Privacy 360° – Datenschutz und Datensicherheit: Überlappungen und Widersprüche

Eine Skizze

http://www.oltra.it/wp-content/uploads/2015/07/privacy_image.jpg

#Digital2016
#Rechtsinformatik2016 #Privacy2016- #IRISWien2016
OCG WIEN, 1010 Wien, Wollzeile 1: 22.11.2016 & 23.11.2016

Research Institute AG & Co KG
Zentrum für digitale Menschenrechte

Christof Tschohl
Wissenschaftlicher Leiter
Research Institute AG & Co KG
[Foto: http://www.idealismprevails.at/wp-content/uploads/2016/03/Pressekonferenz_Stoppt-das-Staatsschutzgesetz_18.01.16_21.jpg]

Das Research Institute (RI) ist ein junges Forschungszentrum an der Schnittstelle von Technik, Recht und Gesellschaft, das sich aus multi- und interdisziplinärer Perspektive Fragen der Menschenrechte im digitalen Zeitalter widmet.

Portfolio:

- Forschung zu technischen und rechtlichen Aspekten von Datenschutz und Datensicherheit ebenso wie zu Technikfolgenabschätzung, Cybercrime und Netzpolitik
- Smart Rights Consulting: Beratung in datenschutzrechtlichen Fragen
- Schulungen für Privatpersonen und Mitarbeiter von Unternehmen
- Maßgeschneiderte technische Lösungen zur praktischen Umsetzung der Compliance-Prozesse (in Zusammenarbeit mit Software-Entwicklern)

Durch die weite Vernetzung in der österreichischen und in der europäischen Forschungslandschaft ist RI Smart Rights Consulting in der Lage, ein individuelles und multidisziplinäres Projekt mit den besten Partnern zu konzipieren und durchzuführen. http://www.researchinstitute.at

Was dürfen Sie erwarten.....

http://privacyindesign.org/wp-content/uploads/2014/11/privacy.jpg

- 1. Rahmenbedingungen
- 2. Begriffsdschungel – „Das Leiden der jungen Wörter“
- 3. Rechtliche Aspekte
- 4. Organisatorische Aspekte
- 5. Technische Aspekte
- 6. Resümee

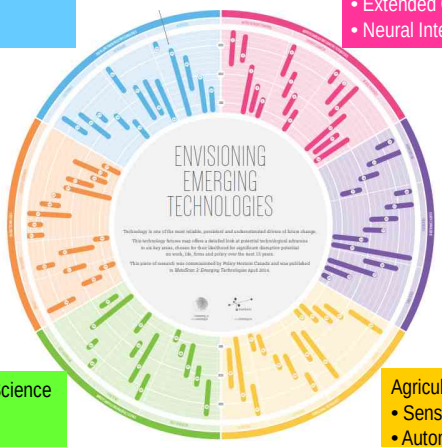
Rahmenbedingungen

http://www.kdnuggets.com/wp-content/uploads/privacy-lock.jpg

Aufkommende Technologien

Digital / Communication Technologies
- Electronics
- Networking
- Interfaces

Neurotechnology / Cognitive Technologies
- Neural Network Computing
- Extended Cognition
- Neural Interfaces



EnergyTechnologies
- Sensors
- Automation
- Engineering

Healthtechnologies
- Augmentation
- Treatments
- Diagnostics

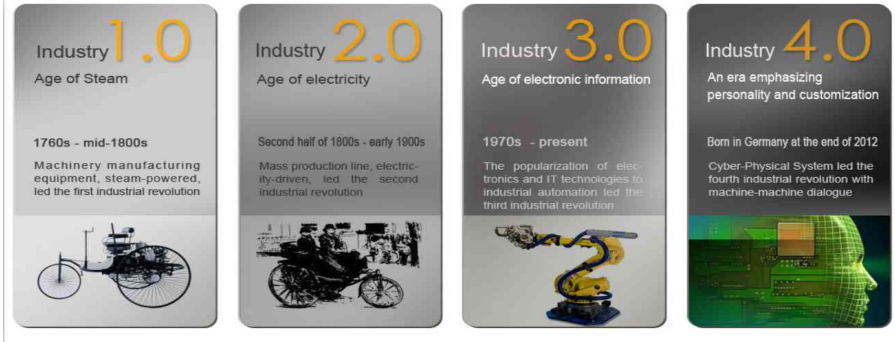
Nanotechnology & Materials Science
- Next Generation
- Functional
- Self-Assembling

