MANCHESTER 1824
The University of Manchester

# Privacy in Web Applications

Mustafa A. Mustafa
Research Fellow in Computer Science

MANCHESTER 1824
The University of Manchester

# OWASP top 10 security risks


Credits: neoscopeit.com

MANCHESTER 1824
The University of Manchester

# OWASP top 10 security risks


Credits: neoscopeit.com

MANCHESTER 1824
The University of Manchester

# Sensitive data exposure

Examples of sensitive data

- Banking information: account numbers, credit card numbers
- Health information
- Personal information: social security number, date of birth, address, …
- User account/passwords


Credits: creativebloq.com

MANCHESTER 1824
The University of Manchester

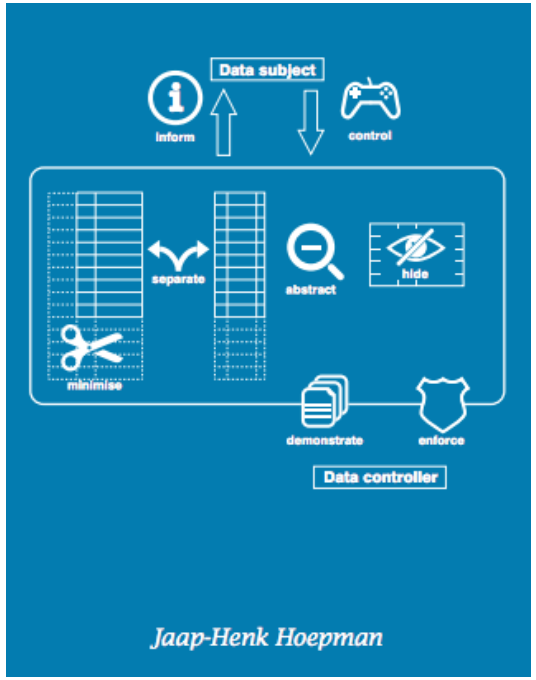
# GDPR

What is the General Data Protection Regulation (GDPR)?


Credits: snel.com

# Privacy design strategies

- There are many available strategies / guidelines
- Hoepman's eight privacy design strategies

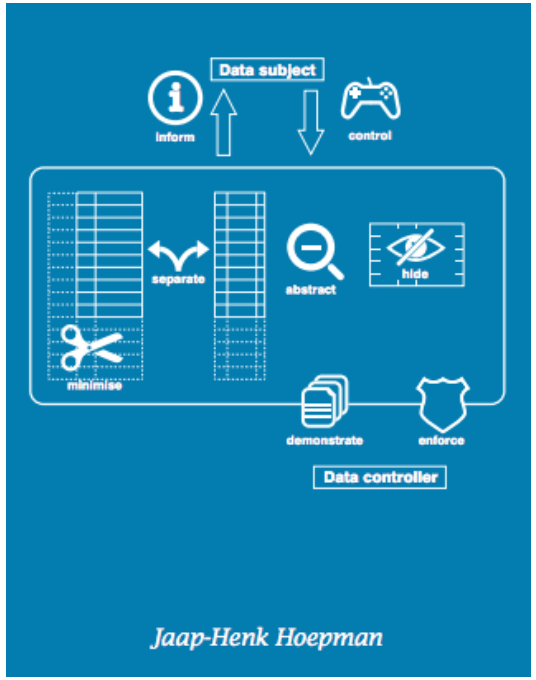



Privacy Design Strategies (The Little Blue Book) by Hoepman, 2020
https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

MANCHESTER 1824
The University of Manchester

# Privacy design strategies

- There are many available strategies / guidelines
- Hoepman's eight privacy design strategies
  1. Minimise
  2. Separate
  3. Abstract
  4. Hide
  5. Inform
  6. Control
  7. Enforce
  8. Demonstrate

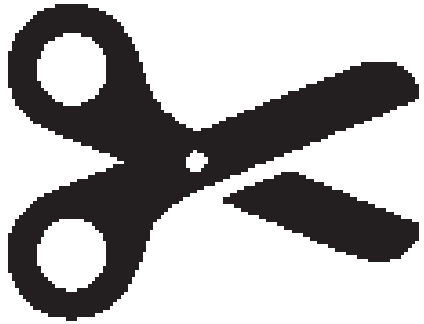



Privacy Design Strategies (The Little Blue Book) by Hoepman, 2020
https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

