Building a Personal Data Focused Incident Response Plan to Address Breach Notification

Thomas V. Fischer

BSides Cyprus 2019

I am …

- Security Advocate & Threat Researcher focused on Data Protection
- 25+ years experience in InfoSec, 30+ in IT
- Spent number years in corporate IR team positions

BSidesLondon Director

ISSA UK – VP of Data Governance

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

Handling Personal Data Focused IR

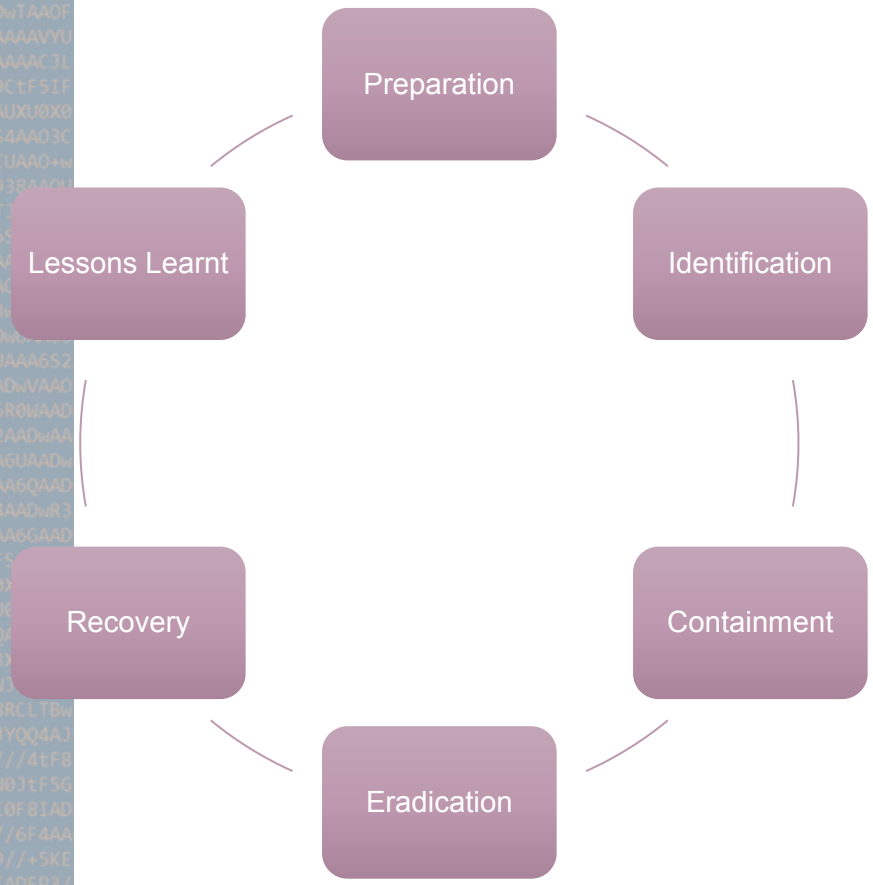
Actual Legislation

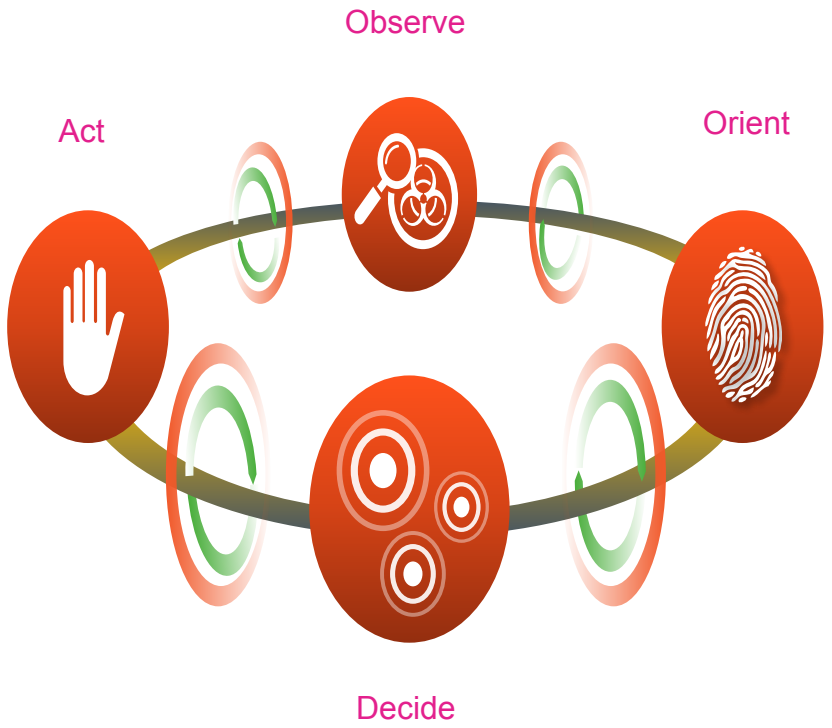
- **The GDPR**
-
-
-

Roadmap Legislation

- South Korea
- Japan
- Canada

What's your Flavour of IR





- Detect
- Contain
- Eradicate
- Remediate
- Recover
- Review
- Communicate

Data Breach Notification to a Supervisory Authority, are you Ready?

- 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
- UNLESS UNLIKELY TO RESULT IN A RISK TO RIGHTS AND FREEDOMS OF PERSON
- Includes notification of data subject

Personal Data?

