GDPR in DevOps

FOR DUMMIES®

GDPR explained and translated into usable requirements

DevOps Days Amsterdam 2017

Edward van Deursen

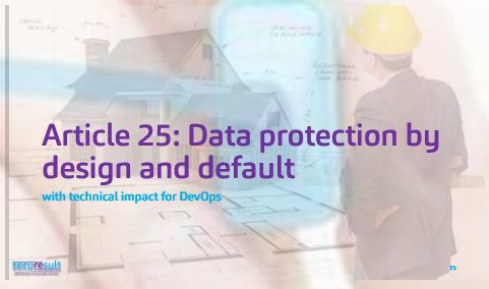
securesult
Cybersecurity, Privacy & Data Protection

OVERVIEW


General
Data
Protection
Regulation
GDRP
What's in it for you?

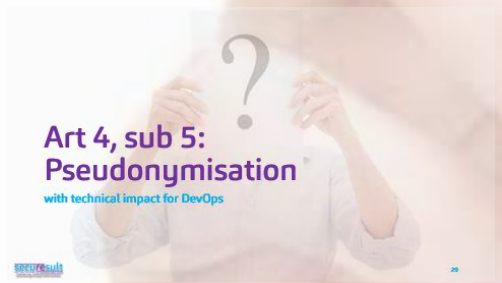

Privacy vs Security
The relation and difference


RELEVANT
The most relevant articles of GDPR
with technical impact for DevOps


Article 25: Data protection by design and default
with technical impact for DevOps


RIGHT TO BE FORGOTTEN
Delete
Art 17: Right to erasure ('right to be forgotten')
with technical impact for DevOps

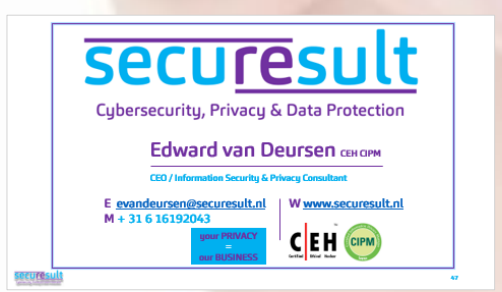

Art 4, sub 4: Profiling
with technical impact for DevOps


Art 4, sub 5: Pseudonymisation
with technical impact for DevOps


PASSWORD PROTECT
HACKING DETECTED
Art 32: Security of processing
As a privacy principle


IN CASE YOU
MISSED IT


PANIC
Reference materials
Don't PANIC, useful links for DevOps on the next slides


securesult
Cybersecurity, Privacy & Data Protection
Edward van Deursen CEH CIPM
CEO / Information Security & Privacy Consultant
E evandeursen@securesult.nl
M + 31 6 16192043
W www.securesult.nl
your PRIVACY = our BUSINESS
CEH
CIPM

GDRP

What's in it for you?

General Data Protection Regulation

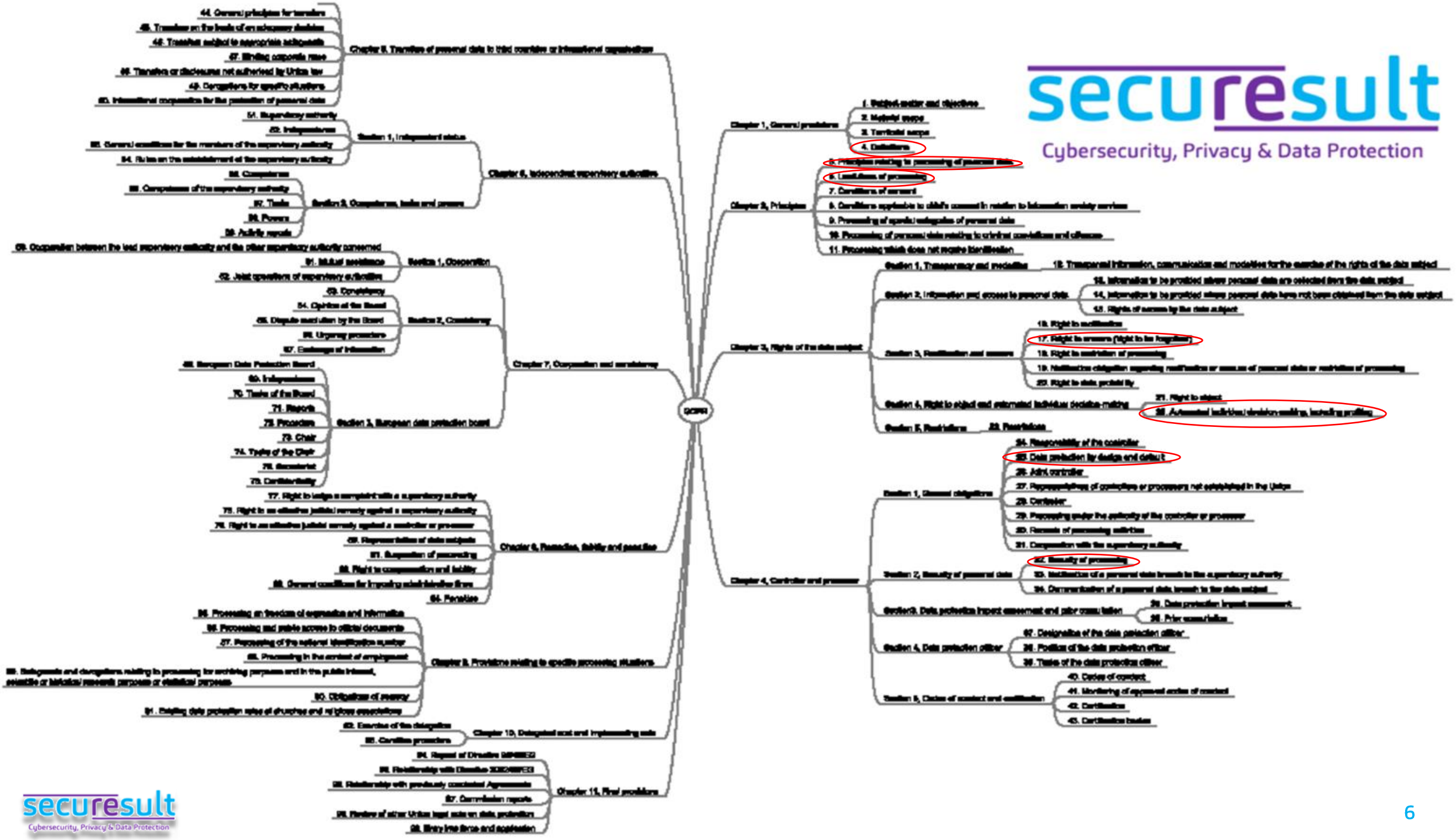
securesult
Cybersecurity, Privacy & Data Protection

