



DIE
ADVOKATUR
SURY

5. Tagung zum Datenschutz – Jüngste Entwicklungen

EuropaInstitut
an der Universität Zürich,
26. Januar 2012

Legal Compliance und Datenschutz –
von der Illusion
über Risiken zur Handlungsempfehlung

Referentin Ursula Sury

- Inhaberin DIE ADVOKATUR SURY GmbH
- Tätigkeitsschwerpunkte: Datenschutz, IT-Recht und Vertragsmanagement
- Leiterin des Kompetenzcenters Management & Law an der Hochschule Luzern
- Mediatorin SKWM
- Nachdiplomstudium Wirtschaftspädagogik HSG
- Datenschutz- und Öffentlichkeitsbeauftragte des Kanton Wallis
- Fachauditorin für GoodPriv@cy, SQS Schweiz

Agenda oder die unendliche Geschichte

- Datenschutz → Naja
- Datenschutz → Ist mir egal
- Datenschutz → Kurz und „schnurz“
- Datenschutz → Ihre/meine persönliche Verantwortung!?
- Datenschutz → Top Risiko
- Datenschutz → Von was leben wir eigentlich?
- Datenschutz → Virtuelle Welt
- Datenschutz → Richtigkeit
- Datenschutz → Verletzungen

Agenda oder die unendliche Geschichte

- Datenschutz → Zentrale Datenbanken
- Datenschutz → Zugriffsrechte
- Datenschutz → Identity Management Systeme
- Datenschutz → Bring your own device
- Datenschutz → Ermächtigungen
- Datenschutz → Anonymisierung
- Datenschutz → Outsourcing
- Datenschutz → Ausland
- Datenschutz → Videokameras

Agenda oder die unendliche Geschichte

- Datenschutz → Mitarbeitende
- Datenschutz → Businessprozess
- Datenschutz → Monitoring
- Datenschutz → IKS
- Datenschutz → Umsetzung
- Datenschutz → Illusion
- Datenschutz → Risiko
- Datenschutz → Handlungsempfehlungen

Datenschutz → Naja

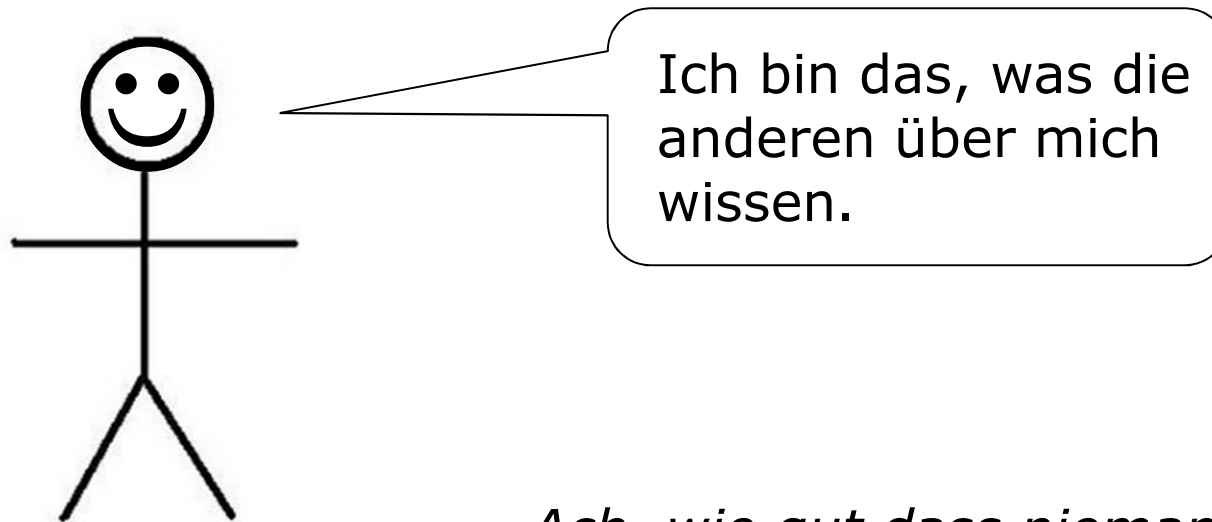
- „Wir haben den Datenschutz im Griff, wir haben eine Firewall“.
- „Wir haben den Datenschutz im Griff, wir unterliegen dem Arztgeheimnis/Berufsgeheimnis“.
- „Wir haben den Datenschutz im Griff, wir geben ohnehin nie Aussagen gegen aussen bekannt“.

