RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: EZCL-W02

Lessons from GDPR Enforcement: What Security Is Appropriate?

John Elliott LLM CIPP/E CISSP CISA CRISC FBCS

Data Protection Specialist

@withoutfire

Two disclaimers

1v0

Nothing in this presentation represents the views of my employer.

This presentation is not intended to be legal advice but a general discussion about the General Data Protection Regulation.
If you require legal advice you are advised to consult a qualified lawyer in your jurisdiction.

Cooperative Learning in the Engagement Zone

- This is a new experience for all of us

- I’m going to talk about GDPR and regulatory action for about 12 minutes
- We’ll then have a short Q&A
- There’s an interesting case study
- Then we’ll wrap up

RSAConference2020

GDPR Essentials

Four Pillars of GDPR

Principles & Definitions	People's Rights	Organization's Responsibilities	Enforcement & Administration
1 - 12	13 - 23	24 - 42	50 - 99
	43 - 49		

Principles. Personal data shall be ….

- Processed lawfully, fairly and transparent
- Used just for the purposes collected
- Minimised – so just the minimum data needed for an activity
- Accurate
- Deleted when no longer necessary
- **Kept securely**

People's Rights

- Be informed of what will be done with their data
  - "privacy notice"
- Have a copy of it if requested
  - And in a structured format
- Fix errors
- Erasure (the right to be forgotten)
- Stop certain types of processing

Organization's Obligations

- Be accountable
- Protection by design and default
- Manage third-parties
- Document processing activities
- **Keep data secure**
- Breach notification
- Impact assessments
- Don't send data to unsafe countries

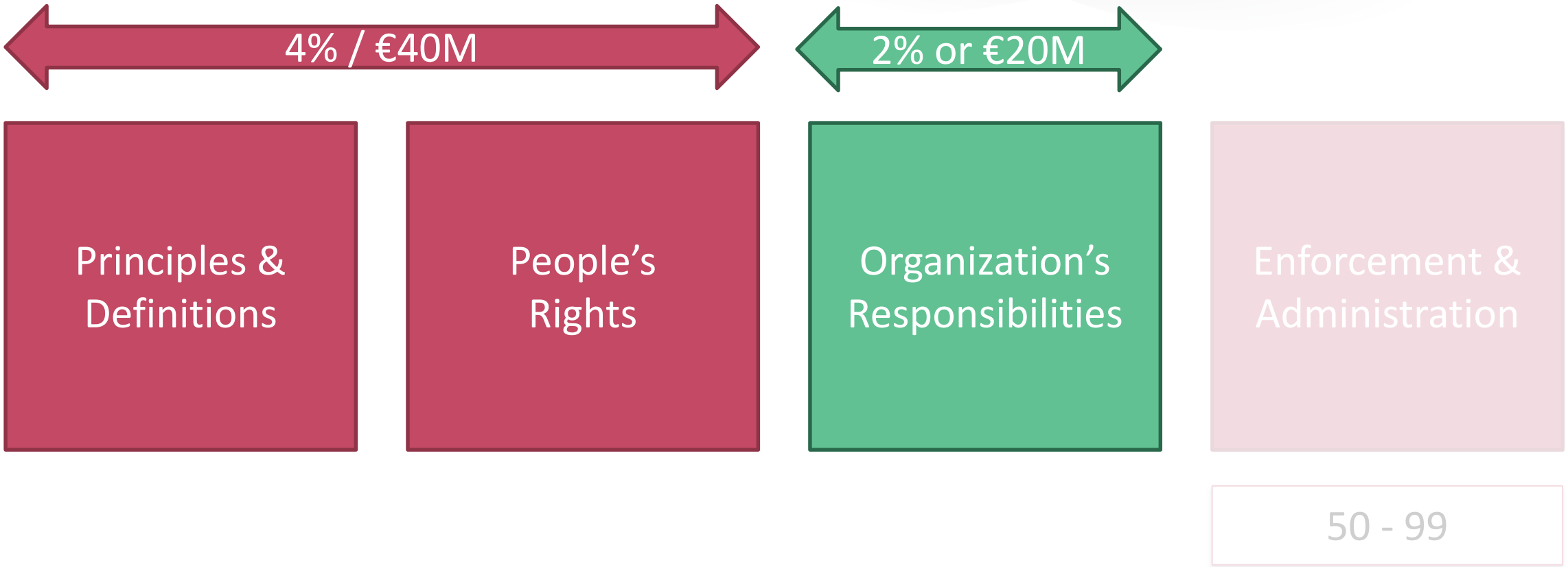
Enforcement 4% of global turnover or €20 million

