Informationstag "IT-Sicherheit in der Marktforschung"

Gemeinsame Veranstaltung von

Bundesverband IT-Sicherheit e.V.

Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.

Deutsche Gesellschaft für Online Forschung e.V.

Verband der Marktforscher Österreichs

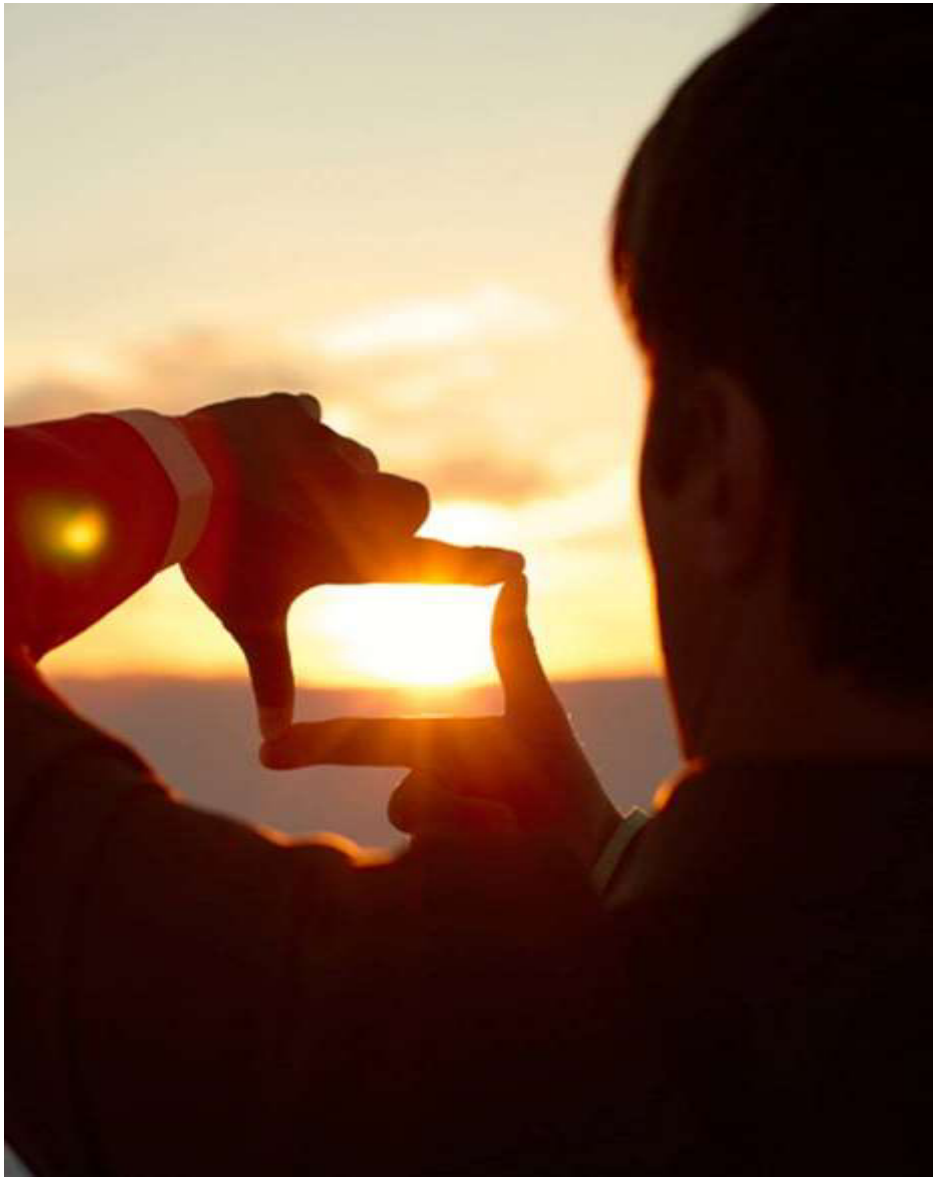
10.06.2016

Wirtschaftskammer Wien, Blauer Saal, Schwarzenbergplatz 14, 1010 Wien

TaylorWessing

Rechtliche Aspekte in der Informationssicherheit

in der Markt- und Sozialforschung



TeleTrusT
Pioneers in IT security.