MANCHESTER 1824
The University of Manchester

# 1. Minimise

- Limit as much as possible the processing of personal data.
- Nothing can go wrong with data you do not collect; they cannot be abused, misused, or get leaked accidentally



- Tactics:
  - Select
  - Exclude
  - Strip
  - Destroy

MANCHESTER 1824
The University of Manchester

# 2. Separate

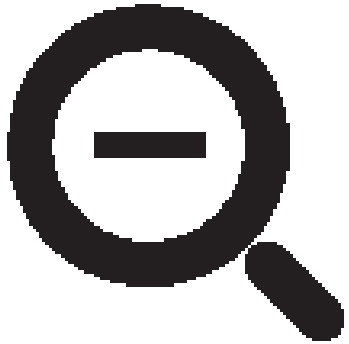
- (Logically or physically) separate the processing of personal data as much as possible.
- This makes it harder to combine or correlate data.

- Tactics:
  - Isolate
  - Distribute

MANCHESTER 1824
The University of Manchester

# 3. Abstract

- Limit as much as possible the detail in which personal data is processed.
- The less detailed a personal data item is, the lower the privacy risk is.

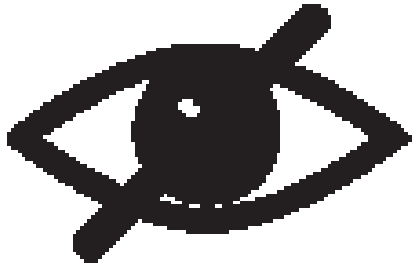


- Tactics:
  - Summarise
  - Group
  - Perturb

MANCHESTER 1824
The University of Manchester

# 4. Hide

- Protect personal data, or make it unlinkable or unobservable.
- Make sure it does not become public or known.



- Tactics:
  - Restrict
  - Obfuscate
  - Dissociate
  - Mix

MANCHESTER 1824
The University of Manchester

# 5. Inform

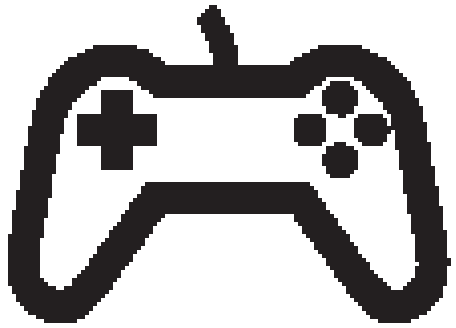
- Inform users about the processing of their personal data in a timely and adequate manner.
- Transparency about which personal data is being processed, how they are processed and for which purpose, is an essential for better privacy protection.

- Tactics:
  - Supply
  - Explain
  - Notify

MANCHESTER 1824
The University of Manchester

# 6. Control

- Provide users adequate control over the processing of their personal data.
- Users want to have control and have a say in how their personal data is processed and shared.

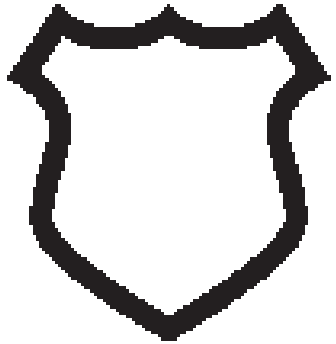


- Tactics:
  - Consent
  - Choose
  - Update
  - Retract

MANCHESTER 1824
The University of Manchester

# 7. Enforce

- Commit to processing personal data in a privacy-friendly way, and adequately enforce this.
- Privacy should be part of the organisational culture and be propagated by higher management.



- Tactics:
  - Create
  - Maintain
  - Uphold

# 8. Demonstrate

- Demonstrate you are processing personal data in a privacy-friendly way
- This strategy addresses the new requirement that organisations need to demonstrate compliance to privacy regulations.

- Tactics:
  - Record
  - Audit
  - Report

MANCHESTER 1824
The University of Manchester

# Thank you!

Mustafa A. Mustafa
mustafa.mustafa@manchester.ac.uk