Principles & Definitions	People's Rights	Organization's Responsibilities	Enforcement & Administration
1 - 12	13 - 23	24 - 49	50 - 99
	43 - 49		

Enforcement 2% of global turnover or €10 million

Principles & Definitions	People's Rights	Organization's Responsibilities	Enforcement & Administration
1 - 12	13 - 23	24 - 49	50 - 99
	43 - 49		

Enforcement Reflects Importance



Article 5(1)(f): the security principle

- Personal Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 32(1) – the security obligation

- 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 …

Penalties …

Article 83(9)

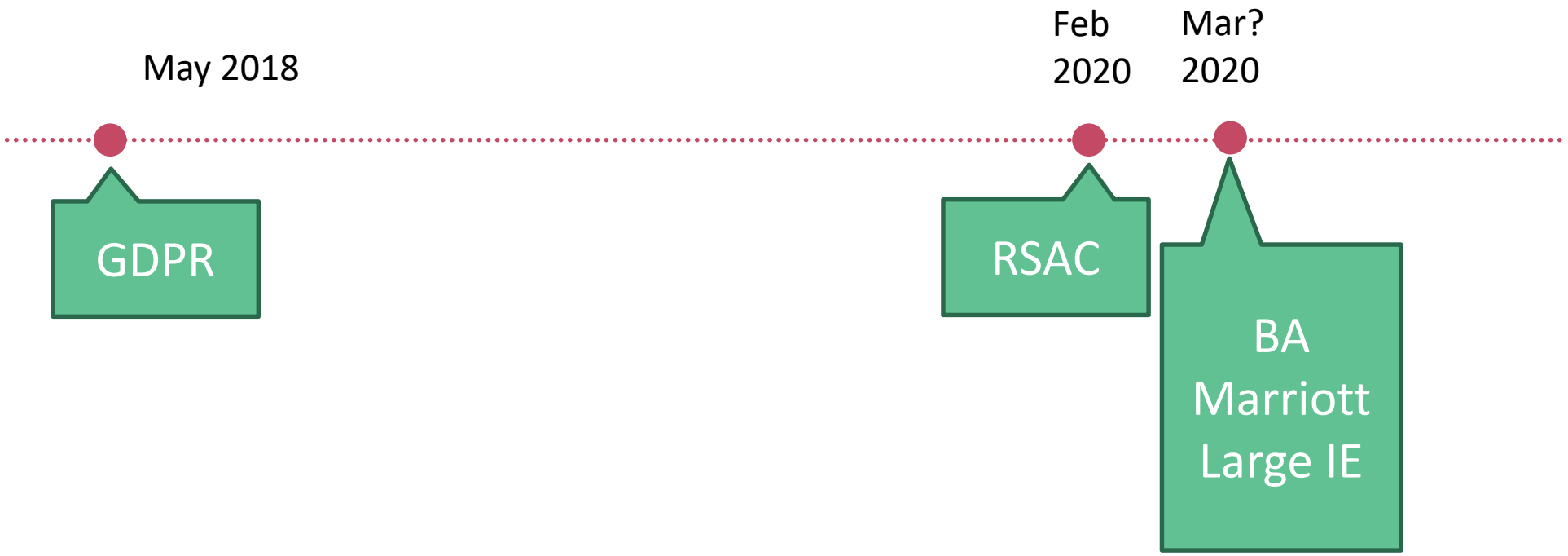
… the fines imposed shall be effective, proportionate and dissuasive.