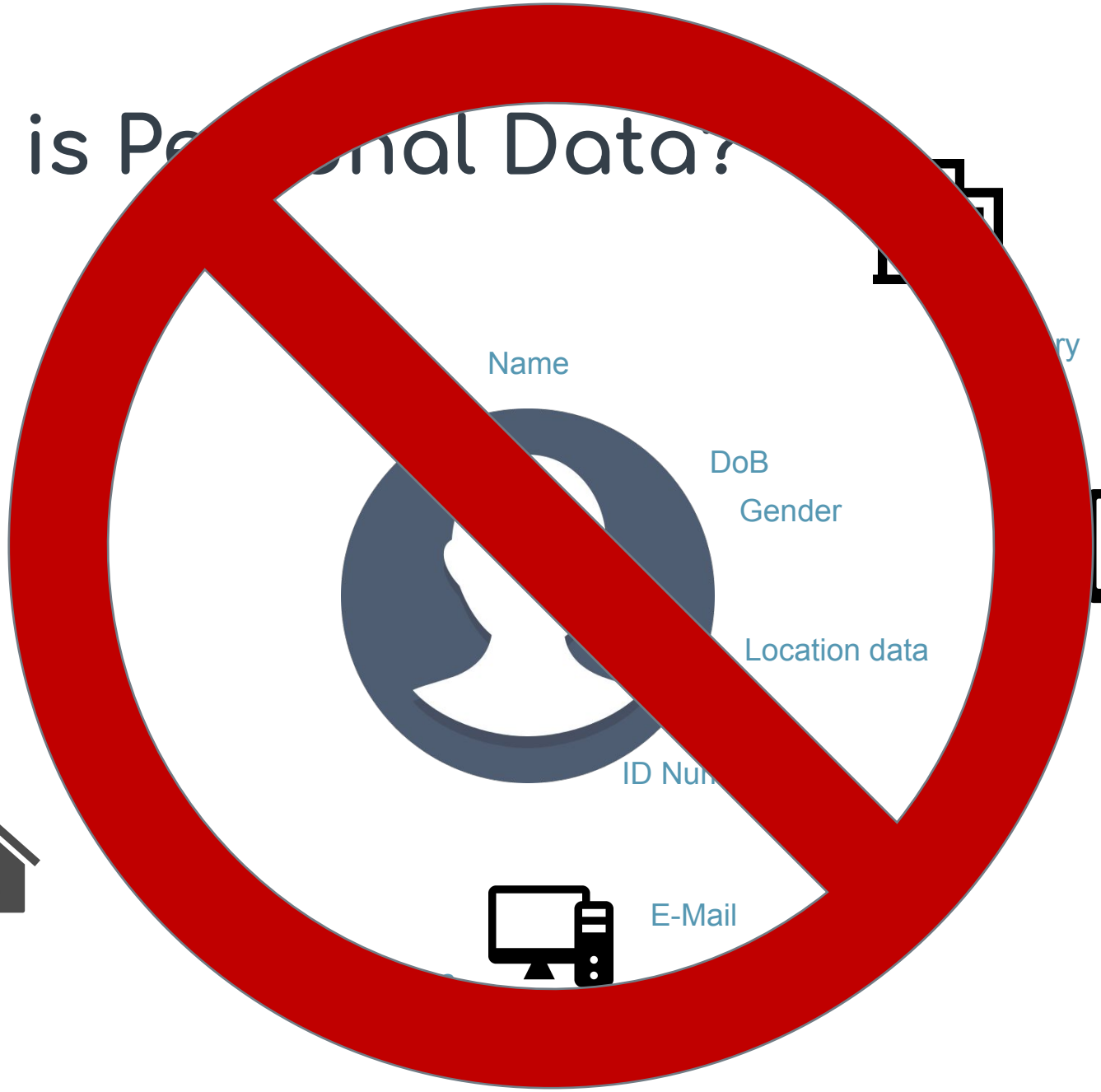
What is Personal Data?

- 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 Pe nal Data?



What is Personal Data?

App Data
Cameras
License Plate
Blackbox

References
Performance
Work history
Vetting
Education
Access log
ANPR
Contacts
Salary

Name
Political Opinion
DoB
Genetic Data
Gender
Religious beliefs
Photos/Videos
Ethnicity
Location data
Trade union
Fingerprint
Demographic
ID Number

Credit rating
Transactions
Mortgage
Credit Card
Loans
Taxes

Behaviour
Health
Tracking
Comms
Contacts
IMEI

IoT
Smart devices
CCTV
Address

MAC Address
E-Mail
IP Address
Social Network
Cookies
Behavioural

Physical/Mental health
Disability
Blood type
Drug test
Genetics
DNA

The Horrendous Truth

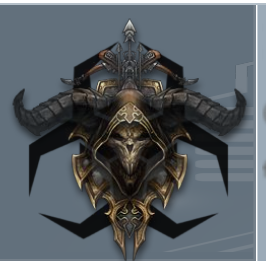
Country Specific Non-Sensitive
Identifier
Name
Date of birth
Gender
Address
Post code
National ID
Passport
Drivers License
Nationality
Regional nationality
Telephone
National healthcare identify
Bank Account IBAN
Bank account national
biometric data
fingerprints
facial recognition
retinal scans
Tax numbers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

Let's Talk

Why, Which, When, Where, Who and How



Why

Has new legislation and compliance requirements made you change your IR process?

Which

Which IR model do you use? OODA, SANS, NIST, Home grown?

When

How do you currently associate a security event to a data breach? And at what time?
What about red team exercises? i.e. How do you test?

What

Does the current generous definition of PII suite new regulation requirements?

Where

Do you know where personal data is stored & used?
Have you identified more sensitive area of data storage?

How

How (or what tools) do you currently use to identify and inventory personal data?
How do we do detect the “non exfiltration” breaches?