10. Juni 2016

Inhalt

01 > Rechtliche Vorgaben im Informationssicherheitsbereich

- Relevante Gesetze für den Informationssicherheitsbereich
- Datensicherheit

02 > Datensicherheit nach dem DSG 2000

03 > EU-Datenschutz-Grundverordnung

- Überblick
- Änderungen

1. Rechtliche Vorgaben im Informations-sicherheitsbereich

Relevante Gesetze für den Informationssicherheitsbereich

- Geschäftsführerhaftung (UGB, GmbHG)
- Arbeitsrecht (ArbVG, AVRAG, ABGB)
- Verbandsverantwortlichkeitsgesetz (VbVG)
- Datenschutzgesetz: Datensicherheit (§ 14 DSG 2000)
- Data Breach Notification Duty (§ 24 Abs.2a DSG 2000)
- EU-Datenschutzgrundverordnung (DSGVO)

Datenschutz und Informationssicherheit

> Informationssicherheit:
  - Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen
  - Schutz jeglicher Informationen
  - Informationssicherheit ≥ Datensicherheit

> Datensicherheit:
  - Auftraggeber und Dienstleister sind verpflichtet, Maßnahmen zur Gewährleistung der Datensicherheit zu treffen

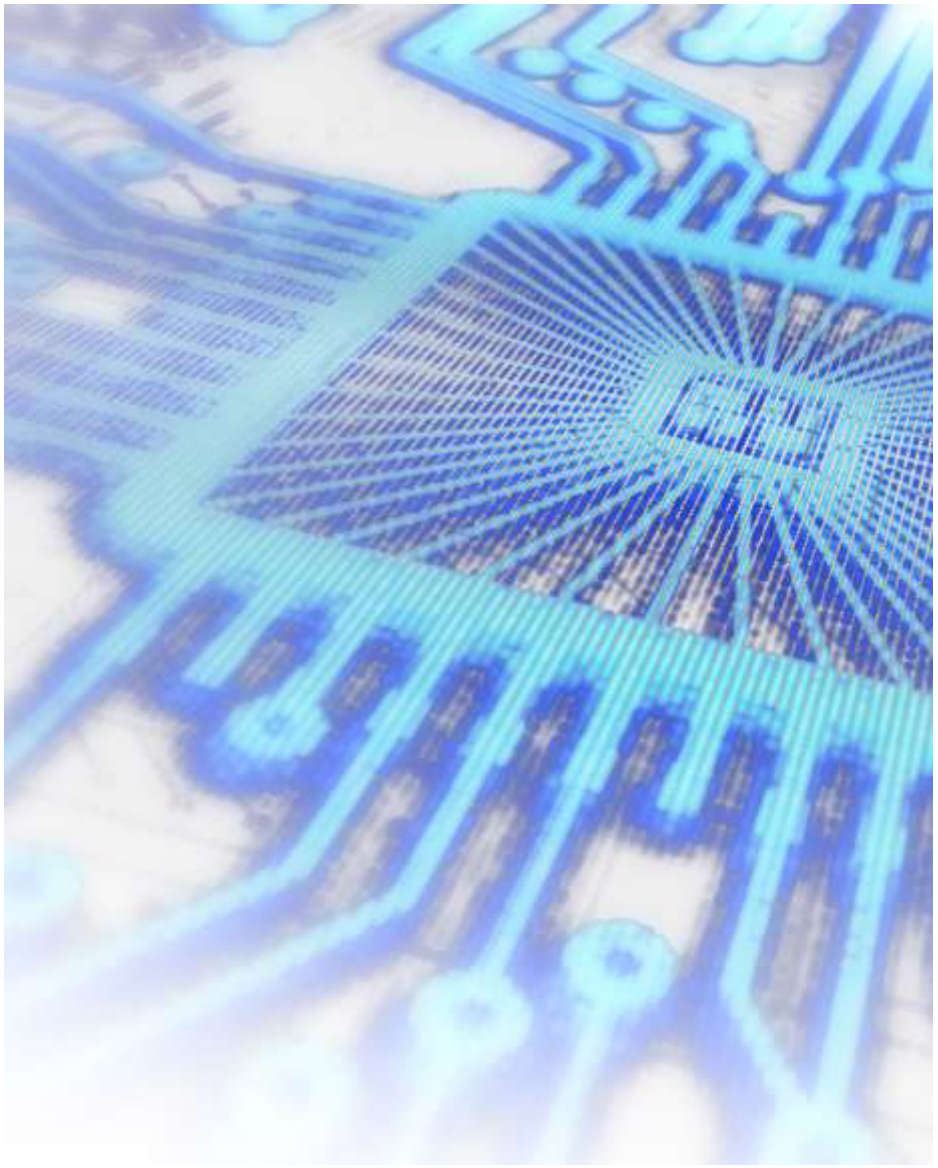
> Anforderungen an den Datenschutz laut DSG und jene an Informationssicherheit oftmals deckungsgleich

