30th ANNUAL FIRST CONFERENCE
KUALA LUMPUR
June 24-29, 2018
30 YEARS OF INCIDENT HANDLING

Don't Ignore the GDPR; It Matters Now!

Thomas V. Fischer

FIRST™
Improving Security Together

I am …

- Global Security Advocate & Threat Researcher focused on Data Protection
- 25+ years experience in InfoSec
- Spent number years in IR team positions

BSidesLondon Director

ISSA UK – VP of Data Governance

- Contact
  - tvfischer+sec@gmail.com tvfischer@pm.me
  - @Fvt
  - keybase.io/fvt

Disclaimer

I am not a lawyer, nor do I play one on TV, nor do I have any legal training. I am not providing any legal advice or presenting any legal opinion on GDPR. This talk represents knowledge gathered on various projects. Speak to your legal council on the risks involved for you organisation

Brussels, 6 April 2016
(OR. en)

Interinstitutional File:
2012/0011 (COD)

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject: Position of the Council at first rea
REGULATION OF THE EUROP
COUNCIL on the protection of na
processing of personal data and
repealing Directive 95/46/EC (Ge

"The protection of natural persons in relation to the processing of personal data is a fundamental right…"

The primary objectives of the GDPR are to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU

Articles & Recitals

- 173 Count
- Explains the law
- Provides context
- Overlap with Articles

Interprets

- 99 Count
- Describes the law

The GDPR in Dates

- Law comes into effect 25 May 2018
- There is a 2 year grace period from above date

2 years Have Past

2015-12
Text Agreed

2016-04-16
Adopted EU
Parliament

2016-05
Regulation enters
into force

2018-05-25
Regulation
Enforceable
(2 year post-
adoption)

Scope

- Companies collecting and processing EU citizen personal data
  - Including foreign companies processing EU data
  - Citizen must be residing in the EU
- Apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not
- Breach notification must be done 72hours of discovery > to **customers** and ***DPA***

Penalties

administrative fines should be "*effective, proportionate and dissuasive*"

€10million or 2% worldwide annual turnover

€20million or 4% worldwide annual turnover

Both cases 'whichever is higher'

Breach Notification

72hours to report to DPA is key requirement in data breaches

1. From the date the breach occurred
2. Only reported in case of data exfiltration
3. All breaches must be reported
4. Includes notification of data subject

Breach Notification

72hours to report to DPA is key requirement in data breaches

- Becoming aware of the breach
- destruction, loss, alteration and unauthorised disclosure of, or access to, personal data
- RISK
  RI
- Includes notification of data subject

7 Key Principles Personal Data Protection

- Lawful, fair and transparent processing
- Purpose Limitation
- Data minimization
- Accurate and up-to-date processing
- Limitation of storage
  - Reduce footprint of data that permits identification
  - Pseudonymisation
- Confidential and secure
- Accountability and liability

Key Data Subject Rights

- Right to be informed/Consent
  - Companies need to tell user they are collecting data, user must accept
- Right to Access
  - Customer give right to ask companies about what, why and where their info is stored
- Right to be forgotten
  - Aka. Data Erasure
  - Customer can request that their information be erase and no longer disseminated
- Data Portability
  - Right to receive their personal data
  - 'commonly use and machine readable format‘

Key Data Subject Rights

- Right to be informed/Consent
- Right to Access
- Right to be forgotten
- Data Portability
- Right to Rectification
- Right To Restriction of Processing
- Right to Object

Consent or Lawful Processing

Legitimate

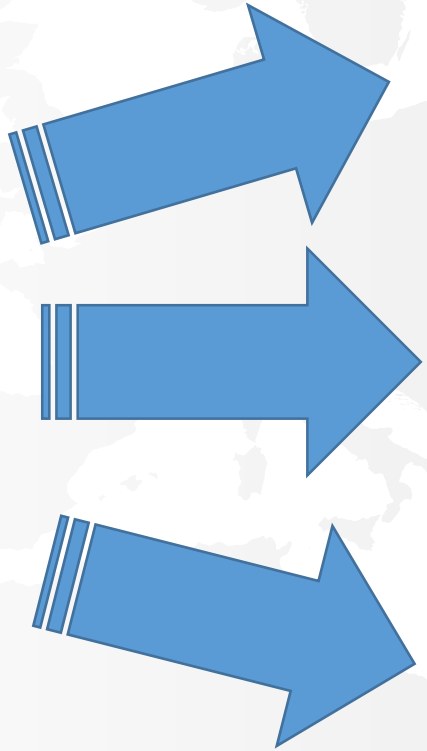
Contractual

Public Interest

Legal

Vital Interest

Forget me, please…



Access and Portability

Granting audit rights to customers

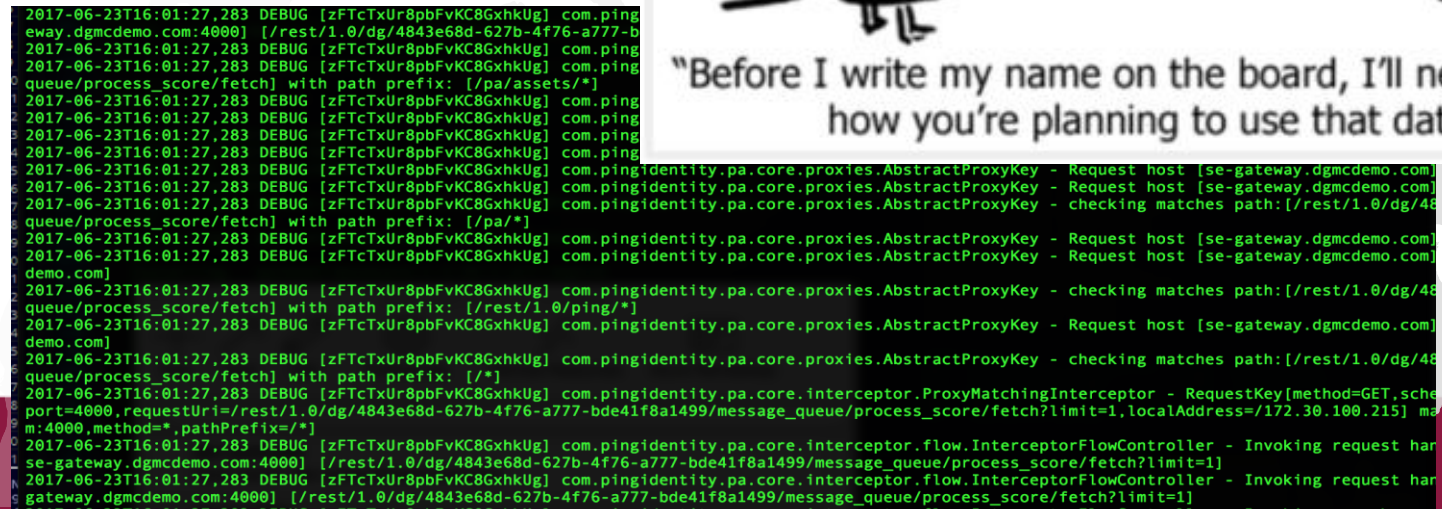
Timely manner

Extracting only the target data

Subject Access Request

Application Review (SDLC)

