Blockchain and the European Union's General Data Protection Regulation (GDPR)

DLTReg 2019, Москва, 27 марта 2019

Jörn Erbguth, Dipl.-Inf., Dipl.-Jur.
Consultant Legal Tech, Blockchain, Smart Contracts and Data Protection
Lecturer at the University of Geneva and Geneva School of Diplomacy

joern@erbguth.ch +41 787256027

What is the biggest threat to our privacy?

Better Privacy Through the Use of Blockchain

Privacy Coins

MONERO

Zcash

Self Sovereign ID

enigma

JOLOCOM

Privacy Frameworks

BLOCKSTACK

Regulatory Approach of the GDPR

Controller

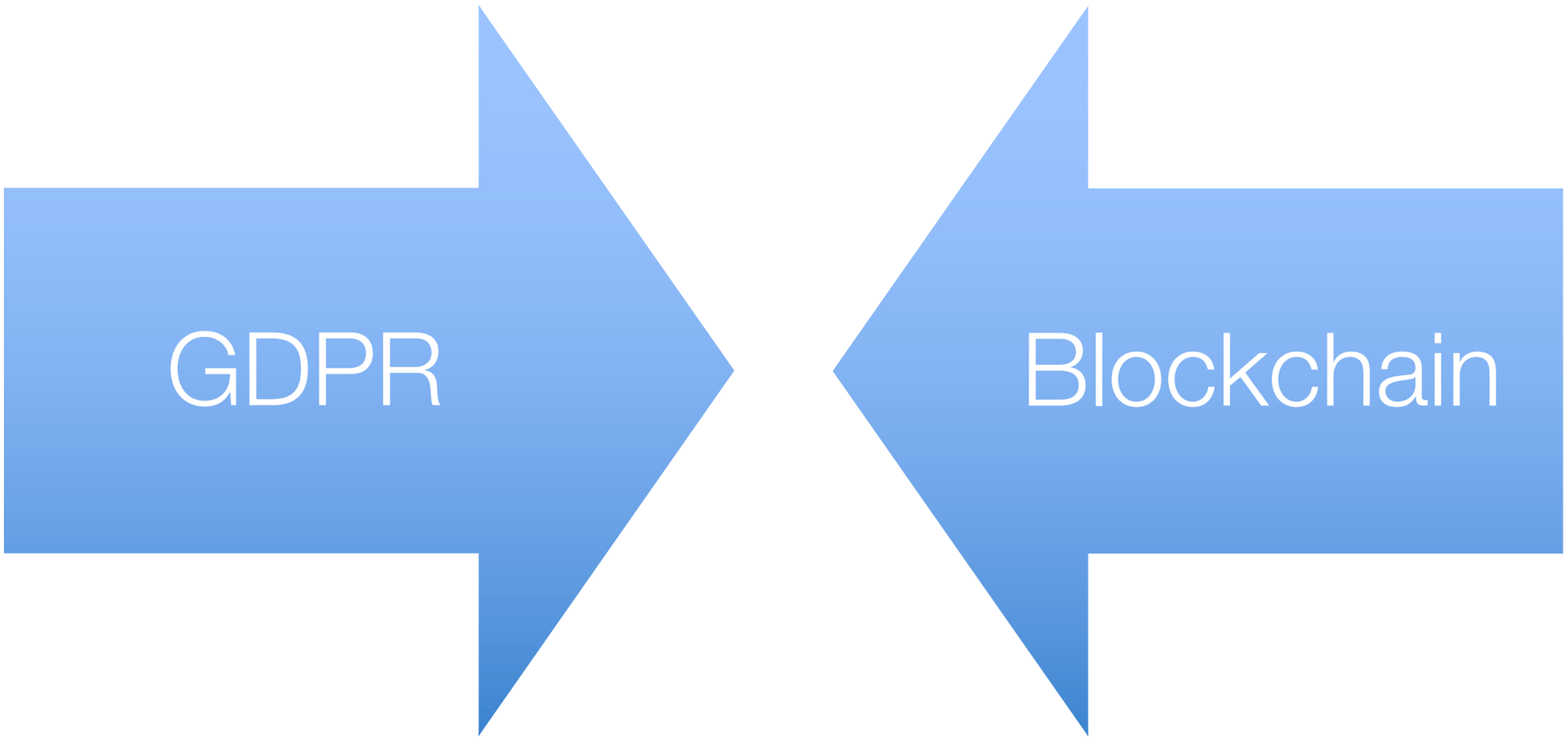
Determines the purposes and means of processing