Der Begriff der Informationssicherheit

> Ziele der Informationssicherheit:

1. Verfügbarkeit der Informationen (≙ Schutz vor Zerstörung)
2. Integrität (≙ Verhinderung von nicht ordnungsgemäßer Verwendung)
3. Vertraulichkeit (≙ Verhinderung der Zugänglichkeit für Unbefugte)

2. Datensicherheit nach dem DSG 2000



Der Begriff der Datensicherheit (§ 14 DSG 2000)

> Ziele der Datensicherheit:

1. Schutz vor zufälliger oder unrechtmäßiger Zerstörung
2. Schutz vor Verlust
3. Schutz vor nicht ordnungsgemäßer Verwendung
4. Schutz vor Zugänglichkeit für Unbefugte

Erfordernisse der Datensicherheit (§ 14 Abs 1.DSG 2000)

> Maßnahmen für Datensicherheit:
  - Nach Art der verwendeten Daten
  - Nach Umfang und Zweck der Verwendung
  - Stand der technischen Möglichkeiten
  - Wirtschaftliche Vertretbarkeit

> Risikobewertung zur Beurteilung des Sicherheitsniveaus

Sicherheitsmaßnahmen (§ 14 Abs. 2 DSG 2000)

> Insbesondere (beispielhafte Aufzählung), soweit erforderlich (abhängig vom jeweiligen Sicherheitsrisiko):

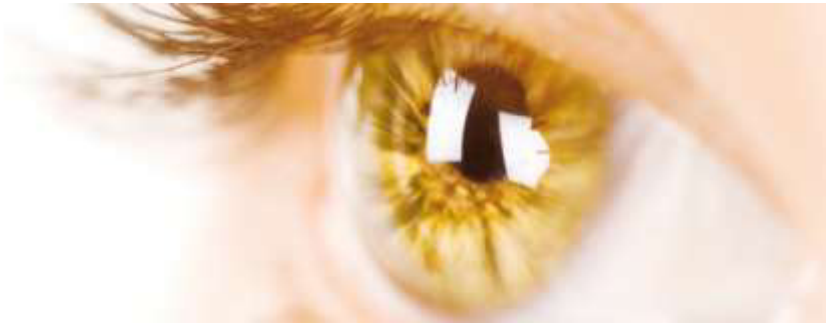
- Aufgabenverteilung ausdrücklich festlegen (Kompetenzklarheitsprinzip)
- Verwendung von Daten an das Vorliegen gültiger Aufträge binden (Auftragsprinzip)
- Jeden Mitarbeiter über Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften belehren (Belehrungspflicht)
- Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers regeln

Sicherheitsmaßnahmen (§ 14 Abs. 2 DSG 2000)

- Zugriffsberechtigung auf Daten, Schutz der Datenträger regeln
- Berechtigung zum Betrieb der Geräte bzw. Programme festlegen und gegen die unbefugte Inbetriebnahme absichern
- Protokoll über Verwendungsvorgänge führen (insb. Änderungen, Abfragen und Übermittlungen)
- Dokumentation über alle vorgenannten Maßnahmen (Beweissicherung)

Nicht in 14 Abs. 2 DSG 2000 enthalten

> Regelungen seit DSG-Novelle 1986; nicht geregelt:
  - Sicherheitsupdates
  - Maßnahmen der Netzwerksicherheit
  - Datensicherungs- und Wiederherstellungsprozesse („Incident Management“)



Typische Anforderungen an den Umgang mit personenbezogenen Daten

- Verpflichtung der Mitarbeiter auf das Datengeheimnis in Form von NDAs (Geheimhaltungsverpflichtung)
- Mitarbeiterschulungen
- Stellenbeschreibungen, Organisationshandbücher, Anweisungen, etc.

