universität wien

GDPR and identity management

Vienna, 12/02/2019

universität wien

<panic mode>

25/05/2018

</panic mode>

universität wien

Hopes

One Continent, one Law

Fit for the internet

One size fits all

universität wien

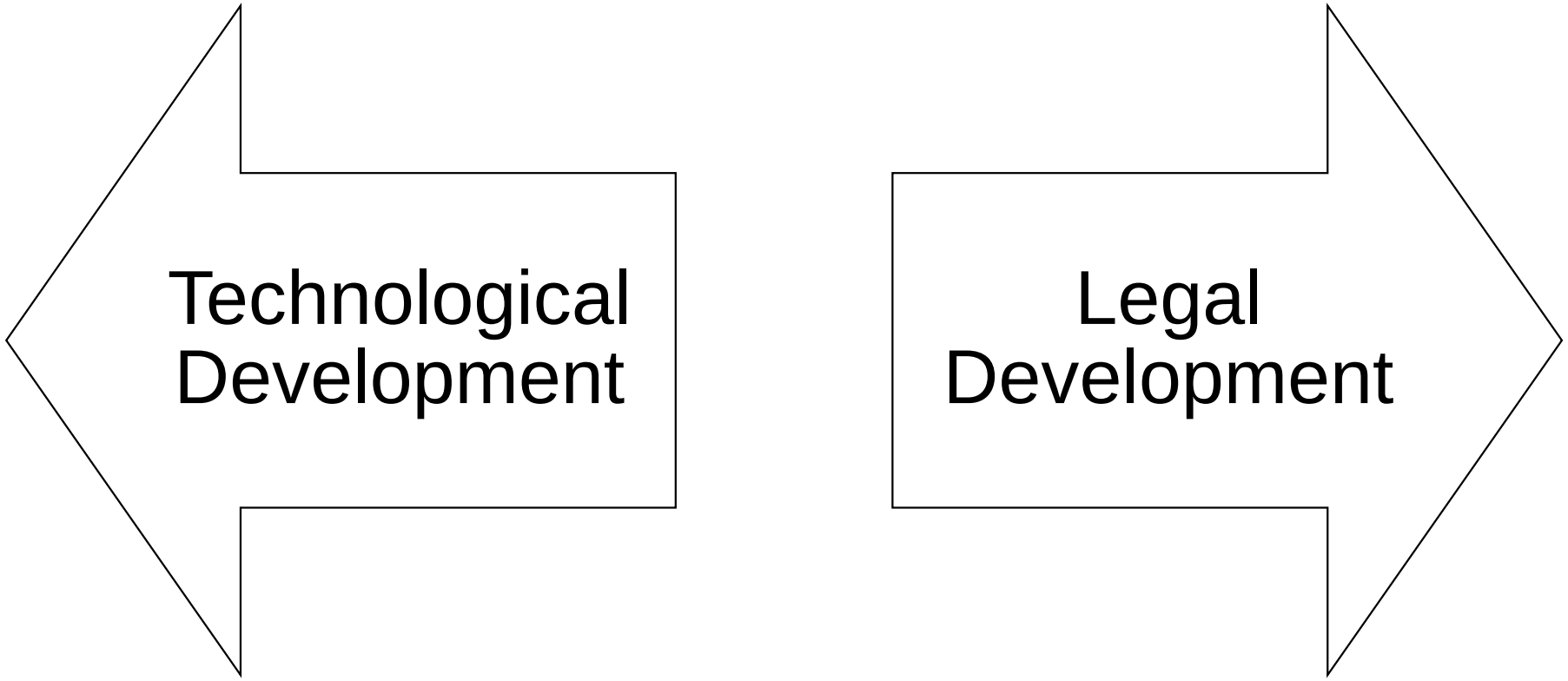
Hopes

~~One Continent, one Law~~

~~Fit for the internet~~

~~One size fits all~~

Lesson(s) learned



universität wien

Issues in 1995

- Enforceability
- Provider Liability
- Access to Justice
- Acces to legal documentation
- Efficacy in (judicial) processes
- Fragmentation of laws
- Fragmentation of technological developments
- Electronic Signatures/Identity/Authenticity
- First Wave of Internet legislation

Issues in ~~1995~~ 2005

- Enforceability
- Provider Liability
- Access to Justice
- Acces to legal documentation
- Efficacy in (judicial) processes
- Fragmentation of laws
- Fragmentation of technological developments
- Electronic Signatures/Identity/Authenticity
- „Pause“ of Internet legislation

universität wien

Issues in ~~1995~~ ~~2005~~ 2015 ff.

- Enforceability
- Provider Liability
- Access to Justice
- Acces to legal documentation
- Efficacy in (judicial) processes
- Fragmentation of laws
- Fragmentation of technological developments
- Electronic Signatures/Identity/Authenticity
- Second Wave of Internet Legislation

