Don’t Ignore the GDPR; It Matters Now!
Thomas V. Fischer
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 your organisation.
“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 72 hours of discovery > to customers and DPA
Penalties

The maximum fine is €10 million. It doesn’t require the data processor/controller to stop processing. It is only fined once and applies to data controllers and processors.

Administrative fines should be “effective, proportionate and dissuasive.”

- €10 million or 2% worldwide annual turnover
- €20 million or 4% worldwide annual turnover

Both cases ‘whichever is higher.’
Breach Notification

72 hours 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

72 hours 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

• 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
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 organizations or their users.

The supporting assets used to store the data have different levels of vulnerabilities towards feared events such as illegitimate access, 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, such 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 likelihood 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.

PIA
An overview of the requirements and methodology

- Evaluation / Scoping
- Automated decision-making
- Systematic monitoring
- Sensitive data
- Large scale
- Matched datasets
- Vulnerable data subjects
- New technology
- Prevent data subject from exercising a right

It is first essential to identify the processing’s features

The processing meets several criteria and is likely to present high risk to the rights and freedoms of data subjects

A developed risk assessment is then necessary

It starts with the study of the processing’s context

Potential impacts
- e.g. lung cancer

Data
- e.g. elaboration

Risk sources
- e.g. cyber criminals

Severity

Likelihood

Follows the evaluation of each risk (involvement, data category, data subject) on the rights and freedoms of data subjects

Supported assets
- e.g. servers

There are high residual risks and no additional measures are considered.

It is mandatory to consult the data protection authority.

There are any high residual risks?
To address those risks, appropriate technical and organisational measures must be implemented.

There are low residual risks.
The processing can be carried out.

With the data, it is possible to deduce the users’ residential address and know when the homes are vacant. Several houses are then burglarised.

Question is, how to avoid this situation?

The collected data are sent on remote servers.

The servers are hacked by a criminal organisation and data are accessed.

Let’s imagine an innovative service relying on its users’ geolocation.

The service is released on the market and widely adopted by users.
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.”
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?

- Name
- DoB
- Gender
- Religious beliefs
- Location data
- Genetic Data
- Photos/Videos
- Political Opinion
- Fingerprints
- Demographic
- ID Number
- Ethnicity
- Trade union
- App Data
- Cameras
- License Plate
- Blackbox
- Credit rating
- Transactions
- Mortgage
- Credit Card
- Loans
- Taxes
- IoT
- Smart devices
- CCTV
- Address
- MAC Address
- IP Address
- Cookies
- E-Mail
- Social Network
- Behavioural
- References
- Work history
- Vetting
- Education
- Access log
- Contacts
- Salary
- ANPR
- Behaviour
- Health
- Tracking
- Comms
- Contacts
- IMEI
- Physical/Mental health
- Disability
- Blood type
- Drug test
- Genetics
- DNA
- Address
- IoT
- Smart devices
- CCTV
- App Data
- Cameras
- License Plate
- Blackbox
- Credit rating
- Transactions
- Mortgage
- Credit Card
- Loans
- Taxes
- Political Opinion
- Religious beliefs
- Location data
- Genetic Data
- Photos/Videos
- behavioural
- Demographic
- ID Number
- Ethnicity
- Trade union
# The Horrendous Truth

## Country Specific Non-Sensitive

<table>
<thead>
<tr>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Date of birth</td>
</tr>
<tr>
<td>Gender</td>
</tr>
<tr>
<td>Address</td>
</tr>
<tr>
<td>Post code</td>
</tr>
<tr>
<td>National ID</td>
</tr>
<tr>
<td>Passport</td>
</tr>
<tr>
<td>Drivers License</td>
</tr>
<tr>
<td>Nationality</td>
</tr>
<tr>
<td>Regional nationality</td>
</tr>
<tr>
<td>Telephone</td>
</tr>
<tr>
<td>National healthcare Identify</td>
</tr>
<tr>
<td>Bank Account IBAN</td>
</tr>
<tr>
<td>Bank account national</td>
</tr>
<tr>
<td>biometric data</td>
</tr>
<tr>
<td>fingerprints</td>
</tr>
<tr>
<td>facial recognition</td>
</tr>
<tr>
<td>retinal scans</td>
</tr>
<tr>
<td>Tax numbers</td>
</tr>
<tr>
<td>VAT</td>
</tr>
<tr>
<td>Company registration</td>
</tr>
</tbody>
</table>

## Economic
- Credit card

## Non-government Identification numbers
- Cultural identification
- Security Clearance
- Legal status

## Physical Appearance
- Photo/Headshot
- physical - height
- physical - weight
- physical - eye colour
- physical - hair colour
- physical - birth marks

