

# NEUES EU-DATENSCHUTZRECHT: COMPLIANCE CHECK

Am 25. Mai 2018 wird die Datenschutzgrundverordnung (DS-GVO) der EU wirksam werden, die erhöhte Nachweis- und Kontrollpflichten beinhaltet. Um die Einhaltung des neuen Rechts sicher zu stellen, müssen die Organisationen umfangreiche Kontrollmechanismen etablieren. Das Prinzip der Nachweisbarkeit verlangt von den Organisationen, die Compliance belegen zu können. Ein Verstoß kann zu erheblichen **Bußgeldern** von bis zu EUR 20.000.000 oder 4 % des jährlichen Umsatzes führen. Wir **empfehlen**, sich frühzeitig vorzubereiten, um eine Compliance bis Mai 2018 sicher zu stellen.

## 1. Information

Zunächst sollten Sie sich umfassend über die neuen Regelungen informieren und Ihre Datenverarbeitung prüfen lassen.

## 2. Eruierung der Datenprozesse

Danach sind die Bereiche ausfindig zu machen, in denen Datenprozesse stattfinden: Typischerweise sind dies vor allem HR und CRM (inkl. Marketing).

## 3. Analyse der Prozesse

Jeder Prozess muss im Einzelnen darauf analysiert werden, ob die Datenschutzprinzipien eingehalten sind. Zusätzlich müssen die Unternehmen die Rechtsgrundlage jedes Datenprozesses bestimmen. Soweit der Prozess auf einer Einwilligung beruht, ist zu prüfen, ob den Betroffenen nachweislich die erforderlichen Informationen gegeben wurden.

## 4. Analyse der internen Prozesse

Ferner müssen die internen Prozesse sowie die IT-Systeme überprüft werden. Es sind die organisatorischen und technischen Maßnahmen zur Datenschutzsicherung zu definieren und Verantwortlichkeiten zu bestimmen. Die Aufsichtsbehörden erwarten, dass Datenschutzberichte bis in die obersten Managementebenen eskaliert werden. Hinsichtlich der erforderlichen technischen Maßnahmen ist ein IT-Experte zu Rate zu ziehen.

## 5. Richtlinien und Erklärungen

Sobald die internen Prozesse geprüft wurden, müssen die entsprechenden organisatorischen und technischen Maßnahmen in interne Richtlinien umgesetzt werden. Unternehmen sollten insbesondere über eine Datenschutzrichtlinie zur Verarbeitung von Arbeitnehmerdaten sowie eine zu Kundendaten verfügen. Ebenfalls sollten Handlungsanweisungen zum Vorgehen bei Datenschutzverstößen und Datenübertragungen existieren. Ferner ist auch Ihre Datenschutzerklärung zu aktualisieren bzw. zu erstellen, in denen Sie Personen, die mit Ihnen in Kontakt treten, über die Nutzung Ihrer personenbezogenen Daten informieren.

## 6. Dokumentation

Für bestimmte Datenverarbeitungsprozesse bestehen Dokumentationspflichten. Wir empfehlen Ihnen generell, jegliche Datenprozesse zu dokumentieren, um Ihrer Nachweisbarkeitspflicht zu genügen.

## 7. Datenschutzbeauftragter

Bestimmte Arten von Unternehmen sind verpflichtet, einen Datenschutzbeauftragten zu bestellen. Sie müssen prüfen, ob dies auch für Ihr Unternehmen zutrifft.

## 8. Sensibilisierung und Schulung

Mitarbeiter mit Zugang zu personenbezogenen Daten müssen über die neuen Anforderungen informiert werden.

Überwachung und Sicherheit sind kontinuierliche Prozesse, die Sie fortlaufend während des gesamten Datenverarbeitungsprozesses zu beachten haben.

Die vorliegende Zusammenfassung gibt einen generellen Überblick über ein Datenschutzaudit. Ob diese für Ihr Unternehmen unter Ihrer Rechtsprechung zutrifft, bedarf der konkreten Analyse. Soweit Sie ein solches Verfahren durchführen möchten, kontaktieren Sie bitte eine unserer Kanzleien zur Beratung.