RSAConference2020

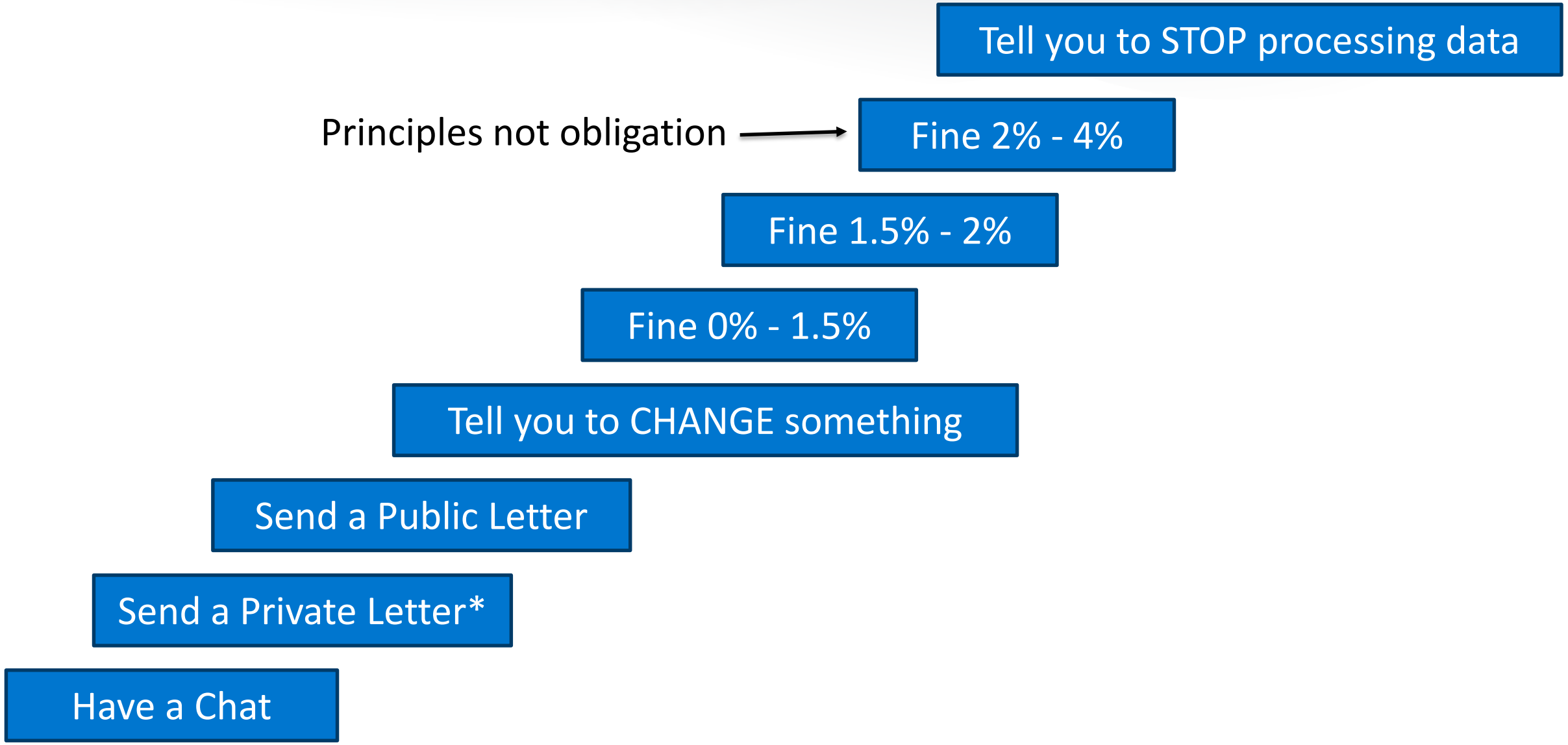
What's appropriate

Firstly what's your regulatory risk appetite?