universität wien

Legel Development

Very, very slow progress

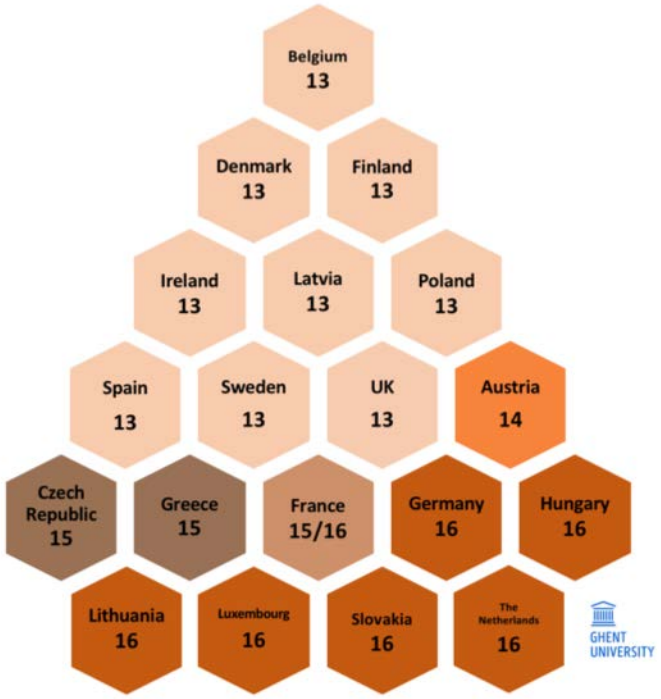
Disconnected from the technological environment

universität wien

Reality - GDPR

- No Revolution
- Higher penalties
- Higher visibility
- More administration/documentation
- Some opportunities and reliefs
- Serious risk of (further) fragmentation

Fragmentation: Age of Consent (information society services, art. 8)



Relief/Burdon – Art 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for […] scientific […] purposes […], shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

universität wien

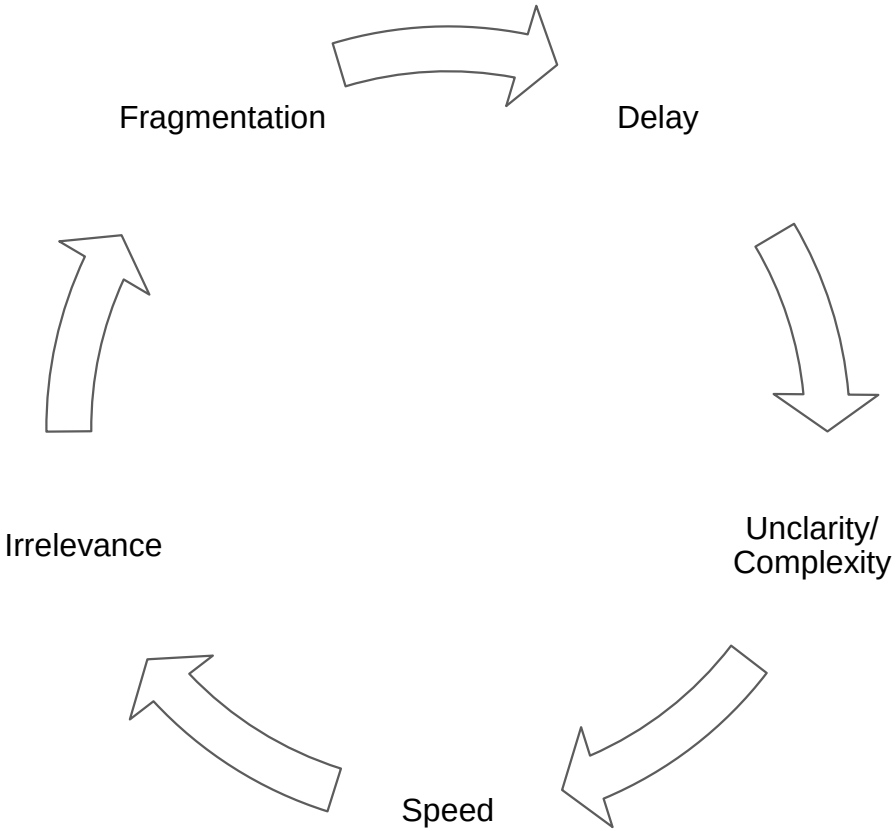
My Background

- Law, Academic, Data Protection
- > 20 European Research Projects in all roles (coordinator, WP-leader, external advisor, etc.) at the crossings of IT – cloud - health – research
  - ACGT, p-Medicine, EURECA, Linked2Safety, OPTIMIS, CHIC, AETIONOMY, PONTE, myhealthavatar, HARMONICSS, EVIDENCE, MAPPING, ….

My Lessons learned

- Data Protection Law is a weapon of mass destruction
  - Projects underestimate complexity of legal requirements and – at the same time – use some kind of „fake law“ as argument for everything
  - Data Protection Authorities are (more or less) out of the game (so far)
  - Ethics Comitteees speak about ethics – not (necessarily) about data protection law
  - Legal Compliance is a task for the project‘s and the partner‘s C-management
  - Everybody hates obligations, liability, paperwork, contracts
  - Data Access Committees are not always sufficiantly governed by legal standards
  - Consent Procedures can be supported
- Projects benefit hugely from a legal/ethical WP, need to know exactly about data flows, need to take compliance as a top priority

Broken Law


Fragmentation
Delay
Unclarity/
Complexity
Speed
Irrelevance

universität wien

Legal Foundations

More of the same: Art. 5

- 1. Personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

- Lawfulness
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Security

universität wien

Accountability

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Legal Permission, Art. 9

- 1. Processing of […] genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
- 2. Paragraph 1 shall not apply if one of the following applies: […]
- j) processing is necessary for […] scientific […] purposes […] in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject..

universität wien

Art. 9 IV

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

universität wien

Art. 89 as specific clause for research

Art 89 par 1

1. Processing for […] scientific or historical research purposes […] shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

- Safeguards!
- Data Minimisation!
- Pseudonymisation!
- Anonymization!