Processor

Processes data on behalf of the controller

Data-Subjects

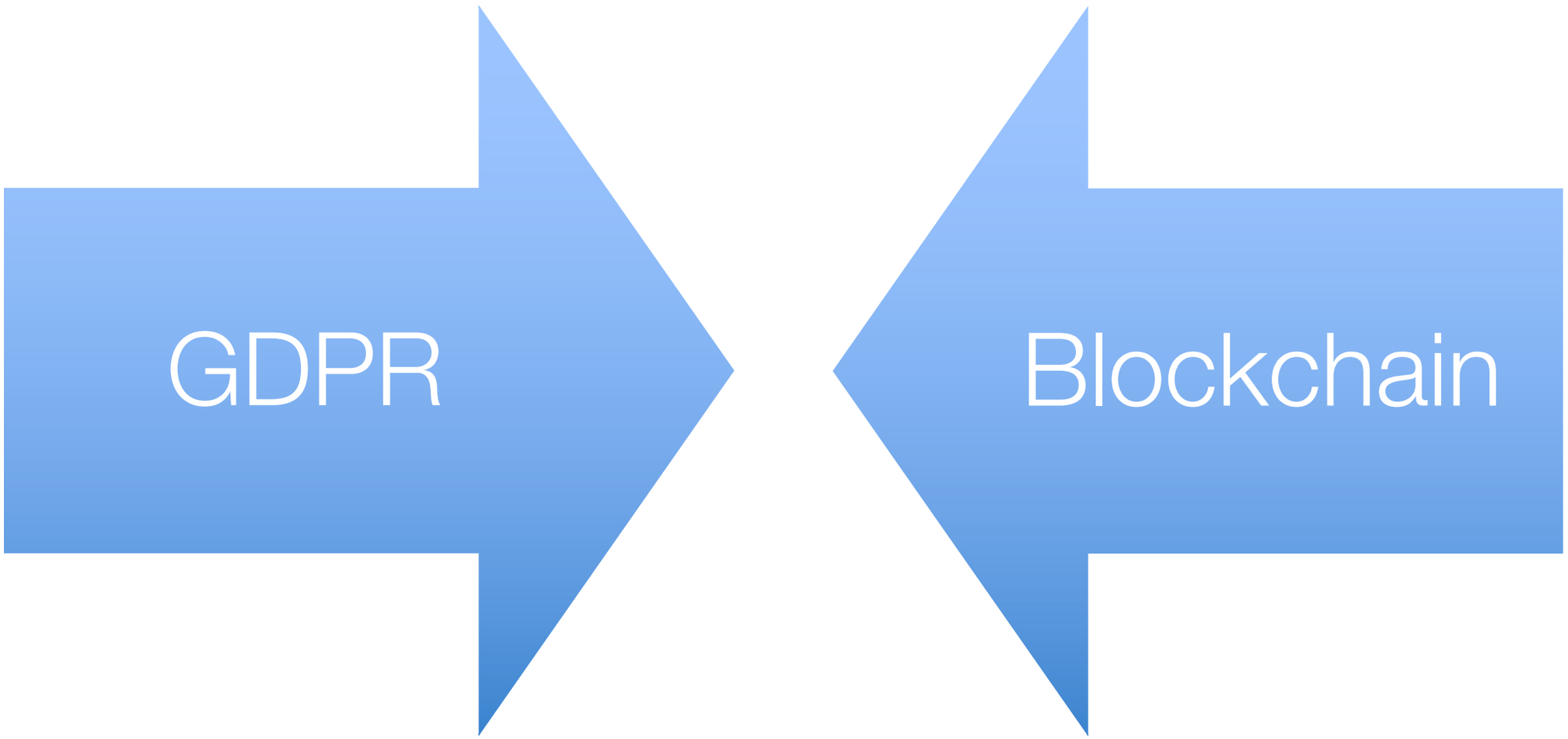
GDPR vs. Blockchain



Clear responsibilities
controller
processor

distributed responsibility
anonymous participation

GDPR vs. Blockchain



Right to …

Art. 16: rectification

Art. 17: erasure

Art. 18: restriction of processing

immutable

public

Charter of Fundamental Rights of the European Union

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

General Data Protection Regulation (GDPR)

- Processing of personal data is forbidden
- Unless there is proper justification
- Obligations for controllers and processors
- Rights for data subjects
- GDPR restricts the transfer of personal data to third countries
- Includes obligation to information security
- Fines up to 20 mill. € or 4% of worldwide annual turnover

How to evaluate GDPR compliance

- Does GDPR apply?
- Is there processing of personal data?
- Is there a justification for this data processing?
- Do I comply with the obligations of GDPR?

Does the GDPR apply? (Art. 2, 3)

- Some entity that is considered a controller or a processor is in the EU
- Offering goods or services to data subjects in the EU
- Monitoring behavior of data subjects in the EU
- Not if only for personal use or household activity

Personal data (Art. 4.1)?

