UiO : Department of Private Law
University of Oslo

The Role of Anonymisation and Pseudonymisation under the EU Data Privacy Rules

Samson Esayas, researcher

NRCCL

Agenda

- **Personal data**
- **Roles under the EU Data Privacy**
  - As an exemption from the application of DP rules in entirely
  - As an exemption from notification of personal data breaches
  - As integral part of compliance
    - Data security
- **Concluding remarks**

Con.

- **EU Data Privacy rules SHALL apply to**
  - Processing of personal data
- **Personal data**
  - *any information relating to an identified or identifiable natural person* (Art. 2(e))
- **Four main elements**
  - Any information
  - Relating to
  - Identified or identifiable
  - Natural person

Personal data vs. A&Ps data

- **Data Privacy rules DO NOT apply if**
  - Data cannot be considered to relate to an individual, or
  - The individual cannot be considered to be identified or identifiable
- **Anonymisation**
  - A process of manipulating (conceal or delete or aggregate) identifying information to make it difficult or impossible to identify data subjects (Ohm, 2009)
- **Pseudonymisation**
  - Replacing names or other direct identifiers with codes or numbers
- **Role depends on outcome**
  - Irreversibly prevent identification
  - Prevent identification with a possibility to re-identify

UiO : Department of Private Law
University of Oslo

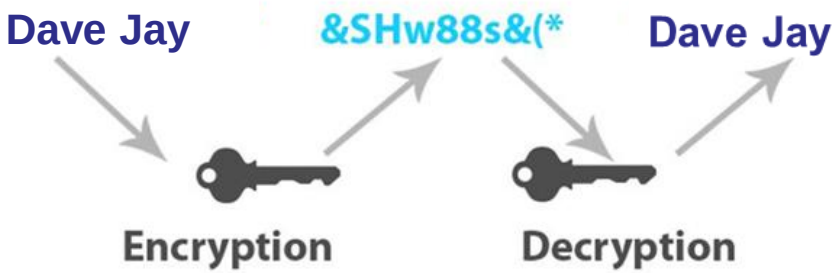
Anonymisation and Pseudonymisation as an Exemption from the Entire Application of Data Privacy Rules

Personal data vs. anonymous data

- **Privacy rules SHALL NOT apply to**
  - *data rendered anonymous in such a way that the data subject is no longer identifiable (Recital 26 DPD)*
- **Identifability is assessed taking into account**
  - *all the means likely reasonably* to be used either by the controller or by any other person to identify the said person
- **Factors**
  - 'All means' – technology, other information, expertise
  - 'Likely' - 'probability' of identification
  - 'Reasonably' - 'difficulty' in identification
  - 'To be used either by the controller or by any other person'
- **Different techniques different outcomes**

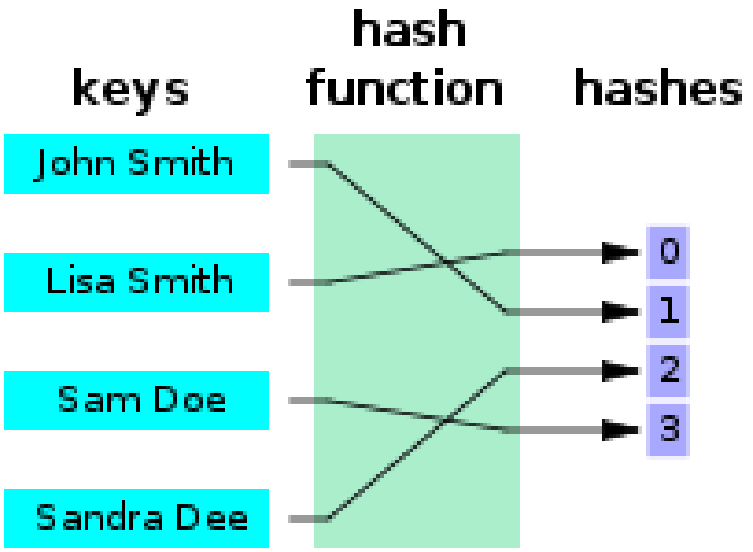
Pseudonymisation:

Encryption



- &SHw88s&(* suffers from heart attack

Hasing



- 3 earns $100K

Pseudonymisation as an exemption?