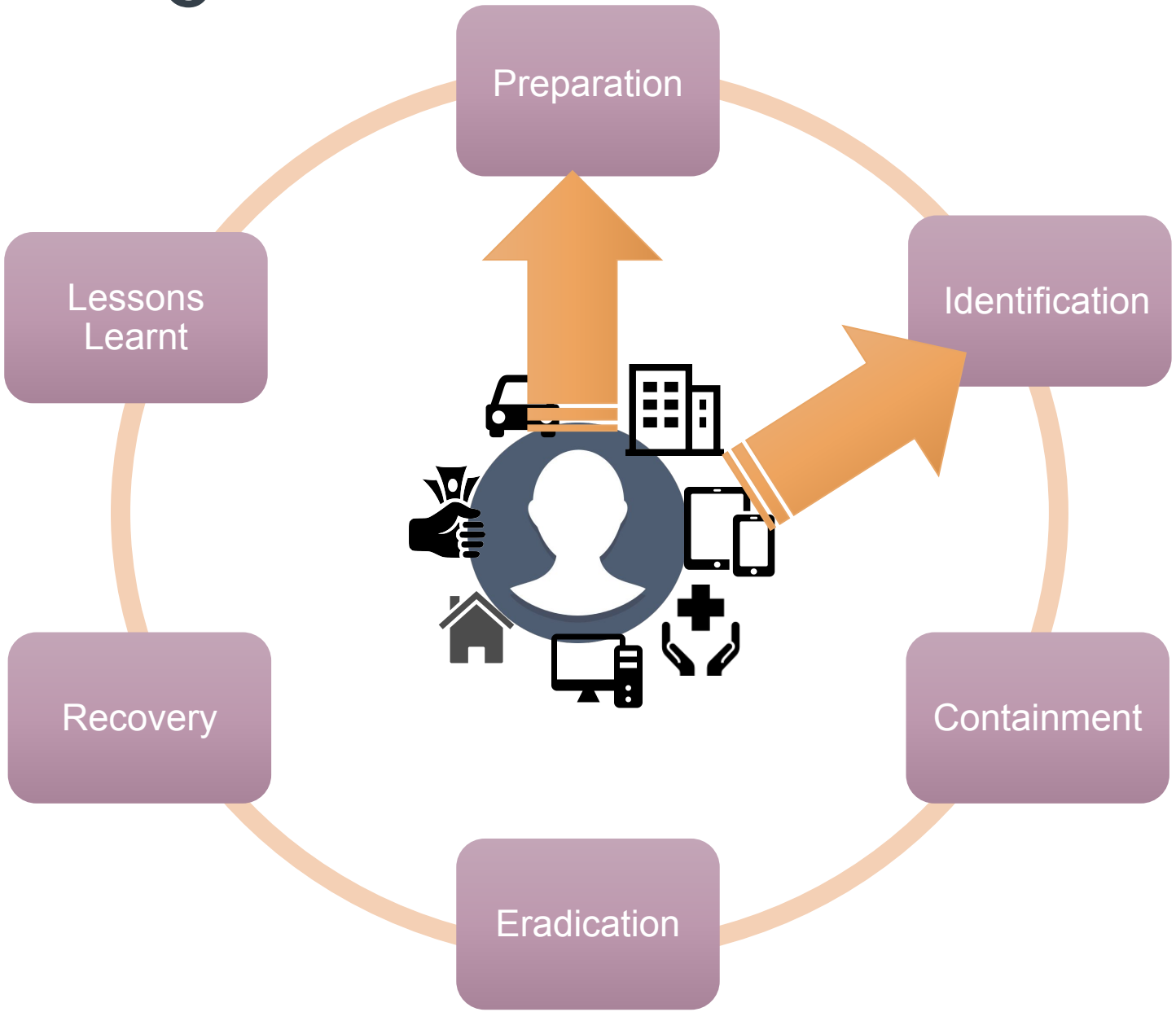
Who

Is the DPO in the team?
    When do you bring the DPO in?
How does your interaction with PR/Comms work?
Which DPAs do you inform?

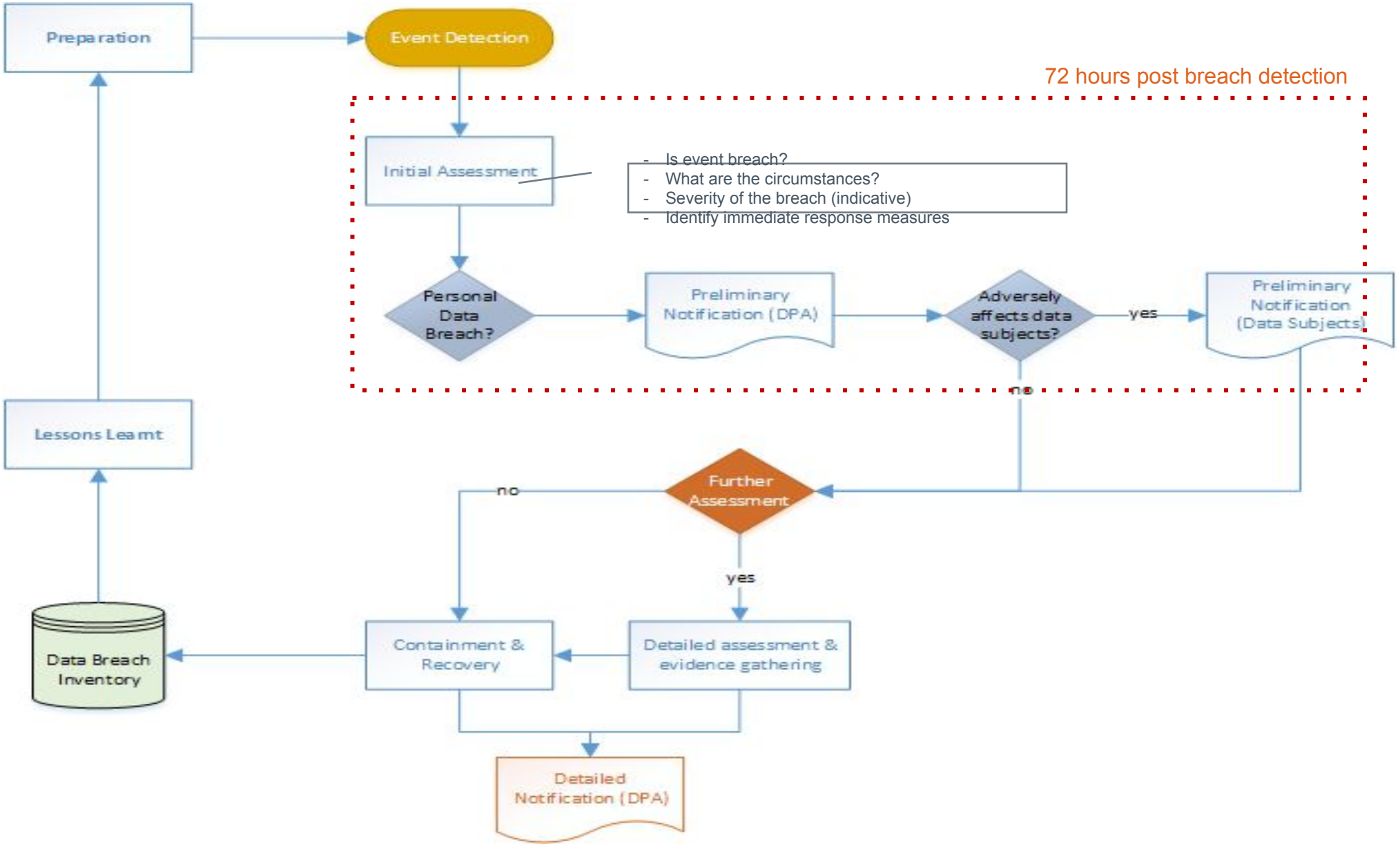
- Data Governance/ Protection
- Information Security
- IT Operations
- H.R.
- Legal
- P.R.
- Facilities Management