- Opt-in not out…
- Human readable consent forms
- Make sure
  - Right data is collected
  - Review being used in agreed way



Pesky but Useful: Articles 25 and 35

Privacy by Design & Default

- Pseudonymisation
- Data minimisation
- Only Necessary data
- Yet another Opt-in

- **Protection Impact Assessment**
- WP29 Guidance on DPIA
- FR DPA: CNIL SOFTWARE
- https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

PIA

An overview of the requirements and methodology

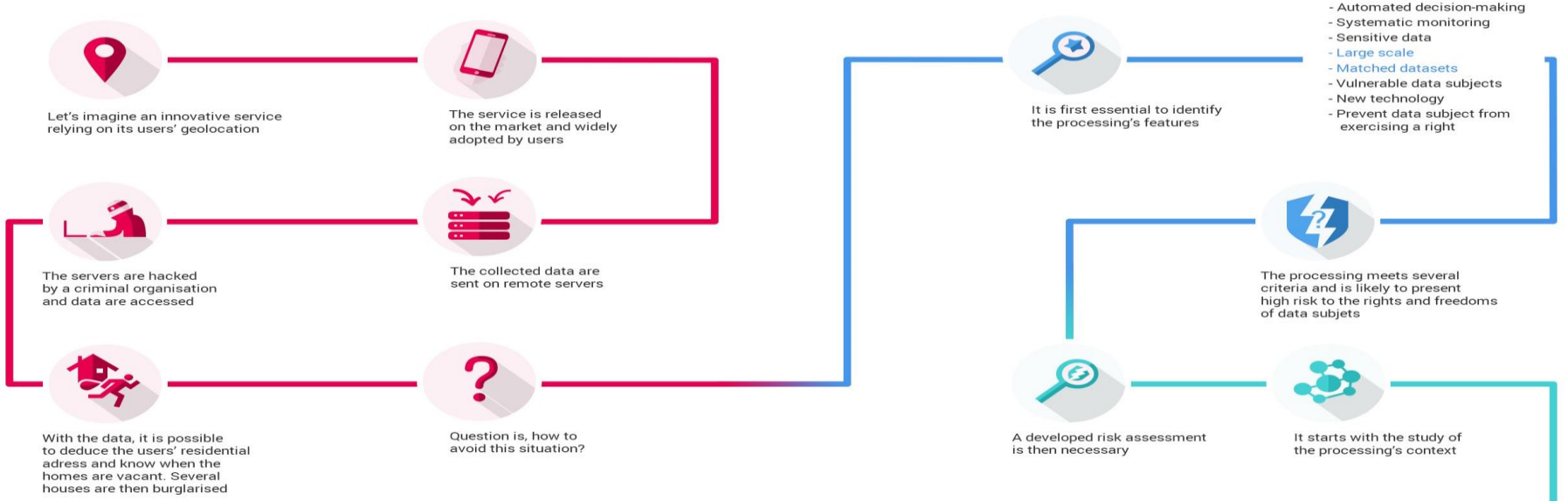
0. Launching a new processing

Every day in the digital realm, numerous services are created.

Those services usually rely on the processing of personal data aiming at fulfilling the needs of organisations or their users.

The supporting assets used to store the data have different levels of vulnerabilities toward feared events such as illegitimate acess, unwanted change, or disappearance of personal data.

Those risks are likely to have significant impacts on the users' privacy.



1. Considering the processing

For the data processor as well as the data subjects, those risks are unwelcome.

Before carrying out a processing, it is essential to analyse it to understand its inherent risks.

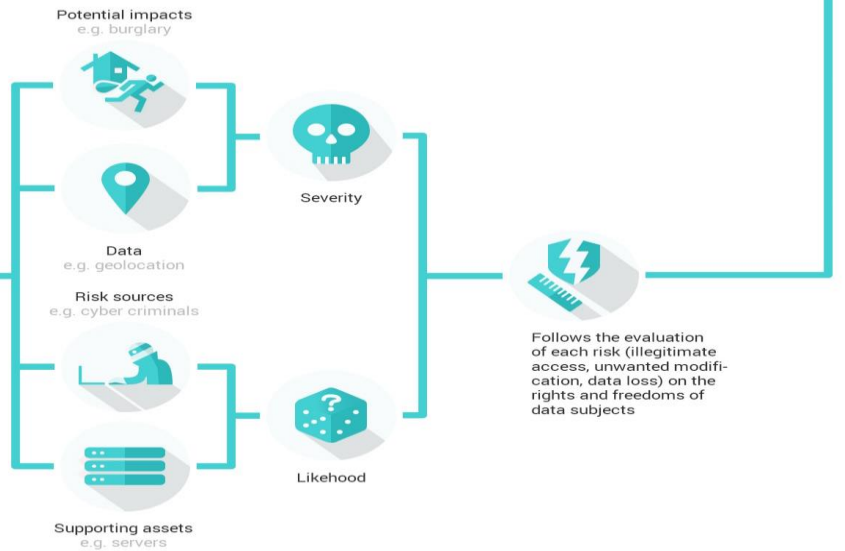
Several factors affect the riskiness of a processing, as the kind of data processed.

Generally speaking, if a processing meets two of the criteria listed, then it is likely to present high risks and would require to carry out a privacy impact assessment.

2. Evaluating the privacy risks

The assessment first establishes the context in which the processing is carried out, including its purpose and technical features.

In addition to studying the fundamental principles, made up of the necessity and proportionality of the processing, each risk has to be analysed to evaluate its severity and likehood according to its potential impacts on the rights and freedoms of data subjects, the data processed, the risks sources and the supporting assets.

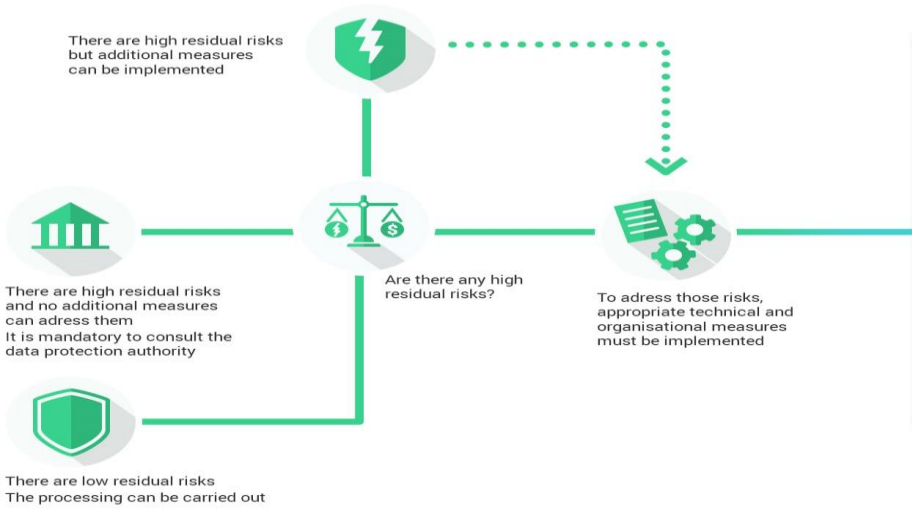


3. Adressing the risks

Once the risks have been identified, it should be determined if they are acceptable given the existing and planned technical and organisational measures.