Agricultural Technologies
- Sensors
- Automation
- Engineering

Von Industrie 1.0 zu Industrie 4.0 (2011)

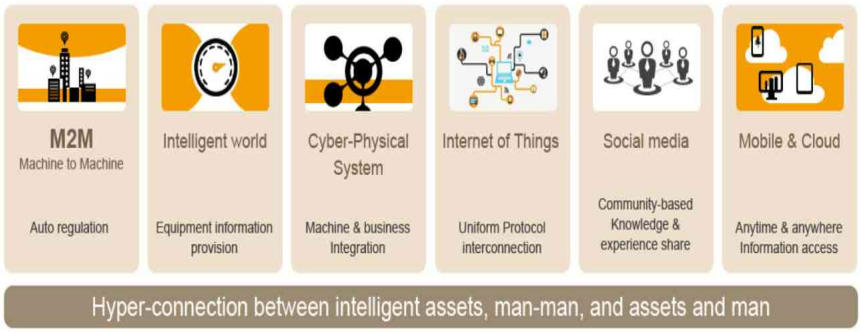
Die Taylorwanne

Industry 4.0 is to build Internet of Things and Services (IoTS) through Cyber-Physical System (CPS) technology, in virtue of deep combination of ICT (Information and Communications Technology) and manufacturing technology,
for the purpose of seamless integration and cooperation among the products, equipment, people and organizations.



http://dopho.cn/en/DophoDetail.aspx?id=2&cid=0102

Schlüsselworte von Industrie 4.0



http://dopho.cn/en/DophoDetail.aspx?id=2&cid=0102

Entwicklungen des Internets und des WWW

»Die vierte Generation der Web-Technologien (Web 4.0) wird vom Internet der Dinge und vom Internet der Dienste geprägt.«

Jörn von Lucke„Deutschland auf dem Weg zu smart Government" VM 4/2016
http://www.nomos-elibrary.de/10.5771/0947-9856-2016-4/vm-verwaltung-management-jahrgang-22-2016-heft-4

Web 5.0	Taktiles Internet	Netzwerkkommunikation nahezu in Echtzeit	Real-Time Government
Web 4.0	Internet der Dinge & Internet der Dienste	Smarte Objekte, Cyberphysische Systeme	Smart Government
Web 3.0	Internet der Daten Semantisches Web	Linked Data, Open Data, Big Data, Big Data Analytics	Open Government Data
Web 2.0	Internet der Menschen Internet zum Mitmachen	Netzwerkkommunikation über Social Media	Open Government
Web 1.0	Internet der Systeme World Wide Web	Netzwerkkommunikation über das World Wide Web	Electronic Government

Abb. 1: Häfler Stufenmodell für die weitere Entwicklung des Internet und des World Wide Webs

Taktiles Internet - Kommunikation nahezu in Echtzeit

Abbildung 1: Reaktionszeiten des Menschen

(Quelle: Fettweis, G.; Alamouti, S., „5G: Personal Mobile Internet beyond What Cellular Did to Telephony," Communications Magazine, IEEE , vol.52, no.2, pp.140-145, February 2014)