DE3100A16C20
Data Breach
2202E6F6163686573
Cyber Attack
106564207368

Handling Data Focused IR



Data Breach Handling Procedure



When a Breach is not a Breach?

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

Preparation

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 Model

PIA

An overview of the requirements and methodology

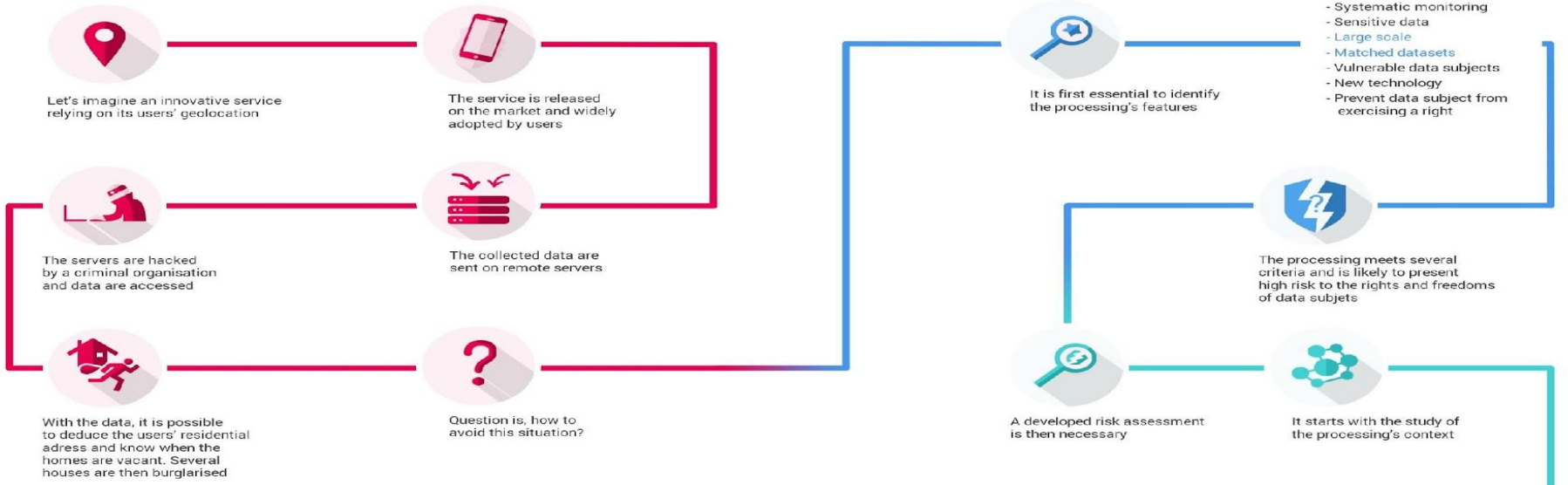
0. Launching a new processing

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.

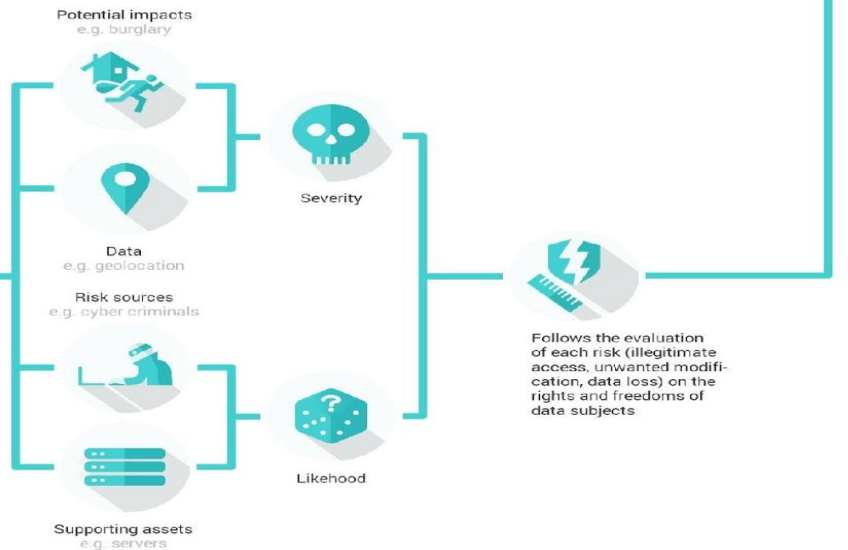
Several factors affect the riskiness of a processing, as the kind of data processed.