But: Art 89 par 2

Where personal data are processed for scientific […] purposes or statistical purposes,

Union or Member State law may provide for

derogations from the rights to [access, rectifiation, restriction, objection]

subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

Derogations

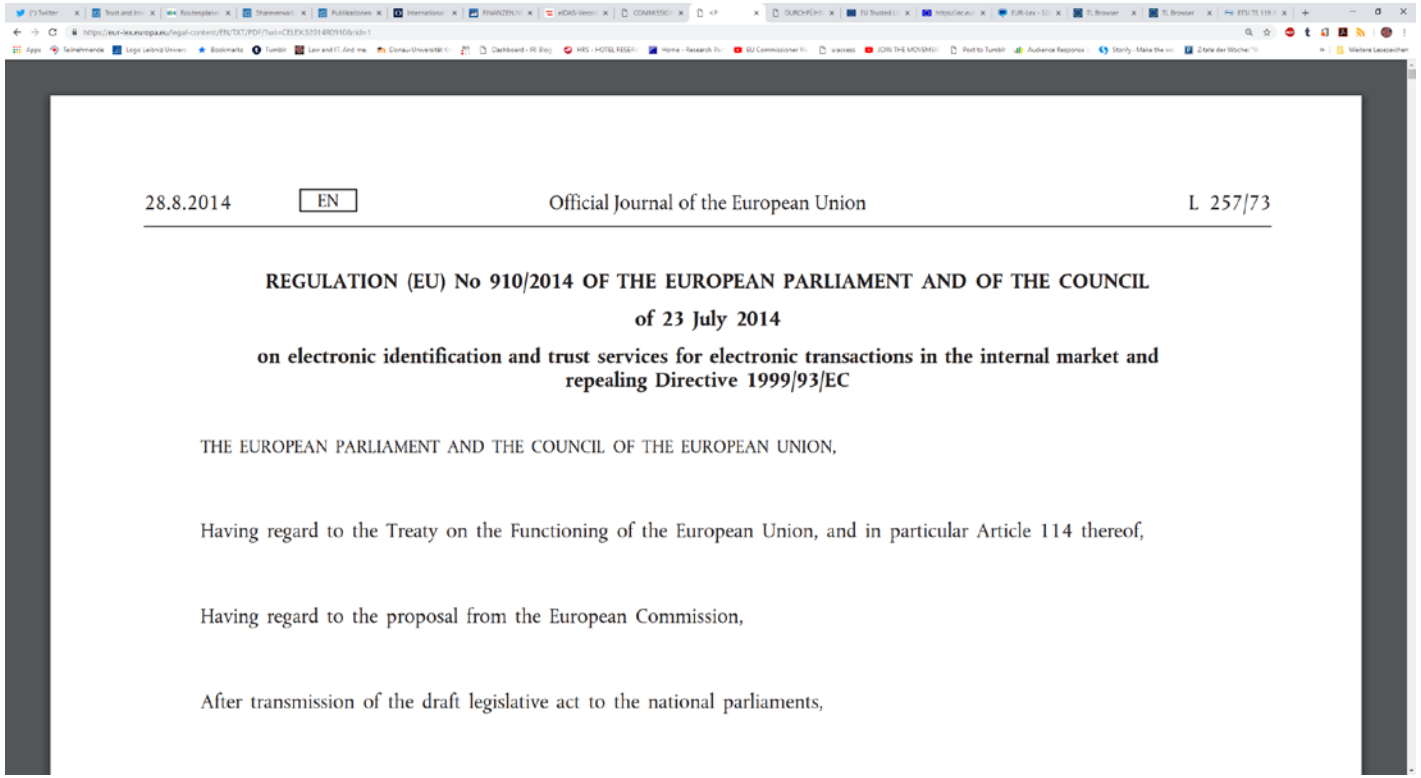
1. National
2. European

28 possible national derogations

~~One Continent One Law~~

"On the Internet, nobody knows you're a dog."

