RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: GRC-W03R

GDPR:
How to Work Out If Your Security Is “Appropriate” (Repeat)

John Elliott **LLM CIPP/E CISSP CISA CRISC FBCS**

Data Protection Specialist

@withoutfire

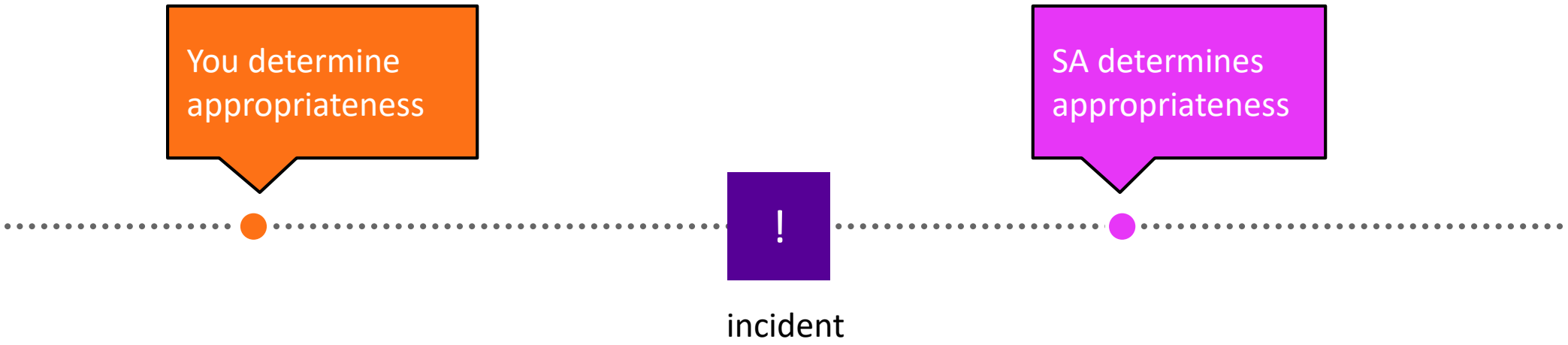
Two disclaimers

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.

The real title of the presentation

How to work out what a national supervisory authority or a court would take into account when determining whether your security was “Appropriate”


You determine appropriateness
SA determines appropriateness
!
incident

National Supervisory Authority (!=NSA)

- UK: Information Commissioner’s Office: ICO
- FR: Commission Nationale de l'Informatique et des Libertés: CNIL
- IE: Data Protection Commission
- NL: Autoriteit Persoonsgegevens

+ 24 others

https://edpb.europa.eu/about-edpb/board/members_en

When would this happen?

As part of an audit by a supervisory authority

Something bad happened

Our tools to help determine what's appropriate

Analyze the words of the law	Look at regulatory advice and regulatory action	Case history and common law	Informed risk assessment

Article 32

"Taking into account
the state of the art,
the costs of implementation
and the nature, scope, context and purposes
of processing …"

Article 32

"… as well as
the risk of varying likelihood and severity for
the rights and freedoms of
natural persons …"

Article 32

"… the controller and the processor shall implement …"

Article 32

"… appropriate technical and organisational measures to ensure a level of security appropriate to the risk."

Article 32

"… appropriate
technical and organisational measures to
ensure a level of security
appropriate to the risk."

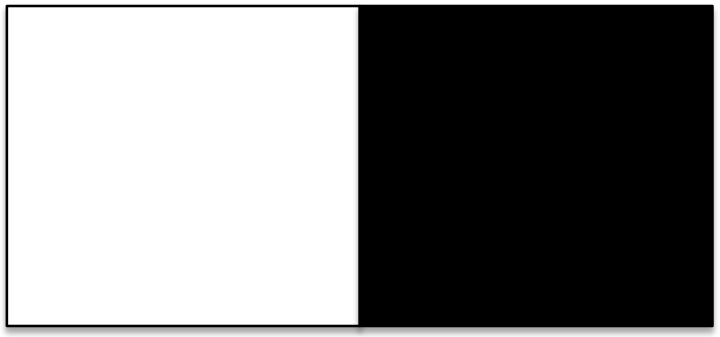
RSAConference2019

Warning: Law turbulence ahead

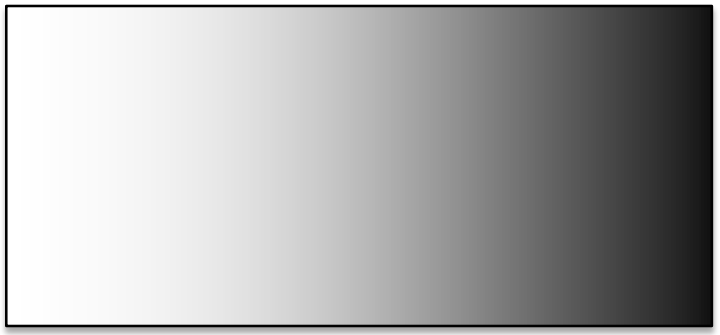
Fasten your seatbelt

Law is non-binary

technology



law



Administration of Estates Act

The residuary estate of an intestate shall be distributed in the manner .. mentioned in this section, namely:

If the intestate leaves issue but no spouse or civil partner, the residuary estate of the intestate shall be held on the statutory trusts for the issue of the intestate

s46(ii) Administration of Estates Act 1925

Administration of Estates Act

Money left over after someone dies without a will shall be distributed like this:

If the dead person has kids, but no spouse or civil partner, the money goes to the kids

s46(ii) Administration of Estates Act 1925

Re: Sigsworth

- Mary Ann Sigsworth died intestate and a widower
- She had one son, Thomas Sigsworth …
  - Q: Should Thomas inherit?
- … who murdered his mother

You decide

- GRC-W03R
- Should Thomas Sigsworth inherit?
  - A: Yes (it's what the law says)
  - B: No (that would be insane, and not good for mothers generally)

- https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3865

Re: Sigsworth

- Mary Ann Sigsworth died intestate and a widower
- She had one son, Thomas Sigsworth …
  - Q: Should Thomas inherit?
- … who murdered his mother
  - Q: Should Thomas inherit?

Thomas Sigsworth could not inherit.