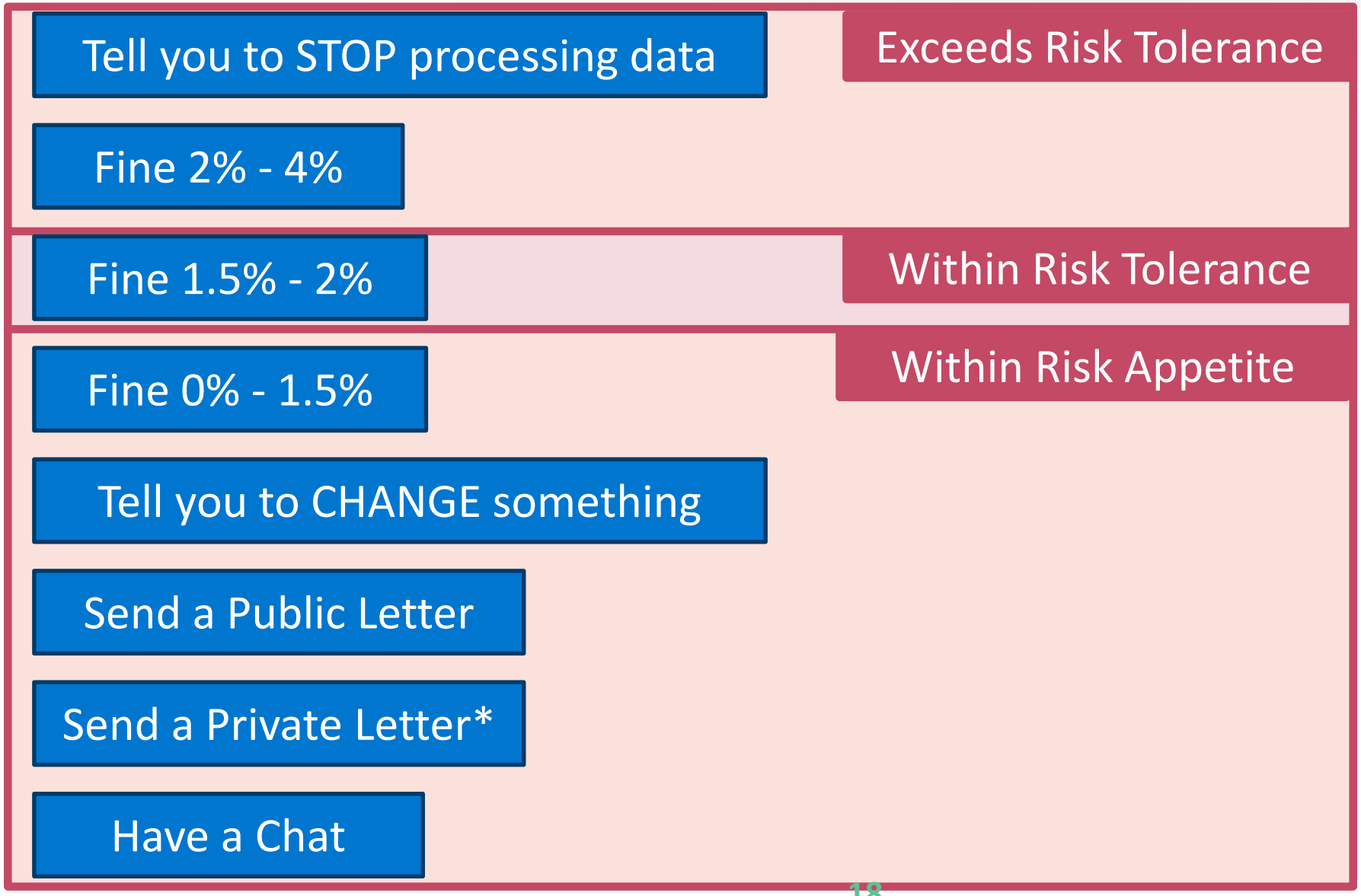
A Note of Caution



What is Enforcement?