Any information relating to an identified or identifiable natural person

- Pseudonymous data is personal data
- Anonymous data is **not** personal data

Recital 26: To determine whether a natural person is identifiable, account should be taken of **all the means reasonably likely to be used** ... either by the controller or by another person to identify the natural person directly or indirectly.

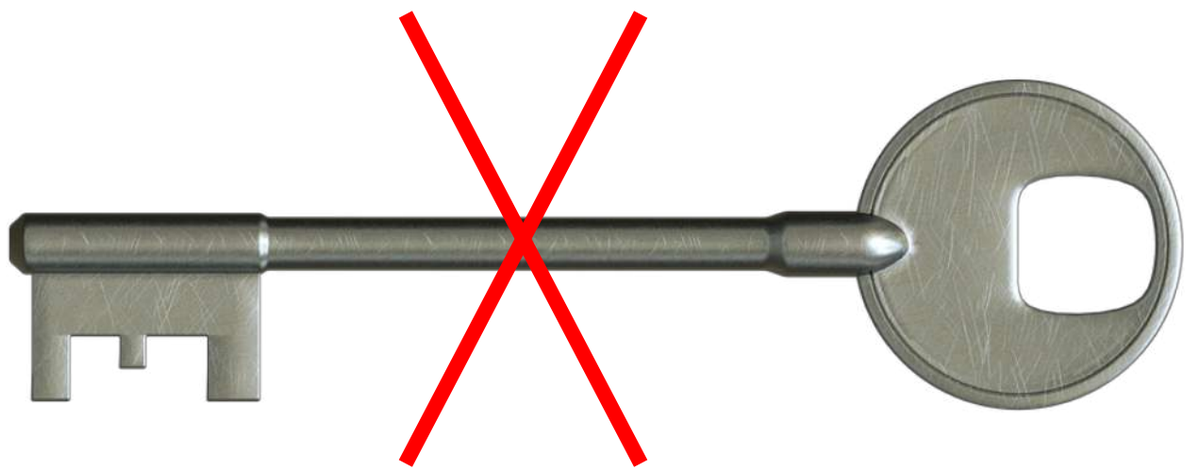
Examples of personal data

- ✓ IP addresses
- ✓ Bitcoin addresses
- ✓ “anonymized” movement profile
- ✓ “anonymized” browsing history
- ✗ aggregated movement profiles
- ✗ aggregated browsing history

Attention: Look at the individual case – do not generalize

Encryption

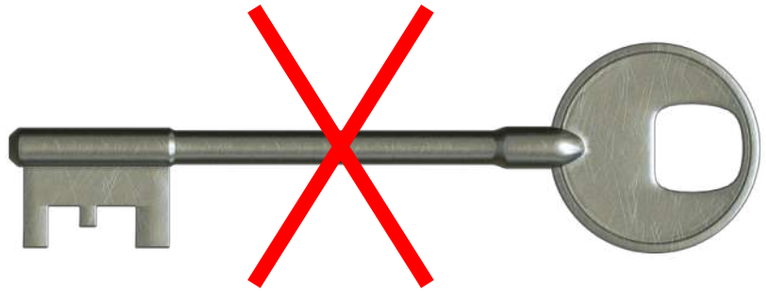
Deletion of the encryption key = deletion of the content?



SAMSUNG
MMCQE28GFMUP – MVA
DFK3OOA842 – SE842A0588
0842
REV 0
F/W VAM05S1Q
Model : Slim 128GB uSATA MLC
SSD P/N : MMCQE28GFMUP – MVA
WARRANTY VOID IF REMOVED
Solid State Drive RATED: DC+3.3V 0.32A SAMSUNG ELECTRONICS CO., LTD
WARNING DELICATE PRODUCT SENSITIVE PARTS INSIDE. DAMAGE MAY OCCUR IF SHOCKED. TOUCHING THE CIRCUITS MAY CAUSE MALFUNCTION. REMOVAL OF THIS COVER WILL VOID ANY AND ALL WARRANTIES.
Slim 128GB uSATA MLC
SEC – M – SLIM28GUSATA(B)
2008.10.07
SAMSUNG
MMCQE28GFMUP – MVA