Web 5.0

http://dopho.cn/en/DophoDetail.aspx?id=2&cid=0102

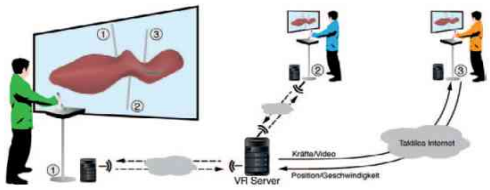
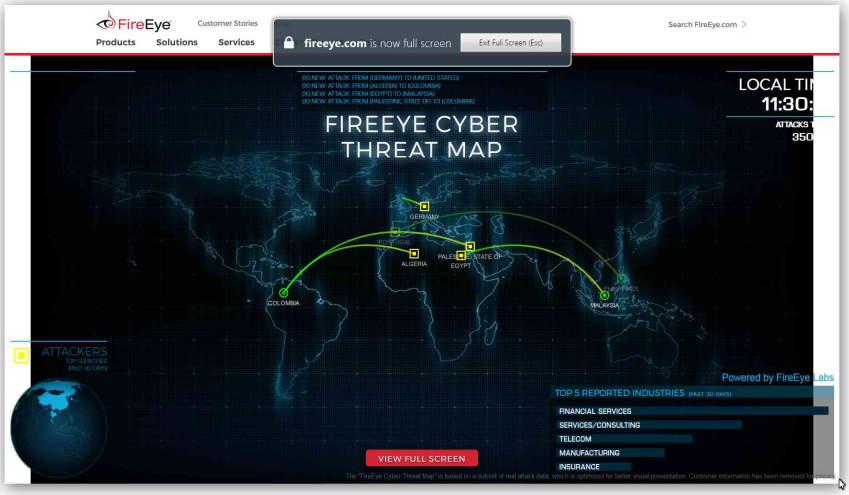


Abbildung 3: Physikalische Kopplung mehrerer Nutzer über eine Simulation der Virtuellen Realität mit haptischer Rückkopplung

(Quelle: C. Schuwerk, E. Steinbach)

Surveillance, Corporate E-Spionage, Data-Thefts, Cyber Attacks, Cybercrime ...

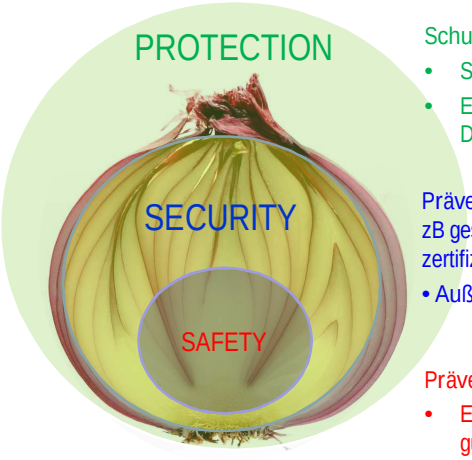


https://www.fireeye.com/cyber-map/threat-map.html

Begriffsdschungel – „Das Leiden der jungen Wörter“

http://www.kdnuggets.com/wp-content/uploads/privacy-lock.jpg

Alles eine Frage der Sicherheit …
…aber nicht alles, was sicher ist, ist safe & vice versa



Johan Botha: Life and the Onion

Schutz, Absicherung, Umwelt, Umfeld, Umgebung

- Sicherheit ist ein Teil dieses Schutzes
- EU-Datenschutz-Grundverordnung – Rahmen: Datensicherheit ein Teil davon

Prävention gegen mutwillige Beschädigungen
zB geschützt vor nicht autorisiertem Zugriff, getestetes, zertifiziertes, lfd. evaluiertes Werkzeug, etc.

- Außenwirkung und Innenwirkung

Prävention gegen schädigende Ereignisse:

- Eigenverantwortung, Achtsamkeit und Sorgfalt, gutes Training, Disziplin, etc.
- Prinzipien der lernenden Organisation

Datenschutz & Privacy

DI Dr.jur. Walter Hötzendorfer RI

Wikipedia:„Datenschutz ist ein in der zweiten Hälfte des 20. Jahrhunderts entstandener Begriff, der teilweise unterschiedlich definiert und interpretiert wird.
Je nach Betrachtungsweise wird Datenschutz verstanden als

- Schutz vor missbräuchlicher Datenverarbeitung,
- Schutz des Rechts auf informationelle Selbstbestimmung,
- Schutz des Persönlichkeitsrechts bei der Datenverarbeitung und auch
- Schutz der Privatsphäre.“

Nichts davon ist falsch. :-)

Zitate

Ann Cavoukian, three-term Information and Privacy Commissioner of Ontario, Canada will form a new international council to advocate and set standards for privacy by design, she told Bloomberg BNA May 4 (129 PRA, 7/7/14):

“I think the time has come where we have to get people all around the world to join in spreading the word that you can have privacy and security, privacy and public safety, privacy and business interests,” Cavoukian said.
“I want to change the prevailing zero-sum mindset” that pits the interest of privacy versus the interest of security.”