Datenschutz → Ist mir egal

- Verkauf von Privacy für ökonomische und Informations-Vorteile
 - Bsp. Cumulus
- Verkauf von Privacy für organisatorische und Vernetzungs-Vorteile
 - Bsp. Facebook, Recommender Systems

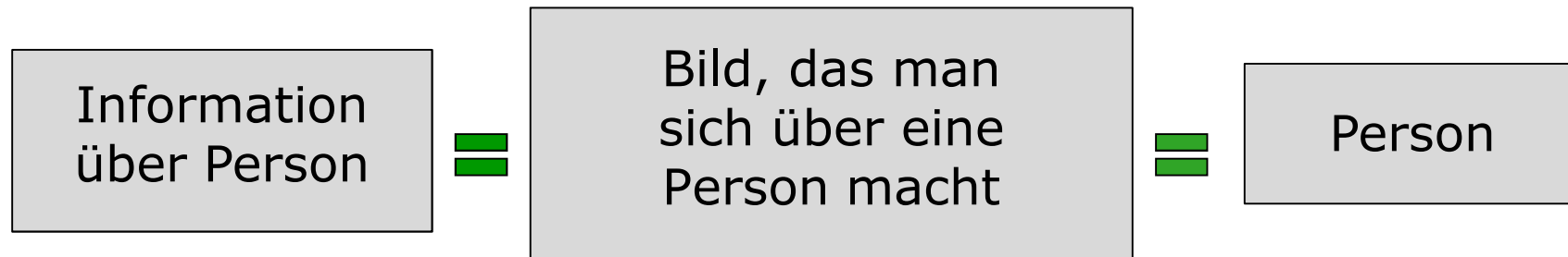
Datenschutz → Kurz und „schnurz“

Datenschutz ist Persönlichkeitsschutz



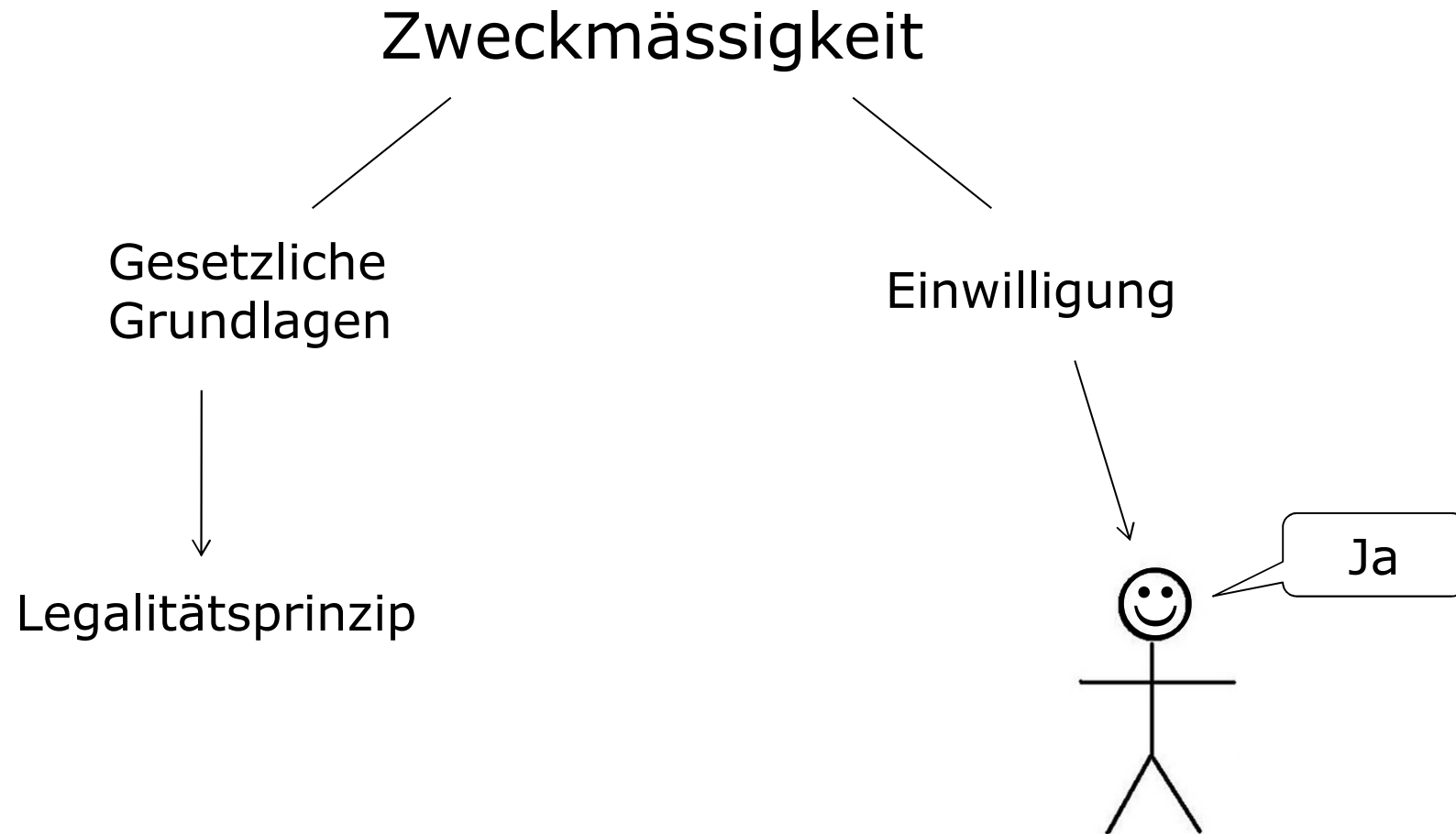
*„Ach, wie gut dass niemand weiss,
dass ich Rumpelstilzchen heiss.“*