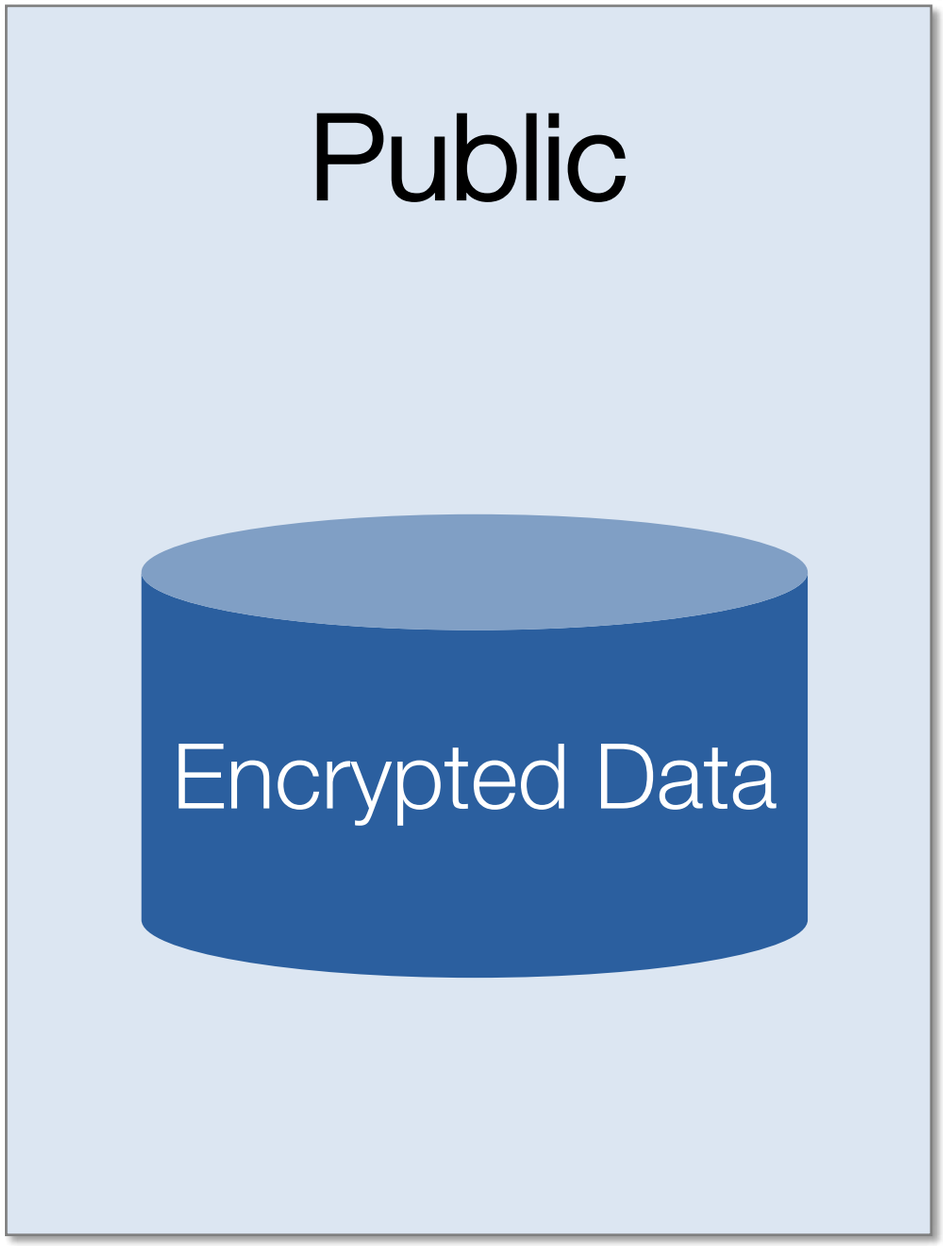
GDPR-compliant deletion?