Data Breach Notification Duty (§ 24 Abs.2a DSG 2000)

> Erweiterte Informationsverpflichtung bei Datenmissbrauch
  - Vorbild:
    - Data breach notification duty (US)
    - Security breach notification duty (US)
  - Wann?
    - Pflicht zur Information bei „systematischer und schwerwiegender unrechtmäßiger“ Datenverwendung
    - Wenn Betroffenen ein Schaden droht

Data Breach Notification Duty (§ 24 Abs.2a DSG 2000)

- Systematische Verwendung?
  - Über einen bestimmten Zeitraum andauernd
  - Strukturiertes bzw. geplantes Handeln
- Schwerwiegende Verwendung?
  - Abhängig von Anzahl der Datensätze
  - Abhängig von „Eingriffsintensität“ der Daten, z.B. sensible Daten, strafrechtsrelevante Daten, Bonitätsdaten
- Drohender Schaden für den Betroffenen
  - Auch immaterielle Schäden?
  - Keine Voraussetzung, dass Betroffene bei Kenntnis des Datenmissbrauchs den Schaden abwenden können

Data Breach Notification Duty (§ 24 Abs.2a DSG 2000)

> Erweiterte Informationspflicht: Wie?
  - „Unverzüglich“
  - „In geeigneter Form“
  - Daher:
    - Primär: persönliche Verständigung
    - Ab einer gewissen Betroffenenzahl: Einschaltung der Medien
    - Auftraggeber hat sicher zu stellen, dass die Betroffenen die Information tatsächlich erhalten
  - Inhalt
    - Keine genauen Vorgaben durch DSG 2000
    - Jedenfalls: Was ist passiert
    - Allenfalls: Was können die Folgen sein
    - Nicht: Empfohlene Vorgangsweise
  - Keine Information an die DSK (im Gegensatz zum BDSG)

Data Breach Notification Duty (§ 24 Abs.2a DSG 2000)

- Erweiterte Informationspflicht
  - Ausnahmen
    - Drohender Schaden im Vergleich zum Informationsaufwand gering oder
    - Information unverhältnismäßig teuer
- Empfehlung
  - Dokumentation
  - Risikoplan
  - Verantwortlicher
- Ausblick → DSGVO (Art 33 DSGVO):
  - Max. 72 Stunden nach Bekanntwerden Verständigung d. Aufsichtsbehörde
  - Benachrichtigung der betroffenen Person bei hohem Risiko für persönlichen Rechte und Freiheiten - Folgenabschätzung

3. EU-Datenschutz-Grundverordnung (DSGVO)

Neuerungen durch die EU-Datenschutz-Grundverordnung (DSGVO)

> Countdown 2018 – ab 25.05.2018 unmittelbar anwendbar
> Öffnungsklauseln – nationale Umsetzung
> Schutz vor astronomischen Geldbußen
> Risiko für Unternehmen und Manager

10 wichtigsten Punkte

1. Rechte auf Vergessen, Datenportabilität und Zugang
2. Klare Einwilligung als Eckpfeiler
3. Informationsrechte und Transparenz
4. Strenge Regeln für Datentransfers in Drittstaaten
5. Zukunftstaugliche Definitionen
6. Harte Sanktionen von bis zu 4% des weltweiten Jahresumsatzes eines Unternehmens bei Verstößen bzw. 20 Mio EUR
7. Datenschutzkonforme Technikgestaltung: Privacy by Design und by Default
8. Weniger Bürokratie
9. Einheitliche Rechtsdurchsetzung
10. Feste Ansprechpartner für Datenverarbeiter in ganz Europa

Neuerungen durch die EU-Datenschutz-Grundverordnung (DSGVO)

> 12 Stufen Plan (ico):
  - Awareness
  - Information you hold
  - Communicating privacy information
  - Individuals‘ rights
  - Subject access request
  - Legal basis for processing personal data
  - Consent
  - Children
  - Data breaches
  - Data protection by Design and Data Protection Impact Assessments
  - Data Protection Officers
  - International

→ **SCHULUNG!**

Besonderheiten: Markt- und Meinungsforschung

> Art. 89 DSGVO – Garantien und Ausnahmen
> Art. 5 DSGVO – Grundsätze der Verarbeitung
> Art. 32 DSGVO – Sicherheit der Verarbeitung

Danke für Ihre Aufmerksamkeit!

Mag. Andreas Schütz, LL.M.
Partner, Taylor Wessing Wien
IP/IT, Head of Data Protection CEE
a.schuetz@taylorwessing.com