Datenschutz → Kurz und „schnurz“



Proust: „Unsere Persönlichkeit innerhalb der Gesellschaft ist eine geistige Schöpfung der anderen.“

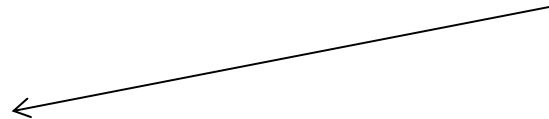
Datenschutz → Kurz und „schnurz“



Datenschutz → Kurz und „schnurz“

Verhältnismässigkeit

Zweck



Wer macht was?

Nur so viel wie
notwendig ist, um
Zweck zu erreichen.

Datenschutz → Kurz und „schnurz“

Richtigkeit

Art. 5 DSGVO

*„Wer Personendaten bearbeitet, hat sich über deren **Richtigkeit** zu vergewissern. Er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.“*

Datenschutz → Ihre/meine persönliche Verantwortung!?

„To comply with“

Art. 716a OR

„Der Verwaltungsrat hat folgende unübertragbare und unentziehbare Aufgaben:

- 1. die Oberleitung der Gesellschaft und die Erteilung der nötigen Weisungen;*
- 2. die Festlegung der Organisation;*

Datenschutz → Ihre/meine persönliche Verantwortung!?

4. *die Ernennung und Abberufung der mit der Geschäftsführung und der Vertretung betrauten Personen;*
5. *die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der **Gesetze**, Statuten, Reglemente und Weisungen;*
6. *die Erstellung des Geschäftsberichtes sowie die Vorbereitung der Generalversammlung und die Ausführung ihrer Beschlüsse."*

Datenschutz → Ihre/meine persönliche Verantwortung!?

Art. 321e OR

„Der Arbeitnehmer ist für den Schaden verantwortlich, den er absichtlich oder fahrlässig dem Arbeitgeber zufügt.

Das Mass der Sorgfalt, für die der Arbeitnehmer einzustehen hat, bestimmt sich nach dem einzelnen Arbeitsverhältnis, unter Berücksichtigung des Berufsrisikos, des Bildungsgrades oder der Fachkenntnisse, die zu der Arbeit verlangt werden, sowie der Fähigkeiten und Eigenschaften des Arbeitnehmers, die der Arbeitgeber gekannt hat oder hätte kennen sollen.“

Datenschutz → Top Risiko

Datenschutzverletzungen sind in der Risikomatrix
Toprisiken.

→ Grund: Datenschutzverletzungen werden immer
in der Presse thematisiert.