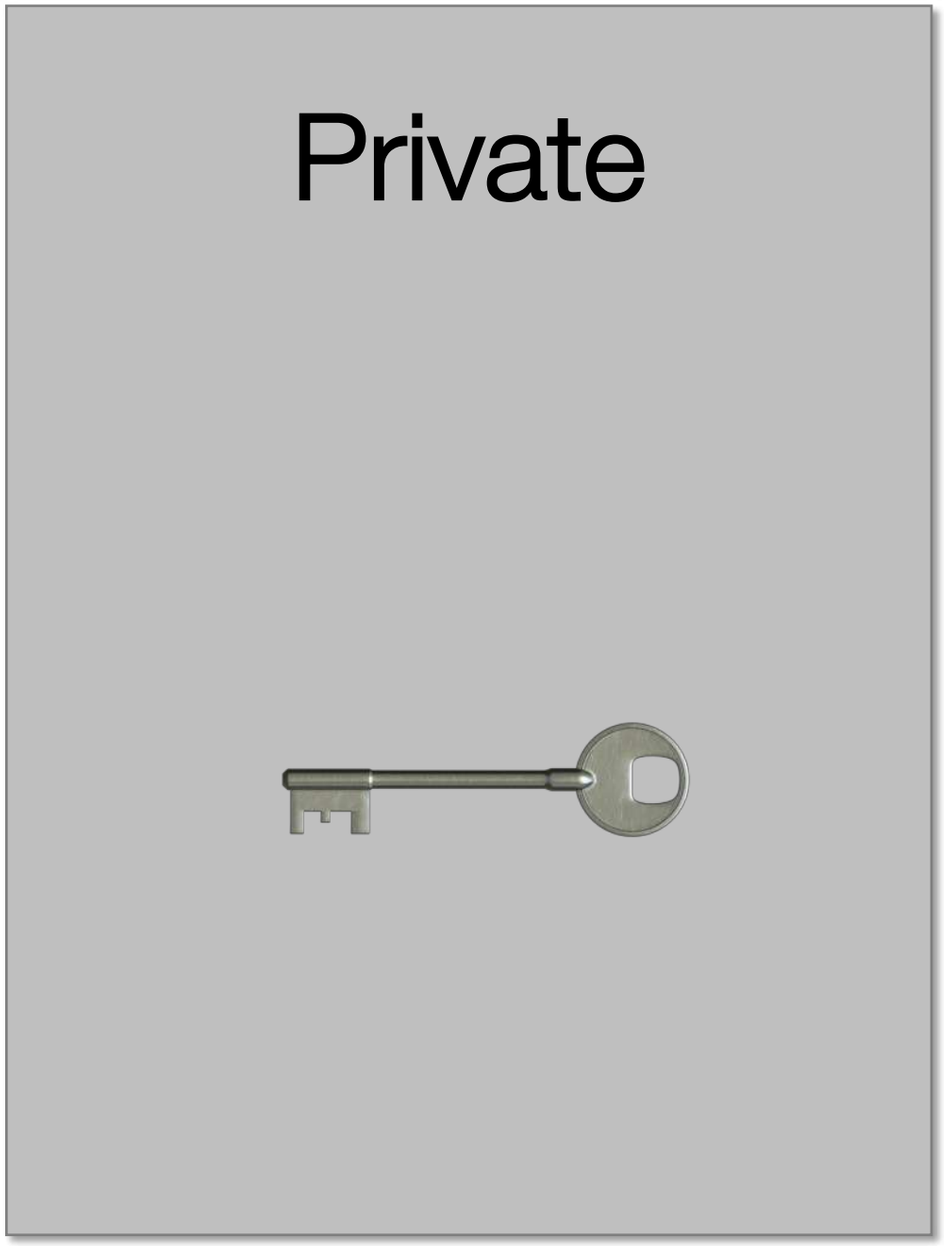
- Deletion of the encryption key = deletion of the content?



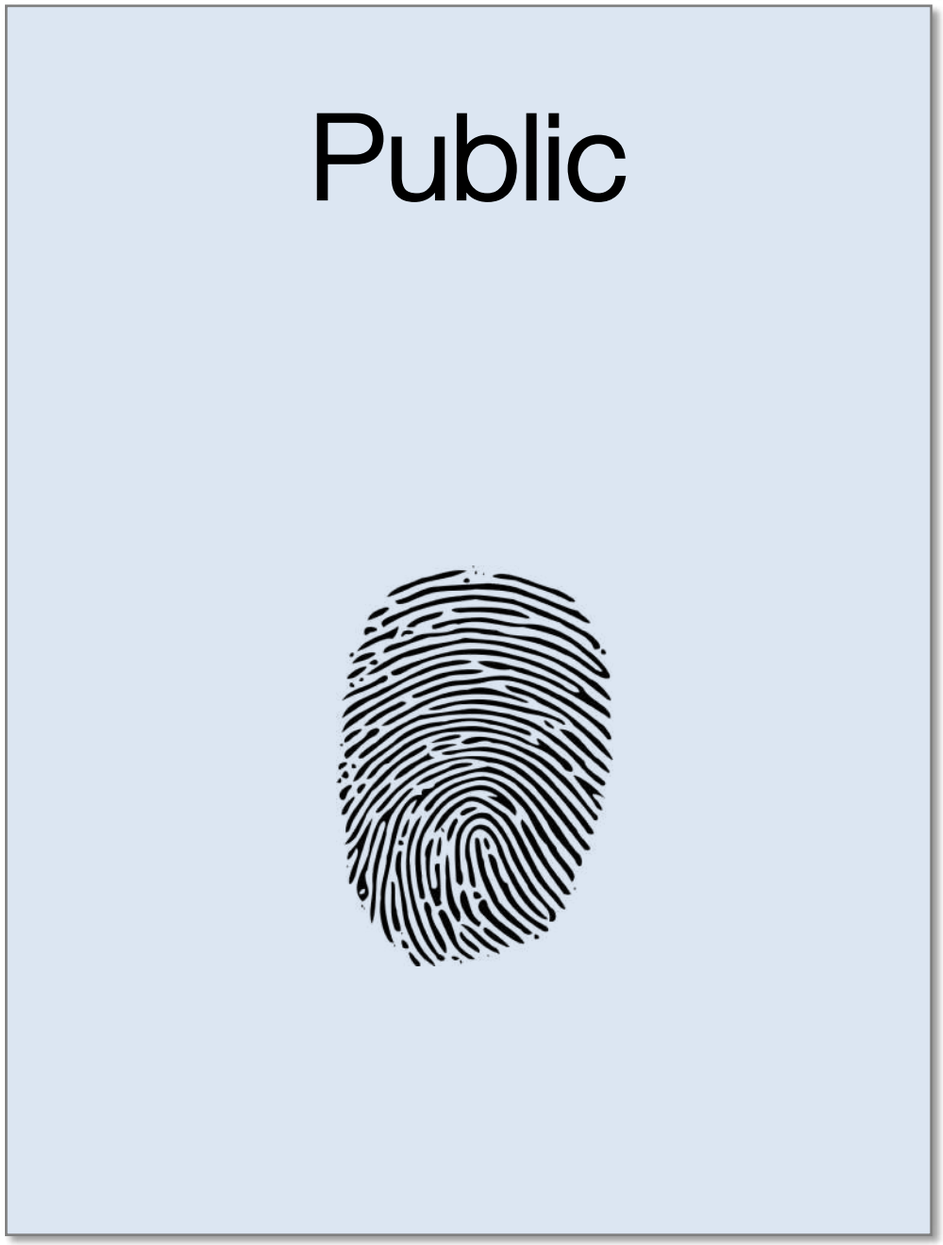
- Austrian Datenschutzbehörde says yes.