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.

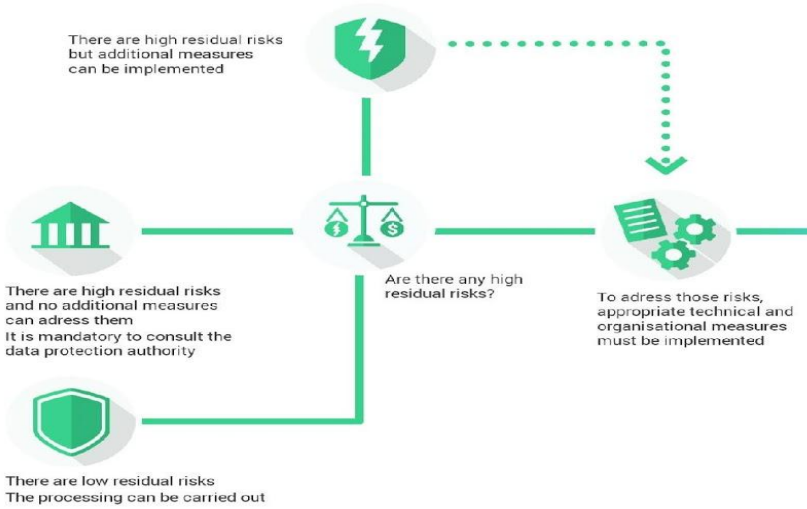


3. Adressing the risks

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.



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

Personal Data Source
- Controller
- Joint Controller
- Direct
- Third Party
- Collector

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

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

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

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

The Personal Data Journey

(Data Flow Mapping)

Data Security

Technical and organisational security measures

Data-in-transit Protection

Separation between users

Identity & Authentication

Secure Administration

Audit Information

Data Transfer

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

EU

US

Data Source

Personal Data Source

Controller

Data Subject

Categories of Individuals

Employees

Former Employees

Successful Candidates

Unsuccessful Candidates

Personal Data

Categories of Personal Data

Contact details

Purpose of Processing

Purpose of Processing

Personnel File

Lawful Processing

Lawful Basis of Processing

Consent

Contract

Legal obligation

Vital Interests

Public Interests

Legitimate Interest

Data Recipients

Categories of Recipients

HMRC

Processor – Bank

Sub-Processor – Courier

Sub-Processor - Printer

Data Retention

Retention schedule

1 year post-employment

3 years post-employment

6 years post employment

Data (e)Discovery…

Discovery Methods

Input		Fingerprint
Fox	fingerprint function	DFCD3454 BBEA788A
The red fox jumps over the blue dog	fingerprint function	008646BB FB7DCBE2
The red fox jumps ouer the blue dog	fingerprint function	8FD87558 78514F32
The red fox jumps over the**dog blue**	fingerprint function	C1304BC6 8F8F75B3
The red fox jumps**oe**r the blue dog	fingerprint function	24C9F62C C3EFBB75