Datenschutz → Top Risiko

Art. 30 DSG, Abs. 2

„In Fällen von allgemeinem Interesse kann er (der EDÖB) die Öffentlichkeit über seine Feststellungen und Empfehlungen informieren. Personendaten, die dem Amtsgeheimnis unterstehen, darf er nur mit Zustimmung der zuständigen Behörde veröffentlichen. Verweigert diese die Zustimmung, so entscheidet der Präsident der auf dem Gebiet des Datenschutzes zuständigen Abteilung des Bundesverwaltungsgerichts endgültig.“

Datenschutz → Top Risiko

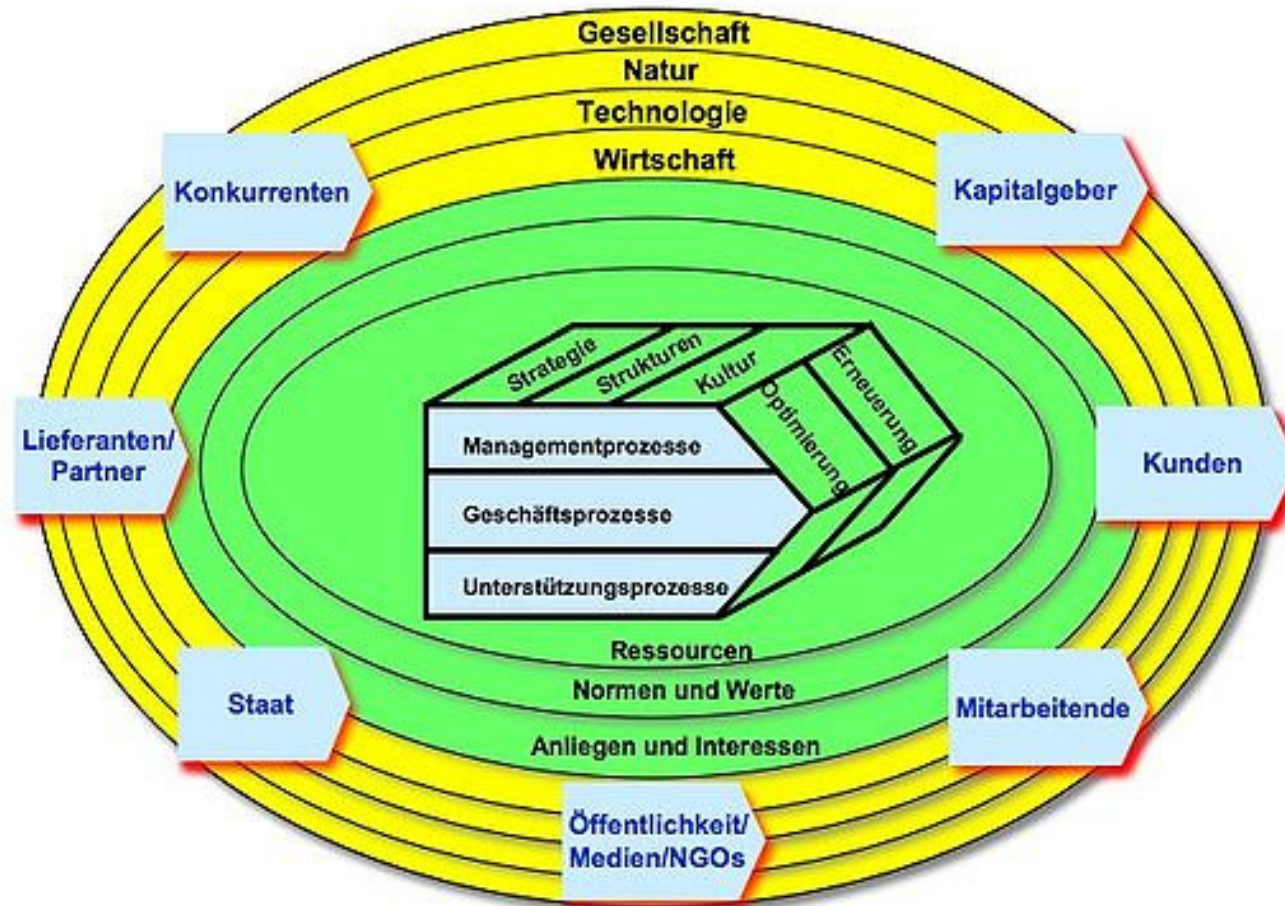
- Datenschutzverletzungen im Auftrag der Führung.
- Wie soll man sich verhalten, um sich nicht haftbar oder strafbar zu machen?

Datenschutz → Von was leben wir eigentlich?

