Data Protection and Electronic Monitoring

10th CEP Conference on Electronic Monitoring in Europe
(Latvia) Riga, April 20 2016

Bavo Van den Heuvel

CIPP/E – CIPM – CIPT
ISO27001 Lead Auditor
Forensic Computer Auditor
Data Protection Officer
bavo@cranium.be
www.cranium.be
www.dp-institute.eu

About me

Commercial Engineer - University of Antwerp - Belgium 1996

Ca 20 years IT-security, +12 years appointed Data Protection Officer

Data Protection Officer of Flemish Electronic Monitoring (VCET) Belgium

Owner of CRANIUM APPLIED PRIVACY NV: mainly working as Data Protection Officer (DPO): http://www.cranium.be

Also co-founder and trainer at Data Protection Institute where future DPO's from public and private sector are trained to be ready for the General Data Protection Regulation (GDPR): https://www.dp-institute.eu

TOC

1. Introduction to personal data, applied EM
2. Processor, controller, applied EM
3. General Data Protection Regulation:
    1. Security
    2. Data protection by default / by design
    3. Data protection impact assessment
    4. Data breaches, applied EM
4. Organisational measures
5. How to set up the security in order to prevent and detect personal data security breaches

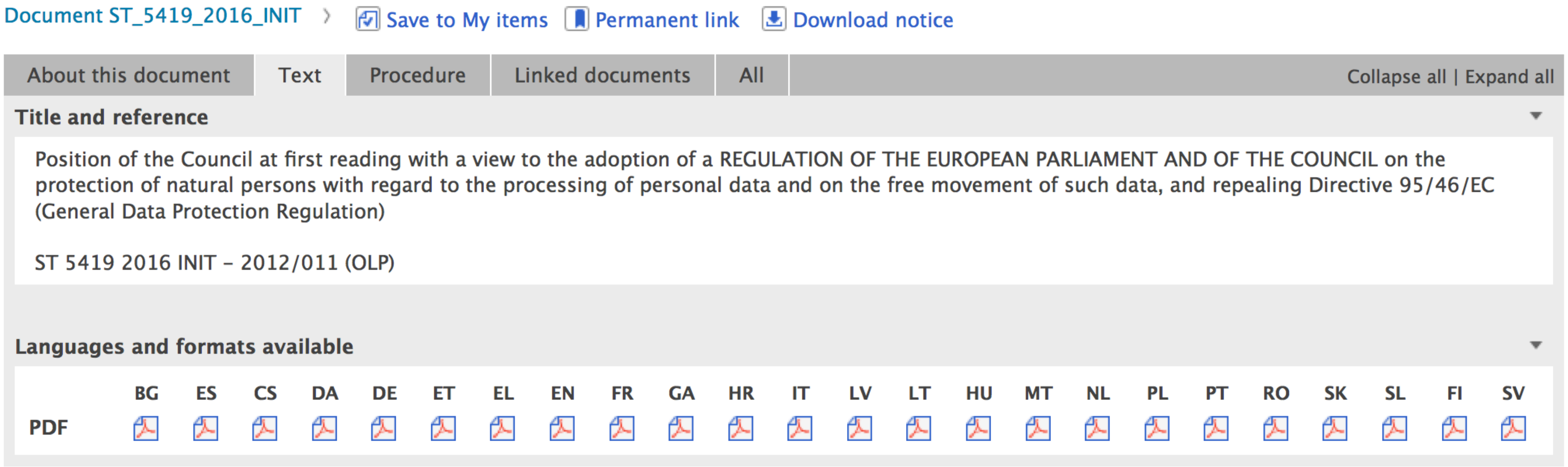
DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

7) (…) Effective protection of personal data throughout the Union requires the strengthening of the rights of data subjects and of the obligations of those who process personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.

Source:
http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1460028379747&uri=CONSIL:ST_5418_2016_INIT

General Data Protection Regulation

- http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_5419_2016_INIT



Title and reference

Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

ST 5419 2016 INIT – 2012/011 (OLP)

Languages and formats available

	BG	ES	CS	DA	DE	ET	EL	EN	FR	GA	HR	IT	LV	LT	HU	MT	NL	PL	PT	RO	SK	SL	FI	SV
PDF	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄	📄

copyrighted material!