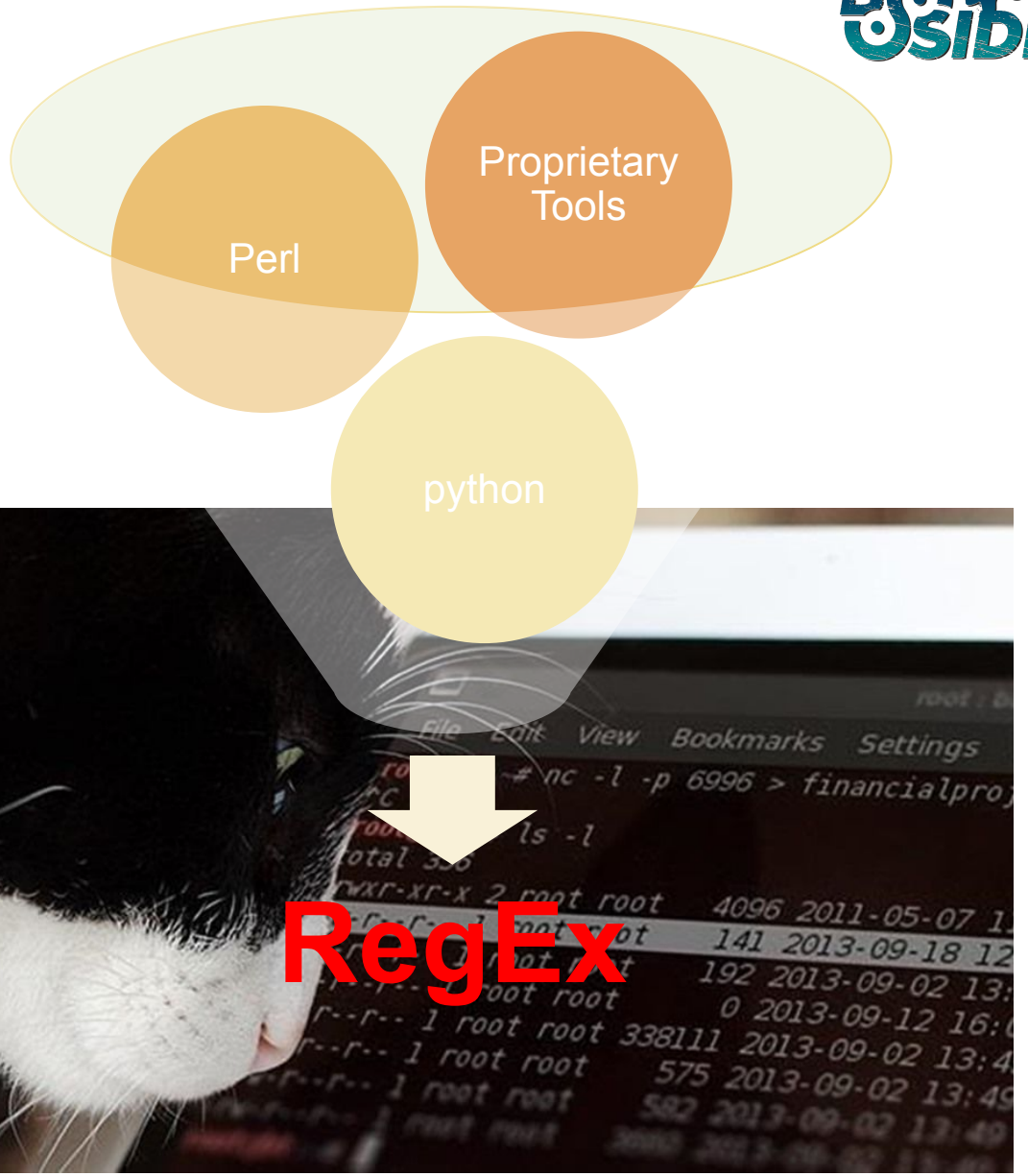
Fingerprinting

Pattern

RegEx

Finding The Data..

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



UK Passport

Format:

