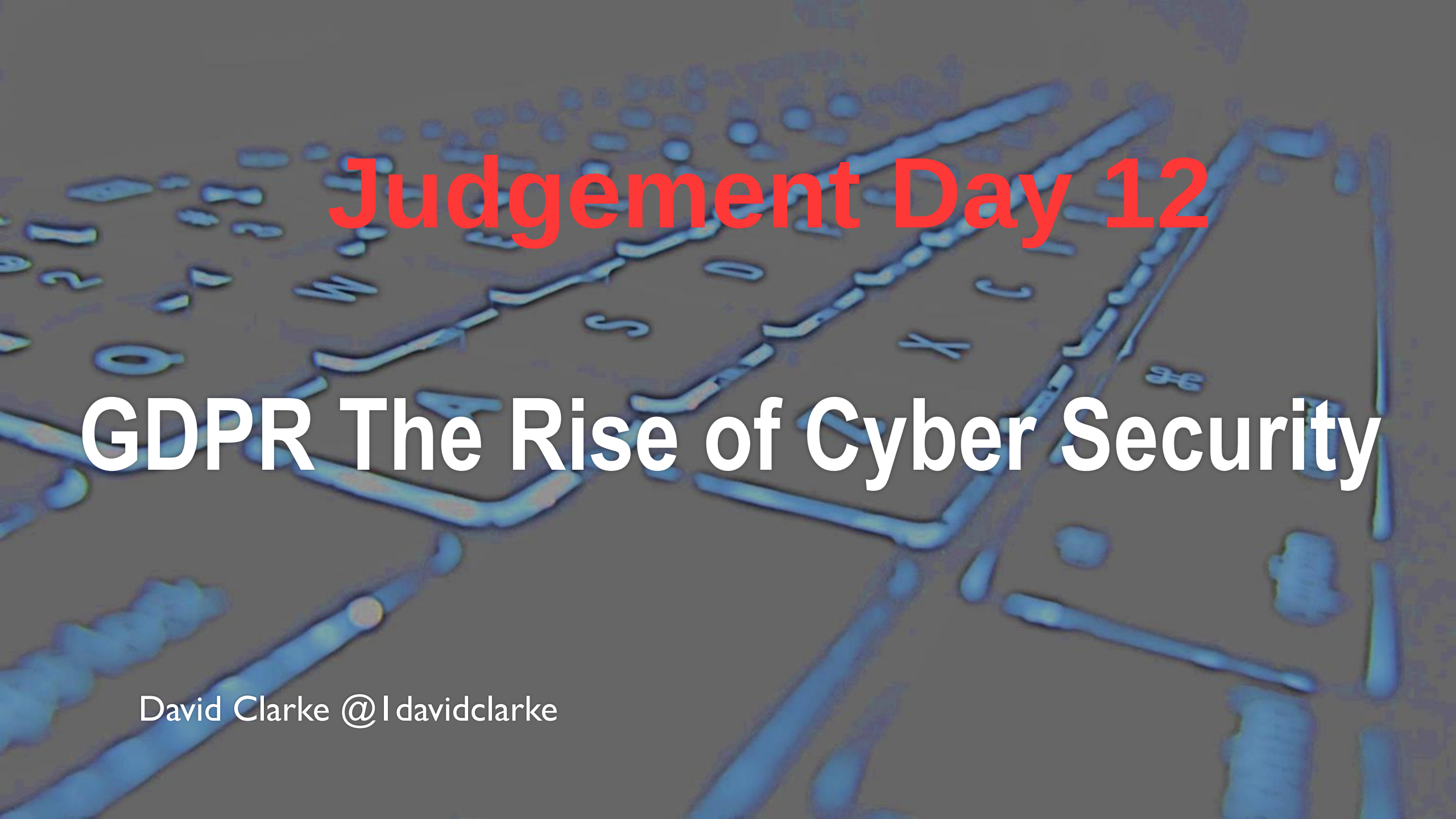

Judgement Day 12
GDPR The Rise of Cyber Security
David Clarke @1davidclarke

David Clarke FBCS

- Board Advisor to Regtech Startups and GRC Consultancies.
- Multiple Global ISO27001 for $Billion Dollar Contracts.
- PCI-DSS for a UK Credit Card Transmission Service.
- CPNI Member 10+ years *(Centre for the Protection of National Infrastructure (CPNI) is the United Kingdom government authority which provides protective security advice to businesses)*
- Creation of Global Infrastructure for Worlds Largest private trading Network, Trading $ 3 Trillion a day.
- Management of Multiple Global Security Operations Centres.
- CERT, Leading Edge Technological deployments and architectures.
- GDPR Technology Forum – Founder LinkedIn Forum

Recognized as one of the top 10 influencers by Thompson Reuter top 30 most influential thought-leaders and thinkers on social media, in risk management, compliance and regtech in the UK.