GDPR

Article 1 Subject-matter and objectives

- This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

(…)

Directive vs GDPR

Directive

Article 1 Subject-matter and objectives

- This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Article 9 *Specific processing conditions*

- Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, Regulation (EU) 2016/...* (=GDPR) shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.

Definitions, security measures are comparable between Directive and GDPR: please check official texts!

Today we will discuss GDPR

GDPR on personal data

Art 4 definitions:

- 1) 'personal data' means any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

Personal data and EM

Idea: outside the house of the offender only authorised people may know he/she is monitored

- Directly or indirectly
- Identified or identifiable
- Pseudonymisation is not anonimisation
- Sensitive data: visible bracelet
- Central processing, hosting, external processor, companies
- But also: maintenance, interception, proprietary encryption

GDPR Data Controller

- Definition: art 4 (5) 'controller' means the natural or legal person, public authority, agency or any other body **which alone or jointly with others determines the purposes and means of the processing of personal data**; (…);

Article 4 Definitions

- (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

GDPR Processing

GDPR Data Controller

- Article 22: responsibility of the controller:
- 1. Taking into account the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals**, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. These measures shall be reviewed and updated where necessary**. 2. (...)
- 2a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 **shall include the implementation of appropriate data protection policies by the controller.**
- (…)

GDPR Data Processor

Definition: Art 4) (6) '**processor**' means a natural or legal person, public authority, agency or any other body **which processes personal data on behalf of the controller**;

Art 26

- 1. Where a processing is to be carried out on behalf of a controller, the controller shall **use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
- (…)
- 4. **Without prejudice to Articles 77, 79 and 79b, if a processor in breach of this Regulation determines the purposes and means of data processing, the processor shall be considered to be a controller in respect of that processing.**

GDPR Processor Contract

art 26 (…)

- 2) The carrying out of processing by a processor shall be **governed by a contract or other legal act under Union or Member State law**, binding the processor to the controller, **setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller and stipulating in particular that the processor shall**:
- (a) **process the personal data only on** documented instructions **from the controller, including with regard to transfers of personal data to a third country or an international organisation**, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;
- (b) ensure that p**ersons authorised to process the personal data have committed themselves** to confidentiality or are under an appropriate statutory obligation of confidentiality;

GDPR Processor Contract

- art 26 (...)
- (c) **take all measures required pursuant to Article 30**; (*security of processing*)
- (d) respect the conditions referred to in paragraphs 1a and 2a for enlisting **another processor**; (*subcontractors of processor*)
- (e) taking into account the nature of the processing, **assist the controller** by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to **respond to requests for exercising the data subject's rights** laid down in Chapter III;(*new!*))

GDPR Processor Contract

- art 26 (...)
- (f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34 taking into account the nature of processing and the information available to the processor; *(art 30 security of processing, art 31 data breach notification, art 32 data breach communication, art 33 data protection impact assessment, art 34 prior consultation of DPA)*
- (g) at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of data processing services, and delete existing copies unless Union or Member State law requires storage of the data;
- (h) make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The processor shall immediately inform the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions. *(new! In advantage of controller)*

Processor contract and EM public tendering

- Make this contract part of your public tender!
- Your contract template will be used, not the template of the possible supplier
- You can specify the details on each point
- Ask for all details on the required security measures
- ! Take care: international data transferts! Privacy Shield / Safe Harbour, other countries outside EU-28

Art 30 Security

Article 30 Security of processing

1. Having regard to **the state of the art and the costs of implementation** and **taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals,** **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 systems and services processing personal data;
- (c) **the ability to restore the availability and access to 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.

Article 30 Security of processing (…)

1a. In assessing the appropriate level of security **account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed**.