Regulation 910/2014



28.8.2014 EN Official Journal of the European Union L 257/73

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 July 2014

on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Hopes

~~One Continent, one Law~~

~~Fit for the internet~~

~~One size fits all~~

universität wien

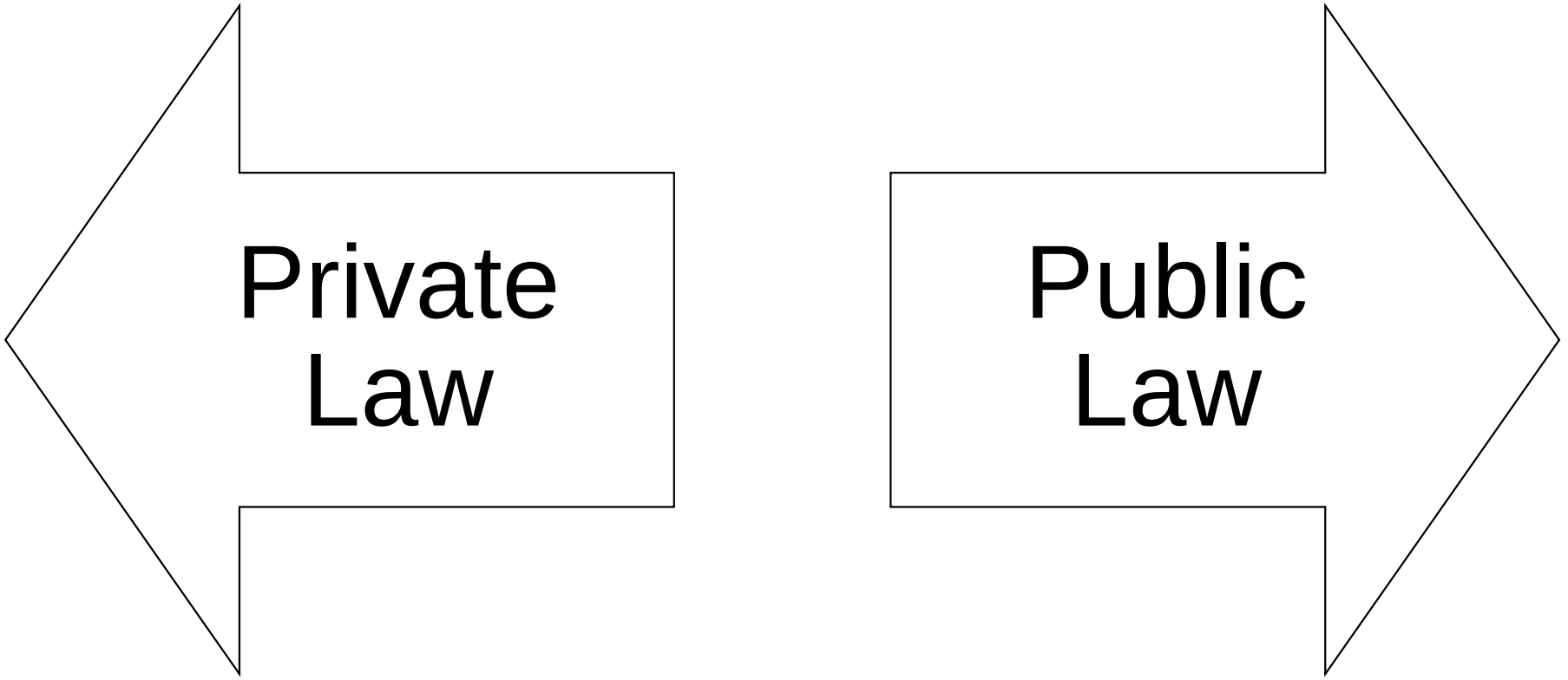
Recital 11

- This Regulation should be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council (4). In this respect, having regard to the principle of mutual recognition established by this Regulation, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. Furthermore, requirements under Directive 95/46/EC concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies.

universität wien

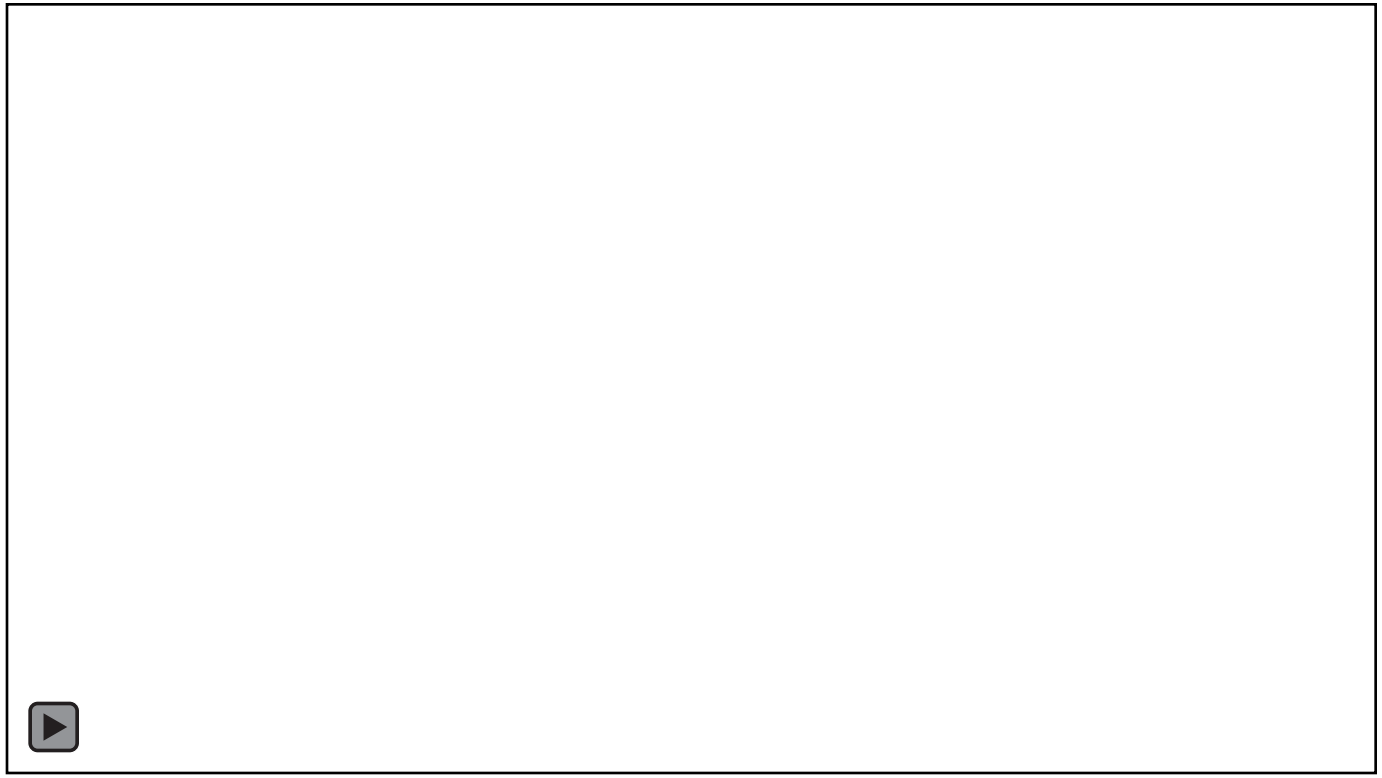
Recital 14

Some conditions need to be set out in this Regulation with regard to which electronic identification means have to be recognised and how the electronic identification schemes should be notified. Those conditions should help Member States to build the necessary trust in each other's electronic identification schemes and to mutually recognise electronic identification means falling under their notified schemes.


