



Implementierung in der Praxis

Die Umsetzung der DSGVO in Ihrem Unternehmen in 12 konkreten Schritten

Linde Business-Breakfast, 5. Dezember 2017



Schritt 1

Unterstützung aus dem Management sichern

DSGVO-Umsetzung erfordert

- Personalressourcen
- Budget
- (unternehmens-)politische Unterstützung

Motivation des Managements?

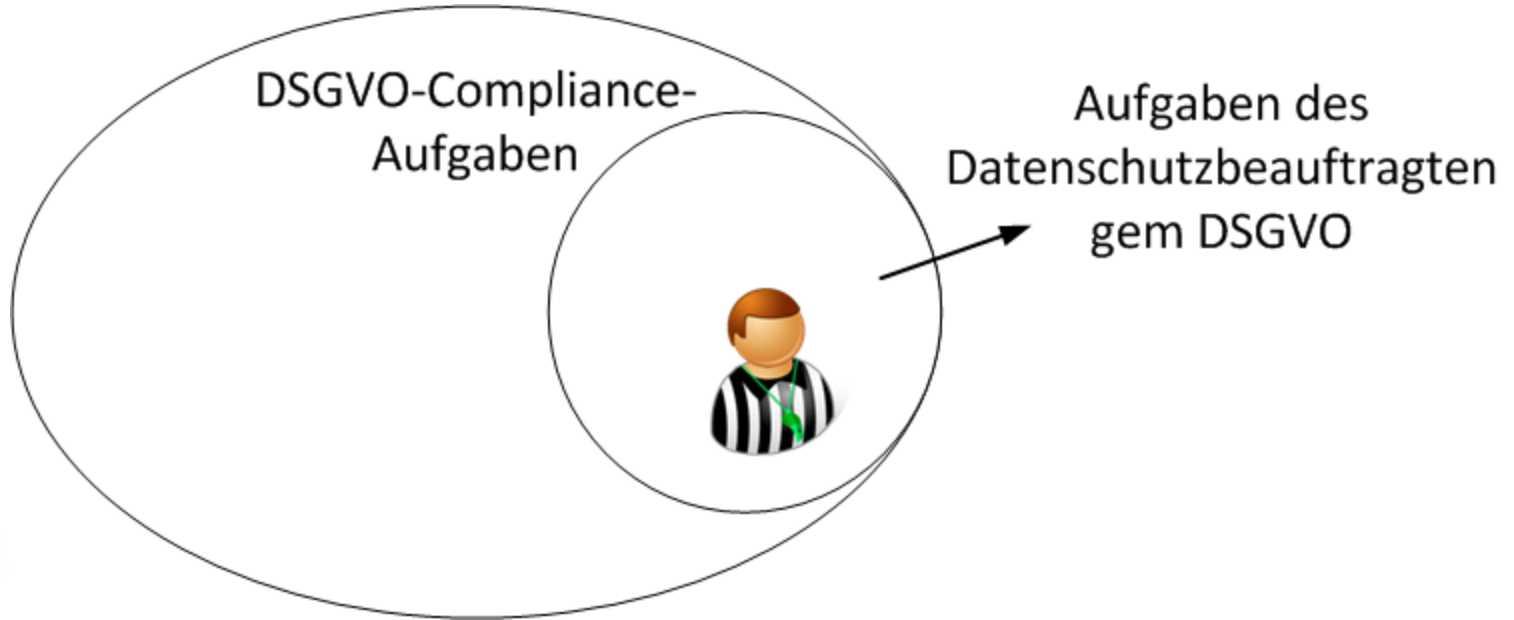
- persönliche Haftung (im Regress) für Verstöße
- negative PR und Verlust der Managementposition

Schritt 2

Datenschutzbeauftragten/Manager ernennen



Datenschutz-Manager?



Schritt 3

Ersten Überblick verschaffen

Welche Arten von IT-Systemen nutzt das Unternehmen?

- Mitarbeiterdaten: Lohnbuchhaltung, E-Mail-System, Telefonsystem, Human Capital Management (HCM) System (z.B. Workday oder SAP SuccessFactors), ...
- Kundendaten: Rechnungswesen, CRM System (zB Salesforce.com), ...
- Lieferantendaten: Rechnungswesen, SCM Systeme (zB Oracle SCM), ...

Wie sieht die gesellschaftsrechtliche Struktur des Unternehmens aus?

- Welche Gesellschaften/Niederlassungen in welchen Ländern?
- Beteiligungsstrukturen?

Welche Geschäftssparten hat das Unternehmen?

- B2B und/oder B2C

Schritt 4

Ziele des Datenschutzmanagements definieren

Konzernweite Datenschutzstrategie vs. dezentraler Ansatz

- Für welche Gesellschaften ist die Datenschutzstrategie verbindlich?

Aus personenbezogenen Daten einen wirtschaftlicher Wert gewinnen?

- Defensive vs. offensive Datenschutzstrategie

100% Compliance oder pragmatischer Compliance-Ansatz?

- Betriebswirtschaftliche vs. politische Risiken

Wer ist wofür zuständig?