Founder and Owner of Linkedin GDPR Technology group 7000 + Members
https://www.linkedin.com/groups/1201767

GDPR/ Cyber Security High Level Action Plan

What is Expected .....

Desired Outcomes

Minimise Risk

Reduce the Overhead and fines of an ICO GDPR Audit and Data Breach

Demonstrate Accountability

“data must be processed fairly and lawfully” Elizabeth Denham ICO Commissioner

What is Expected .....

- Max Fines up to 4% of Global Revenue or 20,000,000 Euro whatever is higher
- Accountability
- Data Protection Officer for High Risk Processing
- Subject Access Requests
- Consent Management
- Appropriate Technical and Organisational Controls and measures
- Children's Data
- International Transfers
- Data Breach 72 Hour Breach Notification

Data Protection is a matter for the board room. Farming out aspects of it to the IT department or fundraising arm will not work. You are accountable. You have the power to set the standards for your organisation

Denham ICO Commissioner

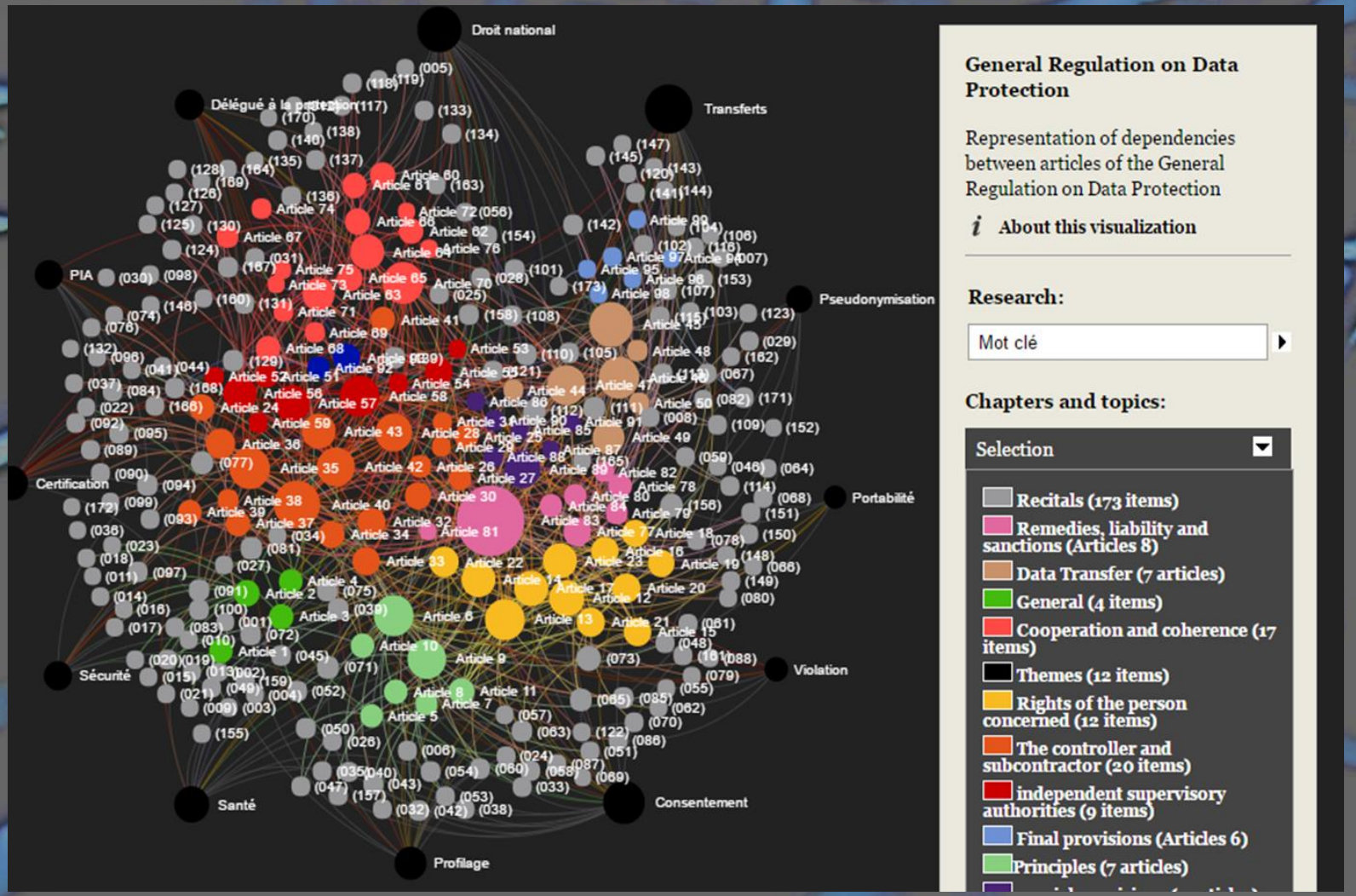
Bringing IT into the 21st Century……Is IT Safe?