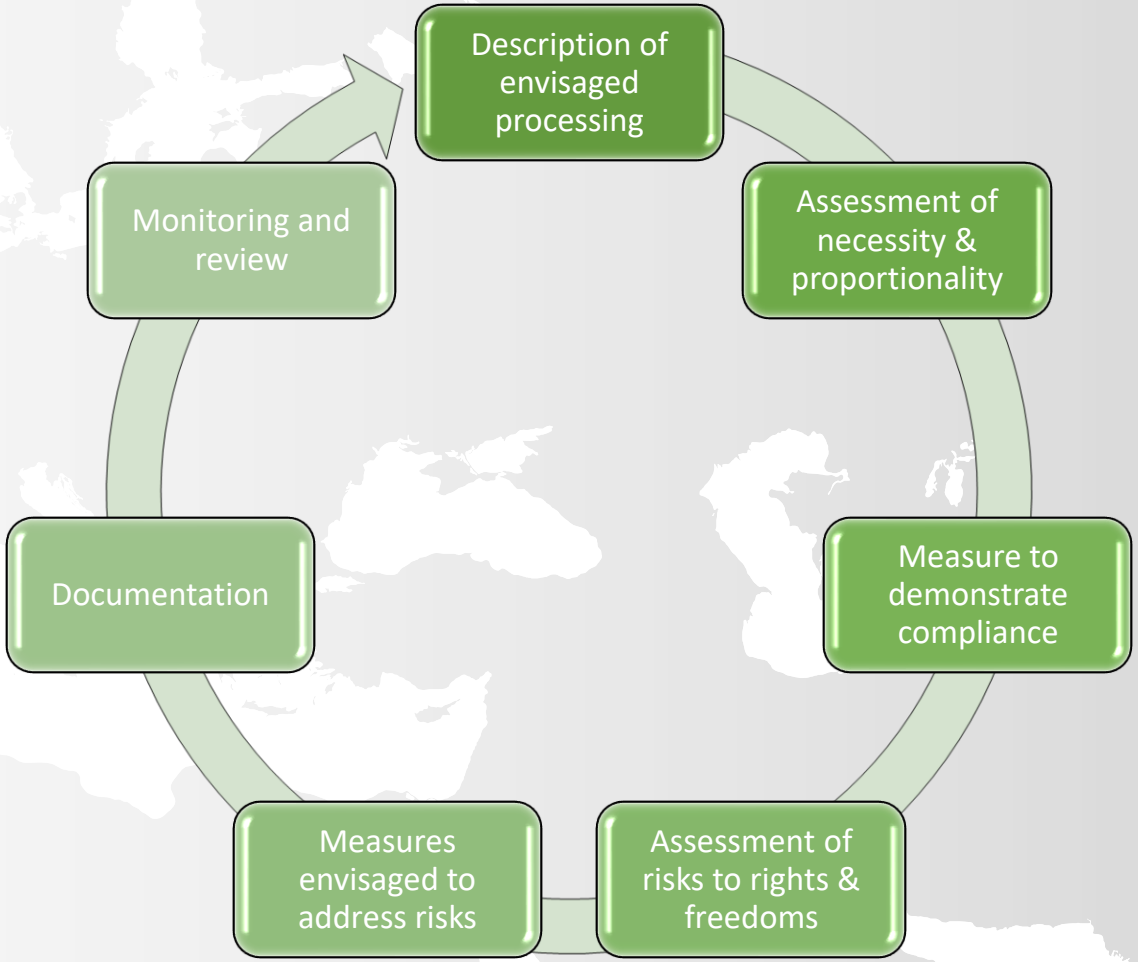
If it doesn't seem possible in regard of the foreseen measures, the data protection authority has to be consulted.

In any case, it is mandatory to implement the planned controls before carrying out the processing.



Data Protection Impact Assessment

- Continual process, not a one-time exercise
- Data Controller remains accountable
  - Not transferable to a data processor (for example)
- Minimum features (article 35)
  - Description of processing and purposes
  - Assessment of necessity and proportionality
  - Assessment of risks to rights of data subjects
  - Measures introduced to
    - Address any risks
    - Demonstrate compliance with Regulation



"Before I write my name on the board, I'll need to know how you're planning to use that data."

Personal Data?

What is Personal Data?

- The GDPR defines iT and interprets
  - Article 4(1)
  - Recitals 15,26,28,29,30,31,34,35,36,37
- Any information relating to an identified or identifiable Natural Person
- Directly or Indirectly

What is Personal Data?

App Data
Cameras
License Plate
Blackbox

References
Performance
Work history
Vetting
Education
Access log
ANPR
Contacts
Salary

Name

Credit rating
Transactions
Mortgage
Credit Card
Loans
Taxes

Political Opinion
Genetic Data
Religious beliefs
Ethnicity
Trade union
Demographic