D-Day for GDPR is 25 May 2018

securesult
Cybersecurity, Privacy & Data Protection

GDPR: What is it?

- General Data Protection Regulation
  - For all citizens of EU
  - Replacing Directive 95/46/EC (not a law)
  - To harmonize privacy laws in EU
  - Update laws to new technologies, like
    - Mobile devices
    - Profiling
  - Possibility of certification
  - 99 articles about rights and obligations of which
    - > 50% is about Privacy Authorities and their cooperation
    - a few have technical impact

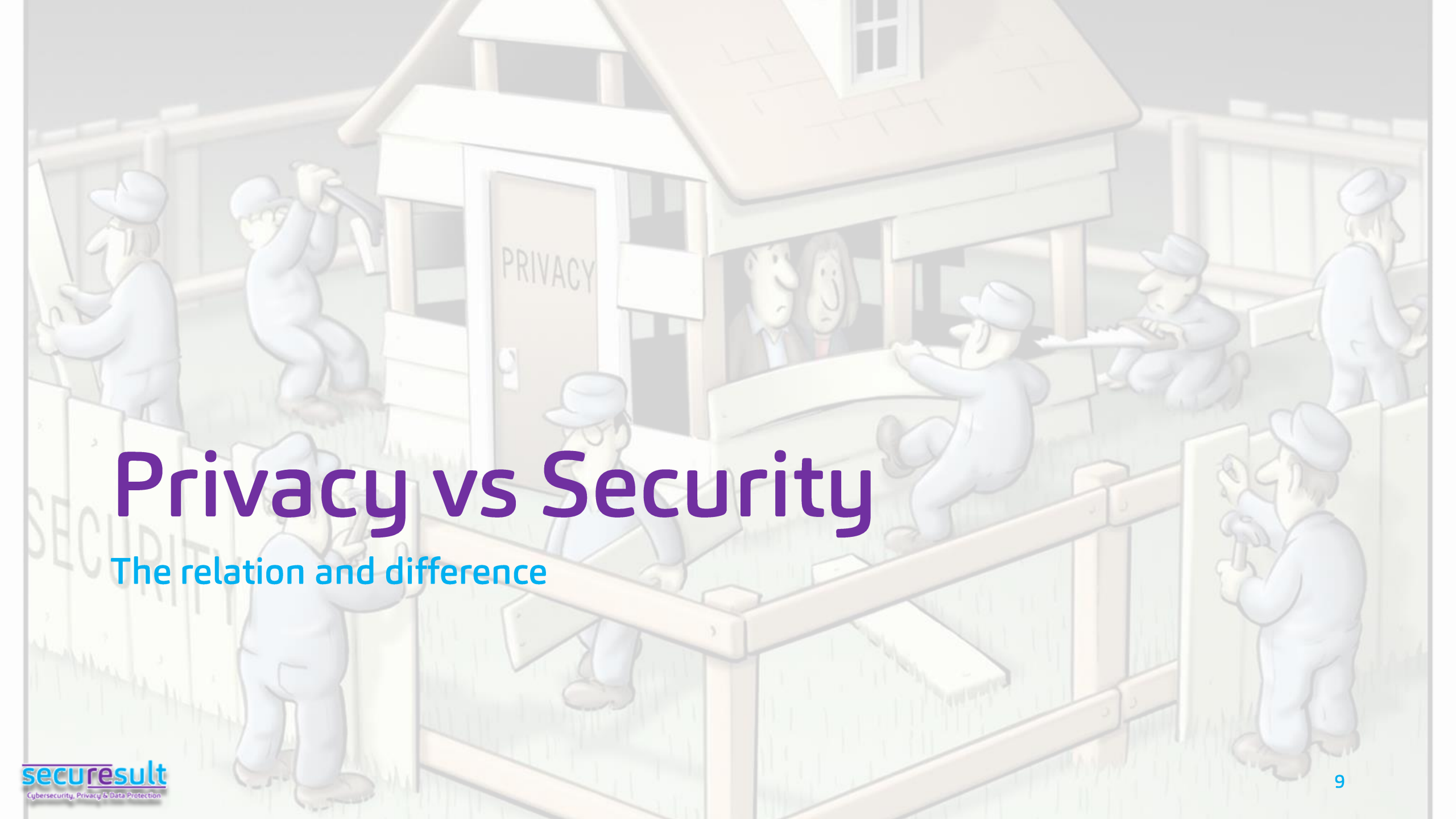



IMPORTANT
VERY IMPORTANT

GDPR in DevOps for Dummies

If you don't have personal information,
you can't lose or leak it!

If you process personal data,
guard it with your life!



Privacy vs Security

The relation and difference

Privacy vs Security

1. **Any information…**
2. **Relating to an…**
   - Content,
   - Purpose or
   - Result