(…)

2b. The **controller and processor** shall take steps to **ensure that any person acting under the authority of the controller or the processor who has access to personal data shall 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 30 Security

Art 4 Definition: (9) 'personal data breach' means **a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;**

Examples in EM context:

- Interception of communications between bracelet - home monitoring device – central monitoring system
- Unauthorised access by monitoring specialists / law enforcement
- Disclosure of data at rest related to EM
- Proprietary encryption algorithms (with backdoors)
- But also: destruction, loss, alteration

Data Breach (Notification)

Data Protection By Design

Art 23 1. Having regard to the state of the art and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals 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 way 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.

Data Protection By Default

Art 23 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; this applies to the amount of 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 individuals.**

2a. An approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2.

Organisational measures

- Supplier chain = processors: supplier of EM, installers, hosting company, monitoring personnel, maintenance company, (unknown) subcontractors
- (il-)legal interception
- Law enforcement employees

=> contracts, confidentiality agreements, audits, penetration testing, (external) certifications

Set up security in order to prevent and detect personal data security breaches

- Do not use proprietary crypto algorithms or protocols:
  - For handshake and authentication between EM equipment
  - For encryption of communications
- Have external penetration tests
- Monitor communication lines yourself
- (for EU citizens: do not store data in a data center under control of American company cf FISA / Snowden files)
- Do not forgot the protection of your desktop / laptop computers etc!

Encryption prevents Data Breach?

Picture: Sophos

What if: off the shelf usb-stick with personal data is lost, AES 128 bit software encrypted

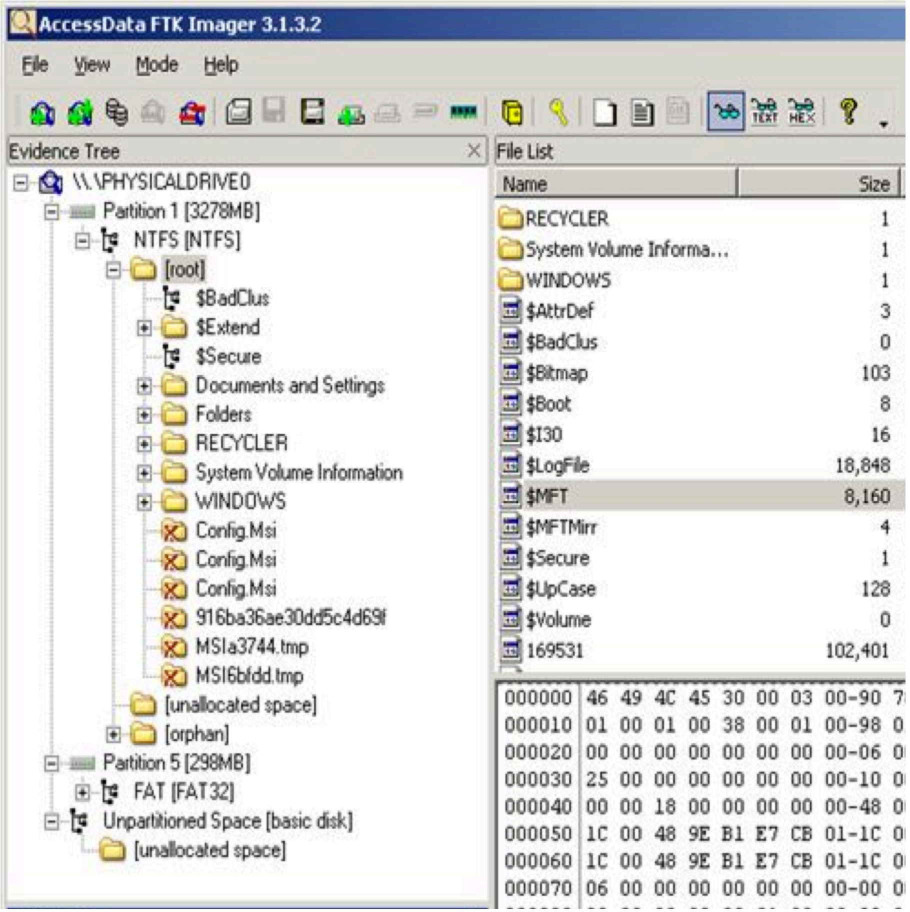
But: Password: 1234 and amount of trials before deletion: ∞