- Rollen und Verantwortlichkeiten definieren

Schritt 5

IT-Tools für Datenschutz-Management auswählen

Richtige Werkzeuge erleichtern die Arbeit – MS Office-Vorlagen vs. Online-Tools:

- Verzeichnis der Verarbeitungstätigkeiten
- Privacy Impact Assessments
- Verzeichnis der Sicherheitsverletzungen

Schritt 6

Infos über Datenverarbeitungsprozesse erheben

Für jede Verarbeitungstätigkeit zu klären:

- Wer ist der Verantwortliche?
 - Welche Datenkategorien werden verarbeitet?
 - Zu welchen Zwecken erfolgt die Verarbeitung?
 - Werden Auftragsverarbeiter eingesetzt? (Welche? Wo? Vertragsgrundlage?)
 - Werden Daten an andere Verantwortliche übermittelt? (Welche? An wen? Zu welchen Zwecken? Wohin? Vertragsgrundlage?)
 - Verarbeitung auf Grundlage einer Einwilligung? (Kopie der Einwilligungserklärung?)
 - Kopie der Datenschutzerklärung (sofern vorhanden)
 - Datensicherheitsmaßnahmen
- Vorbedingung für VZ der Verarbeitungstätigkeiten (Schritt 7) und Prüfung der Rechtmäßigkeit (Schritt 8)

Schritt 7

Verzeichnis der Verarbeitungstätigkeiten erstellen

Informationen aus Schritt 6 mit Tools aus Schritt 5 erfassen

Zu klärende Fragen im internationalen Konzern

- Sprache des Verzeichnisses – ist Englisch für zuständige Behörde ausreichend?
- Zugänglichkeit des Verzeichnisses – ist Online-Zugang für zuständige Behörde ausreichend?

Schritt 8

Rechtmäßigkeit der Verarbeitungstätigen prüfen

Für jede Verarbeitungstätigkeit

- Rechtsgrundlage für Datenverarbeitung identifizieren
- ggfls. wirksame Zustimmungserklärungen entwerfen
- Datenschutzmitteilungen korrekt gestalten
- Auftragsdatenverarbeitungsvereinbarungen mit Dienstleistern abschließen
- Wo erforderlich Standardvertragsklauseln für internationale Datenübermittlungen vereinbaren

Schritt 9

Privacy Impact Assessments durchführen

Für jede Verarbeitungstätigkeit

- Prüfen, ob prima facie ein hohes Risiko für Betroffene gegeben ist (z.B. sensible Daten, Profiling oder „schwarze Liste“ der Datenschutzbehörde)
- Nur wenn prima facie hohes Risiko gegeben ist: Privacy Impact Assessment durchführen
- Wenn PIA ein hohes Risiko ergibt: Konsultation mit der Datenschutzbehörde

Schritt 10

Datenschutzrelevante Unternehmensrichtlinien

Datenschutzrelevante Unternehmensrichtlinien erstellen

- Richtlinie zum Umgang mit personenbezogenen Daten
- Richtlinie zur Informationssicherheit
- Richtlinie zur Reaktion auf Zwischenfälle
- Richtlinie zur Nutzung der Unternehmens-IT
- BYOD-Richtlinie
- ...

Schritt 11

Konzept für Info-Maßnahmen und Schulungen

Konzept für unternehmensinterne Informationsmaßnahmen und Schulungen erstellen

- Wen wie oft schulen?
- Kreatives Awareness-Raising
- Compliance am Papier vs. tatsächliche Compliance

Schritt 12

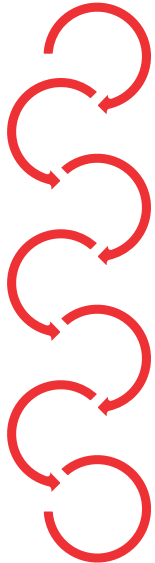
Datenschutz im täglichen Betrieb aufrechterhalten

DSGVO-Umsetzung kontinuierliche Compliance-Maßnahmen:

- Audits durchführen
- Schulungen abhalten
- Auf Zwischenfälle reagieren
- Anfragen von Betroffenen bearbeiten
- Neue Verarbeitungstätigkeiten erfassen
- An das Management berichten

Schritte 1 bis 12

Übersicht



- 1) Unterstützung aus dem Management sichern
- 2) Datenschutzbeauftragten/Manager ernennen
- 3) Ersten Überblick verschaffen
- 4) Ziele des Datenschutzmanagements definieren
- 5) IT-Tools für das Datenschutz-Management auswählen
- 6) Informationen über Datenverarbeitungsprozesse erheben
- 7) Verzeichnis der Verarbeitungstätigkeiten erstellen
- 8) Rechtmäßigkeit der Verarbeitungstätigkeiten prüfen
- 9) Datenschutz-Folgeabschätzungen durchführen
- 10) Datenschutzrelevante Unternehmensrichtlinien erstellen
- 11) Konzept für Informationsmaßnahmen & Schulungen
- 12) Datenschutz im täglichen Betrieb aufrechterhalten



Dr. Lukas Feiler, SSCP CIPP/E

Senior Associate
Baker McKenzie

Schottenring 25
1010 Vienna
Austria

T: +43 1 24 250

lukas.feiler@bakermckenzie.com

www.bakermckenzie.com

Diwok Hermann Petsche Rechtsanwälte LLP & Co KG is a Member of Baker & McKenzie International, a Verein organized under the laws of Switzerland with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

© 2017 Diwok Hermann Petsche Rechtsanwälte LLP & Co KG