## Generic No Country or language

<table>
<thead>
<tr>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Tags</td>
</tr>
<tr>
<td>IPv4</td>
</tr>
<tr>
<td>IPv6</td>
</tr>
<tr>
<td>IMEI</td>
</tr>
<tr>
<td>GPS Coordinates</td>
</tr>
<tr>
<td>Social Networks</td>
</tr>
<tr>
<td>email address</td>
</tr>
<tr>
<td>RFID tag</td>
</tr>
<tr>
<td>CCTV Footage</td>
</tr>
</tbody>
</table>
Reduce Risk Footprint
Data Minimisation
Pseudonymisation

• Only real technical suggestion!!!
• No it doesn’t mean encryption

<table>
<thead>
<tr>
<th>Name</th>
<th>Token/Pseudonym</th>
<th>Anonymized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clyde</td>
<td>qOerd</td>
<td>xxxxx</td>
</tr>
<tr>
<td>Marco</td>
<td>Loqfh</td>
<td>xxxxx</td>
</tr>
<tr>
<td>Les</td>
<td>Mcv</td>
<td>xxxxx</td>
</tr>
<tr>
<td>Les</td>
<td>Mcv</td>
<td>xxxxx</td>
</tr>
<tr>
<td>Marco</td>
<td>Loqfh</td>
<td>xxxxx</td>
</tr>
<tr>
<td>Raul</td>
<td>BhQl</td>
<td>xxxxx</td>
</tr>
<tr>
<td>Clyde</td>
<td>qOerd</td>
<td>xxxxx</td>
</tr>
</tbody>
</table>
When a Breach is not a Breach?

- Exfiltration
- Destruction
- Alteration
- Unauthorised Disclosure
- Unauthorised Access
Data Breach Handling Procedure

Preparation

Event Detection

Initial Assessment

- Is event breach?
- What are the circumstances?
- Severity of the breach (indicative)
- Identify immediate response measures

Personal Data Breach?

Preliminary Notification (DPA)

Adversely affects data subjects?

- yes
  - Preliminary Notification (Data Subjects)
- no
  - Further Assessment

- yes
  - Detailed assessment & evidence gathering
  - Detailed Notification (DPA)
- no
  - Containment & Recovery

Lessons Learnt

Data Breach Inventory

72 hours post breach detection
Handling Data Focused IR

- Preparation
- Identification
- Containment
- Eradication
- Lessons Learnt
- Recovery

Observe
Act
Orient
Decide
Handling Data Focused IR

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learnt
The Personal Data Journey
(Data Flow Mapping)

Data Source
Controller
Joint Controller
Direct
Third Party
Collector

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

Data Transfer
Names of third countries or international organisations that data is transferred to
EU
US

Data Source
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 Source
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

Lawful Processing

Data Recipients

Lawful Processing

Data Flow Mappings
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
Threat and Vulnerability Models

Adapt
- Adapt your existing Models

Assign
- Assign Personal Data related attributes

Identify
- Identify the risks

Use
- Use the DPIA

Think
- Will this Harm the Data Subject
Data (e)Discovery...
Discovery Tools

- FreeEed.org

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

- Multiple modes
Discovery Methods

**Input**
- Fox
- The red fox jumps over the blue dog
- The red fox jumps over the blue dog
- The red fox jumps over the blue dog

**Fingerprinting**
- DFCD3454 BBEA788A
- 00864BBB FB7DCBE2
- 8FD87558 78514F32
- C1304BC6 8F8F75B3
- 24C9F62C C3EFBB75

**Pattern**

**RegEx**
Finding The Data..

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

➢ Focus your detection

RegEx
UK NI (National Insurance) [A-CEGHJ-PR-TW-Z]{1}[A-CEGHJ-NPR-TW-Z]{1}[040?[0-9]{2}\{2}\{040?[0-9]{2}\}040?[a-zA-Z]{2}\{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}|[0-7]-[0-4][0-9]-[0-9][0-1][0-9]-[0-9][9]-[0-8][0-9]-[0-6][0-9]-[0-4][0-9][0-9][0-2][0-9]-[0-9]{2})$
How the F@#$ do you RegEx
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
    - Build Focused Queries
    - Rules Using Lookup Data
    - Events Database
      - Alerts Notifications
      - Personal Data Dashboards
      - Personal Data Reports
      - Extract Reports
      - Personal Data Breach
      - Forensics

- Extract Key Personal Data locations
- Extract Network Paths/Servers/Locations
- Update Endpoint Rules
- Personal Data Network Locations
- Network Detection
- Notifications
- Endpoint Detection
- Personal Data Path/Servers/Locations
- Update Network Rules
- Key Personal Data Paths

SIEM or Monitoring Console
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

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

```plaintext
<search>
<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

Final Thoughts

Thinking of skipping this section
Compliance???
Not Compliance

- Risk Management
- Cultural Shift
- Accountability
“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