UKAN
UK ANONYMISATION NETWORK

Anonymisation Decision-making Framework

Brussels Privacy Symposium 8th November 2016
Elaine Mackey

The Anonymisation Decision-making Framework

Authors: Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor

The book can be downloaded free at http://ukanon.net/ukan-resources/ukan-decision-making-framework/

UKAN
UK ANONYMISATION NETWORK

The UK Anonymisation Network

About UKAN

UKAN
UK ANONYMISATION NETWORK

- The UK Anonymisation Network (UKAN) was set up in 2012
- It was set up as a means of establishing best practice in anonymisation
- It offers practical advice and information to anyone who handles personal data and needs to share it

UKAN
UK ANONYMISATION
NETWORK

The Anonymisation Decision-making Framework

Anonymisation Decision-making Framework

UKAN
UK ANONYMISATION NETWORK

ADF - A framework for undertaking well thought out anonymisation

- ❑ It unifies the technical, legal, social and ethical aspects of anonymisation to provide a comprehensive guide to doing anonymisation in practice
- ❑ It can facilitate data protection/privacy by design (a feature of the GDPR)

Principles underpinning ADF

1. You cannot decide whether data are safe to share or not by examining the data alone

   Key concept: data situation approach

   Key concept: functional anonymisation

2. But you still need to examine the data

3. Anonymisation is a process to produce safe data but it only makes sense if what you are producing is safe **useful** data

Principles underpinning ADF

UKAN
UK ANONYMISATION NETWORK

4. Zero risk is not a realistic possibility, if you are to produce useful data

The risk of re-identification should be remote

5. The measures, which you put in place to manage re-identification risk, should be proportional to the risk and its likely impact

10 components of the ADF

UKAN
UK ANONYMISATION NETWORK

1. Describe your (intended) data situation
2. Understand your legal responsibilities
3. Know your data
4. Understand the use case
5. Meet your ethical obligations
6. Identify the processes you will need to go through to assess disclosure risk
7. Identify the disclosure control processes that are relevant to your data situation
8. Identify your stakeholders and plan how you will communicate with them
9. Plan what happens next, once you have shared or released the data
10. Plan what you will do if things go wrong

Anonymisation activities

- *A data situation audit:* identifying those issues relevant to your proposed data share or release (covered by components 1-5)
- *Risk analysis and control:* the technical processes needed to assess and manage the disclosure risk associated with your data situation (covered by components 6-7)
- *Impact management:* measures to manage the (expected or potential) consequences of your share (covered by components 8-10)

1. Describe your (intended) data situation

- □ What is a data situation - the concept captures the idea of a relationship between some data and their environment
- □ How do you define your data situation - map the data flow, from the point at which it is collected to the point after which it is shared
- □ Data shares are dynamic data situation where data is moved from one environment to another

2. Understand your legal responsibilities

The movement of data across multiple environments can complicate the question of who is responsible for it.

We address the question of whether you are a data controller, processor or user by considering:

- The status of the data in each environment
- The provenance of the data
- The enabling conditions for the share
- The mechanism for the share e.g. data share agreement, license

3. Know your data

UKAN
UK ANONYMISATION NETWORK

A top level assessment of your data requires consideration of:

- ❑ **Data type:** statistics or text; level of information e.g. microdata or aggregated?
- ❑ **Variable types:** direct and indirect identifiers; variable sensitivity
- ❑ **Dataset properties:** its age, quality, file structure, population or sample data etc.

4. Understand the use case

Establishing your use case by:

- ❑ Why: Clarifying your reason for sharing or releasing your data
- ❑ Who: Identifying the user groups who may wish to access your data
- ❑ How: Establishing how those accessing your data might want to use it

5. Meet your ethical obligations

Why talk about ethics?

- We are not dealing with zero risk
- Data subjects might not want data about them being re-used in general, by specific third parties or for particular purposes

What can you do?

- Where possible seek consent for data reuse
- Be transparent and where practical engage with your stakeholders
- Good governance is vital

6. Identify the processes you will need to go through to assess disclosure risk

UKAN
UK ANONYMISATION NETWORK

Four-part process for assessing disclosure risk

1. Incorporation of your top level assessment
2. An analysis to establish relevant, plausible scenarios for your data situation.
3. Data analytical approaches - to estimate risk given the scenarios that you have developed under procedure 2
4. Penetration testing, which involves validating assumptions made in procedure 2, by simulating attacks using 'friendly' intruders

7. Identify the disclosure control processes that are relevant to your data situation

Depending on your risk analysis in component 6 you have two (non-exclusive) choices to:

- ❑ Change the data (specification)
- ❑ Reconfigure the data environment

This is functional anonymisation in practice

8. Identify your stakeholders and plan how you will communicate with them

UKAN
UK ANONYMISATION NETWORK

Who needs to know about the share?

- Data subjects?
- The wider public?
- Users?
- Specialist interest groups?

What do they need to know?

- This is likely to be different for different stakeholders

9. Plan what happens next once you have shared or released the data

UKAN
UK ANONYMISATION NETWORK

Don’t release and forget

- ❑ Keeping a register of all the data you have shared
- ❑ Compare proposed share activities to past shares, to take account of the possibility of linkage between releases leading to a disclosure
- ❑ Be aware of changes in the data environment and how these may impact on your data

10. Plan what you will do if things go wrong

You can, for example:

- ❑ Ensure you have a clear, robust audit trail
- ❑ Ensure you have a crisis management policy which addresses:
  - *Managing the situation*
  - *Communicating the situation*
- ❑ Ensure you have adequately trained staff
- ❑ Ensure you undertake a review of your processing activities to prevent a reoccurrence

A periodic review is good practice - not just when a problem arises

ADF facilitates data protection and privacy by design

The framework is a mechanism for:

- Undertaking a proactive approach to doing anonymisation
- Ensuring privacy is the default setting
- Embedding privacy into the data situation
- Seeking to achieve optimal data safety and data utility
- Ensuring full lifecycle protection through the data situation approach
- Promoting transparency and stakeholder engagement
- Promoting respect for user privacy by encouraging examination of ethical as well as legal considerations in data protection

Based on Cavoukian Privacy by Design 7 Foundational Principles, 2011. Please see https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Thank you!

Disclaimer

UKAN
UK ANONYMISATION NETWORK

- Texts, marks, logos, names, graphics, images, photographs, illustrations, artwork, audio clips, video clips, and software copyrighted by their respective owners are used on these slides for non-commercial, educational and personal purposes only. Use of any copyrighted material is not authorized without the written consent of the copyright holder. Every effort has been made to respect the copyrights of other parties. If you believe that your copyright has been misused, please direct your correspondence to: elaine.mackey@manchester.ac.uk stating your position and I shall endeavour to correct any misuse as early as possible.