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}\
0?[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}
```

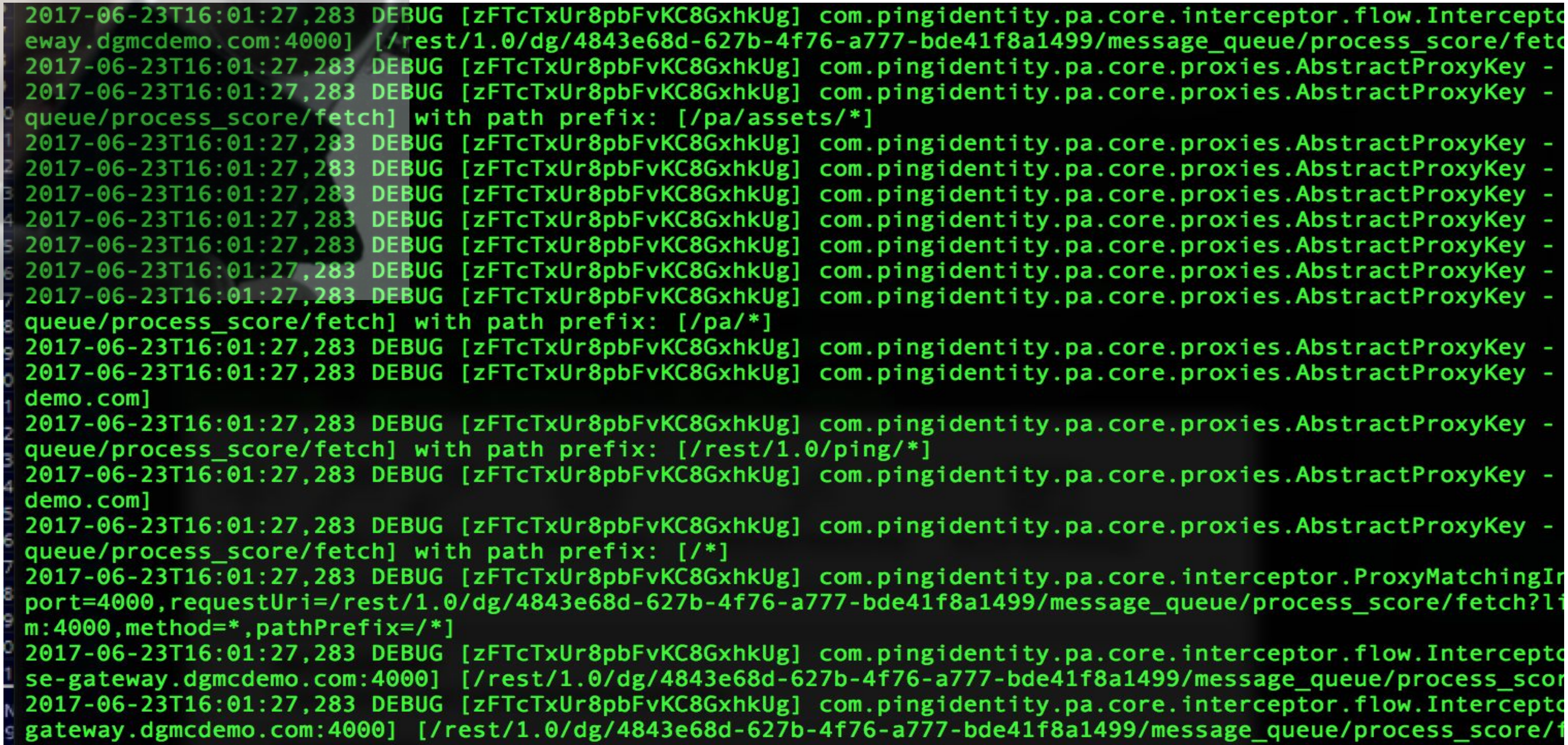
https://en.wikipedia.org/wiki/Passports_of_the_European_Union

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

Don’t Forget...


2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.interceptor.flow.Intercepto
eway.dgmcdemo.com:4000] [/rest/1.0/dg/4843e68d-627b-4f76-a777-bde41f8a1499/message_queue/process_score/fetc
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
queue/process_score/fetch] with path prefix: [/pa/assets/*]
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
queue/process_score/fetch] with path prefix: [/pa/*]
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
demo.com]
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
queue/process_score/fetch] with path prefix: [/rest/1.0/ping/*]
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
demo.com]
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.proxies.AbstractProxyKey -
queue/process_score/fetch] with path prefix: [/*]
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.interceptor.ProxyMatchingIr
port=4000,requestUri=/rest/1.0/dg/4843e68d-627b-4f76-a777-bde41f8a1499/message_queue/process_score/fetch?li
m:4000,method=*,pathPrefix=/*]
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.interceptor.flow.Intercepto
se-gateway.dgmcdemo.com:4000] [/rest/1.0/dg/4843e68d-627b-4f76-a777-bde41f8a1499/message_queue/process_scor
2017-06-23T16:01:27,283 DEBUG [zFTcTxUr8pbFvKC8GxhkUg] com.pingidentity.pa.core.interceptor.flow.Intercepto
gateway.dgmcdemo.com:4000] [/rest/1.0/dg/4843e68d-627b-4f76-a777-bde41f8a1499/message_queue/process_score/f


Identification

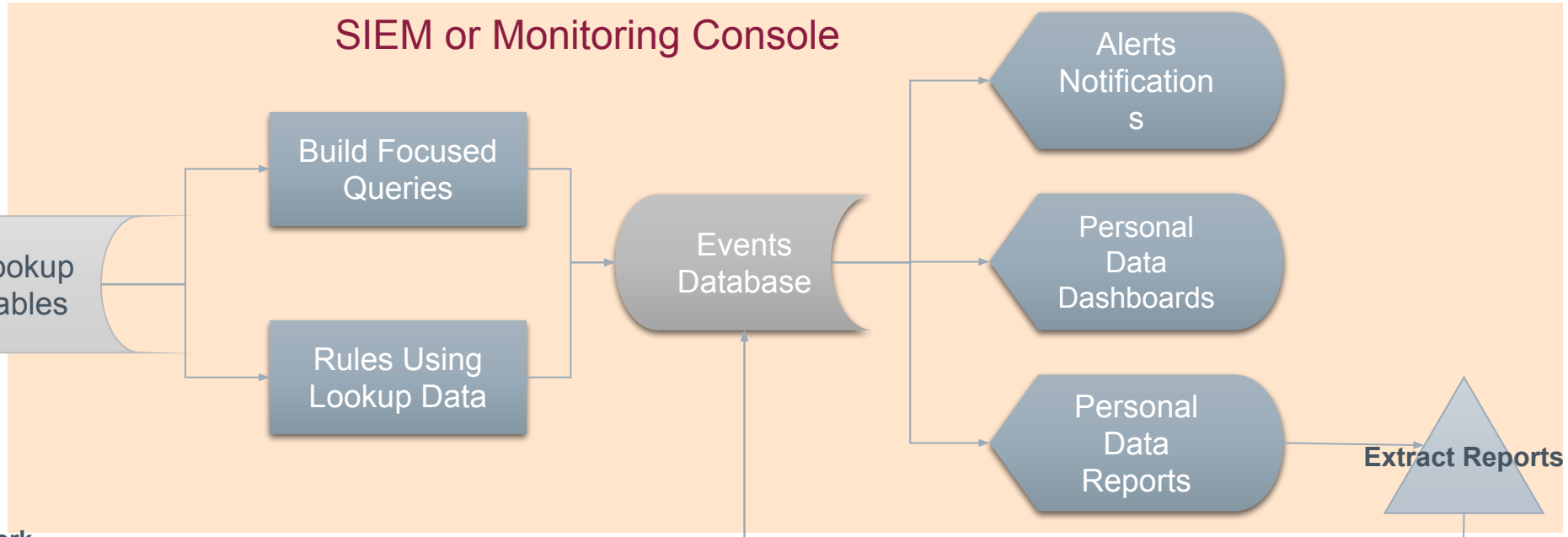
ACTIVE

- Endpoint
- Network

PASSIVE

- Discovery Data
- SOC/SIEM

Building a Data Focused Detection



Run Data Discovery

CSV Dump

Lookup Tables

Build Focused Queries

Rules Using Lookup Data

Events Database

Alerts Notifications

Personal Data Dashboards

Personal Data Reports

Extract Reports

Extract Key Personal Data locations

Extract Network Paths/Servers/Locations

Update Endpoint Rules

Update Network Rules

Personal Data Network Locations

Network Detection

Key Personal Data Paths

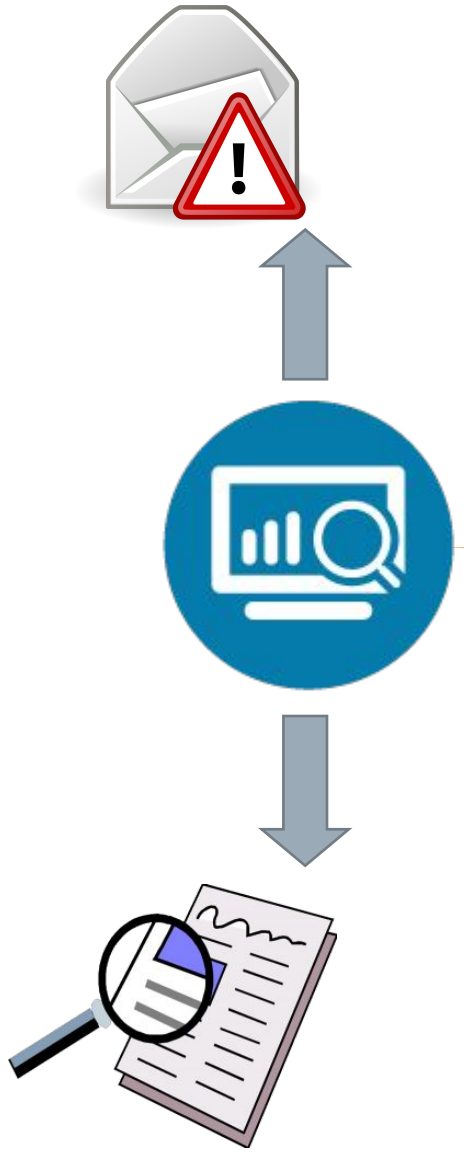
Endpoint Detection

Personal Data Breach

Forensics

Notifications

How? Let's Talk Tools



Discovery

- FreeEed.org
- McAfee
- Symantec
- Forcepoint
- Digital Guardian

Detection

- McAfee
- Symantec
- Forcepoint
- Digital Guardian
- Sysmon (with some work – evtid 2/11/15)
- WMI + Sysmon
- CASB
- Next Gen Products

Enable your Audit Daemons

- Windows
- Set auditing via UI or GPO

  `Local Policies > Audit Policy > Audit Object Access`

- Capture EventLog

Event ID	Name	Description	Data It Provides