Solutions:

- Good: BYOD usb stick, policy that asks to encrypt with winzip (even when you ask strong password you can not check user or know the content on the lost stick), but then again an attacker can keep on guessing
- Better: pinpad on stick, AES encrypted, 7-15 long: auto delete after 10 guesses
- Best: centrally managed solution: only company accepted sticks, policy enforced password, logs of what data on what stick

copyrighted material!

- People only "worked on fileserver"
- Computer trash was emptied
- But: most data is still recoverable from "free space"



Evidence Tree

```
⊟ \\.\PHYSICALDRIVE0
   ⊟ Partition 1 [3278MB]
      ⊟ NTFS [NTFS]
         ⊟ [root]
              $BadClus
            ⊞ $Extend
              $Secure
            ⊞ Documents and Settings
            ⊞ Folders
            ⊞ RECYCLER
            ⊞ System Volume Information
            ⊞ WINDOWS
              Config.Msi
              Config.Msi
              Config.Msi
              916ba36ae30dd5c4d69f
              MSIa3744.tmp
              MSI6bfdd.tmp
           [unallocated space]
         ⊞ [orphan]
   ⊟ Partition 5 [298MB]
      ⊞ FAT [FAT32]
   ⊟ Unpartitioned Space [basic disk]
        [unallocated space]
```

File List

Name	Size
RECYCLER	1
System Volume Informa...	1
WINDOWS	1
$AttrDef	3
$BadClus	0
$Bitmap	103
$Boot	8
$I30	16
$LogFile	18,848
$MFT	8,160
$MFTMirr	4
$Secure	1
$UpCase	128
$Volume	0
169531	102,401

```
000000 46 49 4C 45 30 00 03 00-90 7
000010 01 00 01 00 38 00 01 00-98 0
000020 00 00 00 00 00 00 00 00-06 0
000030 25 00 00 00 00 00 00 00-10 0
000040 00 00 18 00 00 00 00 00-48 0
000050 1C 00 48 9E B1 E7 CB 01-1C 0
000060 1C 00 48 9E B1 E7 CB 01-1C 0
000070 06 00 00 00 00 00 00 00-00 0
```

Lost Laptop contains no data?

http://www.technobuffalo.com/wp-content/uploads/2010/04/pileofharddrives.gif

- Risk towards security of processing:
  - Lost laptop: empty space contains lots of data
  - Partial encryption asks for discipline
  - Working from file server: temporary files on harddisk
  - End of life: storage media in: computer, multifunctionals, CCTV-recorders, smartphones, tablets, PABX,…