3. **Identified or identifiable…**
   - Direct or indirect
   - Taking into account all means reasonably likely to be used by the controller or any other party
4. **Natural person**

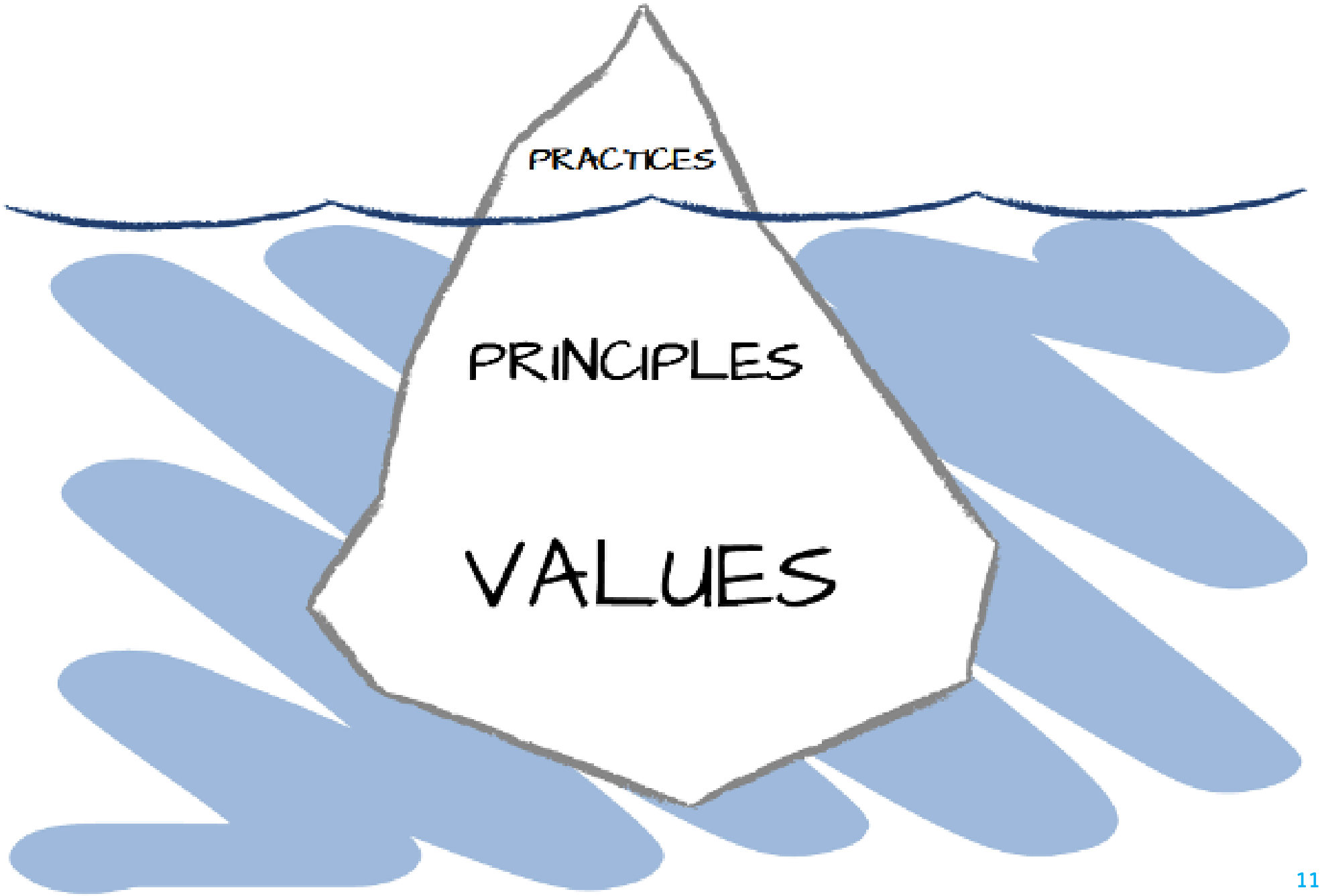
Personal Data

The rest

Non-Personal Data

Special categories of Personal Data

- Personal data revealing
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade union membership
- Genetic and biometric data
- Data concerning
  - Health
  - Sex life
  - Sexual orientation
- Data related to
  - Criminal convictions
  - Criminal offences
  - Related security measures


PRACTICES
PRINCIPLES
VALUES

Privacy vs Security

Privacy principles

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability
- Lawfulness, fairness and transparency
- Proportionality

Personal Data

The rest

"You can have security without privacy…
But you can't have privacy without security."