What's your risk

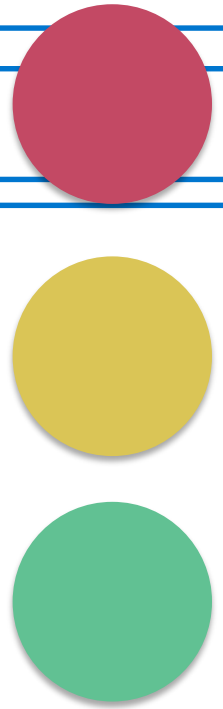


Causes

Ignored previous, ongoing harms	Tell you to STOP processing data
Deliberate, wilful avoidance	Fine 2% - 4%
Negligence	Fine 1.5% - 2%
Inappropriate	Fine 0% - 1.5%
Individual bad practices that are easy to resolve	Tell you to CHANGE something
	Send a Public Letter
Accidents & Mistakes	Send a Private Letter*
	Have a Chat

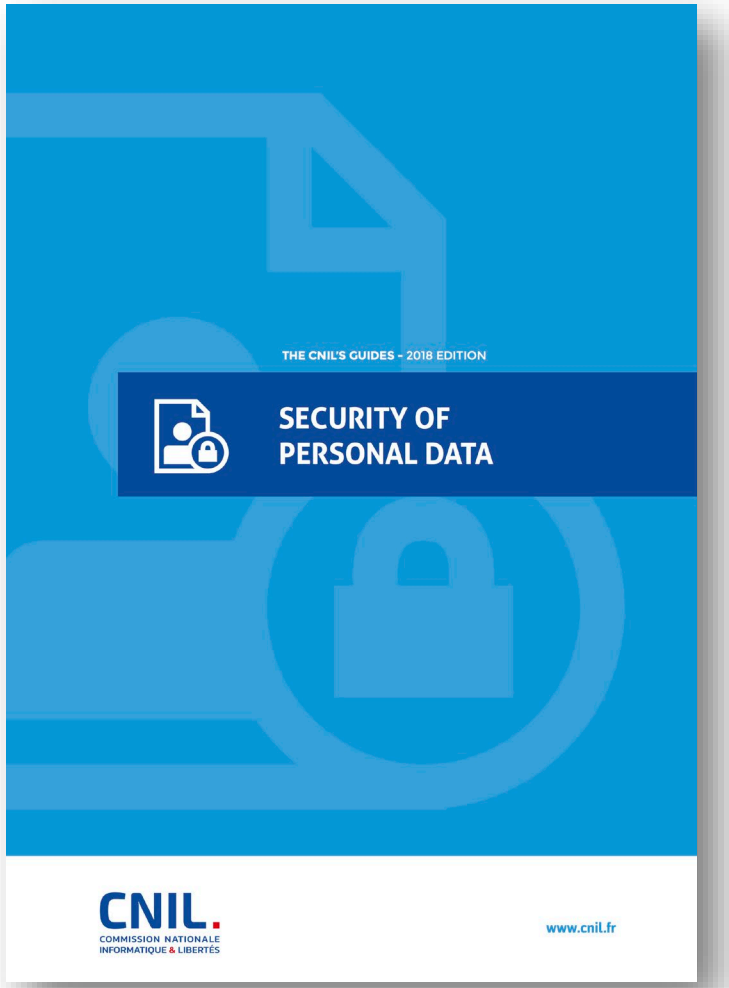
Causes

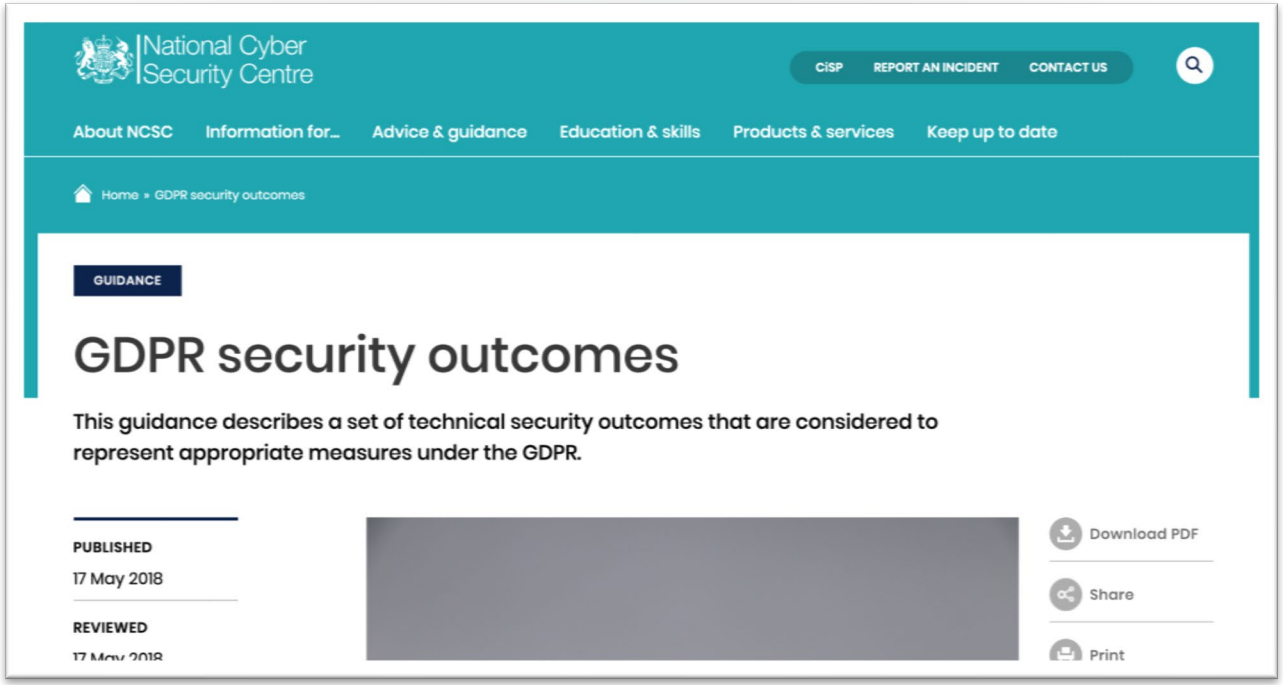
Ignored previous, ongoing harms	Tell you to STOP processing data
Deliberate, wilful avoidance	Fine 2% - 4%
Negligence	Fine 1.5% - 2%
Inappropriate	Fine 0% - 1.5%
Appropriate	Tell you to CHANGE something
	Send a Public Letter
	Send a Private Letter*
	Have a Chat



Sources of appropriateness

Sources of published appropriateness





RSAConference2020

Some enforcement action

UVW (Insurance Company)

Inappropriate

Regulator	Netherlands
When	October 2019
Amount	€900,000
Why	Inappropriate security
Details	Lack of multi-factor authentication (MFA) protecting access to health data(i.e. special category personal data) by employees.

MisterTango UAB

Inappropriate

Regulator	Lithuania
When	May 2019
Amount	€ 61,500
Why	Excessive data collection, excessive retention, inappropriate security, failure to notify
Details	Payment company that also collected lots of additional information (probably via JavaScript click-stream type analysis) not relevant to the transaction. Data retained for 216 days, not 10 minutes. Payments made public for 2 days, 9,000 people's data exposed "One person in IT"

Bergen Municipality for a School

Inappropriate

Regulator	Norway
When	March 2019
Amount	€170,000 (NOK 1.6 million)
Why	Inappropriate security
Details	Login system to a school's management system could easily be bypassed, data exposed of 35,000 people, mostly children.