Source: https://www.fbi.gov/news/stories/2009/august/image/RCFL3.jpg

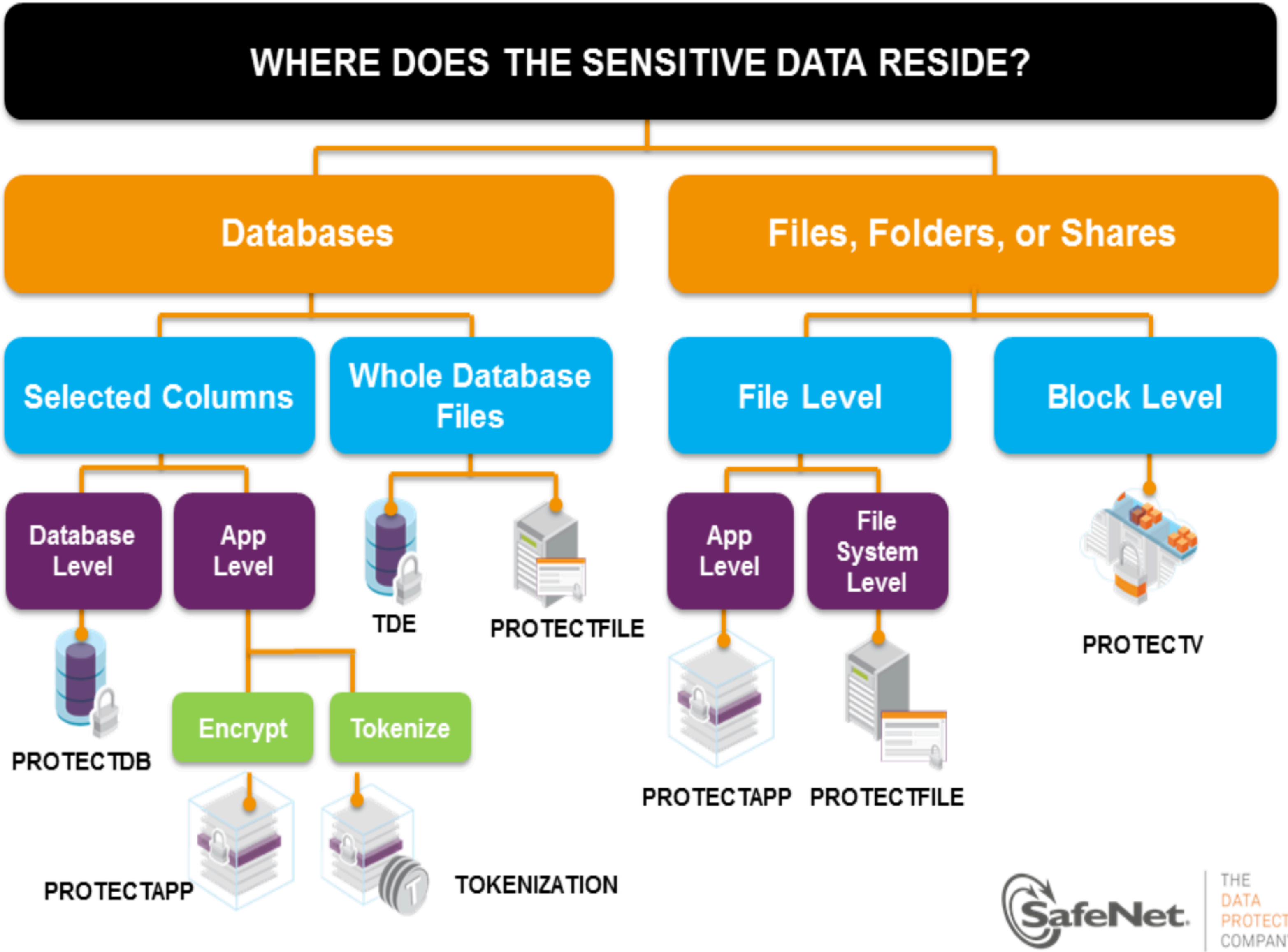
Demo of file recovery: simple tool, no admin rights necessary: http://portableapps.com/apps/utilities/wise-data-recovery-portable

Solutions:

Sector level encryption (is also good solution for end of life): file vault on OS X, right bitlocker on Windows, other tools: Diskcryptor

⇒ always have a fall back in case of lost key: challenge/response or (virtual) vault

⇒ More: https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software



WHERE DOES THE SENSITIVE DATA RESIDE?

- Databases
  - Selected Columns
    - Database Level
      - PROTECTDB
    - App Level
      - Encrypt
        - PROTECTAPP
      - Tokenize
        - TOKENIZATION
  - Whole Database Files
    - TDE
    - PROTECTFILE
- Files, Folders, or Shares
  - File Level
    - App Level
      - PROTECTAPP
    - File System Level
      - PROTECTFILE
  - Block Level
    - PROTECTV

SafeNet THE DATA PROTECTION COMPANY

- Solution:
  - Boxcryptor or others on top of unencrypted cloud storage services
  - Tresorit, Teamdrive, Spideroak
  - Mitigation through encryption of DB, App, files, system files, harddisk sector
- More: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

Thank you!

bavo@cranium.be