Non-Personal Data

Special categories of Personal Data

- Personal data revealing
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade union membership
- Genetic and biometric data
- Data concerning
  - Health
  - Sex life
  - Sexual orientation
- Data related to
  - Criminal convictions
  - Criminal offences
  - Related security measures

The most relevant articles of GDPR

with technical impact for DevOps

GDPR for DevOps
The most relevant articles

Articles:

4 Definitions
- Sub 4 Profiling
- Sub 5 Pseudonymisation

5 Principles relating to processing of personal data

6 Lawfulness of processing

17 Right to erasure ('Right to be forgotten')

22 Automated individual decision-making, including profiling

25 Privacy by design and default

32 Security of processing

Article 25: Data protection by design and default

with technical impact for DevOps

securesult
Cybersecurity, Privacy & Data Protection

Art 25: Data protection by design and by default

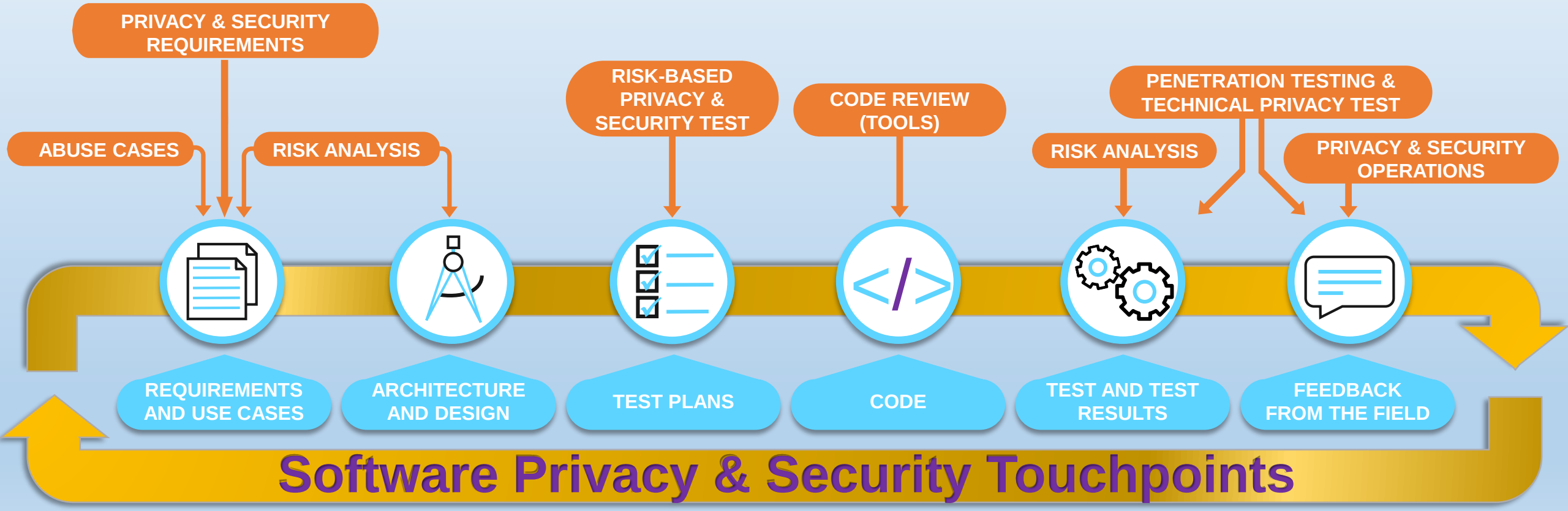
1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Art 25: Data protection by design and by default