4656	A handle to an object was requested	Logs the start of every file activity but does not guarantee that it succeeded	The name of the file
4663	An attempt was made to access an object	Logs the specific micro operations performed as part of the activity	What exactly was done
4660	An object was deleted	Logs a delete operation	The only way to verify an activity is actually a delete
4658	The handle to an object was closed	Logs the end of a file activity	How much time it took

Augment your Existing Log/SIEM

- Feed your SIEM
  - Endpoint detection too
- 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

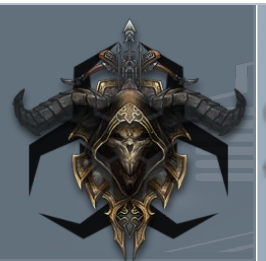
- Data Processing Context
- Ease of Identification
- Circumstances of Breach

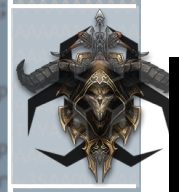
ENISA Personal Data Breach
Severity Assessment Methodology

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.).

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

Final Thoughts





BOSIDES CYPRUS

GDPArrrrr: Using Privacy Laws to Steal Identities

James Pavur

DPhil Student & Rhodes Scholar at Oxford University

Cybersecurity Center for Doctoral Training

What About Non-Breach Events?

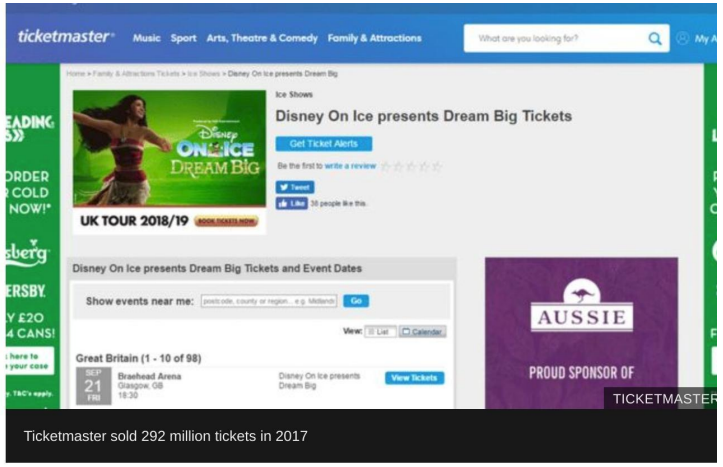
- Subject Access Requests (SARs) are exploitable
- Where else?

Data Breaches are Here to Stay

About 28% of organisation are not ready of the GDPR (survey)

1 in 6 Business unprepared for a Data Breach

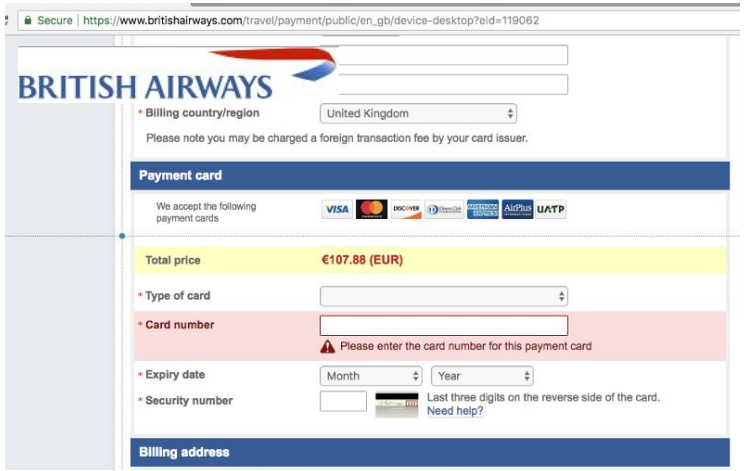
340m individual records publicly accessible server 2 terabytes of data



Ticketmaster sold 292 million tickets in 2017

Ticketmaster has admitted that it has suffered a security breach, which the BBC understands has affected up to 40,000 UK customers.

Malicious software on third-party customer support product Inbenta Technologies caused the hack, the firm said on Twitter.



According to BA, the stolen data did not include travel or passport information. It does, however, appear to have included the personal and financial details of those booking travel via the BA website and mobile app during the affected period. As many as 380,000 payment cards were exposed to the intruders.


;--have i been pwned?
You've been pwned!
You signed up for notifications when your account was pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:
Email found:
tvfischer@gmail.com
Breach:
HauteLook
Date of breach:
28,510,459
Number of accounts:
Dates of birth, Email addresses, Names, Passwords
locations, Names, Passwords
You've been pwned!
You signed up for notifications when your account was pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:
Email found:
tvfischer@gmail.com
Breach:
ShareThis
Date of breach:
9 Jul 2018
Number of accounts:
40,960,499
Compromised data:
Dates of birth, Email addresses, Names, Passwords
In July 2018, the social bookmarking and
I have never been to these sites???

"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
› tvfischer@pm.me
› keybase.io/fvt