SEC4YOU

Advanced IT-Audit Services

Nachlese

# Datenschutzgrundverordnung

## Risikoanalyse als Vorstufe zur Datenschutz-Folgenabschätzung

Manfred Scholz / 21.3.2018 V1.0

# Rückblick

- WS01 Das Verzeichnis der Verarbeitungstätigkeiten (7.11.2017)
- WS02 Betroffenenrechte (12.12.2017)
- WS03 Technische und organisatorische Maßnahmen gemäß Artikel 32 (18.1.2018)
- WS04 Interne und externe Dienstleister gemäß Artikel 28 (23.2.2018)

Teilnehmer erhalten immer die Unterlagen aller Termine!

**Nachlese auf https://sec4you.com**

# Einführung

Betrachtung der Anforderungen der DSGVO
aus fachlicher Sicht

# Einführung

- **Was** ist zu tun?
- **Wie** ist es zu tun?
- **Wo** ist es zu tun?
- **Wer** muss es tun?

# Worum geht es beim Datenschutz?

Schutz der Grundrechte und Freiheiten natürlicher Personen

# Grundsätze der Datenverarbeitung (Art. 5)

- Rechtmäßigkeit (Rechtsgrundlage)
- Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung (Aufbewahrungsdauer)
- Integrität und Vertraulichkeit

# Rechtmäßigkeit der Verarbeitung

Es gilt das Verbot der Verarbeitung personenbezogener Daten
mit **Erlaubnisvorbehalt!**

(Art 6)

# Begriffsdefinitionen

## Personenbezogene Daten

Alle Informationen, die sich auf eine
identifizierte oder **identifizierbare** natürliche Person beziehen
(betroffene Person)

(Art. 4 Abs. 1)

# Begriffsdefinitionen

**Besondere Kategorien personenbezogener Daten**

- die rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- die Gewerkschaftszugehörigkeit
- das Sexualleben oder die sexuelle Orientierung
- Gesundheitsdaten
- **genetische und biometrische Daten**

(Art. 9 Abs. 1)

# Begriffsdefinitionen

## Der Verantwortliche

Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet.

(Art. 4 Abs. 7)

# Begriffsdefinitionen

## Der Auftragsverarbeiter

Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten **im Auftrag des Verantwortlichen** verarbeitet.

(Art. 4 Abs. 8)

# Wesentliche Anforderung


**Rechenschaftspflicht des Verantwortlichen!**

(Art. 5 Abs. 2., Art. 24 Abs. 1)

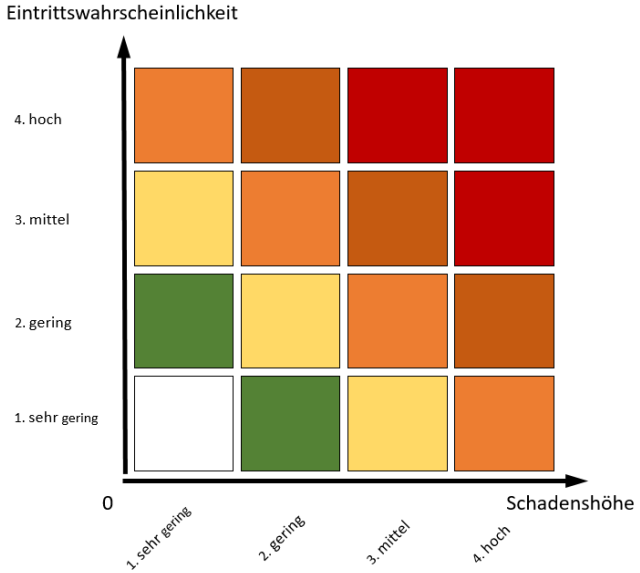
# Wesentliche Änderung

**Nachweispflicht der Einhaltung und Wirksamkeit der umgesetzten Maßnahmen!**

# Sicherheit der Verarbeitung (Art. 32 Abs. 1)

Unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen **Eintrittswahrscheinlichkeit** und **Schwere des Risikos** für die **Rechte und Freiheiten natürlicher Personen** **treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

# Datenschutz-Folgenabschätzung



# Datenschutz-Folgenabschätzung

Hat eine **Form der Verarbeitung**, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung **voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge, so führt der Verantwortliche vorab eine **Abschätzung der Folgen** der vorgesehenen Verarbeitungsvorgänge für den **Schutz personenbezogener Daten** durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(Art 35 Abs.1)

