überwachen
Ermitteln Sie Lücken bei der Compliance Ihres Unternehmens unter Berücksichtigung aktueller und künftiger Datenschutzvorschriften.	Entwickeln Sie einen Fahrplan einschliesslich Prozessen, Systemen und Kontrollen zur Gewährleistung Ihrer Datenschutz-Compliance.	Stellen Sie eine effektive und effiziente (eGRC-automatisierte Rahmenstruktur, Nutzung ausgelagerter DSB-Dienstleistungen) Umsetzung der Compliance-Massnahmen sicher.	Überwachen Sie fortlaufend die Datenschutz-Compliance Ihres Unternehmens. Richten Sie Kontrollen ein. Kommunizieren Sie Ihre Datenschutz-Compliance mit Assessments oder einem Zertifizierungssystem an wichtige Stakeholder.

Kontakt

KPMG AG
Badenerstrasse 172
Postfach
8036 Zürich

kpmg.ch/blc

Matthias Bossardt
Partner
Head of Cyber Security
and Technology Risk
+41 58 249 36 98
mbossardt@kpmg.com

Thomas Bolliger
Partner
Information Management
& Compliance
+41 58 249 28 13
tbolliger@kpmg.com