DoB
Gender
Photos/Videos
Location data
Fingerprint
ID Number

Behaviour
Health
Tracking
Comms
Contacts
IMEI

IoT
Smart devices
CCTV
Address

MAC Address
IP Address
Cookies

E-Mail
Social Network
Behavioural

Physical/Mental health
Disability
Blood type
Drug test
Genetics
DNA

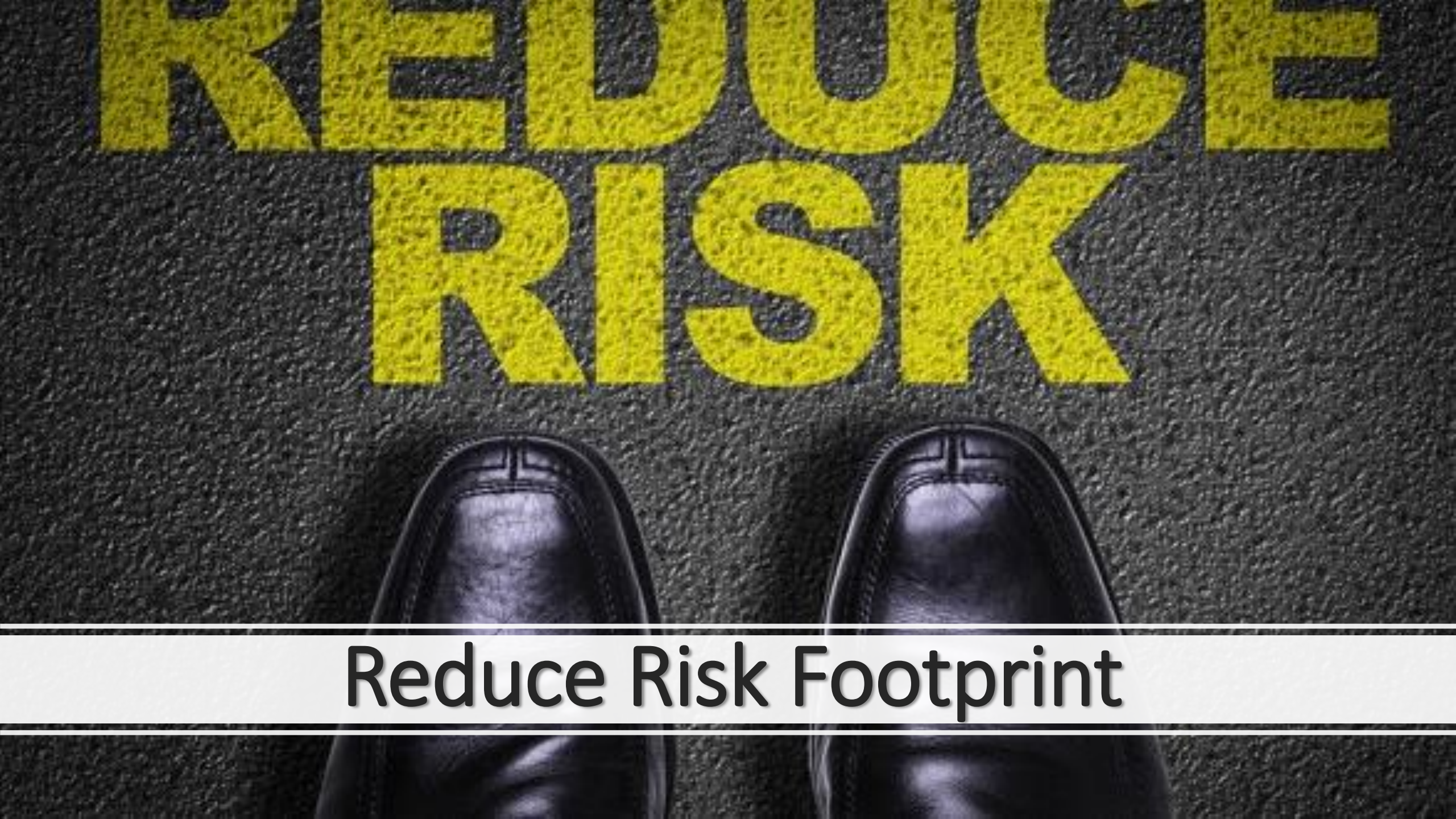
The Horrendous Truth

Country Specific Non-Sensitive
Identifier
Name
Date of birth
Gender
Address
Post code
National ID
Passport
Drivers License
Nationality
Regional nationality
Telephone
National healthcare identify
Bank Account IBAN
Bank account national
biometric data
fingerprints
facial recognition
retinal scans
Tax numbers
VAT
Company registration
Economic

Economic
Credit card
Non-government Identification numbers
Cultural identifcation
Security Clearance
Legal status
Physical Appearance
Photo/Headshot
physical - height
physical - weight
physcial - eye colour
physicall - hair colour
physical - birth marks

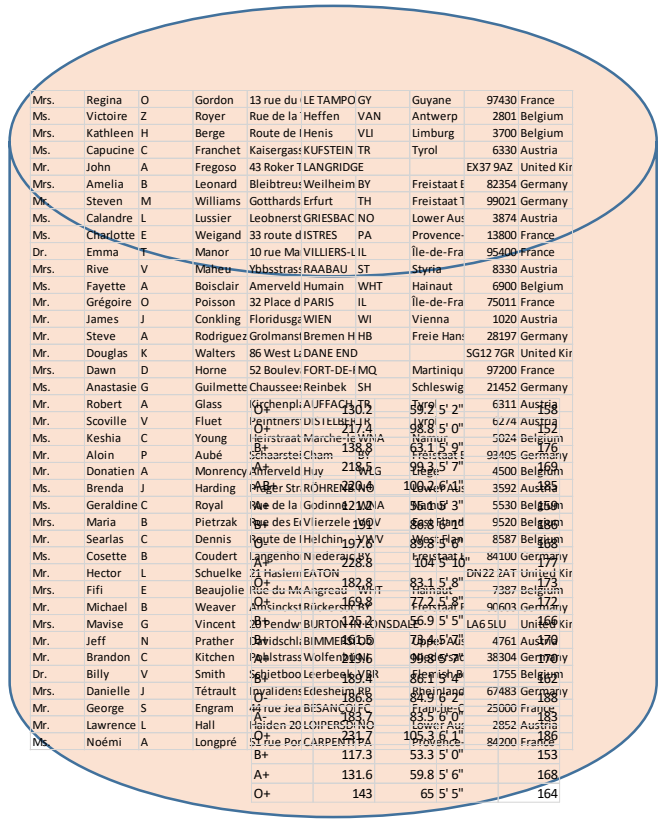
Country Specific Sensitive
Identifier
Race/Ethnicity
Religion
Health/Medical Terms
Labour Union membership
Political affiliations
Criminal records
Biometric data
Sexual orientation
Genetic data
Philosophical
Mental health attributes

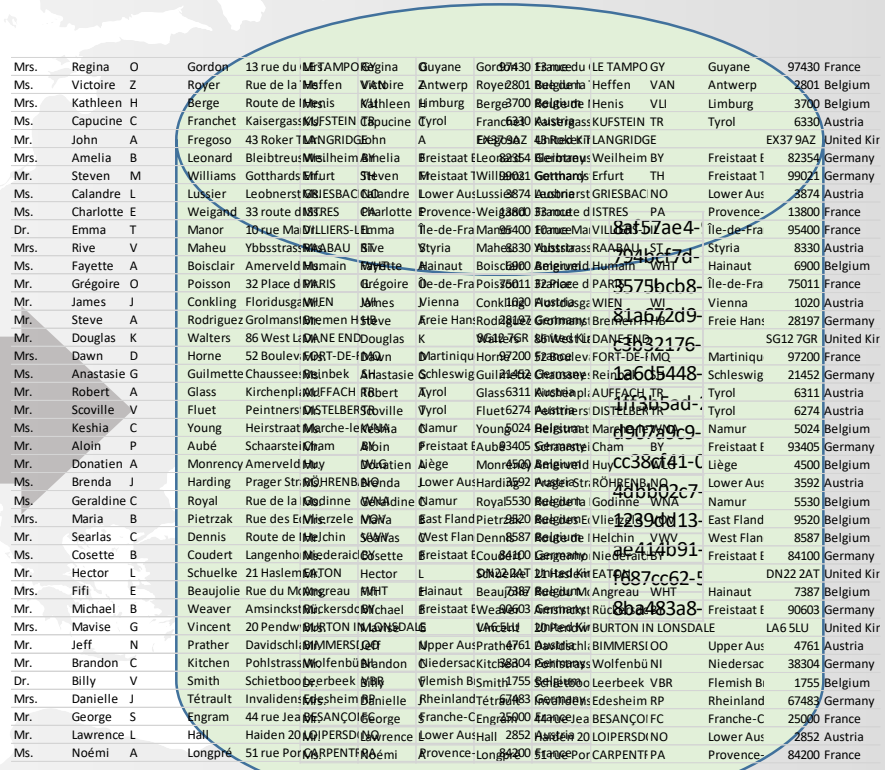
Generic No Country or language
Identifier
Country Tags
IPv4
IPv6
IMEI
GPS Coordinates
Social Networks
email address
RFID tag
CCTV Footage