Angela Merkel warnt auf dem IT-Gipfel vor lähmenden Datenschutz. Datensparsamkeit könne nicht die Richtschnur sein für die neuen Produkte. Außerdem will sie künftig Bürgerdaten auf einer zentralen Plattform versammeln.
http://www.heise.de/newsticker/meldung/IT-Gipfel-2016-Merkel-plaediert-fuer-Datensouveraenitaet-statt-Datenschutz-3490629.html
Vizekanzler Sigmar Gabriel eine Wende zur "Datensouveränität" gefordert, die nicht mehr zur Maxime erklärte, Daten zu minimieren.

Rechtliche Aspekte

http://www.kdnuggets.com/wp-content/uploads/privacy-lock.jpg

Herausforderungen in der Praxis

Konkreter Sorgfalts- und Haftungsmaßstab	• Konkretisierung der Sicherheitsmaßnahmen • Verhältnis Aufwand / Risiko • Prioritäten setzen • Gesetzliche Verpflichtungen in Abgrenzung zu Selbstverpflichtung
Bestehende Strukturen und Unternehmenskultur	• Legacy-Systeme und Migration • Unternehmenskultur und gewohnte Prozesse • Stabile IT “Grundsysteme” vs agile Anwendungsentwicklung (insb. CRM)
Kollision von Interessen und Zielen	• IT-Sicherheit vs Arbeitnehmer-Datenschutz • Kundendatenschutz vs Kooperationspflicht • Betriebsgeheimnisse vs Transparenz der DV • IT-Sicherheit vs Informationsfreiheit

Arbeitnehmer-Datenschutz (Art. 88 DSGVO)

- ✓ Die gesetzlichen Regeln müssen geeignete und konkrete Maßnahmen beinhalten. Folgende Schutzzwecke nennt Art 88 DSGVO:
  - Wahrung der Menschenwürde der Datensubjekte (der von Datenverarbeitung betroffenen Personen), ihrer legitimen Interessen und Grundrechte
- ✓ Im Besonderen nennt Art 88 DSGVO folgende Themenfelder:
  - Transparenz der Verarbeitung
  - Übertragung von Daten innerhalb einer Gruppe des Unternehmens oder Gruppen von Unternehmen und Überwachung am Arbeitsplatz.
- ✓ Zulässige Zwecke der nationalen gesetzlichen Regelungen ErwG 155 und Art 88 DSGVO:
  - Einstellung von Arbeitnehmern, Erfüllung des Arbeitsvertrags
  - Erfüllung von gesetzlich oder tarifvertraglich festgelegten Pflichten
  - Management, Planung und Organisation der Arbeit
  - Gleichheit und Diversität am Arbeitsplatz
  - Gesundheit und Sicherheit am Arbeitsplatz
  - Inanspruchnahme der individuellen oder kollektiven Rechte und Leistungen aus dem Arbeitsverhältnis
  - Beendigung des Beschäftigungsverhältnisses

Modell der stufenweisen Kontrollverdichtung

Entwickelt von Kotschy/Reimer (ZAS 2004/29) aus Ansätzen in der Judikatur, vlg. die Systematik der §§ 79e ff. BDG

Stufe 1: Maschinelle Überwachung zur Gewährleistung der Systemfunktionalität

- Zunächst anonymisiert: Erkennung von Abweichungen vom „normalen“ Betriebsverhalten (z.B. durch Statistik)
- Gewährleistung der Funktionsfähigkeit der IT-Systeme rechtfertigt rein automatisierte inhaltliche Überwachung (z.B. anti-Virus Programme)

Stufe 2: Signifikante Abweichung von der „normalen“ IT-Nutzung

- Wenn Stufe 1 signifikante Abweichungen zeigt, wird Stufe 2 ausgelöst (z.B. bei missbräuchlicher Verwendung)
- Kontrolle wird auf die personenbezogene Ebene ausgeweitet → Identifikation des Missbrauchenden
- Grenzwerte für „Abweichungen“ müssen definiert werden!