- Food
- Cars
- Planes
- Buildings
- Finance
- Healthcare

We've had frustration too, with directors ducking away from fines by putting their company into liquidation. Liquidation isn't a get out of jail free card – our work with insolvency practitioners saw one director disqualified for six years for trying to take this route – but we believe the public want to see stronger action

Denham ICO Commissioner

GDPR Complex?



Queensbury Rules

Following Rules for alignment.....

- To be a fair stand-up boxing match in a 24-foot ring, or as near that size as pr
- No wrestling or hugging allowed.
- The rounds to be of three minutes' duration, and one minute's time between rounds.
- If either man falls through weakness or otherwise, he must get up unassisted, 10 seconds to be allowed him to do so, the other man meanwhile to return to his corner, and when the fallen man is on his legs the round is to be resumed and continued until the three minutes have expired. If one man fails to come to the scratch in the 10 seconds allowed, it shall be in the power of the referee to give his award in favour of the other man.
- A man hanging on the ropes in a helpless state, with his toes off the ground, shall be considered down.
- No seconds or any other person to be allowed in the ring during the rounds.
- Should the contest be stopped by any unavoidable interference, the referee to name the time and place as soon as possible for finishing the contest; so that the match must be won and lost, unless the backers of both men agree to draw the stakes.
- The gloves to be fair-sized boxing gloves of the best quality and new.
- Should a glove burst, or come off, it must be replaced to the referee's satisfaction.
- A man on one knee is considered down and if struck is entitled to the stakes.
- That no shoes or boots with spikes or springs be allowed.
- The contest in all other respects to be governed by revised London Prize Ring Rules.

The 19 new risks as drivers of change

Desired Outcomes

Minimise Risk and Overhead

Demonstrate Accountability

Minimise Risk

"data must be processed fairly and lawfully" Elizabeth Denham ICO Commissioner

New Threats and Risks

1. Breach less Liability
2. Data Audit without Breach
3. 72 Hour Breach Notification
4. New 6 New Privacy Rights
5. Demonstration of Accountability is required
6. Class Action is Easier
7. Customer Contact Points can Highlight Non Compliance
8. Charities, Government ,Multinationals are easy targets
9. Heavy Fines up to 4% of global revenue.
10. Appropriate Technical and Organisational Measures.
11. Existing Client Data Unusable after May 2018.
12. Internal data may be at risk of non compliance.
13. Complex data landscape
14. Comprehensive data governance program required
15. Liability beyond data controllers
16. Criminalisation, Anonymisation, SARS Tampering.
17. Directors and Officers "Neglect" Liabilities.
18. Business 2 Business contractual obligations.
19. Accountability