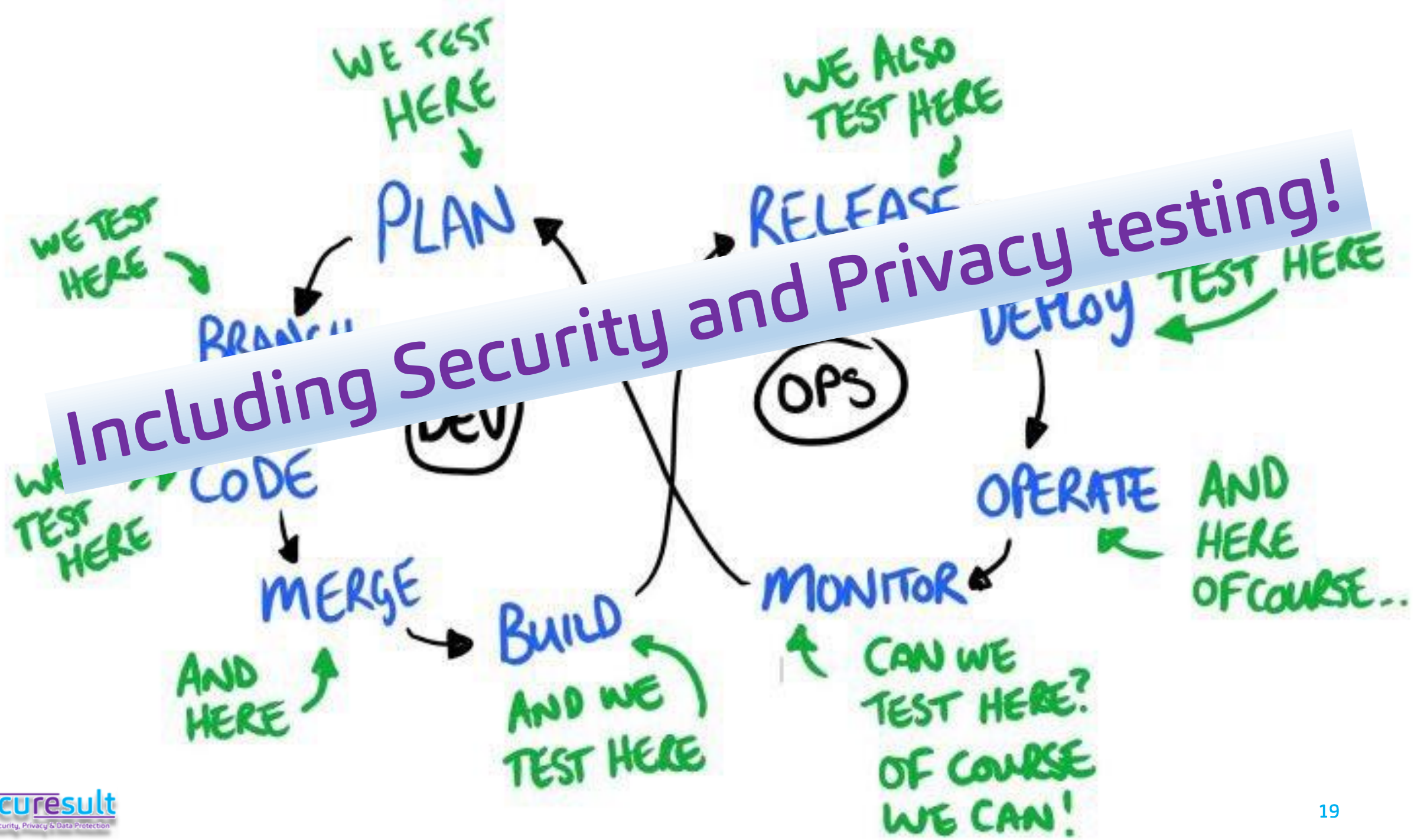
1. Taking into account the state of the a
   context and purposes of processing a
   rights and freedoms of natural perso
   time of the determination of the mea
   implement appropriate technical and
   which are designed to implement da
   effective manner and to integrate th
   the requirements of this Regulation
2. The controller shall implement appr
   that, by default, only personal data
   processing are processed. That oblig
   extent of their processing, the period
   measures shall ensure that by defau
   individual's intervention to an indefi
3. An approved certification mechanism
   demonstrate compliance with the re

- Taking into account
  - The state of the art
  - The cost of implementation
  - The nature, scope, context and purposes of processing
  - Risks of varying likelihood and severity
- Implement appropriate technical and organisational measures
  - such as: Pseudonymisation
- Data-protection principles
  - Such as: data minimisation
- Integrate the necessary safeguards

Privacy-by-Design / Security-by-Design
Shift left in software development



securesult
Cybersecurity, Privacy & Data Protection



Including Security and Privacy testing!

Examples for Definition of Done: Data protection by design and by default

- For every epic or user story the impact on privacy is judged by the DPO.
- A Technical Privacy Analysis is executed based on the changes that go to production. (Meaning: privacy impact must be defined during refinement of requirements)
- A(n automated) security test is successfully executed and has no defects of categories ‘Critical’ and ‘High’.

Art 17: Right to erasure ('right to be forgotten')

with technical impact for DevOps

Art 17: Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) (the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). ;

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Art 17: Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the contr
shall have the obligation to erase personal data without und

(a) the personal data are no longer necessary in relation to the

(b) the data subject withdraws consent on which the processing
other legal ground for the processing;

(c) (the data subject objects to the processing pursuant to Artic
objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a l

(f) the personal data have been collected in relation to the offe

2. Where the controller has made the personal data public and
available technology and the cost of implementation, shall
personal data that the data subject has requested the erasu

3. Paragraphs 1 and 2 shall not apply to the extent that proces

(a) for exercising the right of freedom of expression and inform

(b) for compliance with a legal obligation which requires proce
task carried out in the public interest or in the exercise of of

(c) for reasons of public interest in the area of public health in a

(d) for archiving purposes in the public interest, scientific or his
right referred to in paragraph 1 is likely to render impossibl

(e) for the establishment, exercise or defence of legal claims.