# Datenschutz-Folgenabschätzung

**Voraussetzungen für eine DSFA (Art 35 Abs.3)**

- **Systematische** und **umfassende** Bewertung persönlicher Aspekte mit erheblicher Rechtswirkung
- **Umfangreiche** Verarbeitung besonderer Kategorien personenbezogener Daten oder strafrechtliche Verurteilungen und Straftaten
- **Systematische umfangreiche** Überwachung öffentlicher Bereiche
- Die Art der Verarbeitung befindet sich auf der Liste der Aufsichtsbehörde

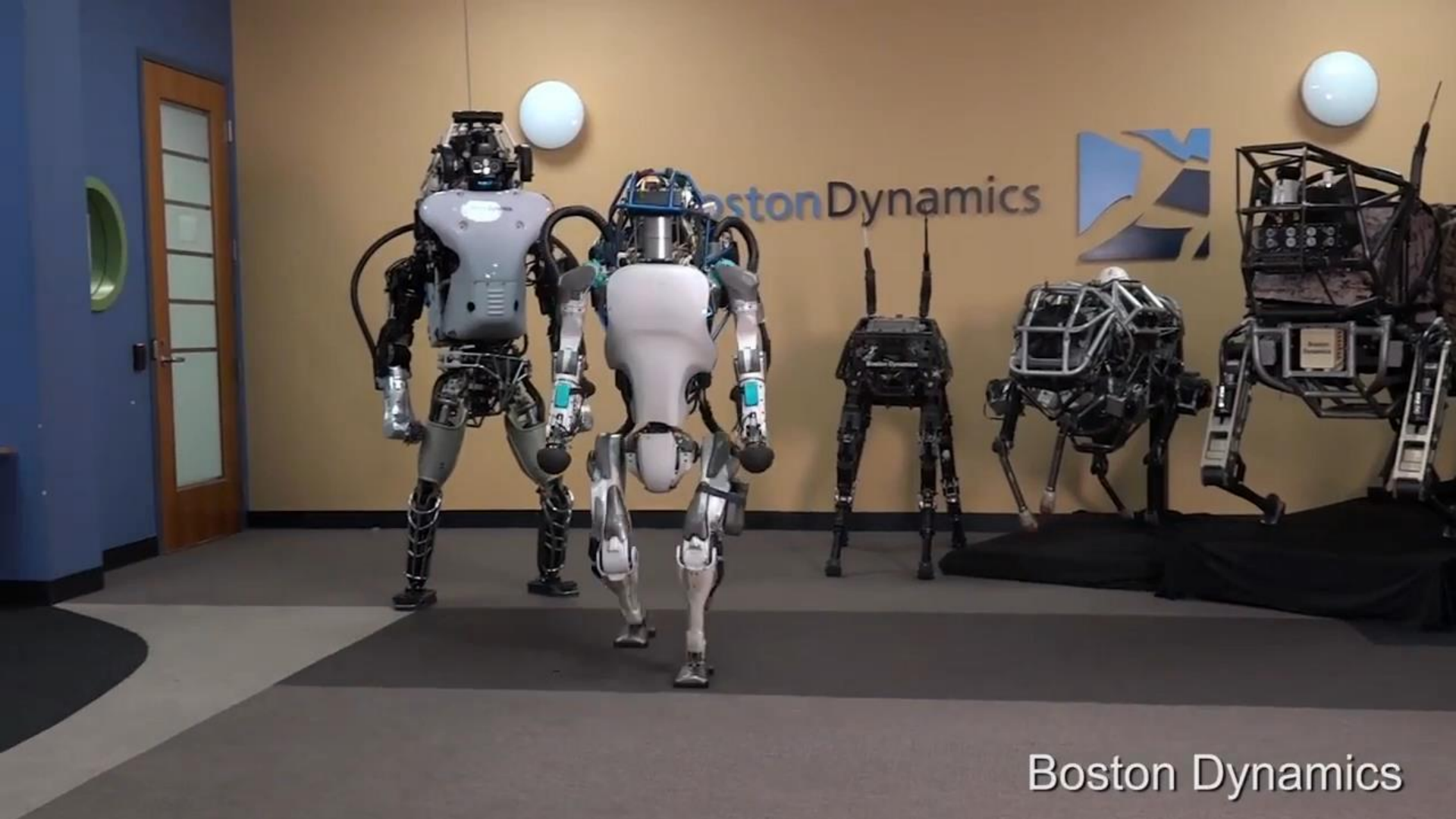
(Art 35 Abs.1)

# Datenschutz-Folgenabschätzung

Anforderungen der DSGVO entsprechen im Prinzip der „**Vorabkontrolle**“
gemäß Art 20 RL 95/46/EG oder §18 Abs.2 DSG 2000