Private
Law
Public
Law


TRUST
einfach sicher
Startseite
Showbox
DSGVO Matrix
Datenverarbeitung gemäß DSGVO – Datenverarbeitungsverzeichnis und Matrix
Die DSGVO enthält eine Vielzahl von Anforderungen an Unternehmen, die personenbezogene Daten von europäischen BürgerInnen erheben oder verarbeiten. Bei Verstößen gegen die DSGVO drohen empfindliche Strafen: Der Strafrahmen der DSGVO reicht bis zu 20 Millionen Euro bzw. vier Prozent des weltweiten Jahresumsatzes.
Das Modul ‚DSGVO Matrix' unterstützt Sie beim Archivieren Ihrer relevanten Daten: Mittels Schritt für Schritt Anleitung können Sie die relevanten Daten einpflegen, um in Folge die Datenmatrix zu erstellen, welche vom Gesetzgeber vorgeschrieben wird. In der Matrix selbst können Angaben zur Verarbeitung und Weitergabe von Daten gemacht werden. Ihre DSGVO-Matrix können Sie in Folge bei Prüfungen vorlegen und stellen damit die Transparenz Ihres Unternehmens sicher.
Sie möchten die Erstellung von Datenanwendungsverzeichnissen nicht selbst übernehmen aber gleichzeitig nicht alle Daten aus der Hand geben? Kein Problem! Je Datenanwendungsverzeichnis wird ein Ordner erstellt. Diese Ordner können für die Bearbeitung mit anderen NutzerInnen geteilt oder exportiert werden. So können Sie sicherstellen, dass die Daten zu jeder Zeit im Eigentum des Unternehmens bleiben.
Die dazugehörigen Dokumente (z.B. Arbeitsverträge, Lieferantenverzeichnisse oder Kundendateien) können direkt im jeweiligen DSGVO-Anwendungsverzeichnis sicher abgelegen. Sollten Sie diese Dokumente nur in analoger Form vorfinden, ist auch das kein Problem: Mittels Scan-Funktion können Sie diese einfach und schnell mit Ihrem Smartphone digitalisieren.
Das Modul DSGVO Matrix unterstützt Sie bei der Einhaltung der DSGVO – schrittweise, anwenderfreundlich und sicher.
Anwendungsbeschreibung:

universität wien



A-Trust DSGVO Video - Preview (v08)

PICAPIPE
Abonnieren 0

150 Aufrufe

Hinzufügen Teilen Mehr 0 0

Hochgeladen am 22.04.2018
Kategorie Menschen & Blogs

KOMMENTARE

Öffentlich kommentieren...

Auf den ersten Blick unmöglich: Eine dreieckige Dose von der Drechselbank
HolzWerken
240.207 Aufrufe

PERFEKTE Gehrungen mit JEDER Tischkreissäge| Das ist der Trick..... | Lets Bastel
Lets-Bastel
288.915 Aufrufe

31 KOCH TRICKS, DIE DICH ÜBERRASCHEN WERDEN
5-MINUTEN TRICKS
225.340 Aufrufe

10 Athleten, die beim Betrügen erwischt wurden!
#Mentale Zuflucht
4.703.162 Aufrufe

Geldvernichtung - Kauf dir bloß kein Auto
Frank Fichert - Sales Quality
1.028.394 Aufrufe

GRANDIOS: #Broder spricht vor der #AfD-Fraktion im Bundestag | Rede
Oliver Flesch
242.338 Aufrufe

Schuldnerin verplappert sich bei Pfändung: Wie wertvoll ist alles? | Achtung Kontrolle | kabel eins
Achtung Kontrolle
499.594 Aufrufe