Stufe 3: Zugriff auf Kommunikationsdaten bei Verdacht auf Rechtsverletzung

- Wenn Stufe 2 einen begründeten Verdacht einer Dienstpflichtverletzung ergibt → wichtig: Schutzmechanismen!
- Dennoch: Zugriff auf personenbezogene Kommunikationsdaten nicht grenzenlos erlaubt (z.B. wegen Verdacht auf „Missbrauch der Arbeitszeit“) → Verhältnismäßigkeit

Datenschutz-Folgenabschätzung (Art 35 DSGVO)

✓ Verpflichtung besteht insbesondere bei Verwendung neuer Technologien, wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen (zB Profiling, Big Data…).

✓ Eine Datenschutz-Folgenabschätzung ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 („sensible Daten" nach DSG) oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

✓ Vorherige Konsultation der DSB (Art 36 DSGVO) falls die DS-FA ein hohes
✓ Risiko zeigt, wenn der Verantwortliche keine geeigneten Maßnahmen trifft

Datensicherheit nach der DSGVO

- Wie bisher (vgl. § 14 DSG): Angemessene technische und organisatorische Maßnahmen
- Neue Konkretisierungen nach der Pflichten des Verantwortlichen nach der DSGVO:
  Art. 32 ff schließt folgende Schutzmaßnahmen ein
  - Pseudonymisierung und Verschlüsselung von personenbezogenen Daten
  - Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
  - Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen
- Haftung auch für Datensicherheit streng
  - Bis zu 20 Mio Euro oder 4 % des weltweiten Konzern-Jahresumsatzes
  - Verschulden: Sowohl Vorsatz als auch Fahrlässigkeit
  - Geldbußen amtswegig durch die Datenschutzbehörden oder Gerichte

Haftung, Handlungspflichen und Gestaltung

- Interne Richtlinien und Organisations-Policy
  - IT Sicherheitsrichtlinie (Global, Regional, Lokal)
  - Konkrete Sicherheitsmaßnahmen
  - Definition von Rollen und Sicherheitsklassen (Administrator, Bereichsleiter, etc)
  - Sicherstellung der Compliance va durch Schulungsmaßnahmen und Information
- Absicherung nach Innen
  - Dokumentation (Risk Assessment, Weisungen, Prüf- und Warnpflichten, etc)
  - Zertifizierungen von Anwendungen, Produkten, Management-Systemen
  - Externe Audits und Beratung durch Fachleute
- Absicherung nach Außen
  - Haftungsausschlüsse und Beweislastregeln in Verträgen, AGB, EULA, etc.
  - "Outsourcing" durch Dienstleisterbestellung; Versicherungen
  - Service-Level-Agreement (SLA), Garantien, Vertragsstrafen, etc.

