

10 SCHRITTE ZUR ERFÜLLUNG DER EU-DSGVO



Am 25. Mai 2018 tritt die EU-DSGVO in Kraft.

Dass eine fehlende Umsetzung der erforderlichen Maßnahmen in hohen Bußgeldern und Imageschäden resultieren kann, werden Sie mehrfach gehört haben. Doch was können Sie jetzt noch tun, wenn Sie noch nicht alle Anforderungen erfüllen?

Mit den folgenden Schritten leiten Sie die richtigen Maßnahmen zur Erfüllung der EU-DSGVO-Anforderungen in die Wege:

DER 10 SCHRITTE-PLAN:

1. Stellen Sie sicher, dass Sie die aktuellen nationalen Richtlinien zum Schutz personenbezogener Daten gemäß Bundesdatenschutzgesetz (BDSG) eingehalten werden.
2. Klären Sie, welche der gespeicherten Daten von der EU-DSGVO betroffen sind. Bei personenbezogenen Daten handelt es sich nicht nur um Namen, Sozialversicherungsnummern oder Bankverbindungen. Es existieren auch weniger offensichtliche Daten wie z.B. KFZ-Kennzeichen, Reisebuchungsnummern, Smartwatch-Daten, Mieteinnahmen oder persönliche Gutscheinnummern.
3. Klassifizieren Sie Ihre Daten und klären Sie, an welchen Stellen diese abgelegt sind. Oftmals liegen diese Daten an mehr Orten als ursprünglich gedacht.
4. Beachten Sie, dass auch die personenbezogenen Daten der eigenen Mitarbeiter unter den Schutz der EU-DSGVO fallen.
5. Definieren Sie, auf welche Weise Sie die Zustimmung zur Speicherung der personenbezogenen Daten einholen. Beachten Sie, dass Sie bei Minderjährigen die Zustimmung der Erziehungsberechtigten benötigen.
6. Implementieren Sie Prozesse für das Ablegen, Verarbeiten und Löschen von personenbezogenen Daten. Mit einem Informationsmanagementsystem (ISMS) lässt sich ein Regelwerk erstellen, mit dem dauerhaft die Gewährleistung der Informationssicherheit gesteuert, aufrechterhalten und kontinuierlich verbessert werden kann.
7. Stellen Sie sicher, dass Sie wissen, wer Zugriff auf die personenbezogenen Daten hat. Eine Zwei-Faktor-Authentifizierung ermöglicht es Ihnen, zu belegen, wer Zugriff auf die sensiblen Daten und deren Management hat.
8. Finden Sie einen sicheren Weg vertrauliche Daten auszutauschen. Gerade personenbezogene Daten dürfen nicht einfach als Anhang per E-Mail weitergeleitet werden. Hier müssen entsprechende Sicherheitsvorkehrungen wie Verschlüsselungsmechanismen verwendet werden.
9. Definieren Sie ein Vorgehen für den Fall von Verstößen gegen die Datensicherheit. Eine Meldung bei der entsprechenden Behörde muss laut der EU-DSGVO ohne unangemessene Verzögerung erfolgen.
10. Bei Unternehmen mit mehr als 250 Mitarbeitern gelten noch strengere Regeln. Sie müssen begründen, warum die personenbezogenen Daten erfasst, dokumentiert und verarbeitet werden. Ferner ist eine konkrete Beschreibung der technischen Sicherheitsmaßnahmen zum Schutz der vorgehaltenen Informationen erforderlich.

Die Europäische Union rät im Rahmen der EU-DSGVO zu einer engeren Zusammenarbeit mit einem Datenschutzbeauftragten.

FRAGEN SIE NACH DEM EU-DSGVO UND ISMS WORKSHOP!
Wir zeigen Ihnen, welche individuellen Maßnahmen Ihr Unternehmen treffen muss und helfen Ihnen dabei.

Bei diesen Schritten handelt es sich um eine Empfehlung zur Umsetzung von erforderlichen Maßnahmen, nicht um eine Garantie, dass Sie hiermit bereits alle Anforderungen der EU-DSGVO erfüllen.

Wir unterstützen Sie bei der Einführung Ihres Informations-sicherheitsmanagementsystems (ISMS) und bieten Ihnen bereits erprobte, praxisnahe Compliance Services & Solutions im Bereich IT-Sicherheit an.

Sprechen Sie uns an:



Ihr Team der Makro Factory
+49 721 97 00 30
info@makrofactory.com



makrofactory
strategies for a virtual world