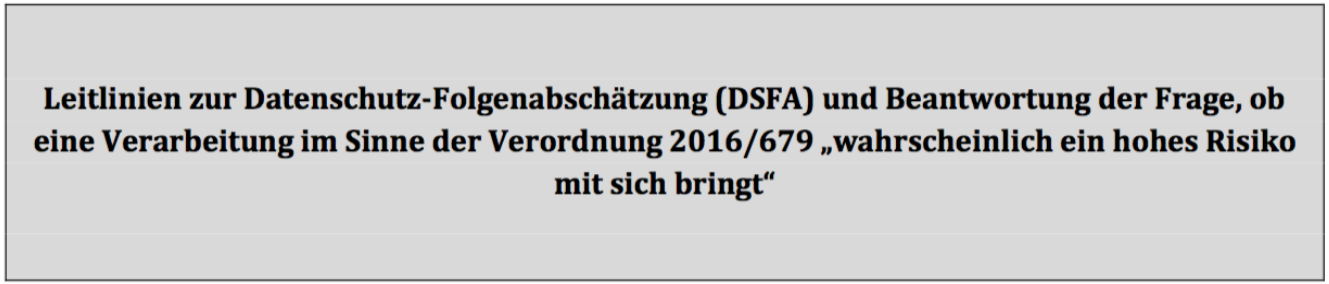
# Datenschutz-Folgenabschätzung


Zum Beispiel „Smart Meter“


stonDynamics
Boston Dynamics

# Datenschutz-Folgenabschätzung

Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) … → Artikel 29 Gruppe




http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

# Datenschutz-Folgenabschätzung


FINAL DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 29134

Information technology — Security techniques — Guidelines for privacy impact assessment

ISO/IEC FDIS 29134:2017(E)

**ISO/IEC 29134** Guidelines for privacy impact assessment

# Datenschutz-Folgenabschätzung

**Mindestinhalte:**

- Systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke und ggfls. Die berechtigten Interessen des Verantwortlichen
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- Abhilfemaßnahmen / Garantien / Nachweise

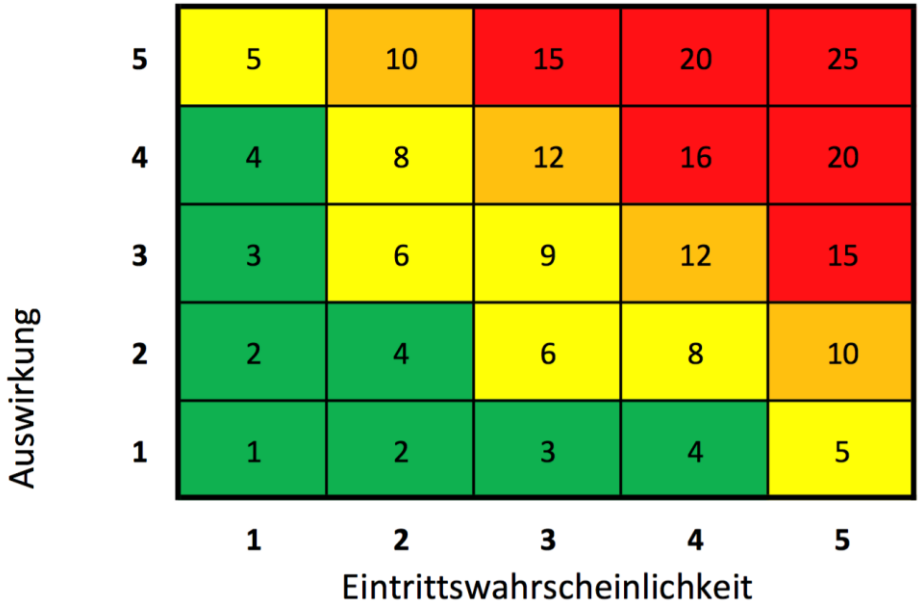
# Sicherheit der Verarbeitung (Art 32)

Risiken müssen auf ein **akzeptables** Maß reduziert werden!