Reduce Risk Footprint

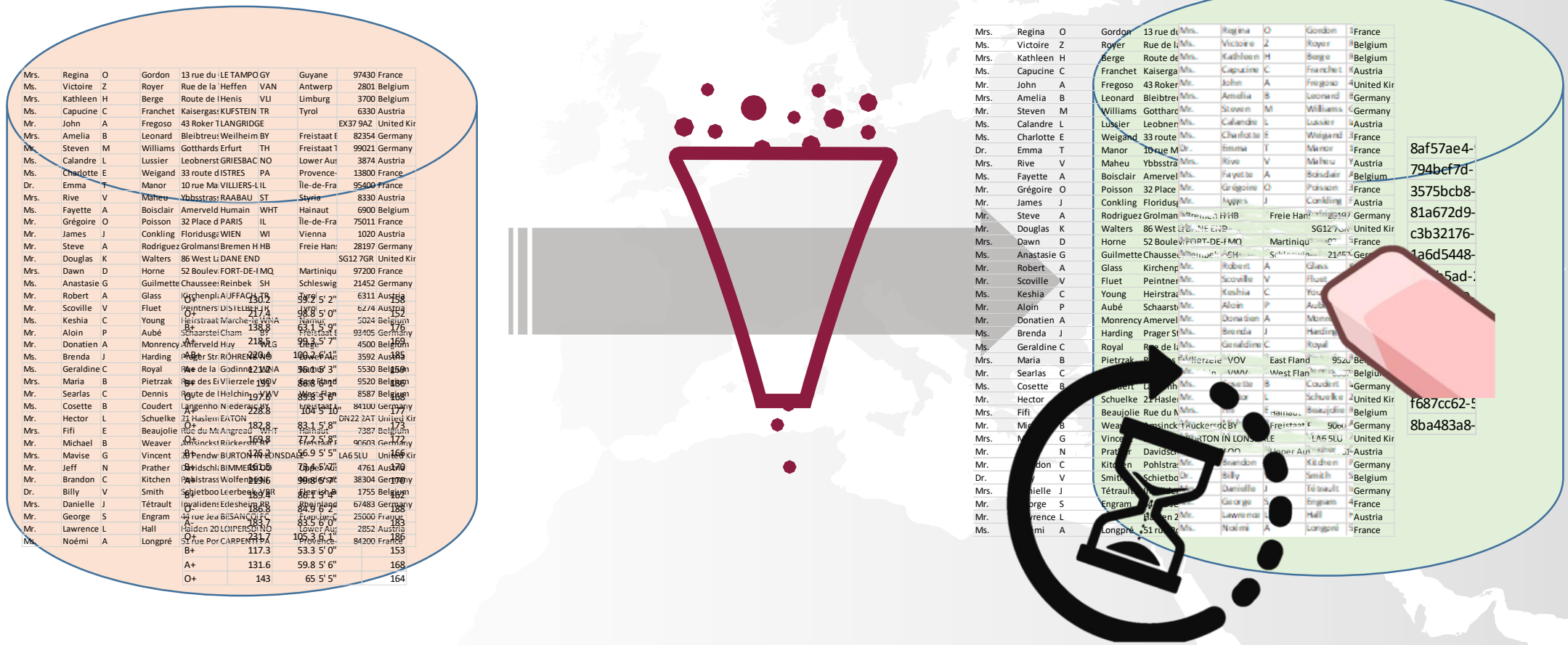
Data Minimisation





Created by Nathan Rofkahr
from the Noun Project

Data Minimisation



Pseudonymisation

- Only real technical suggestion!!!
- No it doesn't mean encryption

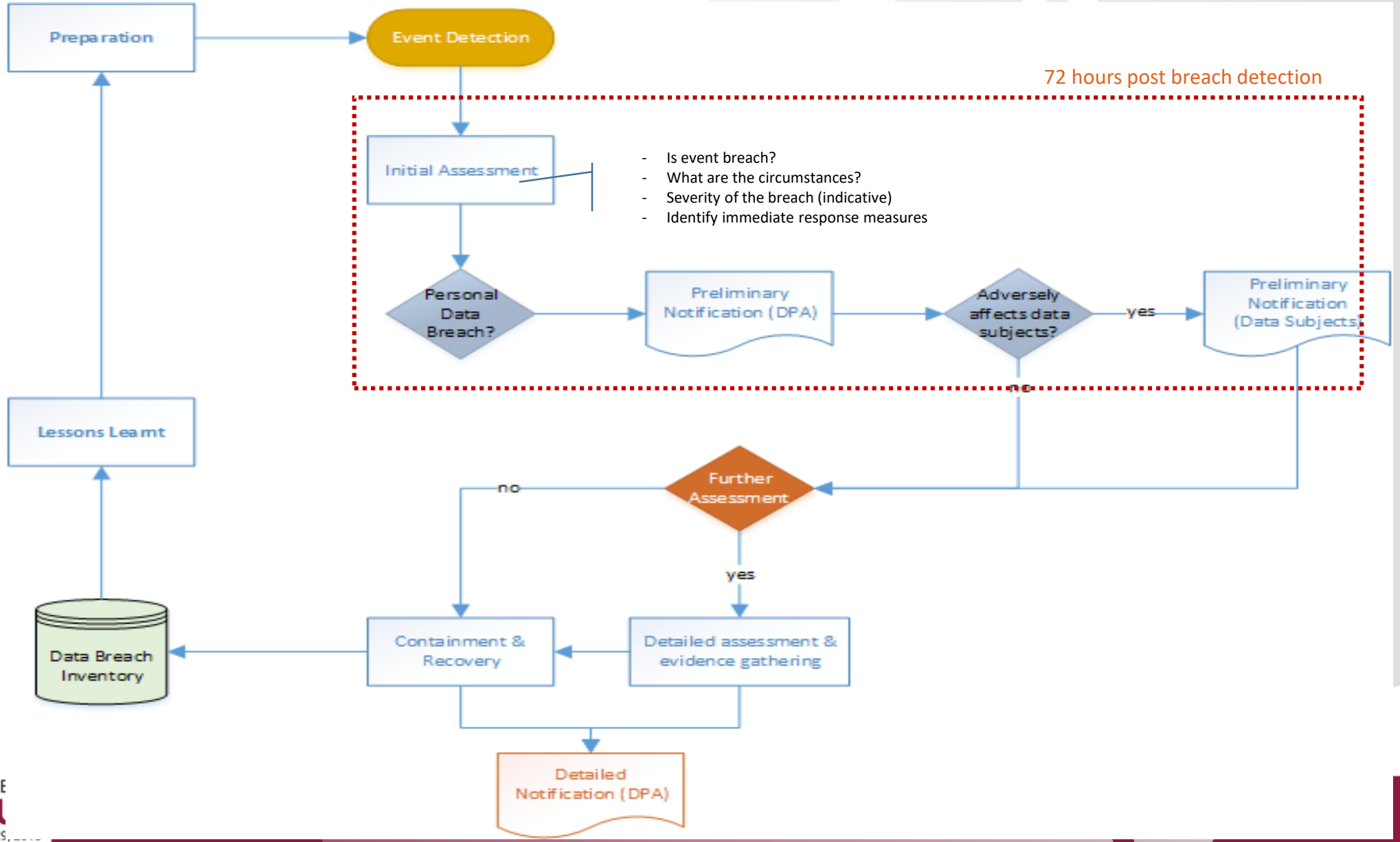
Name	Token/Pseudonym	Anonymize
Clyde	qOerd	xxxxx
Marco	Loqfh	xxxxx
Les	Mcv	xxxxx
Les	Mcv	xxxxx
Marco	Loqfh	xxxxx
Raul	BhQl	xxxxx
Clyde	qOerd	xxxxx