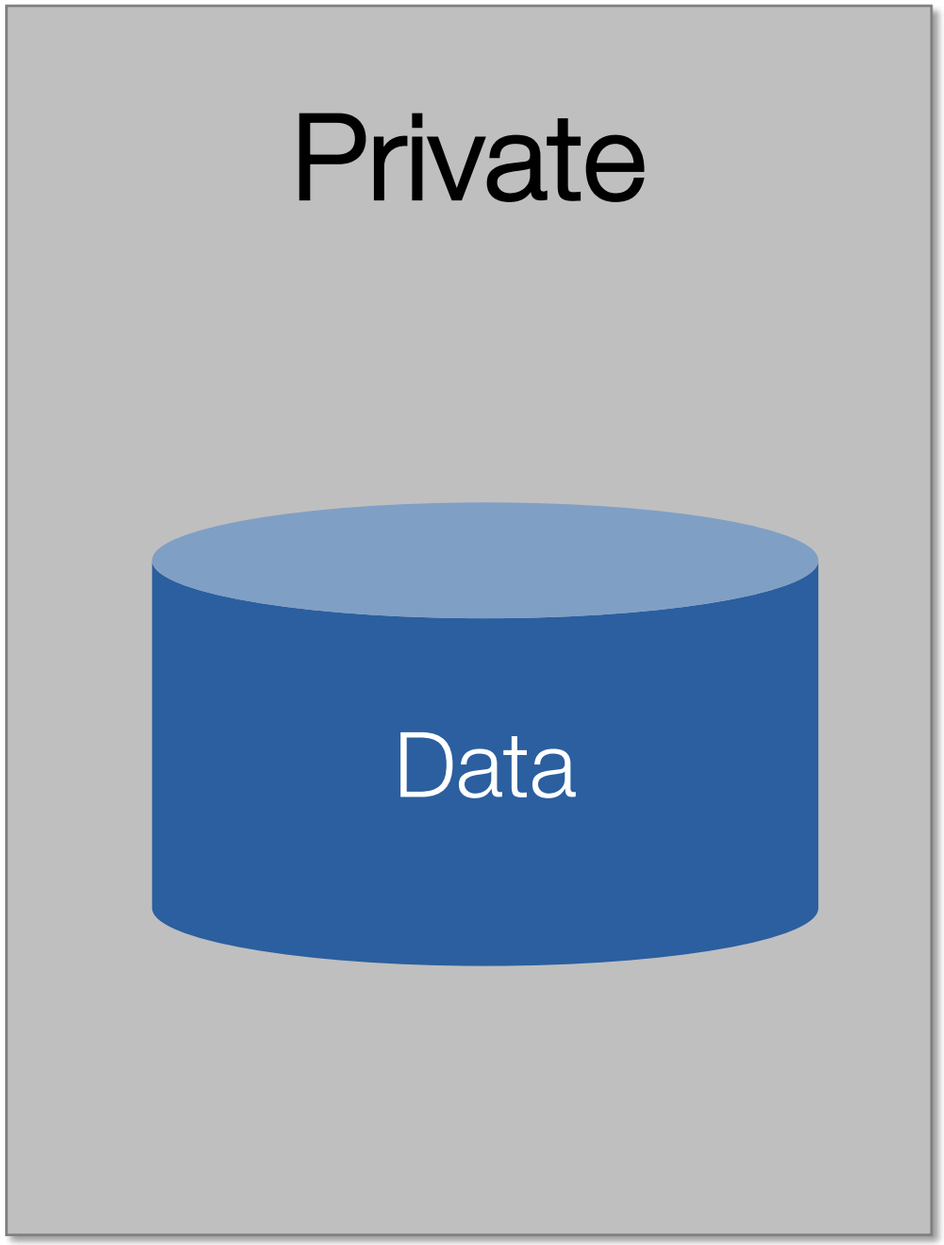
Use of Hash Values





Use of Hash Values





Cryptographic hash functions

- Serve as digital fingerprints
- Virtually unique
- Fixed length (e.g. 256 bits)
- For digital objects of any size
- One-way function