- **Two-way vs. one-way pseudonymised**
- **Two-way: No exemption**
  - Identifiability remains intact
    - Unique attribute (the pseudonymised attribute)
    - Key
      - trusted third party?
- **One-way:???**
  - WP136
  - WP216
    - Combination with other techniques

Anonymisation (WP216)

- **Generalization and randomization techniques**
- **Provides safe harbor if sufficiently robust**
  - Individual no longer identifiable
    - is it still possible to single out an individual?
    - is it still possible to link records relating to an individual?
    - can information be inferred concerning an individual?
  - No identifiable data in the hands of controller or any third party
- **Reasonably impossible**
- **A29WP**
  - *the outcome of such kind of anonymisation should be, in the current state of technology, as permanent as erasure*

Challenges with the A29WP Opinion

- **Highly complex and very subjective**
- **As 'permanent erasure'**
  - Zero risk approach?
  - Utility vs. privacy
- **Information in the hands of any third party**
  - Difficulty in determining
    - What 'other information' is available
    - Who it is available to and
    - How about individual knowledge?
  - There is always some piece of information that could be combined (Ohm 2009)

UiO : Department of Private Law
University of Oslo

Anonymisation and Pseudonymisation as an Exemption from Breach Notification Obligations

Moving from the ‘all or nothing’ approach

- **Personal data breach notification**
  - ePrivacy Directive
  - Regulation 611/2013
  - eIDAS Regulation
  - Draft GDPR

- **Notification to**
  - Regulatory authorities
  - Data subjects or subscribers

Regulation 611/2013

- **Personal data breach**
  - Confidentiality breach
  - Integrity breach
  - Availability breach
- **Notification to regulatory authorities**
  - *No later than 24 hours after the detection of the personal data breach*
- **Notification to a subscriber or individual**
  - *likely to adversely affect the personal data or privacy*
  - *without undue delay*

Exemption from notification

- **Rationales for exemption**
  - Reduce notification fatigue
  - Encourage their use
- **Approaches to exemptions**
  - Automatic safe harbor
  - Rebuttable presumption
  - Factor-based analysis

Exemption under Regulation 611/2013

- **Notification to subscriber or individual NOT needed if**
  - *demonstrated to* the satisfaction of the competent national authority
  - the data affected by the breach was *unintelligible (Article 4(1))*
- **A data is considered to be unintelligible where**
  - encrypted or hashed with a standardized algorithm
  - the key has not been compromised in any security breach
  - it has been demonstrated that the key cannot be ascertained by available technological means by unauthorized person
- **Regulation 611/2013 approach**
  - Exemption only from notification of individuals
  - Factor-based analysis
  - No exemption from 'availability breach'

Anonymisation

- **Not clearly stated**
- **Not necessarily be '*as permanent as erasure*'**

Id	Personal details	Location	Property (P1, P2)
#1	Mr Smith Daddy,	Rome	Luxury house
#2	Ms….	Madrid	Luxury house
#3		London	Business establishment
#4		Paris	
#5		Barcelona	
#6		Milan	
#7		New York	
#8		Berlin	

Serial ID	Location ID	Property
#1	Rome	P1
#2	Madrid	P1
#3	London	P2
#4	Paris	P1
#5	Barcelona	P1
#6	Milan	P2
#7	New York	P2
#8	Berlin	P1

Lack of consistent approach?

- **eIDAS Regulation - departure from Regulation 611/2013**
  - No provision for a safe harbor
- **Draft GDPR**
  - Initial Commission draft similar to 611/2013 but general approach
- **Significant deviation under the Council draft**
  - Risk-based approach to notification of regulatory authorities
  - Pseudonymisation and encryption safe harbor from notification of regulatory authorities
  - Uses an automatic safe harbor as opposed to factor-based analysis

Summary points

- **As an exemption from the application of Data Privacy rules in entirety**
  - **Pseudonymisation**
    - Two-way pseudonymised data – NO
    - One-way pseudonymised data – MAY BE
  - **Anonymisation**
    - Irreversibly prevent identification – as permanent erasure
    - A29WP – not possible to achieve such in an open dataset era
- **As an exemption from data breach notifications**
  - **Anonymisation**
    - Mostly, even without resulting in ‘as permanent as erasure’
  - **Pseudonymisation**
    - Possibly if fulfill certain technical and organizational measures

Thank you!!