DE3100A16C20
Data Breach
2202E6F6163686573
Cyber Attack
106564207368

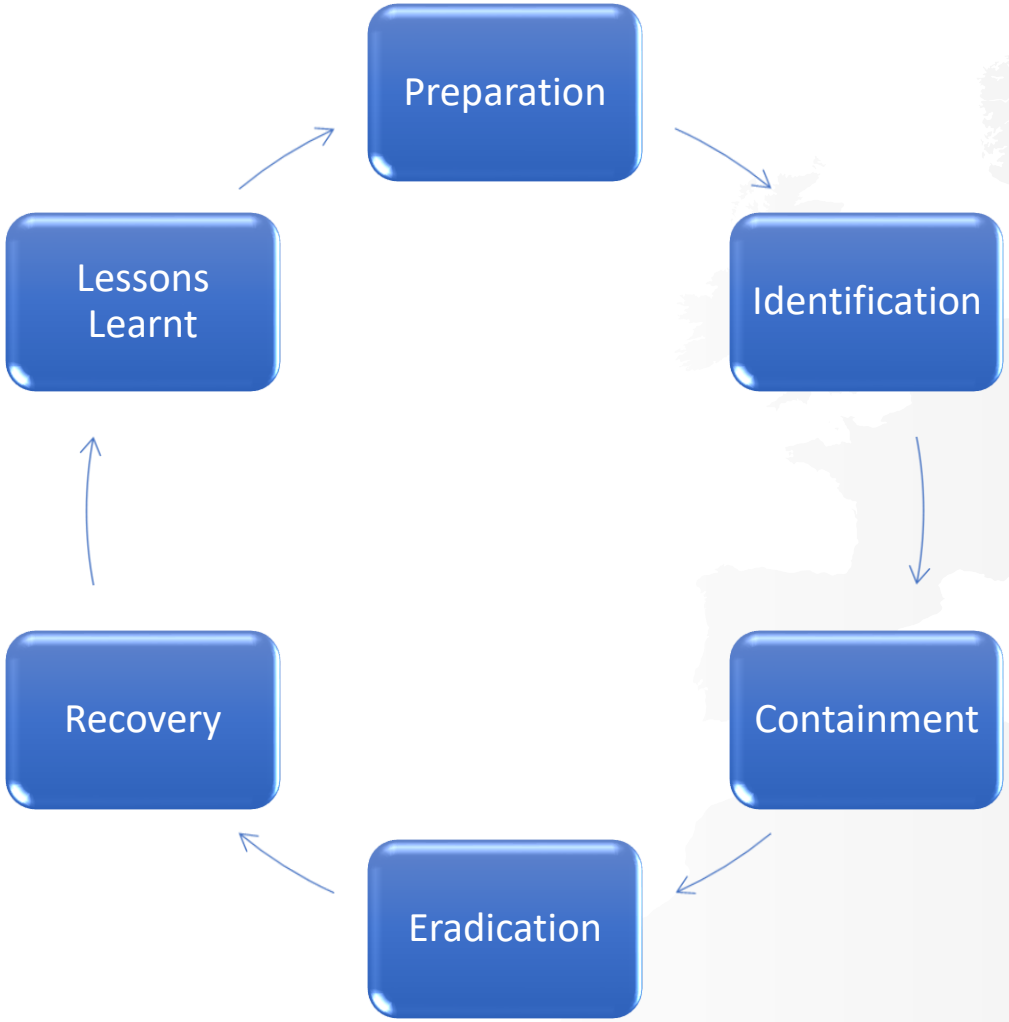
When a Breach is not a Breach?

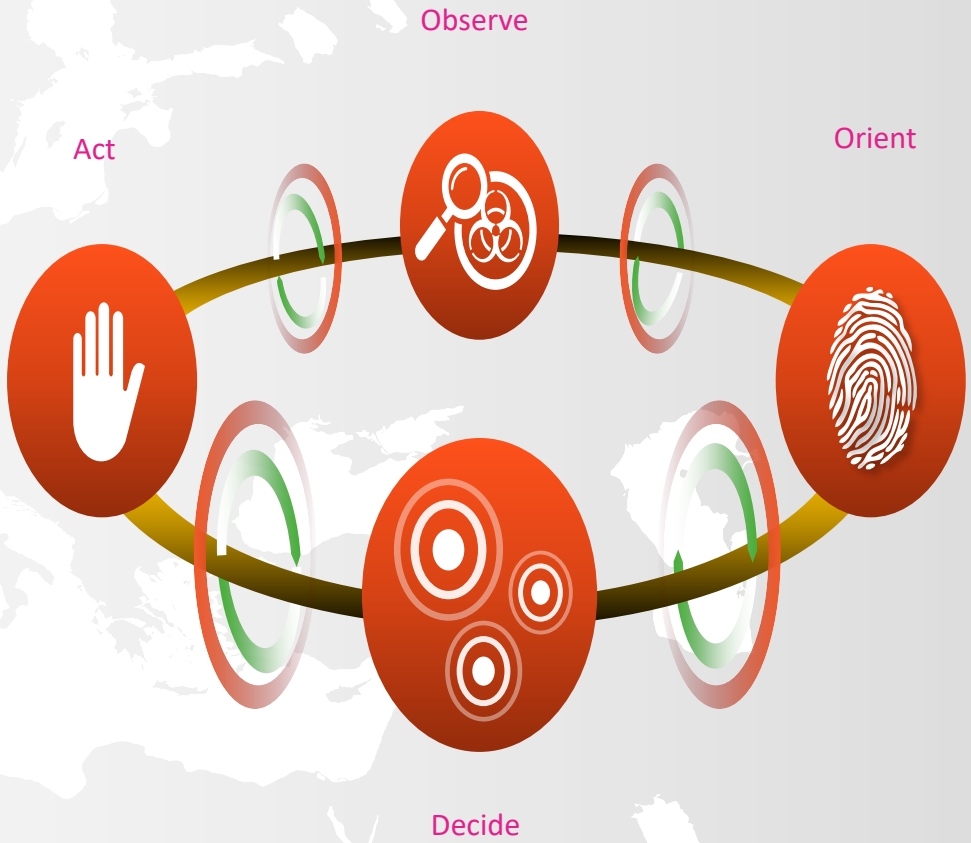
- Exfiltration
- Destruction
- Alteration
- Unauthorised Disclosure
- Unauthorised Access

Data Breach Handling Procedure



Handling Data Focused IR





Handling Data Focused IR

Preparation

The Personal Data Journey

(Data Flow Mapping)

Data Security

Technical and organisational security measures

- Data-in-transit Protection
- Asset Protection & Resilience
- Separation between users
- Governance
- Operational Security
- Personnel Security
- Secure Development
- Supply-chain Security
- Secure Consumer Management
- Identity & Authentication
- External Interface Protection
- Secure Administration
- Audit Information
- Secure use of Service