- Wir leben in der Informations- und Wissensgesellschaft.
- Wir leben vom Empfangen, Generieren, Veredeln, Weitergeben, Lagern → kurz: vom Bearbeiten von Informationen.
- Die meisten dieser Informationen haben einen Bezug zu einer natürlichen und/oder juristischen Person.

Datenschutz → Von was leben wir eigentlich?

Such-, Entscheidungs- und Handlungsfelder im Management



Quelle: Rüegg-Stürm, J. (2003): Das neue St. Galler Management-Modell. Grundkategorien einer integrierten Managementlehre: Der HSG-Ansatz, 2. Auflage, Bern/Stuttgart/Wien: Haupt, S. 22

Datenschutz → Virtuelle Welt

- Warum gehen die Leute so unbedarft mit ihren Persönlichkeitsdaten um?
- Wie fühlen Sie sich, wenn eine fremde Person Ihre Tasche/Schränke/Wohnung durchstöbert?
- Wir haben kein Verständnis für die Dimensionen der virtuellen Welt.
(Dies gilt übrigens auch für das Urheberrecht und seine Dimensionen 😊.)

Datenschutz → Richtigkeit?

- Ein vernachlässigtes Risiko ist die Richtigkeit der Daten.
- Wem glauben Sie? Der Aussage der betroffenen Person oder dem Eintrag in der Datenbank / der Auswertung des IT-Programms?