Licensing act

- Every person who is drunk while in charge on any highway or other public place of any carriage, horse, cattle, or steam engine, or who is drunk when in possession of any loaded firearms, shall be liable to a penalty …, or in the discretion of the court to imprisonment for any term not exceeding one month.

s12 Licensing Act 1872

Corkery v Carpenter

- Shane Corkery was arrested for being drunk in charge of a bicycle on the highway
- It was argued that a bicycle was not a carriage

It won't be a stylish marriage,
I can't afford a carriage,
But you'll look sweet, upon the seat
Of a bicycle made for two.

You decide

- GRC-W03R
- Is being drunk in charge of a bicycle a crime?
  - A: Yes (it is what the law means)
  - B: No (it is not what the law says)

- https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3866

Transfer of Undertakings (Protection of Employment)

- "to provide for the protection of employees in the event of a change of employer, in particular, to ensure that their rights are safeguarded . . ."
- *Any reference. . . above to a person employed in an undertaking or part of one transferred by a relevant transfer is a reference to a person so employed immediately before the transfer…*
  S5(3) TUPE

Litster v Forth Dry Dock and Engineering

- Employees (unfairly) terminated at 15:30
- Business sold at 16:30
- Employees therefore not employed immediately before the transfer

You decide

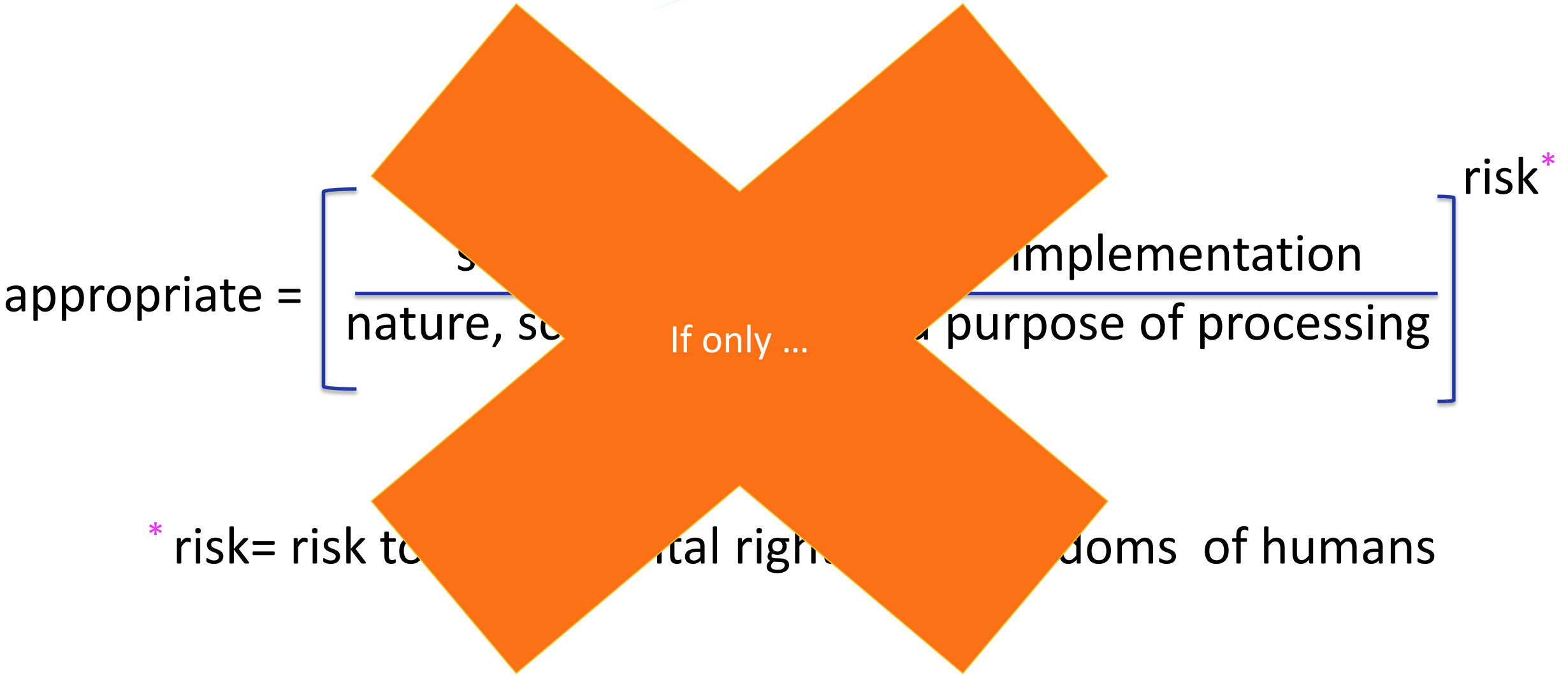
- GRC-W03R
- Should the employees' rights be protected?
  - A: Yes (it is what the law intends)
  - B: No (it is not what the law says)

- https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3867

Litster v Forth Dry Dock and Engineering

- Employees (unfairly) terminated at 15:30
- Business sold at 16:30
- Employees therefore not employed immediately before the transfer