New Strategies to Look After and Protect Data

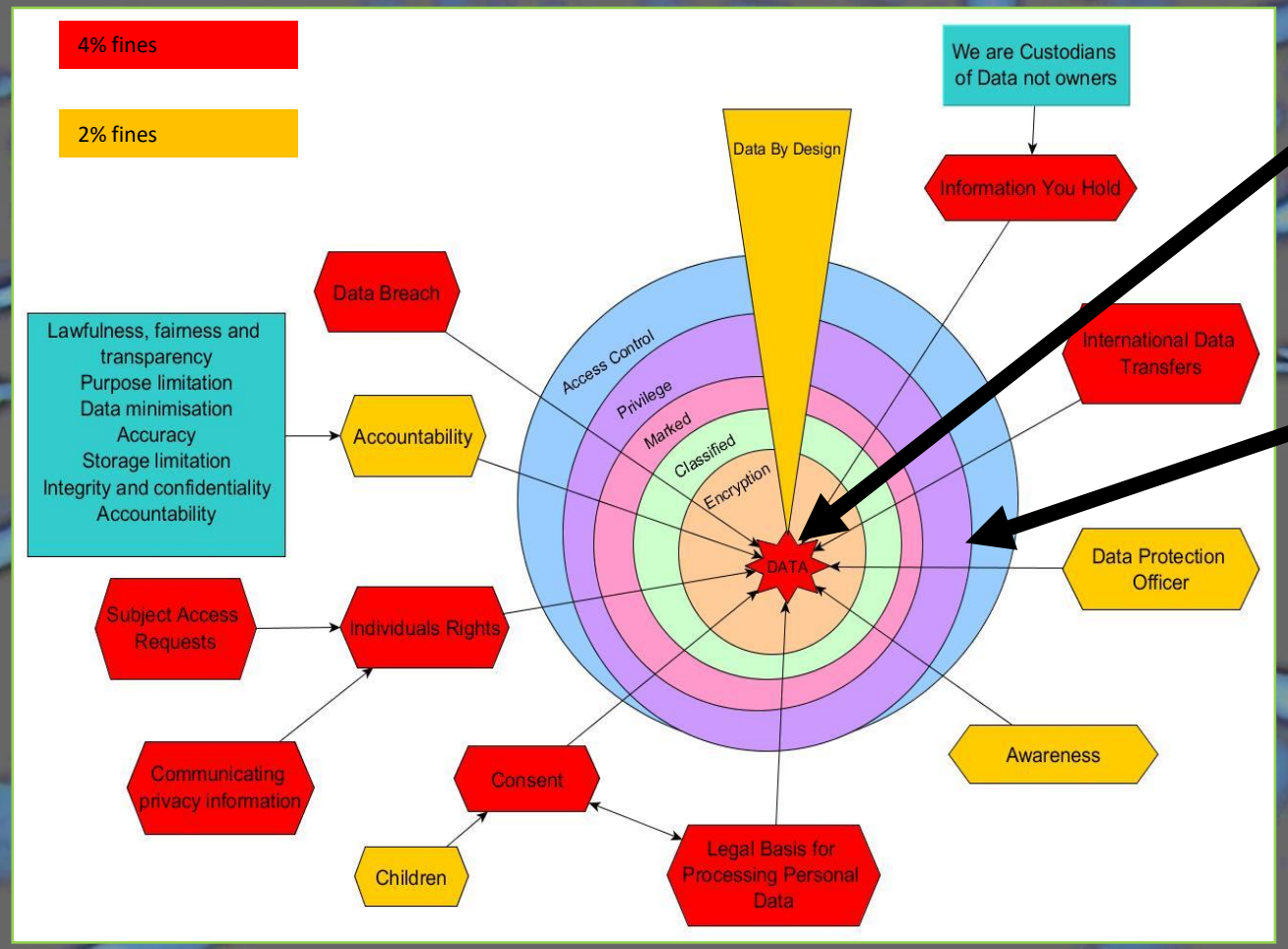
1. Data is not owned it is looked after to demanding Standards
2. Data is looked after inline with users wishes
3. Ability to demonstrate Data Protection and privacy capabilities
4. To use Data a legal basis and business reason is needed
5. Data flow and usage needs to be documented, understood, monitored and governed.
6. Permission/consent to use for every process with non-repudiation.
7. Demonstrate Accountability
8. The pseudonymisation and encryption of personal data
9. Measures to ensure resilience of systems and services processing data.

Threats That can Cost ,No longer just the Bad Guys (T3000)

1. Government Compliance due to Data Protection Legislation ,Fines/Restriction
2. 3rd Parties,Suppliers with weak Data Protection
3. Class/Group Action
4. Breach less Liability (Unable to demonstrate Accountability)
5. Officer in the company (Directors to Secretaries)
6. Compliance across Global Jurisdictions
7. Malevolent Attacks and Compromise
8. Business 2 Business may not do business with each other
9. Whistleblowing
10. Loss of Revenue,Image,Reputation Customers.