Data Transfer

Names of third countries or international organisations that data is transferred to

EU

US

Data Source

Personal Data Source

- Controller
- Joint Controller
- Direct
- Third Party
- Collector

Data Subject

Categories of Individuals

- Employees
- Former Employees
- Successful Candidates
- Unsuccessful Candidates
- Potential Customers
- Existing Customers
- Former Customers
- Accountant
- Auditors
- Business Partners
- Sub-Contractors
- Service Providers
- Suppliers
- Public

Personal Data

Categories of Personal Data

- Contact details
- Bank details
- Pension details
- Tax details
- Pay details
- Annual leave details
- Sick leave details
- Performance details
- Qualifications
- Employment history
- Ethnicity
- Disability details
- Purchase history
- Lifestyle information
- Picture of subject

Purpose of Processing

Purpose of Processing

- Payroll
- Personnel File
- Personnel Management
- Security Vetting
- Recruitment
- Training
- Finance
- System Account Management
- Customer Management
- Direct Marketing
- Criminal Offence

Lawful Processing

Lawful Basis of Processing

- Consent
- Contract
- Legal obligation
- Vital Interests
- Public Interests
- Legitimate Interest

Data Retention

Retention schedule

- 1 year post-employment
- 3 years post-employment
- 6 years post employment
- 6 months post-campaign
- 1 year post campaign
- End of customer relationship
- 1 year - post contact

Data Recipients

Categories of Recipients

- HMRC
- Referees
- Processor – Marketing
- Processor – SaaS
- Processor – IaaS
- Processor – Payment Provider
- Processor – Bank
- Sub-Processor – Courier
- Sub-Processor - Printer

Adapt	Adapt you existing Models
Assign	Assign Personal Data related attributes
Identify	Identify the risks
Use	Use the DPIA
Think	***Will this Harm the Data Subject***

Threat and Vulnerability Mod

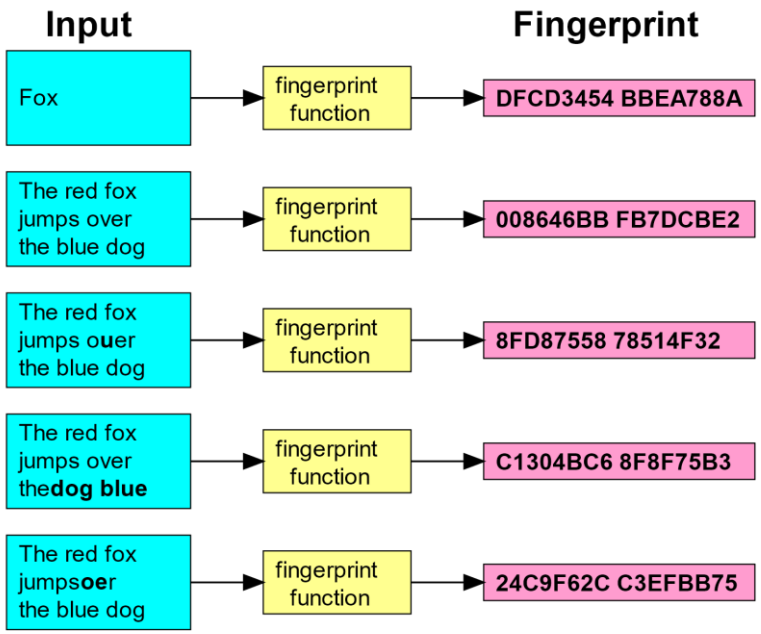
Data (e)Discovery…

Discovery Tools

- FreeEed.org

- Commercial Products
  - McAfee
  - Symantec
  - Forcepoint
  - Digital Guardian
- Multiple modes

Discovery Methods



Fingerprinting

Pattern

RegEx

Finding The Data..

- Talk to the data owners
- Crawling your environment
- Build a map

➢Focus your detection

UK Passport

Format:

Passport n

• E.g. 92

Positions	Length	Characters	Meaning
1–9	9	alpha+num+<	Passport number
10	1	numeric	Check digit over digits 1–9
11–13	3	alpha+<	Nationality (ISO 3166-1 alpha-3 code with modificatior
14–19	6	numeric	Date of birth (YYMMDD)
20	1	num	Check digit over digits 14–19
21	1	alpha+<	Sex (M, F or < for male, female or unspecified)
			piration date of passport (YYMMDD)
			eck digit over digits 22–27
29–42	14	alpha+num+<	Personal number (may be used by the issuing country
43	1	numeric+<	Check digit over digits 29–42 (may be < if all characte
44	1	numeric	Check digit over digits 1–10, 14–20, and 22–43

UK Passport
```
^[0-9]{10}GBR[0-9]{7}[U,M,F]{1}[0-9]{9}$
```

UK NI (National Insurance)
```
[A-CEGHJ-PR-TW-Z]{1}[A-CEGHJ-NPR-TW-Z]{1}\040?[0-9]{2}\
9]{2}\040?[0-9]{2}\040?[a|A-z|Z]{1}
```

UK VAT
```
([GB])?(([1-9]{8})|([1-9]{11}))$
```

UK Bank Account
```
^(\d){8}$
```

UK Bank Sort Code
```
((01|05|08|11|13|14|15|16|17|18|19|72|82|83|84|86|87|90|91|93|94|95|98
)-[0-9]{2}|([2,3,4,5,6][0-9]-[0-9]{2})|(07-[0-4][0-9]|09-[0,1][0-
9]|10-[0-8][0-9]|12-[0-6][0-9]|77-[0-4][0-9]|89-[0-2][0-9]))-[0-9]{2}
```

GR VAT
```
\b(EL|GR)?[0-9]{9}\b
```

GR National ID
```
[A-Z][ -]?[0-9]{6}
```

GR IBAN
```
GR\d{2}[ ]\d{4}[ ]\d{4}[ ]\d{4}[ ]\d{4}[ ]\d{4}[ ]\d{4}\d{3}|GR\d{25}
```

https://en.wikipedia.org/wiki/Passports_of_the_European_Union
https://www.gov.uk/guidance/vat-eu-country-codes-vat-numbers-and-vat-in-other-languages