Demo 2

Kryptografische Hashwerte, datenschutzkonform

UNIVERSITÄT PASSAU

Universität Passau
Juristische Fakultät

Diplomurkunde

Die Juristische Fakultät der Universität Passau verleiht mit dieser Urkunde

Herrn **Jörn Horst Erbguth**

geboren am 5. Dezember 1967 in Marl

den akademischen Grad

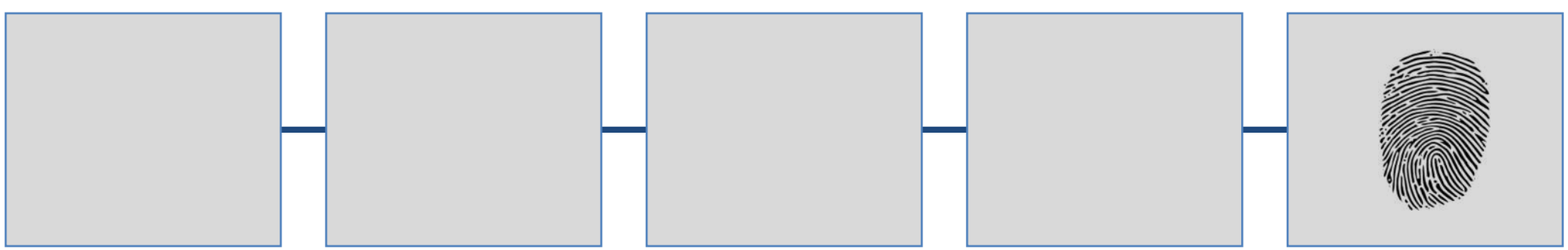
Diplom-Jurist Univ.

(Dipl.-Jur. Univ.)

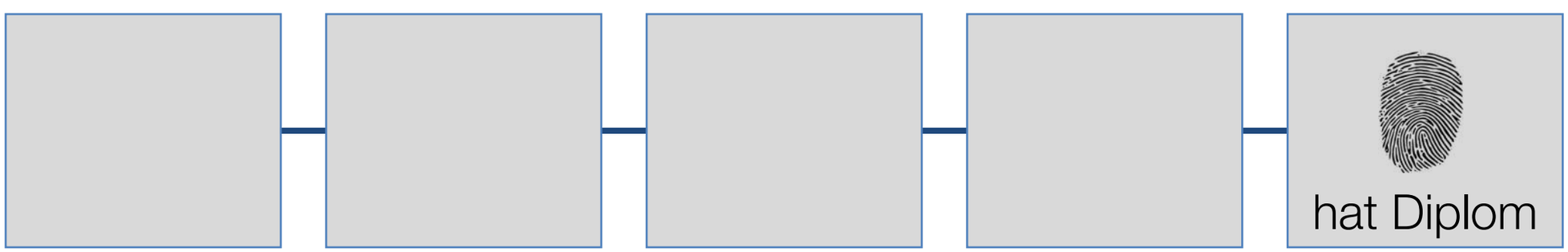
aufgrund der gemäß Ausbildungs- und Prüfungsordnung für Juristen (JAPO) in der jeweils gültigen Fassung am 23. Juli 1992 bestandenen Ersten Juristischen Prüfung.

Passau, den 24. Januar 2018

(Prof. Dr. Hans-Georg Dederer)
Dekan



Kryptografische Hashwerte, nicht datenschutzkonform



Test: Does the Blockchain Leak Personal Data?

Is it possible to derive information about a natural person from the blockchain?