- Right of removal of his/her personal data without undue delay when
  - Personal data is not longer needed for original purpose
  - Data subject withdraws the consent (permission)
  - The data subject objects processing his/her data
  - Personal data has been unlawfully processed

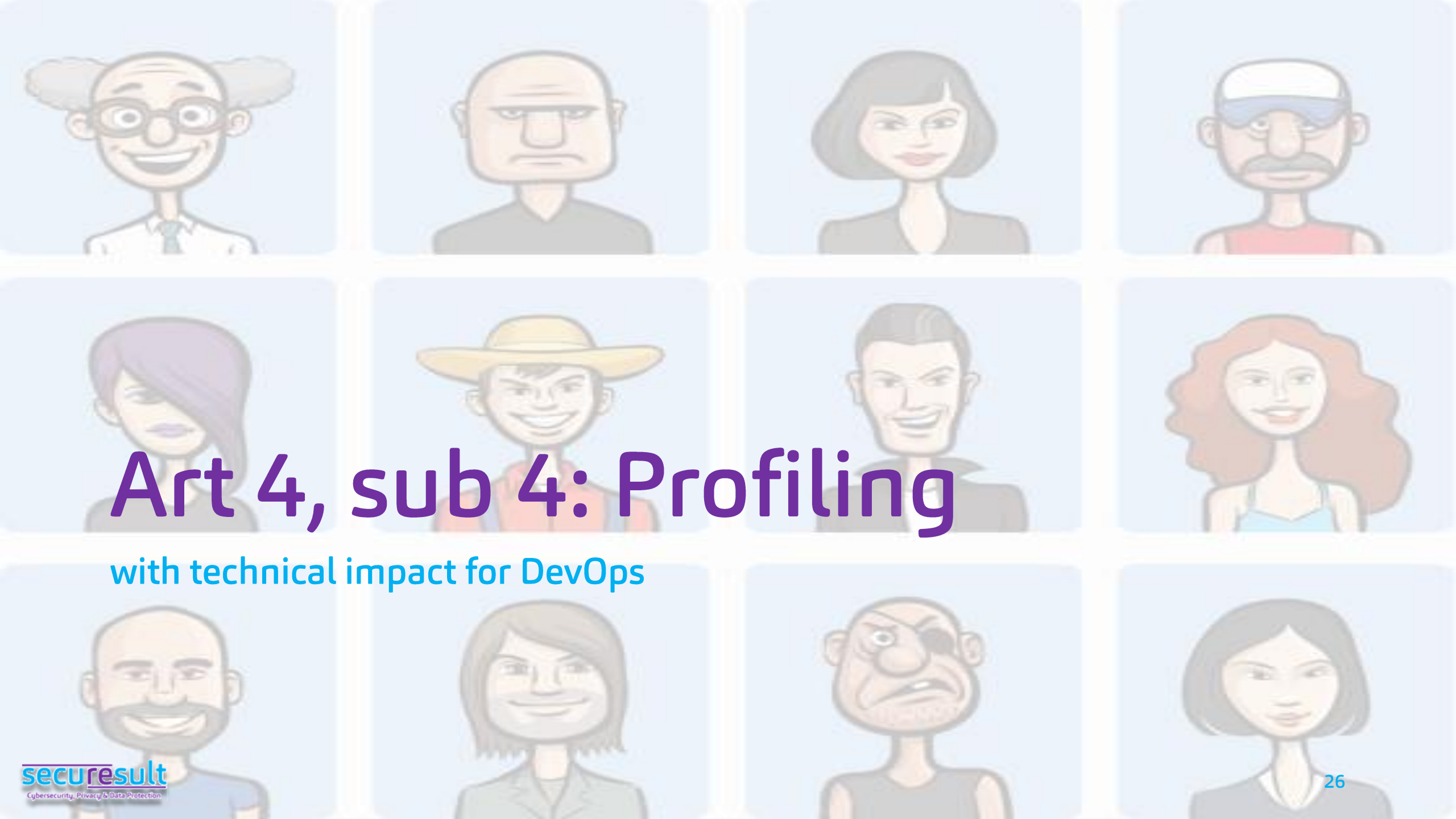
securesult
Cybersecurity, Privacy & Data Protection

Requirements based on Art 17 Right to be Forgotten

- Delete all personal data of a person on request of that person, including:
  - Entries in logfiles
  - Entries in Backups
  - In any form duplicated personal data, like
    - E-mails
    - Documents, spreadsheets, presentations
    - Data handed over to processing party
- Option: Anonymise in case of
  - Historical research
  - Trend analyses

Example User Stories based on Art 17 Right to be Forgotten

- As a data subject (customer/patient/…) I want all my personal data to be permanently removed from the systems when the data isn't used for the predefined purpose, so I'm sure that my personal data is not misused.
- As a Data Protection Officer (DPO) I want all the personal data to be permanently removed from our systems and the systems of our data processing party's and all other duplicates of that personal data when the data isn't used for the predefined purpose, so that we comply to the GDPR.
- As an app user I want all my personal data be permanently removed from my device when the app is removed, so that I'm sure that my personal data can't be misused.