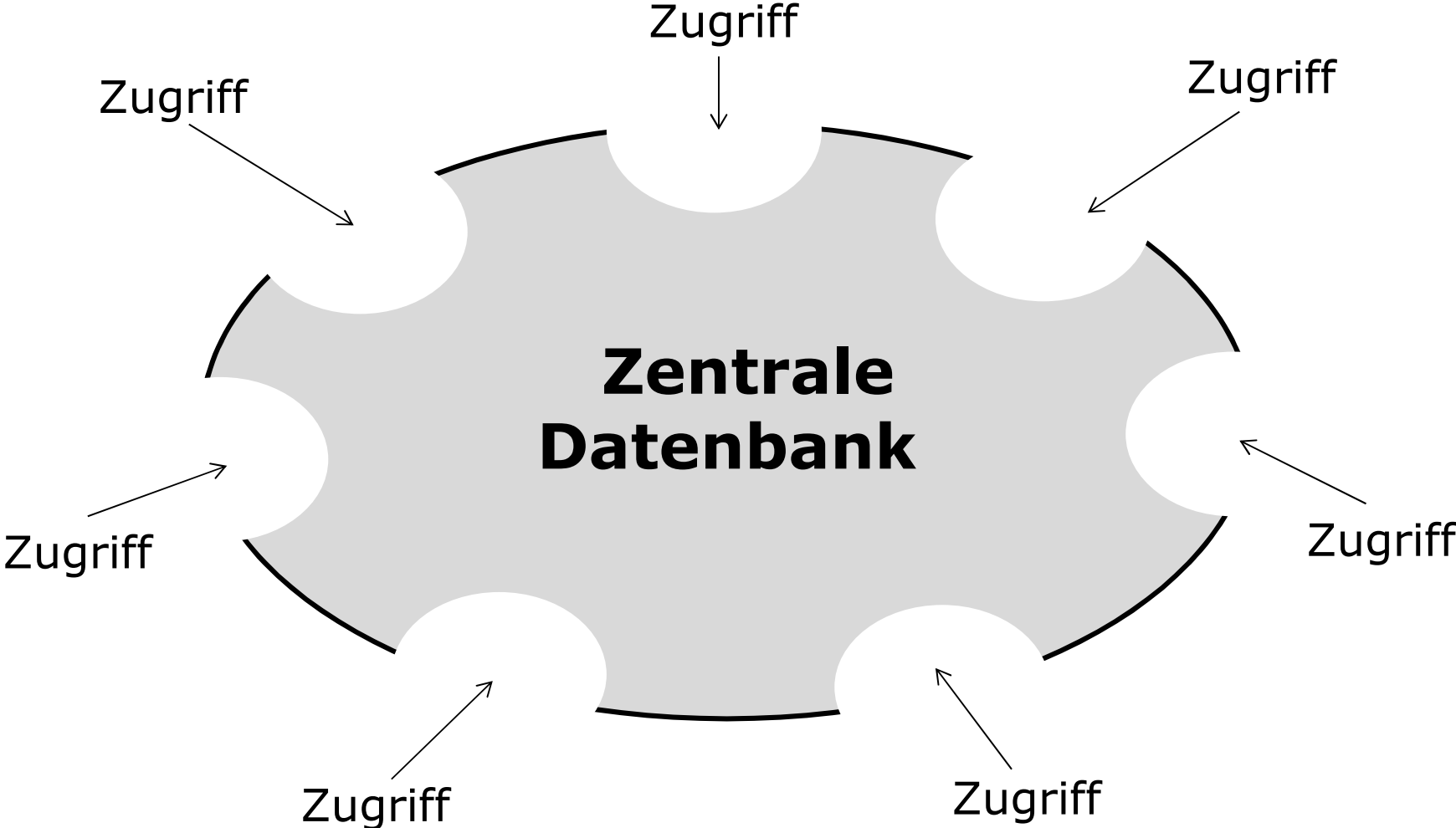
Datenschutz → Datenschutzverletzung

- Whistleblowing
- Mobbing im Internet
- Sammlung von Kontextinformationen durch Google, Amazon, etc.
- Weitergabe von Daten in der Cloud

Datenschutz → Zentrale Datenbanken

- Zentrale Datenbanken im öffentlichen und im privaten Bereich sind die Herausforderungen der Zukunft.
- Viele verschiedene Benutzer aus verschiedenen Organisationen haben Zugriff auf dieselbe Datenbank, eventuell aber nicht auf dieselben Daten, d.h. mit verschiedenen Berechtigungen.
- Wer hat die Oberaufsicht über sämtliche Daten, über die gesamte Datenbank?
- Wer hat somit die „Datenmacht“?

Datenschutz → Zentrale Datenbanken



Datenschutz → Zugriffsrechte

- Wie werden die verschiedenen Zugriffsrechte vergeben?
- Können die Zugriffsrechte überhaupt compliant vergeben werden?
- Wie verhält es sich bei der organisatorischen Umgestaltung, Definition von Stellen? Ist das Berechtigungssystem genügend flexibel? Für Anpassungen?
- Wie wird bei Fluktuationen mit den Berechtigungen umgegangen?

Datenschutz → Identity Management Systeme

- Werden Identity Management Systeme eingesetzt?
- Sind die IDM-Projekte genügend interdisziplinär aufgesetzt und entsprechend organisatorisch verankert?
- Ist man sich der Möglichkeiten verschiedener Identitäten bewusst?

Datenschutz → Bring your own device

- Auflösung der Grenzen zwischen Privatheit des Arbeitnehmenden und der Unternehmung/Arbeitgeberin.
- Verschiebung und Neudefinition der Risikosphären.
- Regelung von Verantwortlichkeiten und Haftung.

Datenschutz → Ermächtigungen

- In Datenbearbeitungen muss konkret eingewilligt werden (höhere Anforderung bei Persönlichkeitsprofilen / besonders schützenswerten Personendaten!).
- Wie soll diesem Erfordernis in Standard-Businessprozessen und formularisierten Verträgen (underwriting) nachgelebt werden?

Datenschutz → Ermächtigungen

- Kunde kann Einwilligung grundsätzlich jederzeit widerrufen.
Welche Auswirkungen hat das auf das Kundenverhältnis und auf schon gespeicherte Daten?
- Achtung: Mit Transparenz bei gleichem Zweck lässt sich einiges an Problemen lösen.

Datenschutz → Anonymisierung

- Viele Managementinformationen lassen sich auch mit nicht personalisierten Informationen eruieren.
- Gilt das Bearbeiten von pseudonomysierten Daten als Bearbeitung von Personendaten?
- Die Diskussion über die Relativität des Personenbezuges, - d.h. die Frage ob eine Information personenbezogen ist, ist nicht eine absolute sondern eine kontextuell relative Frage – ist noch nicht ausgiebig geführt.

Dies ist meine Meinung 😊 → vgl. Logistep - BGE

Datenschutz → Anonymisierung

- Wenn der Personenbezug nur von einer vertrauenswürdigen und weisungsunabhängigen Person im Unternehmen wieder hergestellt werden kann / könnte und dies für die Management Informationen nicht gemacht wird, wie würden sie entscheiden?
- Handelt es sich dann bei den Management-Informationen um personenbezogene Daten?