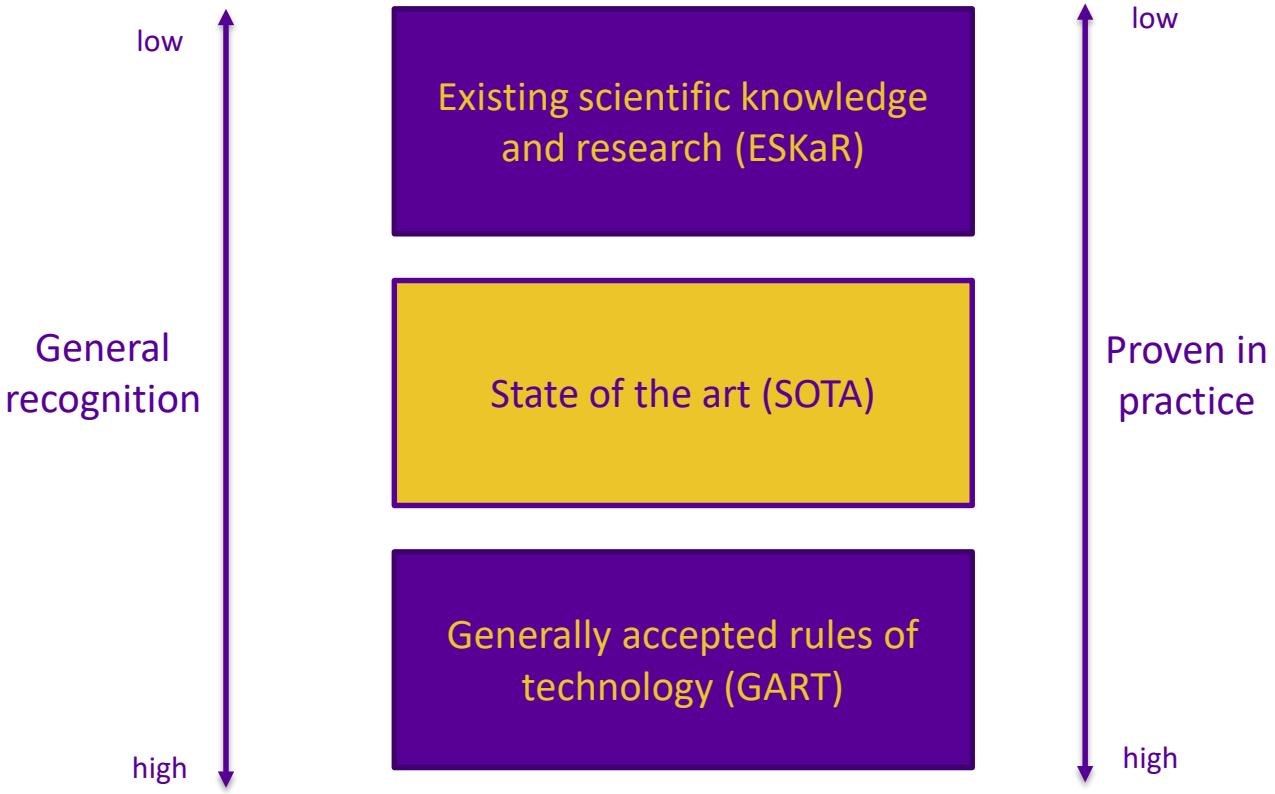
Read as:
"employed immediately before the transfer or would have been so employed if he had not been unfairly dismissed"

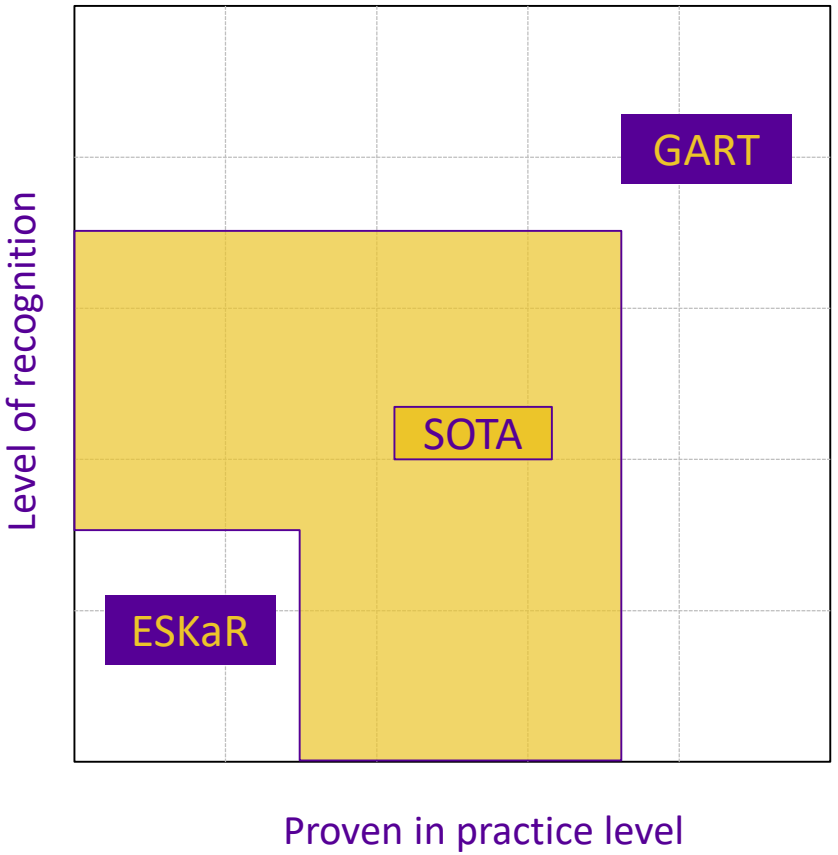

appropriate =
risk*
implementation
purpose of processing
If only …
* risk= risk to
ital right
doms of humans

State of the art guidance

https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

State of the art





“Costs of implementation”

TJ Hooper

Barges pulled by tug boat sank in a storm

Tug boat had no radio to hear storm warning.
Some tugboats had radios.

Question: Should the tug boat have had a radio?

The T. J. Hooper, 60 F.2d 737, 1932 U.S. App. LEXIS 2592 (2d Cir. N.Y. July 21, 1932)

"One line alone did it; as for the rest, they relied upon their crews, so far as they can be said to have relied at all.

An adequate receiving set suitable for a coastwise tug **can now be got at small cost** and is reasonably reliable if kept up; obviously it is a source of great protection to their tows."

Judge Learned Hand

"But here there was no custom at all as to receiving sets; some had them, some did not; the most that can be urged is that **they had not yet become general**. Certainly in such a case we need not pause; **when some have thought a device necessary, at least we may say that they were right, and the others too slack**."

Judge Learned Hand

“Nature, scope and context of processing”

Nature
(what)

Scope
(how much,
what types)

Context
(why)

Nature, scope and context: aka risk

- What personal data?
- How sensitive?
- Is it special category?
- How much?
- What's the risk to the individual associated with a breach of:
  - Confidentiality?
  - Integrity?
  - Availability?

