Zürcher Hochschule
für Angewandte Wissenschaften

School of
Management and Law

# DACH-Compliance-Tagung 2017
# Workshop
# EU-DSGVO: Auswirkungen auf die Compliance-Organisation

**Building Competence. Crossing Borders.**

**Dr. Michael Widmer, LL.M. Rechtsanwalt**
michael.widmer@zhaw.ch, 17. Februar 2017

# I. Grundlagen

## Datenschutz-Grundverordnung («DSGVO»)

# I. Grundlagen

## Datenschutz-Grundverordnung («DSGVO»)

– Inkrafttreten der EU DS-GVO per 25. Mai 2016

– Übergangsfrist bis 25. Mai 2018

– Anwendbarkeit auch auf viele Schweizer Unternehmen (Art. 3 Abs. 1 und 2 DSGVO), bspw.

- EU-Niederlassung (Verarbeitung veranlasst oder vorgenommen durch in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeiter)
- Betroffene Personen mit Aufenthalt in der EU, wenn Verarbeitung im Zusammenhang
  - Angebot von Waren und Dienstleistungen an betroffene Personen in der EU
  - Beobachtung von Verhalten der betroffenen Personen, das in der EU erfolgt

# I. Grundlagen

**Besonderheit für Unternehmen ausserhalb der EU: Art. 27 DSGVO**

*Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern*

*(1) In den Fällen gemäß Artikel 3 Absatz 2 benennt der Verantwortliche oder der Auftragsverarbeiter schriftlich einen Vertreter in der Union.*

*(2) Diese Pflicht gilt **nicht** für*

*a) eine Verarbeitung, die **gelegentlich** erfolgt, **nicht** die **umfangreiche** Verarbeitung **besonderer Datenkategorien** im Sinne des Artikels 9 Absatz 1 oder die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt **und** unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung **voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen** führt, oder*

*b) Behörden oder öffentliche Stellen.*

# Administrativsanktionen / Geldbussen

# I. Grundlagen

## Administrativsanktionen / Geldbussen

- In jedem «Einzelfall wirksam, verhältnismäßig und abschreckend»
- Je nach verletzter Bestimmung bis zu € 10 Mio. oder 2% des gesamten weltweiten Jahresumsatzes oder sogar € 20 Mio. oder 4% des gesamten weltweiten Jahresumsatzes (des Unternehmens)
  - Unternehmensbegriff?
  - Im Wesentlichen bei Verletzungen «formeller» Bestimmungen: €10 Mio. oder 2%
  - Im Wesentlichen bei Verletzungen «materieller» Bestimmungen: € 20 Mio. oder 4%
- Durchsetzung direkt in der Schweiz unklar

# Zivilrechtliche Haftung / Reputationsrisiko

# Einzelne Regelungen der DSGVO

# I. Grundlagen

## Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO)

– Umfangreiche Dokumentations- und Nachweispflichten

*«(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).»*

# I. Grundlagen

## Datenschutzbeauftragter (Art. 37 ff. DSGVO)

*«(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn*
*(…)*
*b) die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke **eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen** erforderlich machen, oder*
*c) die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der **umfangreichen Verarbeitung besonderer Kategorien** von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.*

*(2) Eine Unternehmensgruppe darf einen **gemeinsamen Datenschutzbeauftragten** ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.»*

# I. Grundlagen

## Verzeichnis von Verarbeitungstätigkeiten (Art. 30 Abs. 1 DSGVO)

*(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:*
*a) den Namen und die Kontaktdaten des* ***Verantwortlichen*** *und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des* ***Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten****;*
*b) die* ***Zwecke*** *der Verarbeitung;*
*c) eine Beschreibung der* ***Kategorien betroffener Personen*** *und der* ***Kategorien personenbezogener Daten****;*
*d) die* ***Kategorien von Empfängern****, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;*

# I. Grundlagen

*e) **gegebenenfalls** Übermittlungen von personenbezogenen Daten **an ein Drittland** oder an eine internationale Organisation, einschließlich der **Angabe des betreffenden Drittlands** oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die **Dokumentierung geeigneter Garantien**;*

*f) wenn möglich, die vorgesehenen **Fristen für die Löschung** der verschiedenen Datenkategorien;*