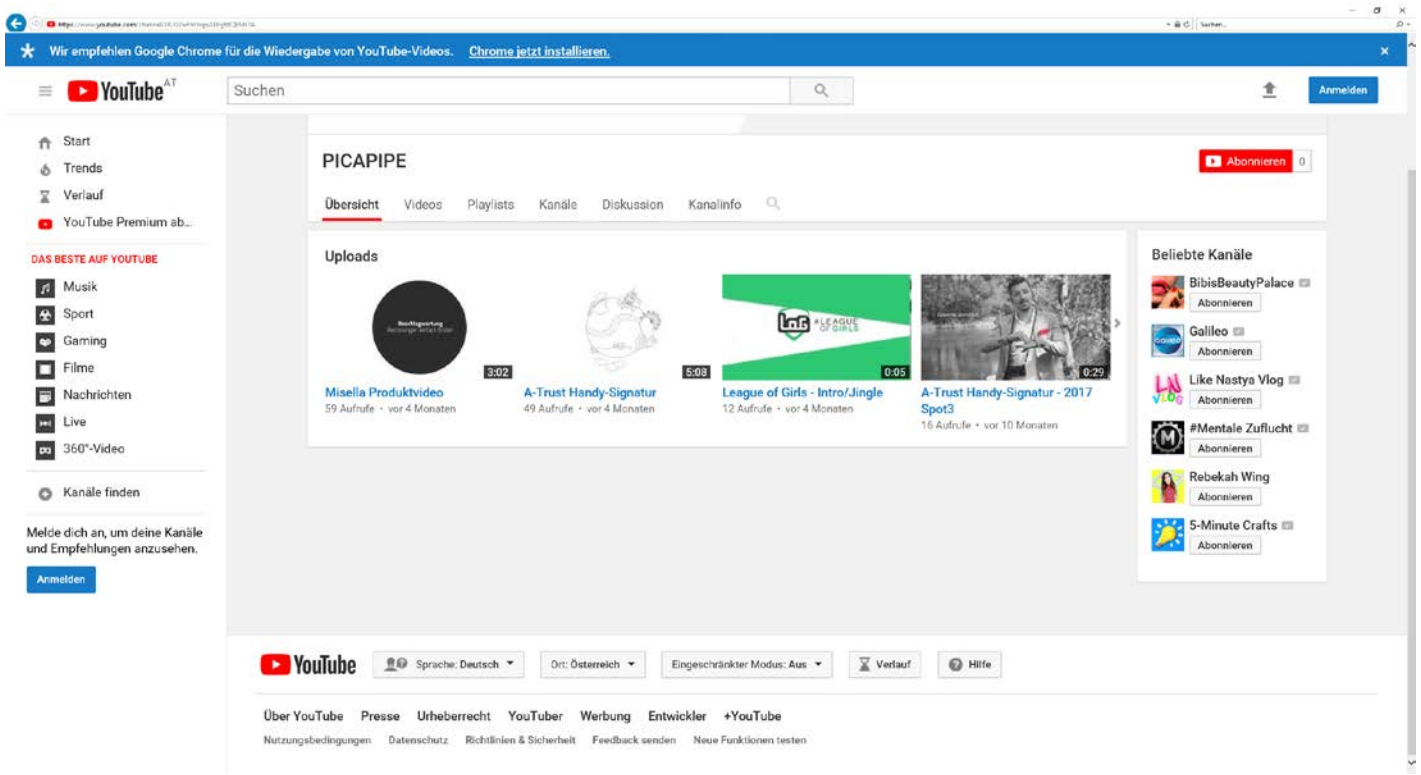
Eine 370€ Enttäuschung - LEGO® Technic 42083 - Bugatti Chiron
Held der Steine Inh. Thomas Panke
2.000.252 Aufrufe

Realer Irrsinn: Neue digitale Stromzähler | extra 3 | NDR
extra 3
848.237 Aufrufe

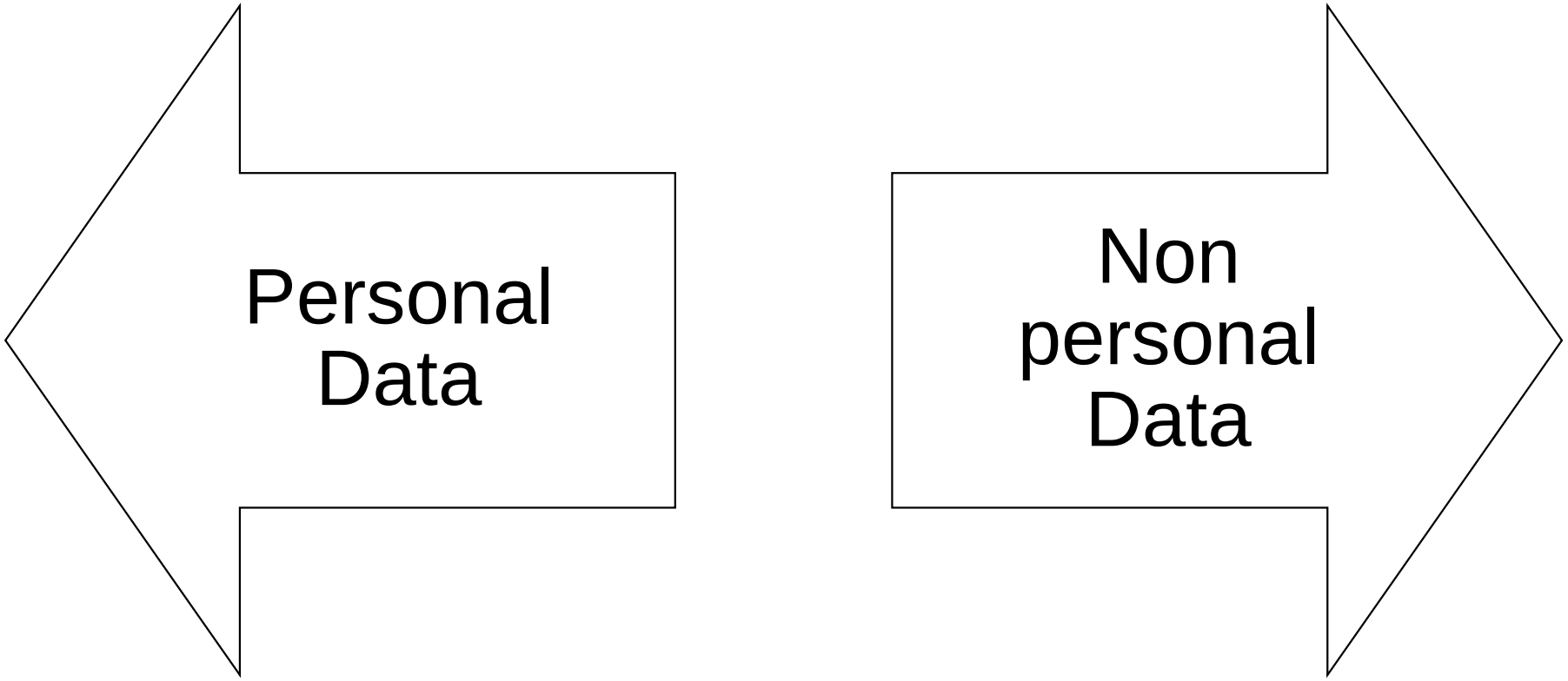
Kölner Raser Szene - Fahrradcops legen CL 500 still.
Hardcore Dortmund
6.789.312 Aufrufe