RSAConference2019

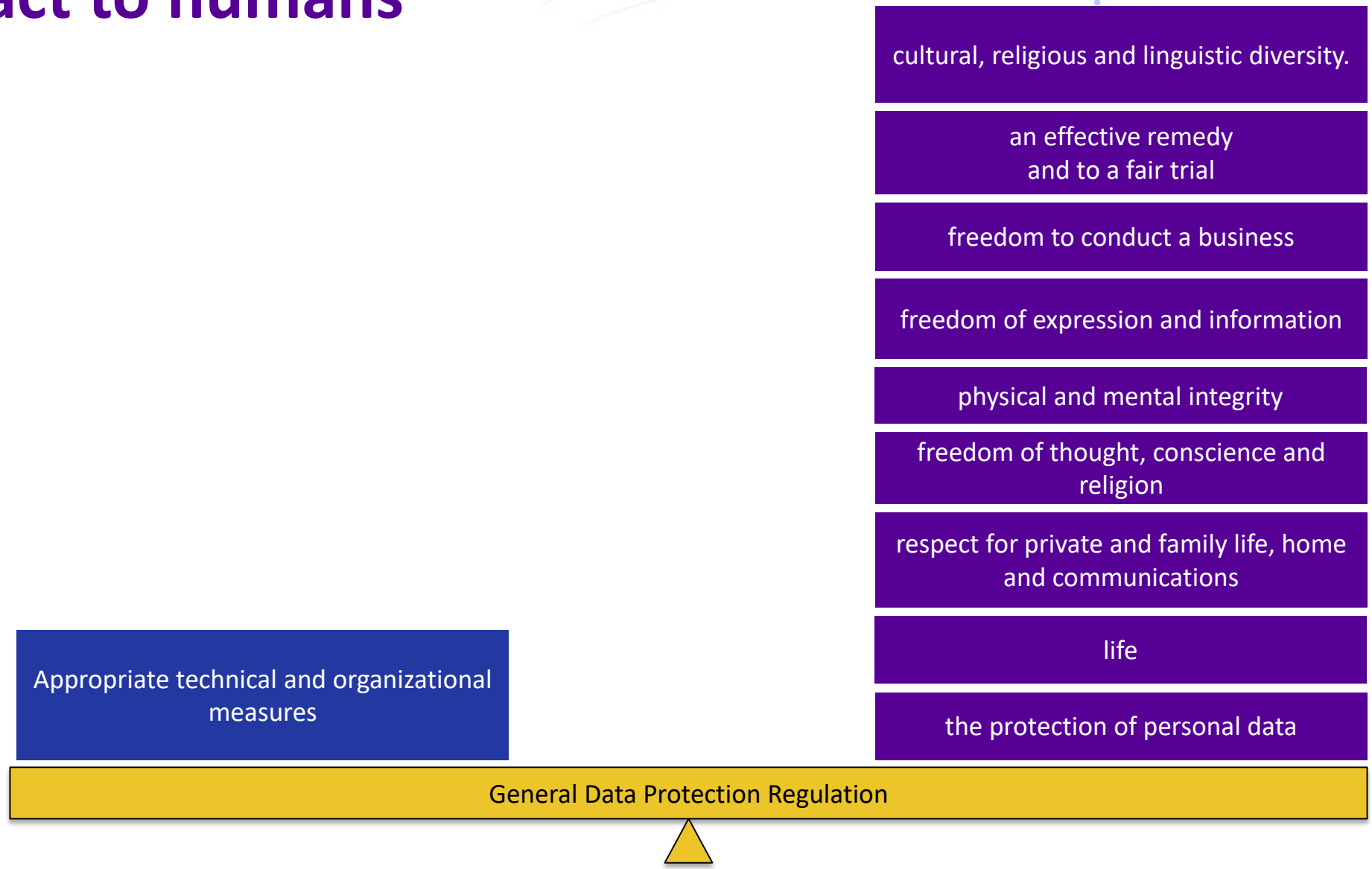
How GDPR thinks of risk

(It’s not how we think about risk)

Risk Calculation

Probability	x	People Impact	=	Risk
1. Unlikely		1. ????		
2. Possible		2. ????		
3. Likely		3. ????		
4. Probable		4. ????		
5. Certain		5. ????		

Impact to humans



Impact to Individuals

Breach of confidentiality, integrity or availability of personal data resulting in …

	1 - Minor	2 - Low	3 - Medium	4 - High	5 - Critical
Privacy	Disclosure of address / contact information	Limited disclosure of financial or special category data	Theft of identity / criminal use of identity	Irretrievable control over data that the data subject would consider sensitive	Life changing damage to career, personal life or reputation

Impact to Individuals

Breach of confidentiality, integrity or availability of personal data resulting in …

	1 - Minor	2 - Low	3 - Medium	4 - High	5 - Critical
Financial	Financial loss up to €100	Financial loss up to €1,000	Financial loss between €1K and €5K	Financial loss up to €10K	Loss of assets, financial loss over €10K

Impact to Individuals

Breach of confidentiality, integrity or availability of personal data resulting in …

	1 - Minor	2 - Low	3 - Medium	4 - High	5 - Critical
Mental integrity	Short-term (day/ few days) stress	Worry, anxiety Temporary effects on mental state	Medium term effects on mental state (< 1 year)	Long term effects on mental state (> 1 year)	Permanent effects on mental state
Physical integrity	Physical discomfort	Hospital outpatient required	Hospital in patient required	Chronic condition	Death or life changing injury

Impact to Individuals

Breach of confidentiality, integrity or availability of personal data resulting in …

	1 - Minor	2 - Low	3 - Medium	4 - High	5 - Critical
Employment	Worry about discrimination in role	Discrimination in role	Significant discrimination in role	Loss of employment	Loss of employment/ inability to secure next role

Risk Calculation

Probability	x	Impact	=	Risk

1. Unlikely
2. Possible
3. Likely
4. Probable
5. Certain

1. Minor
2. Low
3. Medium
4. High
5. Critical

Risk Calculation

Probability	x	Impact	x	Volume	=	Per-system Risk
1. Unlikely 2. Possible 3. Likely 4. Probable 5. Certain		1. Minor 2. Low 3. Medium 4. High 5. Critical		Number of Humans		Population Risk Score

Population Risk

System / Application	Population Risk
System A	958,000,000
System B	623,000,000
System C	432,000,000
System D	281,000,000
System E	178,100,000
System F	178,000,000
System G	178,000,000
System H	80,000,000

Above baseline
Require additional
Protection

Baseline risk

Population Risk

System / Application	Population Risk
System A	958,000,000
System B	623,000,000
System C	432,000,000
System D	281,000,000
System E	178,100,000
System F	178,000,000
System G	178,000,000
System H	80,000,000

Above hygiene

Hygiene

http://withoutfire.com/2018/01/privacy-risk-workshop/

What is a good baseline?