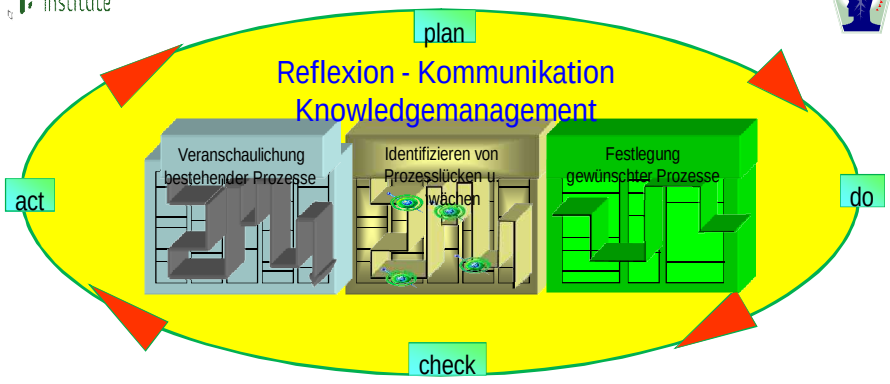
Organisatorische Aspekte

http://www.kdnuggets.com/wp-content/uploads/privacy-lock.jpg

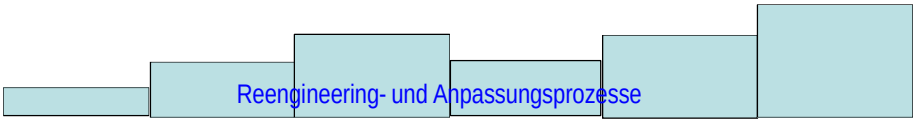
Wir brauchen auch weiterhin analoge Prozesse

Old Organisation + New Technology = COO
COO= Costly Old Organisation

Permanentes Mikro- und Makrozyklen - Monitoring



- Privacy & Security & Risk by Design für analoge und digitale Prozesse & ProzessElemente
- Implementierung nach rechtlichen, organisatorischen, semantischen & technolog. Kriterien.



Essenzen der (Re)Organisation

Kybernetiker wissen: Kontinuierliche Qualitätssteigerungen erfordern

- Möglichst schnelle Rückkopplung der Ergebnisse mit den jeweiligen Einzelkompetenzen im Entwicklungsprozess
- das Berücksichtigen wirksamer Umfeldbedingungen,
- das Bemühen um die Gesamtsicht und
- ständige Wirkungsprüfung.

Gerfried Zeichen, Pionier der Industrierobotik in Wissenschaft und Praxis. http://karrierenews.diepresse.com/home/ratgeber/management/5099226/Ist-das-zu-viel-verlangt?_vl_backlink=/home/ratgeber/management/index.do

„Förderung und Einforderung von Achtsamkeit, Verantwortlichkeit und Risikobewusstsein jedes/jeder MitarbeiterIn“

Renaissance der Unternehmensführung

- Von der zentralen Steuerung zur Dezentralisation.
- Der organisationalen Führung gilt das Hauptaugenmerk.
- Wertschöpfungsstruktur und informelle Struktur überwiegen.
- Die formale Struktur dient der Compliance.

Niels Pfläging & Silke Hermann: Komplexithoden: Clevere Wege zur (Wieder)Belebung von Unternehmen und Arbeit in Komplexität

Technische Aspekte

http://www.kdnuggets.com/wp-content/uploads/privacy-lock.jpg

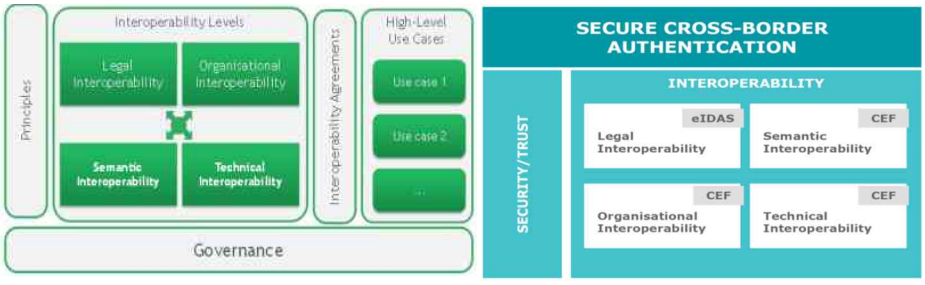
User-Centricity“ – Privacy, Securuty,&Risk by Design

http://challengedetroit.org/blog/ruthmclachlin/files/2014/05/design-thinking.jpg

Design Thinking - Thoughts by Tim Brown, http://designthinking.ideo.com
Cross, Nigel. "Designerly Ways of Knowing." Design Studies 3.4 (1982): 221-27.