Art 4, sub 4: Profiling

with technical impact for DevOps

securesult
Cybersecurity, Privacy & Data Protection

Art 4, sub 4: Profiling

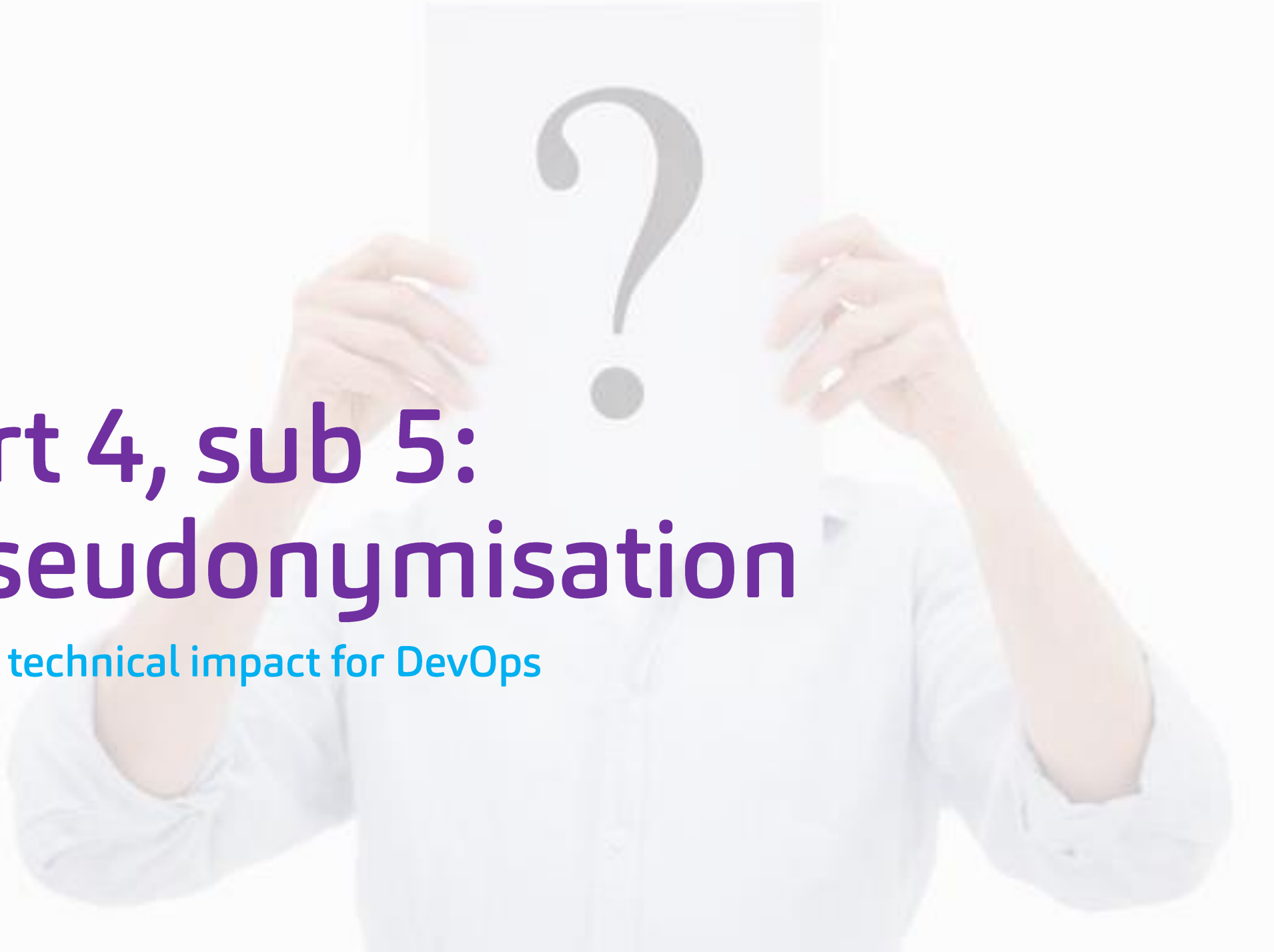
‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Art 4, sub 4: Profiling

'profiling' means any form
data consisting of the use
personal aspects relating t
analyse or predict aspects
performance at work, econ
preferences, interests, relia
movements;

- Automated processing of
- Personal data
- to analyse or predict aspects
  - Performance at work
  - Economic situation
  - Health
  - Personal preferences
  - Interests
  - Reliability
  - Behaviour
  - Location
  - Movements

securesult
Cybersecurity, Privacy & Data Protection



Art 4, sub 5: Pseudonymisation

with technical impact for DevOps

Art 4, sub 5: Pseudonymisation

‘pseudonymisation’ 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;

Art 4, sub 5: Pseudonymisation

'pseudonymisation' means
such a manner that the per
to a specific data subject w
information, provided that
separately and is subject to
measures to ensure that th
an identified or identifiable natural person;

- The personal data
  - can no longer be attributed to a specific data subject without the use of additional information
  - are not attributed to an identified or identifiable natural person

Example User Stories based on Art 4, sub 5 Pseudonymisation

- As a BI analyst I want all personal data which is collected from all our systems for analysing purposes to be pseudonymised, so that we are able to use the valuable, non-personal information.
- As a DPO I want all personal data for scientific research to be pseudonymised, so that we comply to the GDPR.