Der LEGO® 75201 AT-ST ist das schlechteste Star Wars Set aller Zeiten
Held der Steine Inh. Thomas Panke
758.225 Aufrufe

So fake ist DSDS wirklich


Wir empfehlen Google Chrome für die Wiedergabe von YouTube-Videos. Chrome jetzt installieren.
YouTube AT
Suchen
Anmelden
Start
Trends
Verlauf
YouTube Premium ab...
DAS BESTE AUF YOUTUBE
Musik
Sport
Gaming
Filme
Nachrichten
Live
360°-Video
Kanäle finden
Melde dich an, um deine Kanäle und Empfehlungen anzusehen.
Anmelden
PICAPIPE
Abonnieren 0
Übersicht
Videos
Playlists
Kanäle
Diskussion
Kanalinfo
Uploads
3:02
Misella Produktvideo
59 Aufrufe • vor 4 Monaten
A-Trust Handy-Signatur
49 Aufrufe • vor 4 Monaten
5:08
0:05
League of Girls - Intro/Jingle
12 Aufrufe • vor 4 Monaten
0:29
A-Trust Handy-Signatur - 2017 Spot3
16 Aufrufe • vor 10 Monaten
Beliebte Kanäle
BibisBeautyPalace
Abonnieren
Galileo
Abonnieren
Like Nastya Vlog
Abonnieren
#Mentale Zuflucht
Abonnieren
Rebekah Wing
Abonnieren
5-Minute Crafts
Abonnieren
YouTube
Sprache: Deutsch
Ort: Österreich
Eingeschränkter Modus: Aus
Verlauf
Hilfe
Über YouTube
Presse
Urheberrecht
YouTuber
Werbung
Entwickler
+YouTube
Nutzungsbedingungen
Datenschutz
Richtlinien & Sicherheit
Feedback senden
Neue Funktionen testen

GDPR - Definitions



Personal Data

- Art. 4 (1) GDPR
- ‘personal data’ means
- any information
- relating to an identified or identifiable natural person (‘data subject’);
- an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

universität wien

Recital 26

The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. **To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.** The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

universität wien

Pseudonymisation

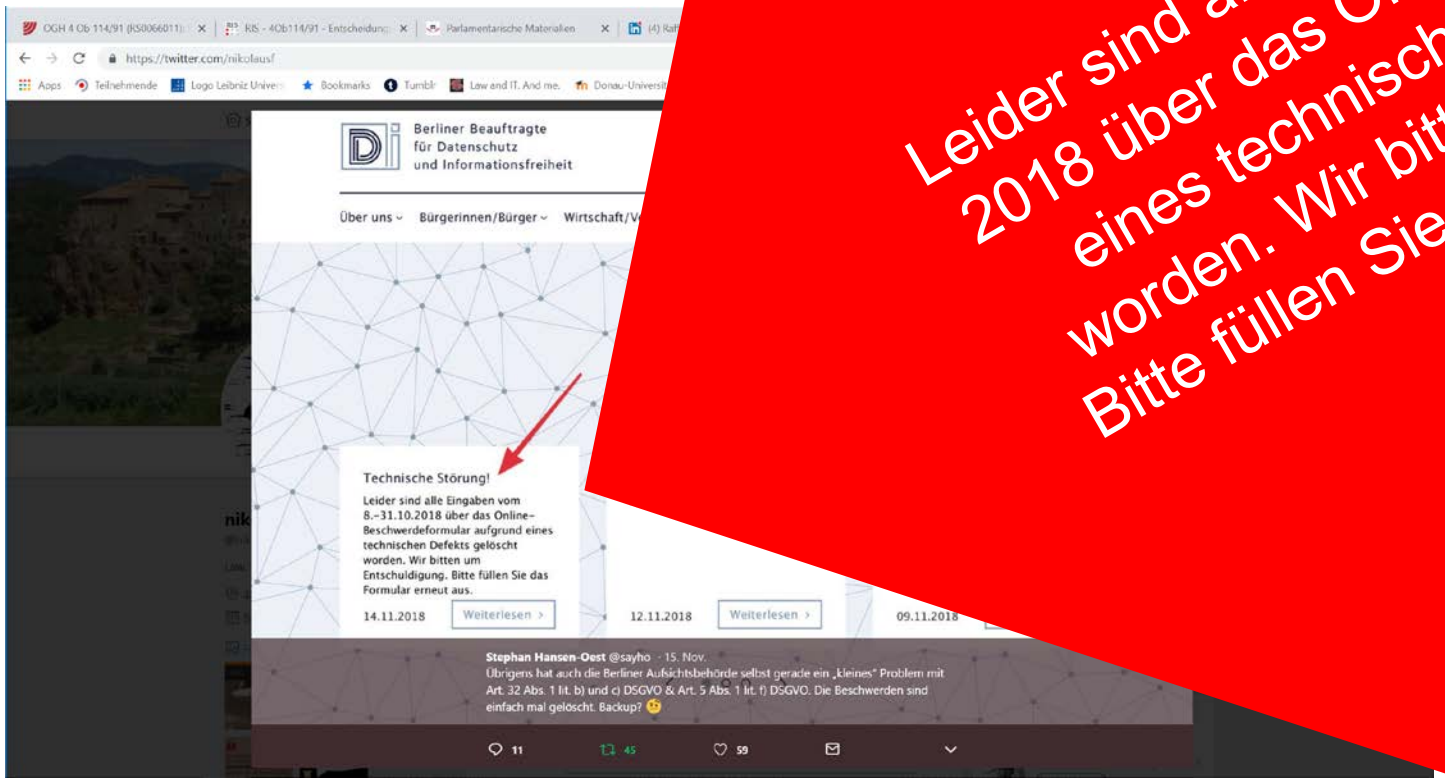
- Art. 4 (5)
- means the processing of personal data in such a manner that the personal data can **no longer** be attributed to a specific data subject **without the use of additional information**, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