# Risikomanagement / Bewertungskriterien

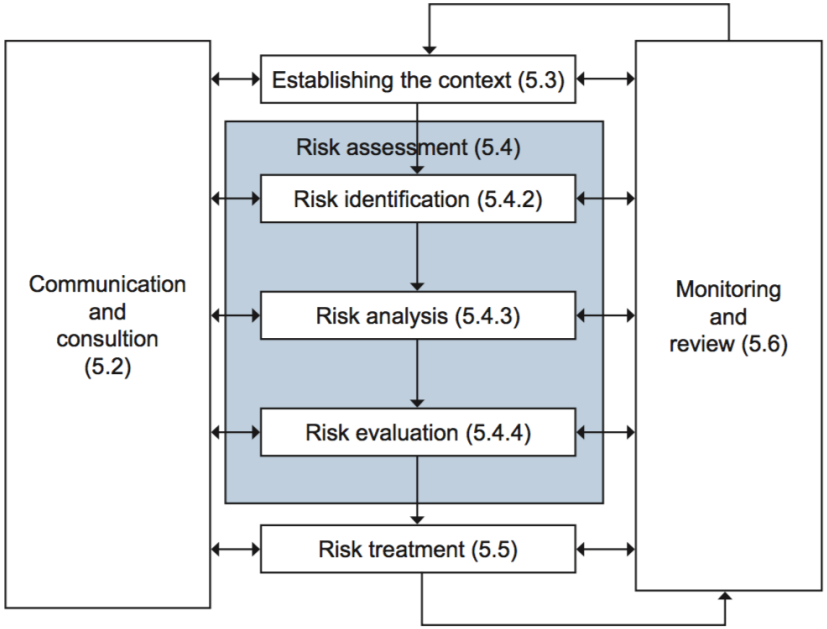
**Eintrittswahrscheinlichkeit** und **Schwere des Risikos**
für die **Rechte und Freiheiten natürlicher Personen** (Art 32)

# Risikomanagement



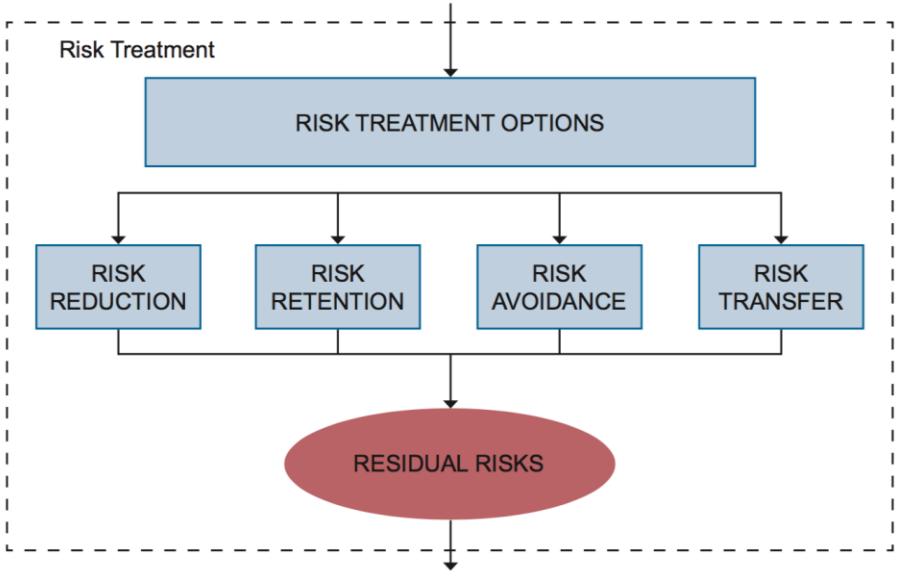
# Risikomanagement

# Risikomanagement




Quelle: ISO 31000

# Risikomanagement




ISACA© Implementierungsleitfaden ISO/IEC 27001:2013

# Einsatz von Tools (Software)

Papier und Bleistift als erster Schritt!

# Risikomanagement

Management von Risiken heisst auch der Mut zur Lücke !

# Seminartipp


## Security Awareness - die menschliche Firewall (CPE 7)

| Kurstermin | CPE | Veranstaltungsort |
|---|---|---|
| 19.04.2018 | 7 | Akademie Interne Revision GmbH \| Anfahrt |

**Seminarthema**

In diesem Seminar werden die notwendigen Elemente erfolgreicher Security Awareness Kampagnen vermittelt. Ausgehend von psychologischen Aspekten und den typischen Herausforderungen werden die erfolgreichen Maßnahmen zur Sensibilisierung, zur Schulung und zum regelmäßigen Training behandelt. Im Rahmen einer Live-Demo wird gezeigt wie die Planung eines Socials Engineering Angriffs durchgeführt wird und welche Werkzeuge typischerweise hierzu angewendet werden (Pishing Emails, USB-Sticks, etc.)

http://www.internerevision.at/seminare/spezialseminare/seminar/security-awareness-die-menschliche-firewall-185/

# Vorankündigung

## DSGVO Workshop „Was & Wie“

**"Prüfungsansätze zum Nachweis der Rechenschaftspflicht gemäß DSGVO Artikel 5 (Einhaltung der Datenschutzgrundsätze)“**

25. April 2018

Star Inn Hotel Wien Schönbrunn, Linke Wienzeile 224, 1150 Wien

# Finale



Manfred.Scholz@sec4you.com
https://sec4you.com
XING, LinkedIn
Tel.: +43 1 2531 797-10