Datenschutz → Outsourcing

- Jede Datenbearbeitung, die man nicht selber vornimmt, sondern durch einen Dritten erledigen lässt, ist datenschutzrechtlich ein Outsourcing.
- Wird die Führungsverantwortung diesbezüglich gewahrt?
Achtung: Sorgfalt bei → Auswahl, → Instruktion und → Kontrolle des Outsourcing-Partners ist gefragt.
- In der Praxis ist die → Sorgfalt bei der Auswahl nicht oder mangelhaft dokumentiert, → die Instruktion nur generisch und somit mangelhaft und → die Kontrolle findet kaum statt.

Datenschutz → Ausland

- Häufig sind sich Unternehmungen nicht bewusst, dass sie ihre Daten auch ins Ausland transferieren oder dass diese Daten im Ausland bearbeitet werden.
- Auch Zugänglichmachen von Zugriffen auf Datenbanken der Schweiz aus dem Ausland gilt als Datenexport.

Datenschutz → Videokameras

- Auch hier gilt das Erfordernis der Zweckmässigkeit, gesetzliche Grundlage oder Einwilligung.
- Die Umsetzung der Verhältnismässigkeit ist auch finanziell aufwändig!
- Das Prüfen anderer geeigneter Mittel für die Zweckerreichung kann sich durchaus rechnen.

Datenschutz → Mitarbeitende

- Mitarbeitende müssen für Datenschutzfragen konkret instruiert und kontrolliert werden.
- Viele Führungsverantwortliche nehmen ihre Führungsverantwortung diesbezüglich nicht wahr.
- Hauptschwierigkeit und Herausforderungen ist der Transfer der allgemeinen Datenschutzgrundsätze in den beruflichen Alltag.

Datenschutz → Businessprozess

- Zweckmässigkeit und Verhältnismässigkeit?
- Was heisst dies konkret bei meiner persönlichen Arbeit?
- Wie soll ich das umsetzen?