universität wien

Information Security, Art. 32

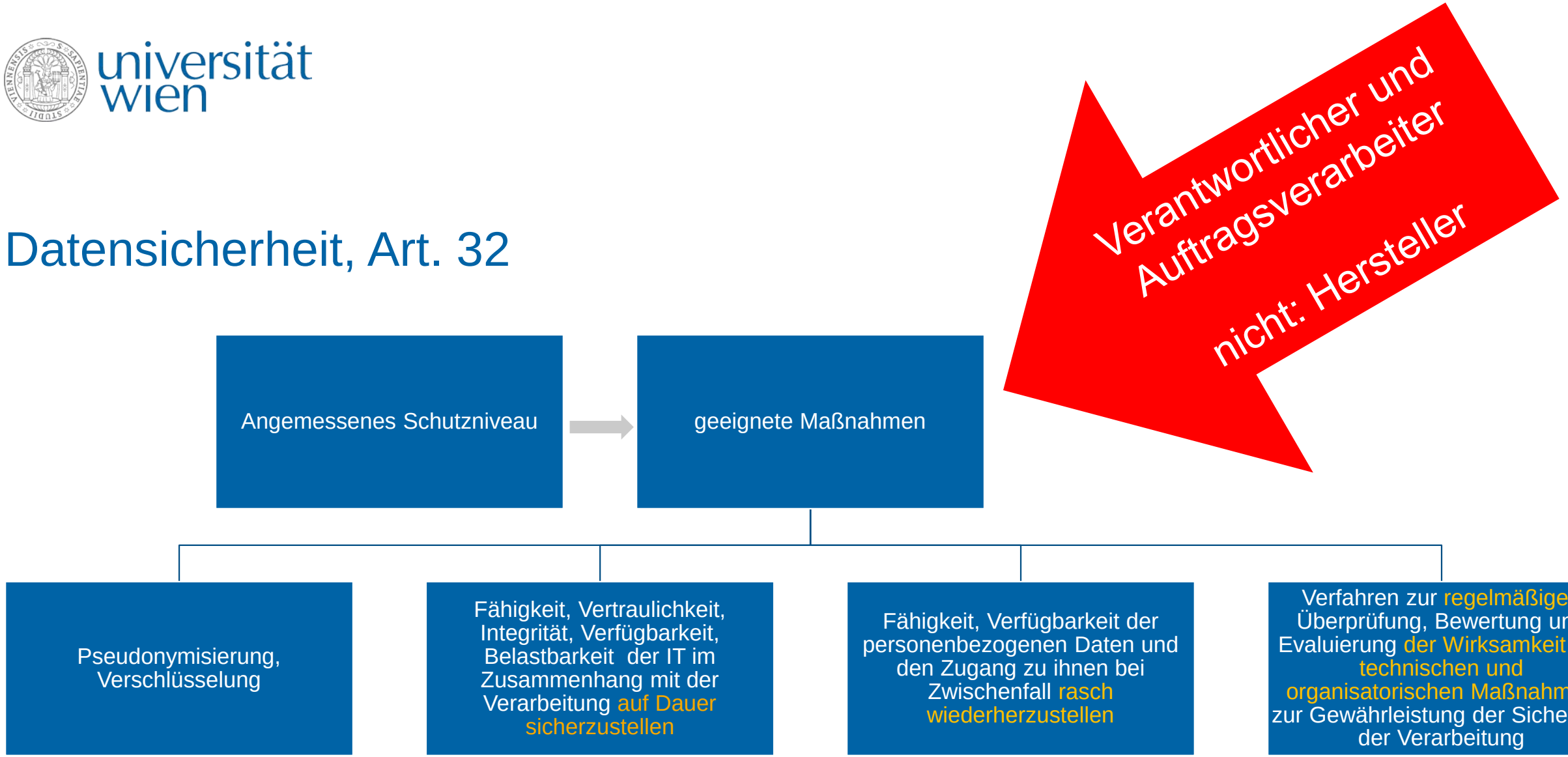
- Taking into account
- the state of the art, the costs of implementation
- and the nature, scope, context and purposes of processing
- as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons,
- the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

universität wien



Technische Störung!
Leider sind alle Eingaben vom 8. – 31. 10. 2018 über das Online-Formular aufgrund eines technischen Defekts gelöscht worden. Wir bitten um Entschuldigung. Bitte füllen Sie das Formular erneut aus.

Datensicherheit, Art. 32



Verantwortlich: der Verantwortliche (= der Kunde)

universität wien

Recital 78, Sentence 4

„ When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. “

universität wien

Thank you!

Nikolaus Forgó, Department of Innovation and Digitalisation in Law, Universität Wien

www.univie.ac.at/id, nikolaus.forgo@univie.ac.at, @nikolausf