Art 32: Security of processing

As a privacy principle

Art 32: Security of processing

1. 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.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

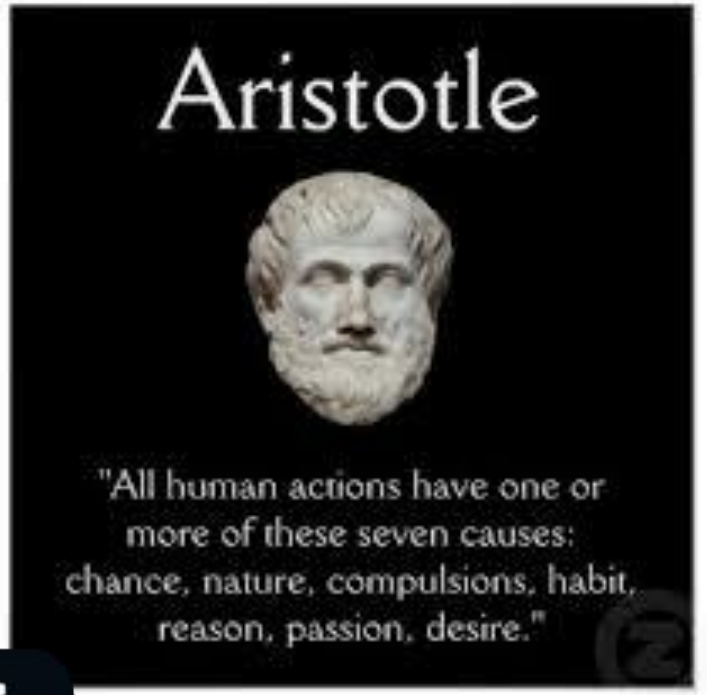
3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Art 32: Security of processing

1. T
   - Pseudonymisation
   - Encryption of personal data
   - Processing systems and services: ensure the ongoing
     - (a) Confidentiality
     - (b) Integrity
     - (c) Availability
     - (d) Resilience
   - Timely restore availability and access to personal data
   - Regularly testing, assessing and evaluating the effectiveness of security measures
2.
3.
   - Accidental or unlawful
     - Destruction
     - Loss
     - Alteration
     - Unauthorised disclosure
     - Access to personal data transmitted, stored or otherwise processed
4.

Purposes of Logging



SOC

Security Operation Center (SOC)

securesult
Cybersecurity, Privacy & Data Protection

Example User Stories & abuser story for logging

- As a DPO I want the following information to be logged, so that we can proof to the data subject who has or hasn't (non-repudiation) created, seen, changed or deleted personal data:
  - UserID related to one natural person
  - Event
  - Date and time of event
  - Used device/IP address
  - Result of action

Tip:
https://www.owasp.org/index.php/Logging_Cheat_Sheet

- As a DPO I want the personal data in logfiles to be encrypted, so that a hacker can't extract personal data from logfiles.
- As a hacker I want to change the logfiles, so that no one can trace my criminal act. (Abuser story, meaning: protect logfiles!)

IN CASE YOU MISSED IT

Let's Recap

- Classification
  - Personal data
  - Special categories of personal data (extra protection needed)
  - Non-Personal data
- Encryption of personal data in rest, transmit or process
- Thorough delete personal data and delete permanent
  - On request or no lawful ground to store or process personal data
  - Option: pseudonymisation
- Authorisation matrix (Principles 'least-privilege' and 'need-to-know')
  - Design of who is allowed to see and/or process personal data
- Logging: who, what, when, where…
  - for audit trail and incident investigation
- DON'T use production data in OTA environments!

Real MEN TEST in PRODUCTION

DON'T

TEST in

PRODUCTION

It's illegal!


IMPORTANT
VERY IMPORTANT

GDPR in DevOps for Dummies

If you don't have personal information,
you can't lose or leak it!

If you process personal data,
guard it with your life!

Reference materials

Don’t PANIC, useful links for DevOps on the next slides

GDPR in DevOps for Dummies Background information

- GDPR text downloadable in all EU languages:
  - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
- Privacy measures
  - https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project
- Security measures
  - https://www.owasp.org/index.php/OWASP_Proactive_Controls
  - https://www.owasp.org/index.php/Logging_Cheat_Sheet
- Software, Mobile and Cloud risks and vulnerabilities
  - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
  - https://www.sans.org/top25-software-errors/
  - https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10
  - https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project

No Security Requirements, and what?

- Use some proven application security principles
  - Apply ***defense in depth*** (complete mediation)
  - Use a ***positive security model*** (fail-safe defaults, minimize attack surface)
  - ***Fail securely***
  - Run with ***least privilege***
  - Avoid ***security by obscurity*** (open design)
  - ***Keep security simple*** (verifiable, economy of mechanism)
  - ***Detect intrusions*** (compromise recording)
  - ***Don't trust infrastructure***
  - ***Don't trust services (and users)***
  - Establish ***secure defaults*** (psychological acceptability)

securesult

Cybersecurity, Privacy & Data Protection

Edward van Deursen CEH CIPM

CEO / Information Security & Privacy Consultant

E evandeursen@securesult.nl
M + 31 6 16192043

W www.securesult.nl

your PRIVACY
=
our BUSINESS