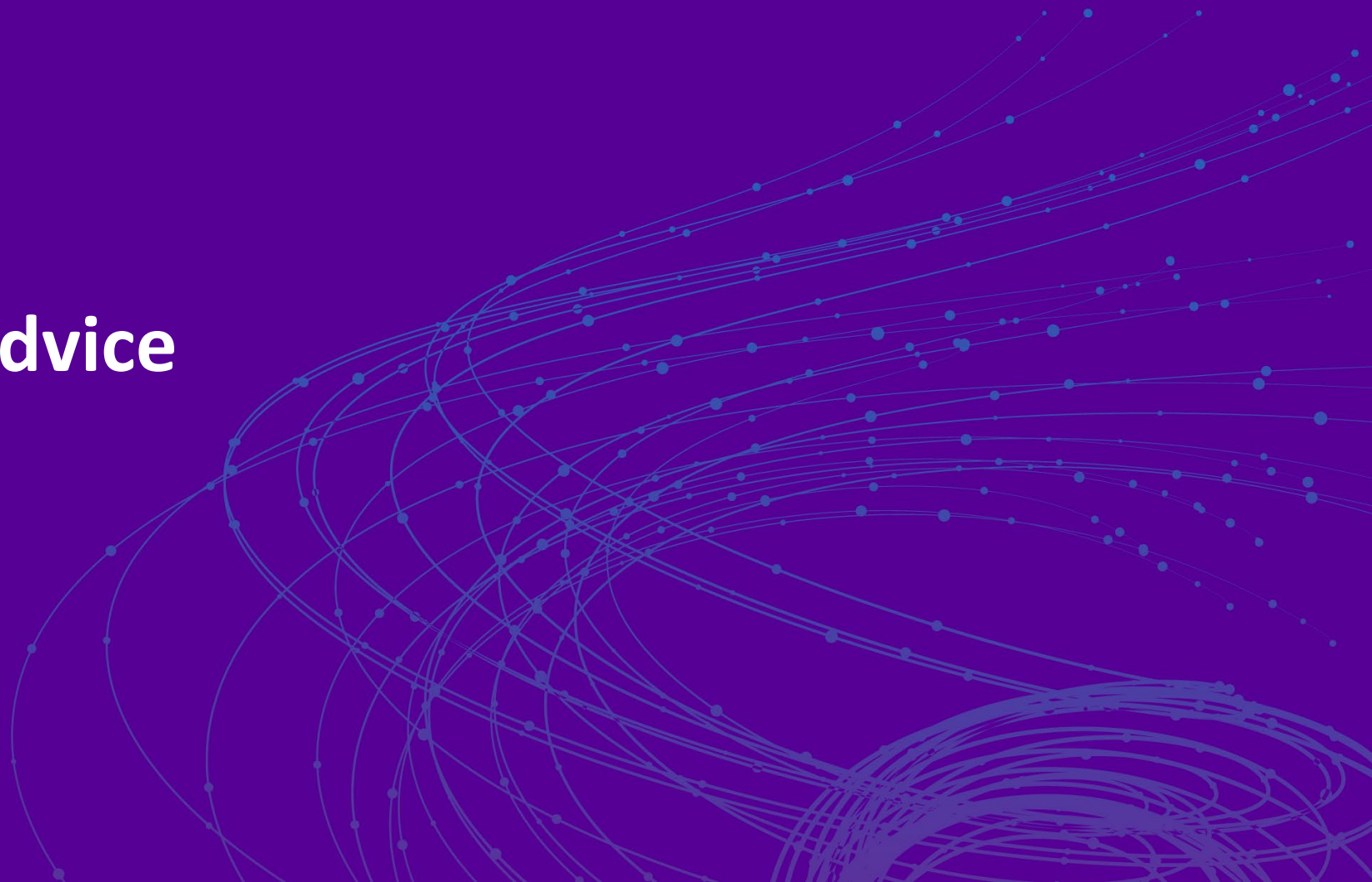
- Aligned with peers
- Documented and rationalized
- Published standards
  - ISO 27001
  - Cyber Essentials Plus
  - NIST
  - CIS 20 critical
  - PCI DSS (if you have card data)

Where are we?

Analyze the words of the law	Look at regulatory advice and regulatory action	Case history and common law	Informed risk assessment