*g) wenn möglich, eine allgemeine **Beschreibung der technischen und organisatorischen Maßnahmen** gemäß Artikel 32 Absatz 1.*

# I. Grundlagen

## Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

*(1) 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. (…)*

- Dokumentations- und Nachweispflichten
- Pflicht zur Konsultation des Datenschutzbeauftragten (sofern benannt)
- Datenschutzmanagementsystem empfohlen

- Mindestinhalt einer Datenschutz-Folgenabschätzung: Art. 35 Abs. 7 DSGVO

# I. Grundlagen

## Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

- **Privacy by Design**
  - So gestalten, dass sie die Datenschutzgrundsätze (bspw. Datenminimierung, Speicherbegrenzung, Integrität und Vertraulichkeit) wirksam umsetzen
  - Verlagert bereits in Phase Produktentwicklung
  - Frühzeitig Datenschutzbeauftragten in datenschutzrelevante Projekte einbeziehen

- **Privacy by Default**
  - Der fragliche Verarbeitungsvorgang soll standardmässig möglichst datenschutzfreundlich eingerichtet sein (bspw. in Bezug auf Menge und Umfang der verarbeiteten Daten, Speicherdauer und Zugänglichkeit), ausser die betroffene Person würde diese vorgegebenen Einstellungen verändern

# I. Grundlagen

**Weitere Themen bspw.**

- Neues Konzept Einwilligung (Art. 6/7 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Auftragsverarbeitung (Art. 28 DSGVO)
- Melde- und Informationspflichten betr. Verletzungen des Schutzes personenbezogener Daten (Art. 33 und 34 DSGVO)

# I. Grundlagen

## Datenschutz und Compliance

– Datenschutz bei der Durchführung von Complianceaktivitäten

– Datenschutz als Gegenstand der Compliance (hierauf konzentrieren wir uns heute)

# II. Gruppenarbeiten

**Ihre konkreten Erfahrungen mit der Umsetzung der DSGVO?**

# II. Gruppenarbeiten

## Grundfragen

- Auswirkungen auf Compliance-Organisation: Umsetzung der DSGVO Anforderungen erfordert Überprüfung und allenfalls Anpassung der unternehmensinternen Prozesse
- Welches sind strategische Grundfragen, welche zu Beginn eines Projekts «DSGVO-Compliance» zu beantworten wären?
- In welche Phasen würden Sie ein solches Projekt gliedern?
- Aufgrund welcher Kriterien könnte man versuchen, Prioritäten zu setzen?

# II. Gruppenarbeiten

**Art. 83 DSGVO**

- Welche Folgerungen für die Umsetzung der Datenschutz Compliance können aus Art. 83 Abs. 4 und 5 der DSGVO bspw. für Fragen der Priorisierung gezogen werden?

- Welche Folgerungen können aus Art. 83 Abs. 2 DSGVO für die Datenschutz Compliance gezogen werden?

- Unter welche(n) Buchstaben von Art. 83 Abs. 2 DSGVO würden Sie bspw. folgende Massnahmen subsumieren?
  - Lösung der bereits bekannten datenschutzrechtlichen Probleme
  - Festlegung eines Notfallplans
  - Compliance Massnahmen / Datenschutz-Managementsystem
  - Schulung von Mitarbeitern / Schaffen von «Awareness»

- Welche weiteren Massnahmen könnte man auch noch treffen?

# II. Gruppenarbeiten

## DSGVO und Compliance

– Welches sind Massnahmen, die sich allenfalls generell treffen lassen?

# II. Gruppenarbeiten

## DSGVO und Compliance

- Was sind Fragen/Themen, die sich zu folgenden Bereichen (neu) ergeben könnten?
  - Rechenschaftspflichten
  - Datenschutzbeauftragte(r)
  - Datenschutzfolgenabschätzung
  - Melde- und Informationspflichten bei Datenschutzverletzungen
  - Auftragsverarbeitung

# III. Folgerung / Schlussbetrachtung / Fazit

# Herzlichen Dank für Ihre Aufmerksamkeit!

**Kontakt**

Dr. iur. Michael Widmer, LL.M.
Rechtsanwalt
ZHAW School of Management and Law
ZSR / ITPZ
Gertrudstrasse 15
8401 Winterthur

+41 (0) 58 934 79 62
michael.widmer@zhaw.ch

itp|z
Zurich Center for Information Technology and Privacy