https://github.com/tvfischer/gdpr-data-patterns-detection

How the F@%$ do you RegEx

Identification

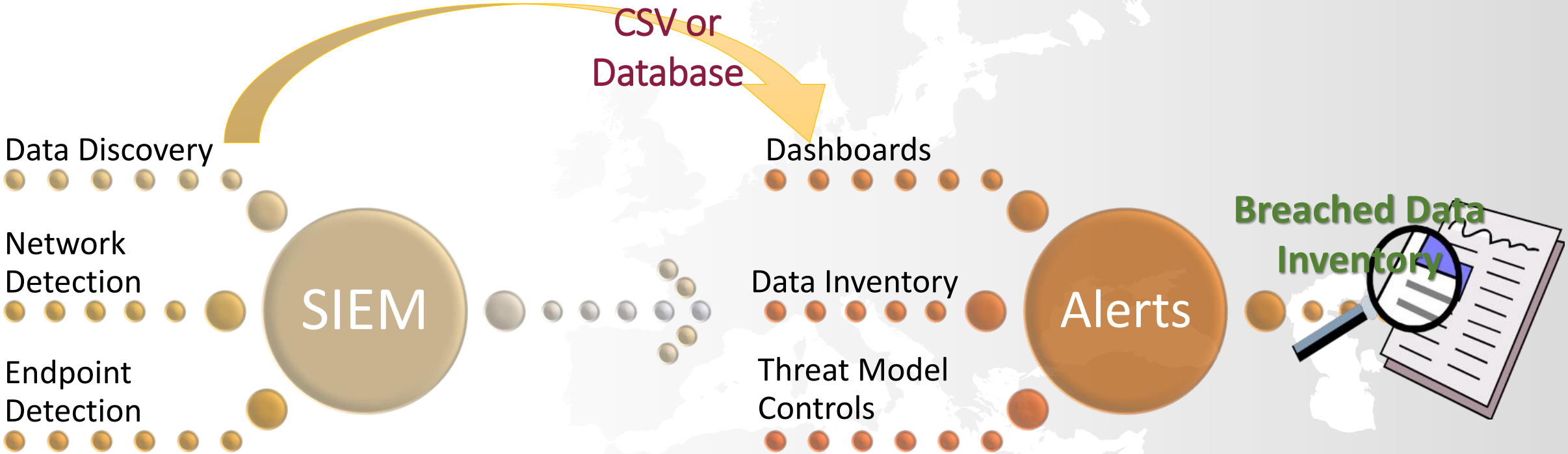
ACTIVE

- Endpoint
- Network

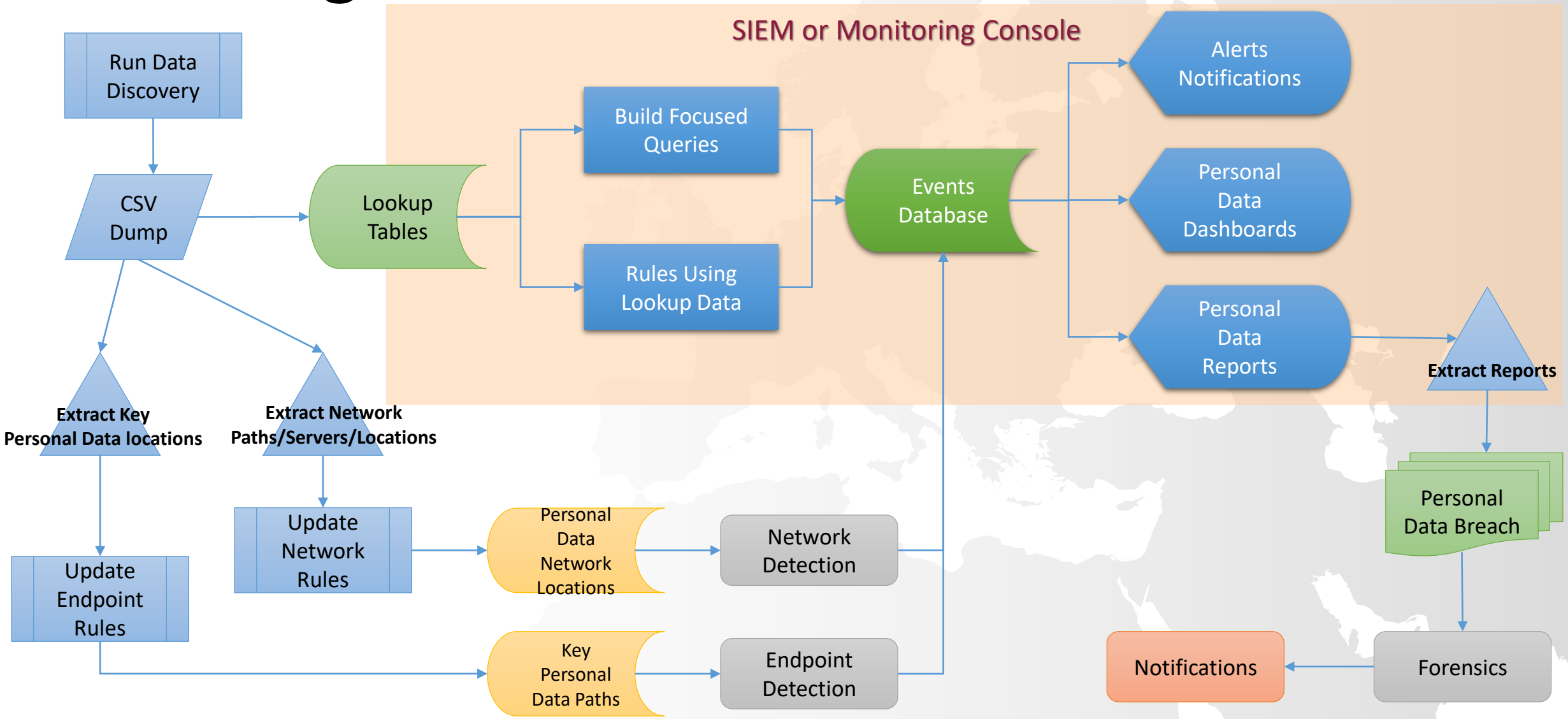
PASSIVE

- Discovery Data
- SOC/SIEM

Tools and Alerts



Building a Data Focused Detection



Augment your Existing Log/SIEM

- Feed your SIEM
  - Endpoint detection tools
- Capture File Events
  - Don't forget – **Not** just copying
- CSV Lookups or External Lookups

```
lookup("personaldatapaths.csv",
    on=[Source_File_Path,Destination_File_Path])
```

```
<search>
 <query>index="$hostname$" Operation in ("File Write","File Copy","File Move","File delete") | ![|inputlookup
 allowedusers.csv | fields User_Name] | [|inputlookup restricted_personaldatapaths.csv | fields Source_File_Path
 | dedup Detail_Event_ID Source_File_Path
 | table gent_UTC_Time, Computer_Name, User_Name, Application, Source_File, Source_File_Path </query>
 <earliest>$timepicker.earliest$ </earliest>
 <latest>$timepicker.latest$ </latest>
</search>
```

```
host=* (Operation="File Write" OR Operation="File Copy" OR Operation="File Move" OR Operation="File Delete"
lookup("personaldatapaths.csv", on=[Filepath,Source_File_Path]) | !(lookup("allowedusers.csv", on=[User,Use
| table([Agent_UTC_Time, Computer_Name, User_Name, Source_File, Source_File_Path])
```

Notification

Categories and approximate number of individuals concerned

Categories and approximate number of personal data records concerned

The name and contact details of the data protection officer

A description of the likely consequences of the personal data breach

Mitigation or remediation efforts

Personal Data Breach Notification

- Data Processing Context
- Ease of Identification
- Circumstances of Breach

Severity of a data breach		
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

ENISA Personal Data Breach Severity Assessment Methodology

https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches/personal-data-breach-notification-tool

Final Thoughts

Thinking of skipping this section

Compliance???

Not Compliance

“At one point I thought changing my name might help with privacy, but that was before the Internet.”
Olivia Wilde

https://github.com/tvfischer/gdpr-data-patterns-detection

… under construction still needs a lot of work

@Fvt

- tvfischer+sec@gmail.com
- keybase.io/fvt