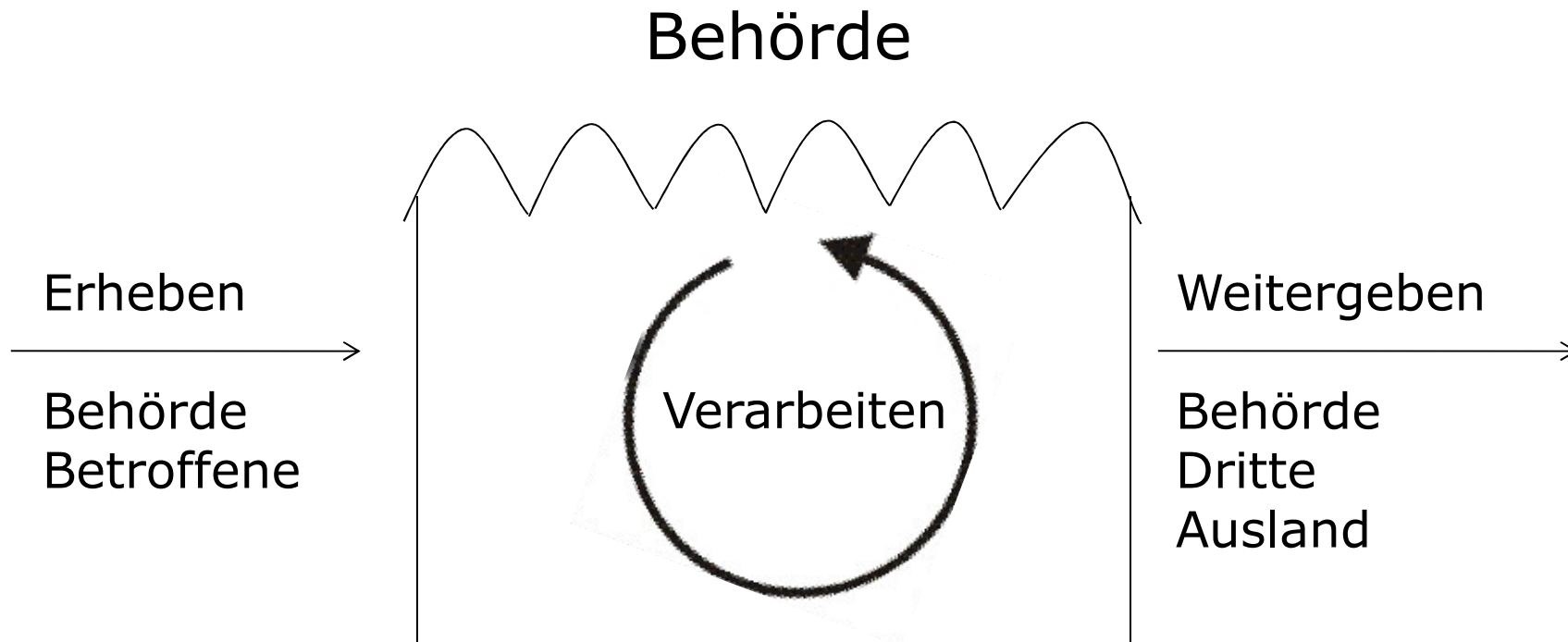
Datenschutz → Monitoring

- Monitoring ist mit genügender Zweckbindung zulässig.
- Verantwortung für Betriebssicherheit und Compliance impliziert ein angemessenes Monitoring!
- Bei Unklarheit gesetzlicher Grundlage Einwilligung einverlangen.
- Mitarbeitende, die wissen, dass die Art und Weise ihrer Datenbearbeitung auch kontrolliert wird resp. bei Unregelmässigkeiten nachverfolgt werden kann verhalten sich erfahrungsgemäss korrekter.

Datenschutz → IKS

- Interne Kontrolle und Datenschutz müssen kein Widerspruch sein.
- Interne Kontrolle soll auch die Einhaltung des Datenschutzes kontrollieren.
- Bei der Risikobeurteilung ist der Datenschutz immer mit zu berücksichtigen.

Datenschutz → Umsetzung



Datenschutz → Umsetzung

- Konformitätsnachweis erstellen resp. durch die einzelnen Mitarbeiter erstellen lassen und dann auf Abteilungs- und Unternehmensebene konsolidieren.
- Alle überflüssigen Datensammlungen löschen.
- Datenschutz in sämtlichen Businessprozessen als Compliance-Teil integrieren und abbilden.
- Datenschutz nicht als separates Thema wie Finance behandeln sondern immer integrieren.

Datenschutz → Umsetzung

Konformitätsnachweis

	Zweck	Verhältnismässigkeit			Richtigkeit
Daten- sammlung	Zweck der Datensammlung Gesetz oder Einwilligung	Anzahl Zugriffs- berechtigte Personen	Haben nur so viele Personen wie unbedingt notwendig Zugriff auf die Daten?	Sind alle Daten für die Zweck- erreichung notwendig?	Wie wird die Richtigkeit der Daten überprüft?
<i>Bezeichnung</i>	<i>Begründung</i>	<i>Anzahl</i>	<i>Antwort mit Begründung</i>	<i>Antwort mit Begründung</i>	<i>Erklärung</i>

- Häufigkeit der internen Kontrollen → jährlich, alle X Monate, etc.
- Aufbewahrungsdauer → Anzahl Jahre
- Inhaber der Datensammlung → Bezeichnung

Datenschutz → Umsetzung

- Berechtigungen regelmässig kontrollieren, nicht genutzte Berechtigungen entziehen.
- Datenschutzverhalten der Mitarbeitenden kontrollieren.
- Über Datenbearbeitungen, Mitarbeitende und Kunden immer transparent und proaktiv informieren, idealerweise über Intranet und Internet.

Datenschutz → Umsetzung

- Integration des Datenschutzes in alle Prozesse
- Klare Instruktion aller Beteiligten
- Kontrolle aller Beteiligten

Datenschutz → Illusion

- Bewusstheit im Umgang mit personenbezogenen Daten fehlt.
- Umsetzung im konkreten Alltag ist für Private und Unternehmungen sehr schwierig.

Datenschutz → Risiko

- Datenschutzverletzungen können für Unternehmungen gravierende Konsequenzen haben.
- Von Privaten werden überall wertvolle Profile erstellt.
- Eine umfassende Umsetzung von Datenschutz ist nicht möglich.

Datenschutz → Handlungsempfehlungen

- Datenschutz ist eine Daueraufgabe und ist Chefsache.
- Datenschutz geht alle an.
- 80:20 Regel

Welche Fragen darf ich Ihnen beantworten?

Publikationen unter



DIE
ADVOKATUR
SURY

www.dieadvokatur.ch

DIE ADVOKATUR SURY GmbH
Alpenquai 4
6005 Luzern

Lucerne University of
Applied Sciences and Arts

**HOCHSCHULE
LUZERN**

www.hslu.ch