What if

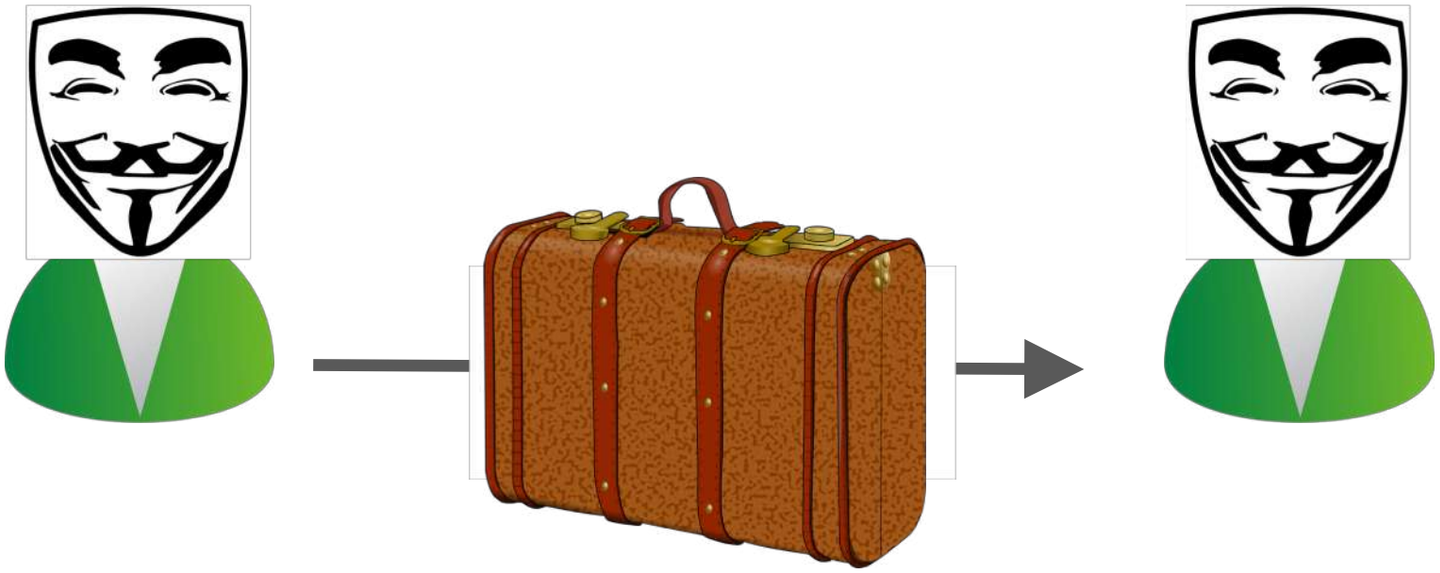
- somebody knows one transaction, can she see further transactions of the same person?
- somebody knows part of a transaction, can she see further details?
- somebody knows personal details of a person, can she discover information about the person's activity?

Zero-Knowledge Proof

Proof of knowing something
without revealing it

Zero-Knowledge Proof – Zcash

- Limiting the purpose of using personal data by technical means
- Only the correctness of the transaction can be proven
- Privacy by design



Opinion of the CNIL

Order of Preference

- Zero-Knowledge Proof
- Hashes with secret key (peppered hashes)
- Encryption
- Hashes without additional secret key
- Clear text

Lawfulness of processing (Art. 6)

- Consent (Art. 6.1 a)
- Performance of a contract (Art. 6.1 b)
- Compliance with a legal obligation (Art. 6.1 c)
- Legitimate interest (Art. 6.1 f)

Controllers, Processors, Data-Subjects

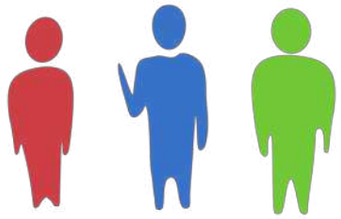
Joint- Controller

Determines the purposes and means of processing

Processor

Processes data on behalf of the controller

Data-Subjects



Who is “Controller” and who is “Processor”?

- Node operators?
- Miner who mines a specific block?
- All miners together?
- User who signs a transaction with her private key?
- Exchange or wallet service that signs a transaction on behalf of a user?
- Entity that administrates permissions for a permissioned blockchain?

Opinion of the CNIL on Controllers and Processors

- User of a public blockchain is a controller
- Somebody who creates and controls a permissioned blockchain is a controller
- Members of a consortium can be joint controllers
- Smart contract developers that publish their contract on a blockchain can be processors
- Node operators are processors

Duties of Controllers and Processors

- Controllers must identify themselves
- Controllers are responsible towards data subjects
- Controllers must have processing agreements with processors
- Controllers must control processors
- Processors must process data only on documented instructions from the controller

Five Ways to Cope with GDPR

- Do not put any personal data (at all) on a blockchain
- Use Privacy Enhancing Technology and ensure that no personal data can be derived from the blockchain
- Obtain a justification that is permanent
- Let users put the data on a public blockchain themselves
- Build specialized blockchains that forget

Blockchain

GDPR Quick Check

beta test V0.2

https://erbguth.ch/QuickCheck

Conclusion

- Blockchain and GDPR both pursue privacy
- GDPR is not technology-neutral
- The use of blockchain can be GDPR-compliant
- Data protection authorities see the privacy benefits of blockchains
- Legal certainty is still missing

Thank you for your attention!

Questions?