RSAConference2019

Regulatory advice



Guidance

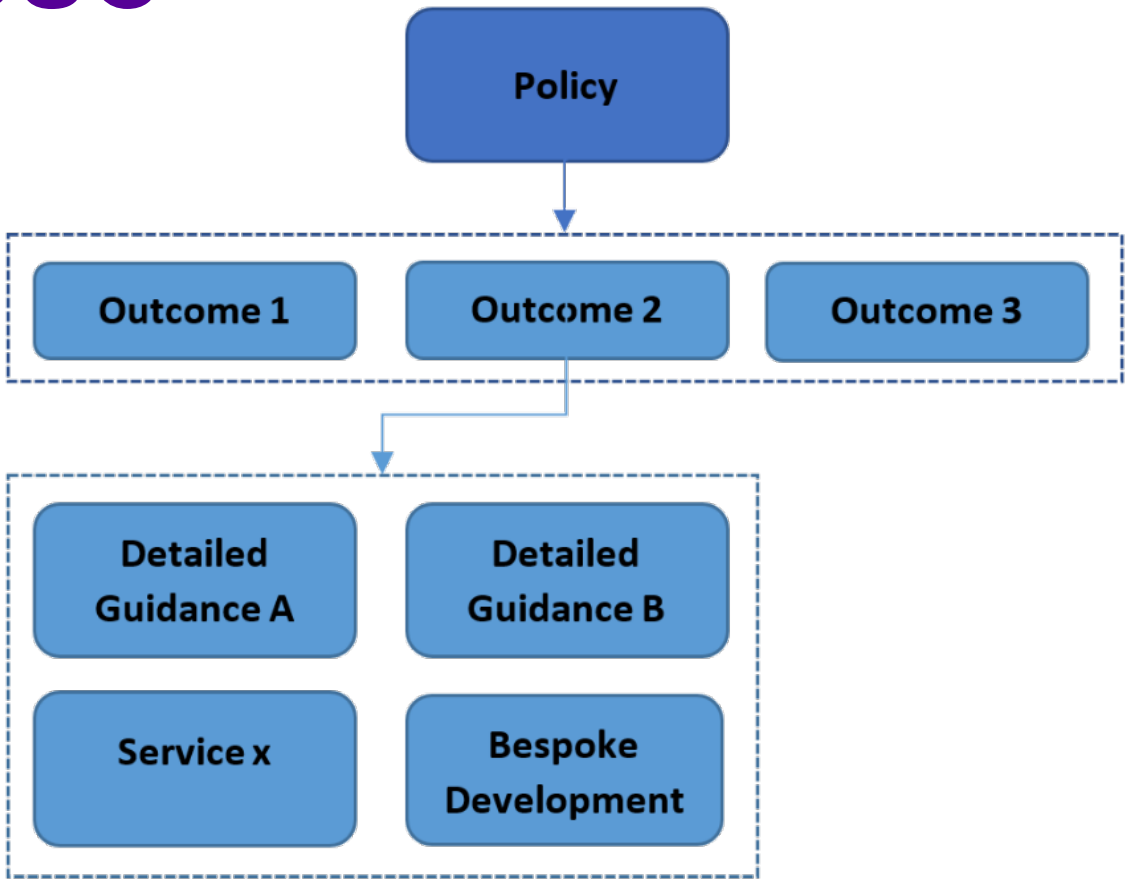
- UK ICO: quite basic
- UK National Cyber Security Centre (NCSC) in conjunction with ICO: outcome based security
- FR CNIL: quite prescriptive

ICO

- Have, review and test policies
- Risk assessment → security measures
- Basic controls are in place (aka hygiene)
- Some systems require more than these
- Testing procedures (assurance)
- Security provided by data processors

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

NCSC



"...Implement appropriate technical and organisational measures..."

This is the abstract and outcome based view of what you must achieve.

Detailed guidance showing examples of how to achieve the outcomes or perhaps appropriate services may be available to procure, or alternatively a competent organisation might develop a bespoke approach.

https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes

NCSC GDPR Outcomes

A) Manage Security Risk	B) Protect personal data against cyber attack	C) Detect security events	D) Minimize the impact
A.1 Governance A.2 Risk management A.3 Asset management A.4 Data processors and the supply chain	B.1 Service Protection Policies and Processes B.2 Identity & Access Control B.3 Data Security B.4 System Security B.5 Staff awareness & training	C.1 Security monitoring	D.1 Response and recovery planning D.2 Improvements

B2. Identity & Access Controls

- You understand, document and manage access to personal data and systems that process this data. Access rights granted to specific users must be understood, limited to those users who reasonably need such access to perform their function and removed when no longer needed. You should undertake activities to check or validate that the technical system permissions are consistent with your documented user access rights.

It is, however, all appropriate

B3: You implement technical controls (such as appropriate encryption) …

B4: You implement appropriate technical and organisational measures to protect systems, technologies and digital services that process personal data from cyber attack …

B5: You give staff appropriate support …

CNIL

THE CNIL'S GUIDES - 2018 EDITION

SECURITY OF PERSONAL DATA

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

www.cnil.fr

THE CNIL'S GUIDES

SECURITY OF PERSONAL DATA

4

LOGGING ACCESS AND MANAGING INCIDENTS

Log access and organise incident management procedures to manage incidents allowing to react in the event of data breach (breach of confidentiality, integrity or availability).

In order to be able **to identify fraudulent access** or **abusive use** of personal data, or to determine the origin of an incident, it is necessary to log certain actions carried out on the IT systems. To do this, logging and incident management measures must be implemented. It must **record relevant events** and guarantee **that these logs cannot be altered.** In any cases, **these elements must not be kept for an excessive time period.**

BASIC PRECAUTIONS

- **Set up logs** (i.e. storing events in "log files") to record users' activities, abnormalities and events related to security.
  - these logs must save events over a rolling period that cannot exceed six months (except in the case of a legal obligation, or a particularly significant risk for the data subjects);
  - **as a minimum, the users' accesses should be logged** with their identifier, the date and time of their connection as well as the date and time of their disconnection;
  - in certain cases, it may be necessary to also keep information on the actions undertaken by the user, the types of data consulted and/or modified, and the reference of the concerned data.
- **Inform the users** of the installation of such a system, after informing and consulting with personnel representatives.
- **Protect the logging equipments and the logged information** against unauthorised access, notably by making it inaccessible to the individuals whose activity is logged.
- Set up procedures detailing the monitoring of processing use and **periodically carry out a review of the logged information** to detect possible anomalies.
- Ensure that **those in charge of the logging management notify the data controller, as soon as possible, of any anomaly or security incident.**
- **Notify the CNIL or the competent Data Protection Authority of any personal data breach and,** except as otherwise provided by the GDPR[8], **also notify the individuals concerned** so that they can limit the consequences of this.

WHAT SHOULD BE AVOIDED

- Using information coming from the logs for another purpose than guaranteeing the proper use of the information processed (for example: using the logs to count the hours worked is a misuse, punishable under the law).