ISA²

Interoperability Solutions for Public Administrations, Businesses & Citizens



Entscheidung des Europäisches Parlament v. 25. Nov. 2015: Interoperabilitätslösungen zur Modernisierung des öffentlichen Sektors, der Geschäftswelt und der BürgerInnen:

- Security & Privacy & Risk by Design & by Default
- Einhaltung des EIF (European Interoperability Framework)
- Offenheit von Spezifikationen und Normen
- Festlegung grundsätzlicher Prinzipien, http://ec.europa.eu/isa/isa2/index_en.htm

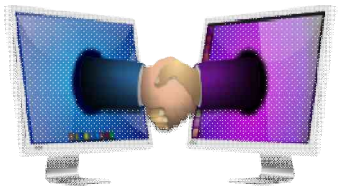
Resümee

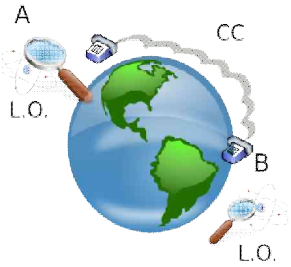
http://www.kdnuggets.com/wp-content/uploads/privacy-lock.jpg

Fairer Ausgleich zwischen Nutzen und Risiko

- ✓ Interdisziplinärer Austausch Management (Organisation) / Recht (Semantik) / Technologie
- ✓ Technikfolgenabschätzung Risikoabschätzung und Prozessorientierung
- ✓ Klarer normativer Rahmen: Transparente Vertragsgestaltung
- ✓ Stärkere Verantwortung von Unternehmen/Organisationen
- ✓ Privacy & Security & Risk by Design

Vielen Dank für Ihre Aufmerksamkeit





Wolfgang Keck
Research Institute AG & Co KG
Smart Rights Consulting – Of Counsel
OCG Forum Privacy - Arbeitskreismitglied
wkeck@tmo.at
www.researchinstitute.at

Ing. Dr. iur. Christof Tschohl
Research Institute AG & Co KG
Smart Rights Consulting
Wissenschaftlicher Leiter
OCG Forum Privacy – Co Arbeitskreisleiter
christof.tschohl@researchinstitute.at
www.researchinstitute.at

Kontakt

Research Institute AG & Co KG
Zentrum für digitale Menschenrechte
Smart.rights.consulting

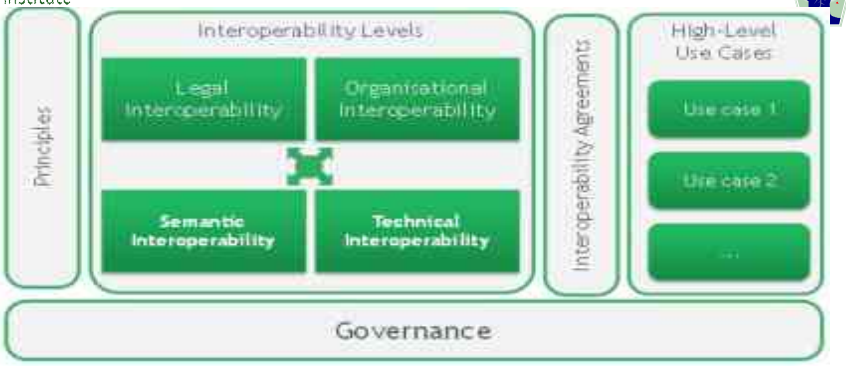
- Wissenschaftliche Leitung: Ing. Mag. Dr. Christof Tschohl
- christof.tschohl@researchinstitute.at
- Vorstand: Georg Benedikt Schmidt

- Sitz: Amundsenstraße 9, 1170 Wien
- Büro im Zentrum: Annagasse 8/1/8, 1010 Wien
- office@researchinstitute.at
- http://www.researchinstitute.at

Unterzeichner	Wolfgang Michael Keck
Datum/Zeit-UTC	2016-11-25T08:31:25+01:00
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.

Backup Folien

The Refinement of the eHealth EIF-model



For the refinement of the model, a more ‚hierarchical' orientation of the interoperability levels is restored. It also combines the parts that are valid across all interoperability levels, such as Principles, Governance, Security, Use Cases and Interoberability Agreements, ito vertical bars, to show that they are relevant for all interoperability levels.

Unterzeichner	Wolfgang Michael Keck
Datum/Zeit-UTC	2016-11-25T08:32:56+01:00
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.