integratio

Auswirkungen der DSGVO auf die Risikobeurteilung in Unternehmen

17. November 2020

Philippe Baumann, Integratio GmbH, Zürich

Datenschutz Forum Schweiz

Risikobeurteilungen sind nichts Neues

In vielen Branchen ein alltägliches Werkzeug

- **Fahrzeug:** Crashtests
- **Medizinaltechnik und Pharma:** Klinische Studien
- **Bau:** Statiker
- **Banken: Vorgaben der FINMA;** Basel I,II,III
- **Anwälte:** Abwägen von Prozessrisiken

Und beim Datenschutz? …..

Risikoanalysen bei der Verarbeitung personenbezogener Daten

Bisher …

- **… wurden Risikoanalysen eher stiefmütterlich behandelt**
- **… wenn angewandt dann mit Schwerpunkt IT-Sicherheit**
  - Risiken: Diebstahl, Verlust, Erpressung, Zerstörung, …
- **… fehlten oftmals Grundlagen:**
  - Verarbeitungsdokumentationen, Datensammlungen, Kategorisierung der verarbeiteten Daten, Kategorisierung der betroffenen Personen, Listen der Empfänger, …
- **Keine oder wenig Konsequenzen bei Nichteinhaltung des Datenschutzes**

Seit 2018 hat sich vieles markant geändert

- **DSGVO-Bussgelder wirken!**
  - Wirksam und abschreckend
  - Haftung der Geschäftsleitung
- **Datenschutz ist Geschäftsleitungs-Thema**
- **Fragestellung nach den Risiken einer Sanktionierung steht im Zentrum**
- **Risikobeurteilung als Forderung der Shareholder**
- **DSGVO: risikobasierter Ansatz**
  - Risikobasierte Entscheidungen: Festlegung der Mittel, Umsetzung TOMs, Meldung Data Breach, Schwellenanalyse für DSFA etc.

Risikobeurteilung als zentrales Element

- **Erfahrung aus der Praxis: Kein Datenschutzprojekt ohne Risikobeurteilung**

- **Risikobeurteilungen müssen professionell, methodisch, nachvollziehbar und dokumentiert sein**
  - Keine individuelle Sicht und persönliche Präferenzen, kein Bauchgefühl

- **Die Sicht auf das eigene Unternehmen reicht nicht mehr aus -> Supply Chain (Auftragsverarbeitung etc.)**

Erfahrung aus der Praxis
Fallstricke

- **Basisinformationen über Verarbeitungen und Daten fehlen oder sind unvollständig**
  - Vor der Risikoanalyse erforderlich: Kartographieren und Dokumentieren der IT-Systeme, Datensammlungen, -flüsse und –verarbeitungen
  - Fokus auf personenbezogene Daten fehlt oftmals
- **Zu komplexe Methodiken der Risikoanalyse**
  - Abgeleitet aus z.B. IT-Security
  - Spezialisierte Mitarbeiter erforderlich
  - Nicht KMU-gerecht
- **Interne Mitarbeiter zu wenig eingebunden**

Erfahrung aus der Praxis
Lösungunsansätze

- **Risikobeurteilungen einheitlich und messbar machen:**
  - Schaffen einer einheitlichen Sprache
    - Gleicher Wortschatz
  - Standardisierte Checklisten, z.B. zur Erfassung von Risiken
  - Standardisierte Formeln zur Bewertung der Risiken
- **Interne Mitarbeiter iterativ einarbeiten**
  - Gleichzeitige Sensibilisierung

Erfahrung aus der Praxis
Mehrwert

Identifikation, Senkung und Management der Risiken.

Weiterer Mehrwert:

- Erhöhter Dokumentationsgrad
- Fundierte Entscheidungsgrundlagen
- Bessere Nachvollziehbarkeit und Transparenz
- Identifikation und Bewertung von Schwachstellen im Unternehmen
- Vorbereitet sein auf das was noch kommt…

Risikobeurteilungen in einem dynamischen Umfeld

- **Zunehmende und vielschichtige Risiken**
  - Cyber-Angriffe, Social Hacking
- **Rechtsgrundlagen, Rechtssprechung:**
  - US Cloud-Act
  - EU-US Privacy Shield-Urteil des EuGH
  - DSGVO, revidiertes DSG
- **Erhöhte Anforderungen**
  - Cyber Security Act (EU)

> Bewältigen mit Risikobeurteilungen als wiederkehrende Aufgabe

Fragen?