FURTHER MEASURES

- See the security recommendations for the implementation of a logging system published by the ANSSI at the following address: : https://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journalisation/

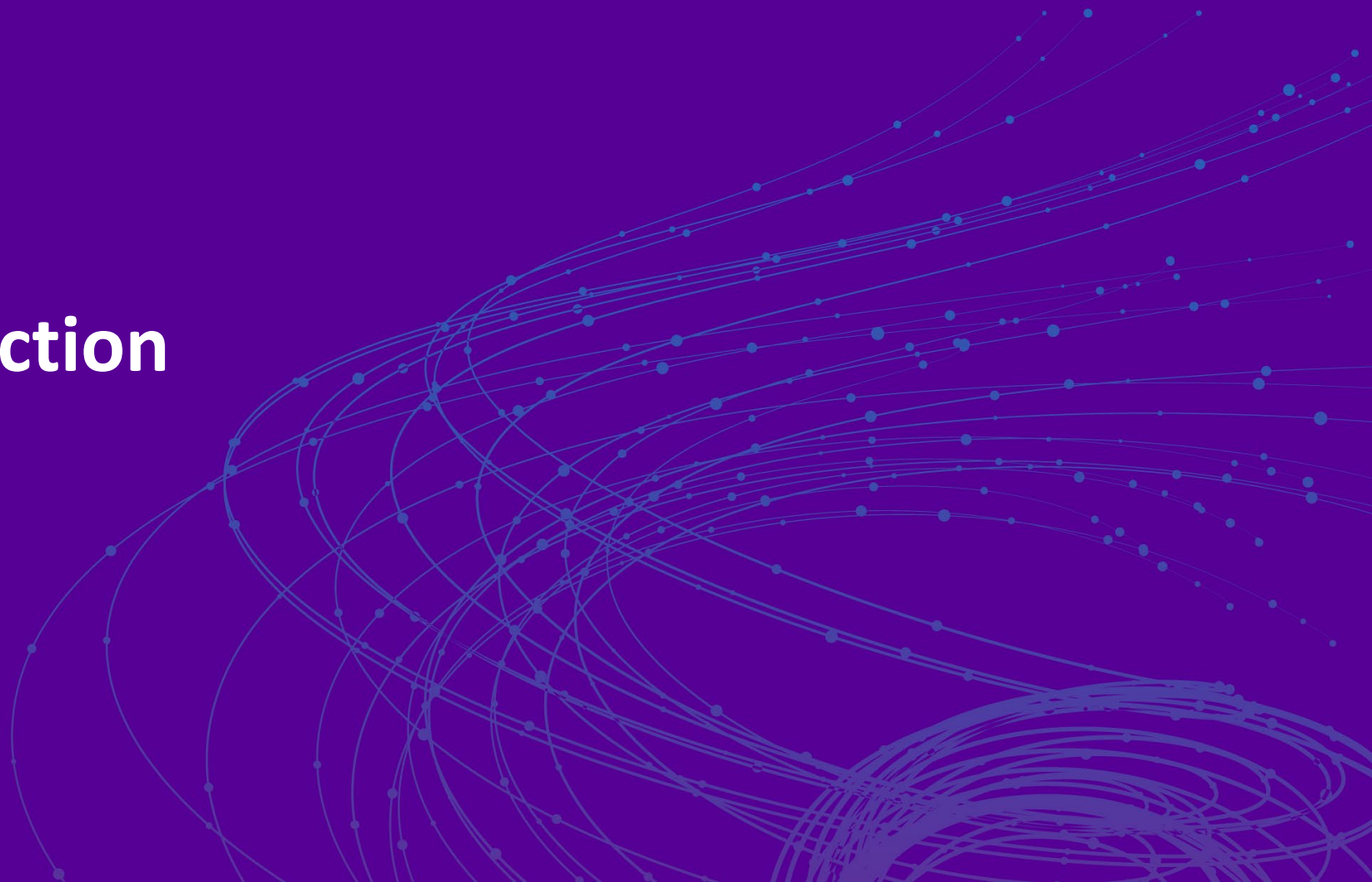
CNIL.

8. articles 33 and 34 of the GDPR

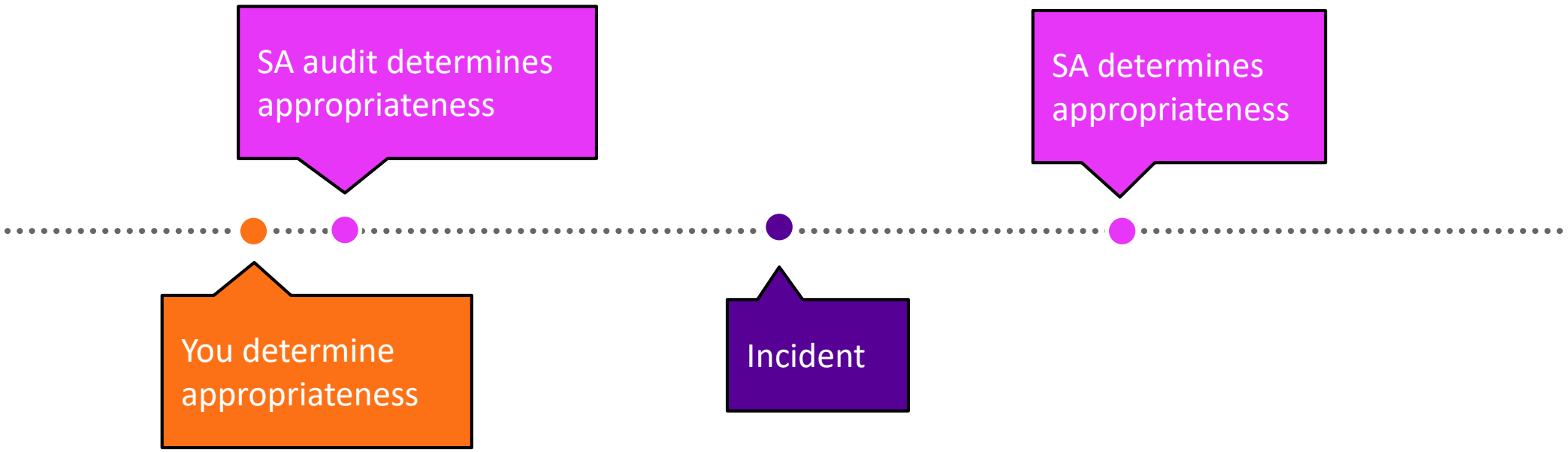
https://www.cnil.fr/en/new-guide-regarding-security-personal-data