Hungarian Democratic Coalition

Inappropriate

Regulator	Hungary
When	March 2019
Amount	€35,000 (HUF 11 million)
Why	Inappropriate security, failure to notify data subjects or the regulator
Details	Personal data of 6,000 party members hacked via SQL injection attack (yes, still in 2019). Passwords were MD5 hashed.

ID Design (Furniture company)

Inappropriate

Regulator	Denmark
When	June 2019
Amount	€200,000 (DKK 1.5 million)
Why	Failure to delete old data
Details	After a system upgrade, old data was never deleted

Deutsche Wohnen

Ignored previous, ongoing harms

Regulator	Berlin (Germany)
When	November 2019
Amount	€14.5 million
Why	Storage of data past retention
Details	After being told by the regulator some 18 months ago that the archive system used for tenant references was incompatible with the GDPR, the company disregarded the regulator's instructions.

Doorstep Dispensaree

Negligence

Regulator	United Kingdom
When	December 2019
Amount	€327,000 (£275,000)
Why	Excessive Storage Inappropriate Security
Details	Paper healthcare records were stored in insecure areas, subject to physical damage. Records retained much longer than necessary.

British Airways

Negligence (probably)

Regulator	United Kingdom
When	Not yet …
Amount	€220 million (£187 million) = 1.5% turnover
Why	Inappropriate security
Details	Criminals installed web skimming (Magecart) on the BA website and took payment card data. Subsequent forensic analysis discovered widespread data compromise. It has been reported that BA was not compliant with PCI DSS at the time of the incident.

Marriott Hotels

Negligence

Regulator	United Kingdom
When	Not yet …
Amount	€118 million
Why	Inappropriate security
Details	In the course of the acquisition of Starwood (2016), insufficient due diligence was done (it seems Starwoord's systems were compromised in 2014 by HNS actors who were still active in 2018 at the time of the merger).

What can we determine

- There isn’t yet any consistency of penalties
- Generally, more penalties have been for violations of principles:
  - No legal basis for processing
  - Processing beyond the reason the data was collected
  - Retaining data for far too long
- The security breaches are obvious and clear
  - Unarguable that there was a breach
  - Size of the penalty hard to determine
- There isn’t good experience yet of when a security breach is principles rather than obligations

RSAConference2020

Case Study

Work in your tables

- IT want to decommission unsupported (unpatchable) SharePoint and the underlying server OS by migrating to cloud-based O365
- A SharePoint site contains c500K poorly indexed HR documents
  - Scans of every type of employee-related document you can think of:
  - Held way beyond retention policy (agreed with workers' councils) potentially contravening other employment laws
  - Much of the data relates to ex-employees
- Although O365 is linked to Active Directory, only single factor authentication (username / password) is currently supported.

Who wants what?

- IT want to migrate all data to O365 as soon as possible
  - They argue that O365 is much more secure than the internal systems and they can't guarantee the security of the system
- Information Security want to wait for six months until MFA is implemented
  - Which also has the advantage that some 25% of records will have been deleted (HR predict 2 years for full data deletion)
- The Data Protection Officer wants all data past retention to be deleted before migration – ie wait two years

RSAConference2020

Wrap-up

What should you do?

- Work out your organization's risk appetite and tolerance
  - And how comfortable you are with second guessing the regulators' view of what's *appropriate*
- Document where you're aiming for
- Read decisions from the 27/28 regulators as they are published Did anything surprise you?
  - Also good to document

References

- CMS Enforcement Tracker
  - https://www.enforcementtracker.com/
- NOYB
  - https://gdprhub.eu/
- European Data Protection Board
  - https://edpb.europa.eu/news/national-news_en
- NCSC Guidance
  - https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes
- CNIL Guide
  - https://www.cnil.fr/en/new-guide-regarding-security-personal-data