RSAConference2019

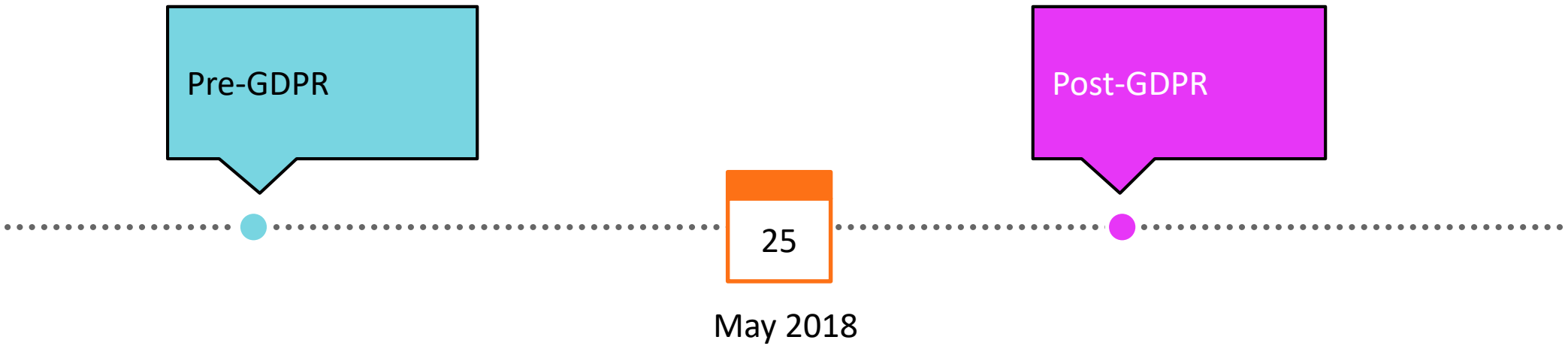
Regulatory action



Timeline of determination



There was regulation before the GDPR



Lack of role based access

Post-GDPR

- Portugal (CNPD)
- Hospital fined €400K
- No data minimization
- No real role based access
  - 985 physician's accounts with access to clinical files
  - 296 active doctors in the hospital

Plaintext password storage

Post-GDPR

- Germany (Baden-Wuerttemberg)
- Social media company fined €20K
- 330K user accounts compromised
- Passwords stored in plainext
  - Should have been hashed

CCTV

Post-GDPR

- Austria
- Smal business fined €4,800K
- Not security (Art 32) related

Advertising and personalization

Post-GDPR

- France (CNIL)
- Google fined €50 Mi
- Not security (Art 32) related

UK ICO

Pre-GDPR

- Encrypt all portable media
- If you process cards, comply with PCI DSS
- Learn how to redact properly
- Patch vulnerabilities, penetration test
- Use a WAF

UK ICO

Pre-GDPR

- Don’t share admin accounts
- Don’t store keys in plaintext!
- Use antivirus
- Know where your data is

RSAConference2019

The case of Carphone Warehouse

An example of how not to do it, and a cautionary tale

Background

Pre-GDPR

- Pre-GDPR
  - But the security provisions of the law generally the same: “appropriate”
- 3 million humans, credit cards, employee database
- Breach of confidentiality in July– August 2015
- Regulatory decision January 2018
- Two key points:
  - Massive security failings
  - Not the cause of the breach

1. The Information Commissioner ("the Commissioner") hereby issues The Carphone Warehouse Limited ("Carphone Warehouse") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA") because of a serious contravention of the seventh data protection principle ("DPP7") from Schedule 1 to the DPA.

2. The amount of the monetary penalty is £400,000.

20. The report by I concluded that, while there was no single root cause of the attack, the attacker clearly had everything he needed to take hold of the System and extract a large amount of information quickly. The subsequent report by F identified a number of deficiencies in the technical provisions and security measures in place for the System. The expert report assists in understanding those reports and also the extent to which the deficiencies referred to in the Commissioner's Notice of Intent played causal roles in the attack on the System that prompted this supervisory action. Based on all of those reports and her own analysis, the Commissioner remains persuaded that, once the attacker entered the system through the vulnerable WordPress installation (albeit having used valid login credentials), he had everything he needed to take hold of the System and to access and extract large amounts of personal data quickly. She also remains of the view that deficiencies in Carphone Warehouse's technical and organisational measures created real risks of such data breaches, and that they played an essential causal role in this particular incident.

(1) Important elements of the software in use on the System were many years out of date. The particular web application in use was released in 2010. The WordPress installation in use dated from 2009. More current versions were available, but Carphone Warehouse continued to use a version that was some six years old at the time of the attack. Although the WordPress

(2) Carphone Warehouse's approach to software patching was seriously inadequate. Although a "Patch Management Standard" was in place, it was not being followed by the relevant business area. No measures were in place to check

(4) Inadequate vulnerability scanning and penetration testing measures were in place at the time. The Commissioner understands that no routine testing procedures were in place.

23. Having regard to the state of technological development, the cost of implementing any measures, the nature of the relevant personal data and the harm that might ensue from its misuse, the Commissioner's view is that there were multiple inadequacies in Carphone Warehouse's technical and organisational measures for ensuring the security of personal data on the System.

(2) It is particularly concerning that a number of the inadequacies related to basic, commonplace measures needed for any such system. See for example the references above to outdated software, inadequate patching measures and the absence of WAF and antivirus measures. Carphone Warehouse has submitted that, in taking this view, the Commissioner is imposing unjustifiably high standards of data security, by reference to industry norms at the relevant time (mid-2015). The Commissioner rejects that submission.

(1) Carphone Warehouse is a large, well-resourced and experienced data controller. According to its website, it is the largest independent telecommunications retailer in Europe, with over 1,100 stores across the UK and Ireland. It describes itself as the number one independent mobile online retailer in the UK. A company of this size and standing was well placed to assess any weaknesses in its data security arrangements and to take appropriate action.

(2) This is all the more so given that a number of the inadequacies related to basic, commonplace measures, the need for which should have been obvious to any data controller working with such IT systems (such as up-to-date software, adequate patching measures, WAF and antivirus software).

RSAConference2019

Summary

What is appropriate?

- Based on risk to humans (not the organization)
- Existing, known technology
- Generally accepted baseline standards
- What do your peers do?
- Organizational size / capability drives regulatory expectation

Big picture

- Keep up with the state of the art
  - Keep attending #RSAC
- Assess risk
- Find your hygiene baseline
- Align to a standard for safety
- Monitor regulatory action and guidance

Now: Risk assess based on humans

- Map personal data across systems
  (you should have done this anyway)
- Develop a process and scale
- Undertake risk assessments
- Find your baseline
- Control areas where there is high risk
- Document how you reach NCSC outcomes

What's appropriate changes with time

RSAConference2019

Questions