Consumer litigation and class actions will quickly follow once this regulation goes live, as has happened in the US' – PAT MORAN

Advanced ways to integrate GDPR and Cyber Security into Business: Faster, Safer, Better and Easier



Article 6 (4e),Recital 83
(e) the existence of appropriate safeguards, which may include **Encryption** or pseudonymisation.

ICO Example

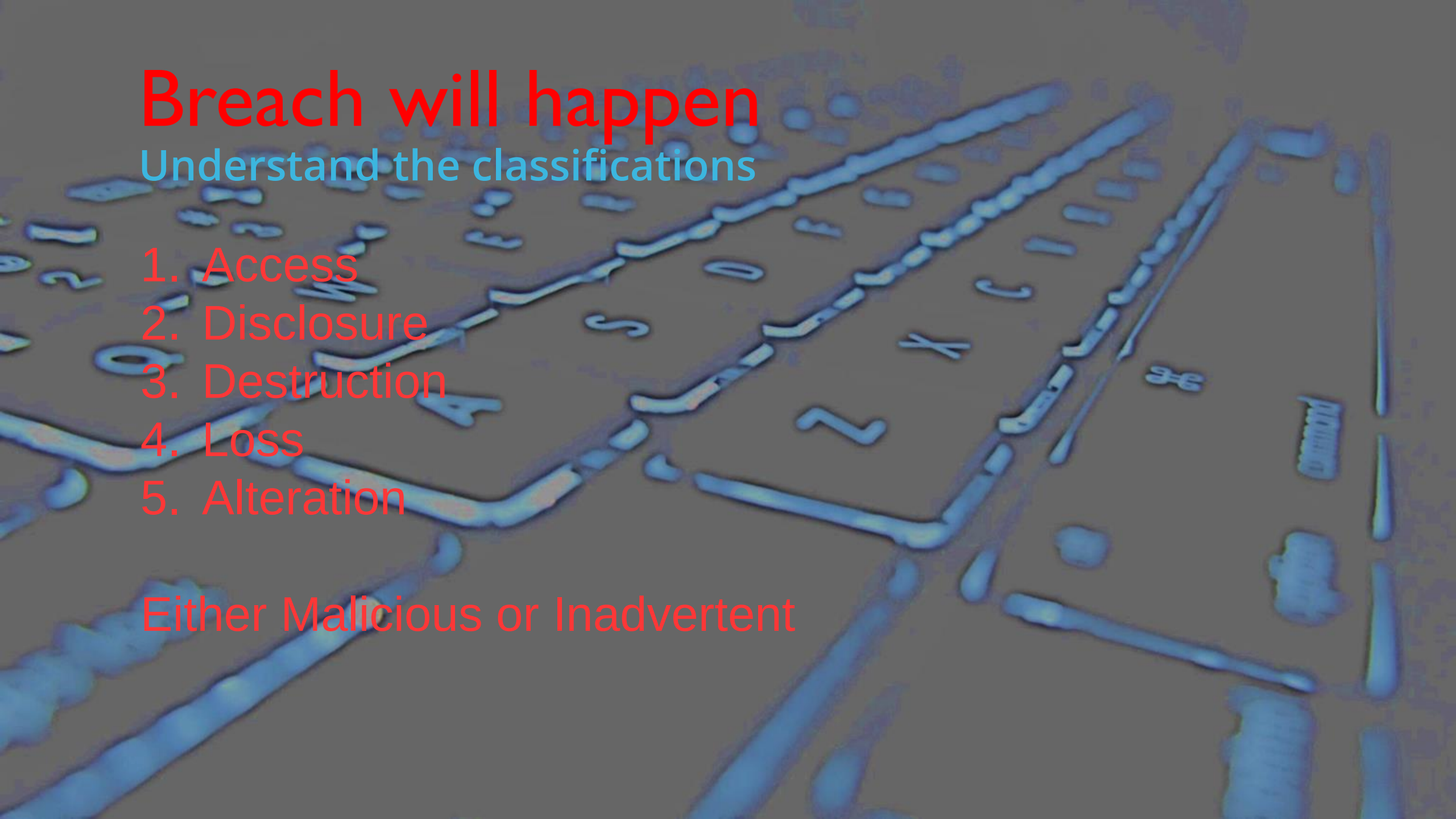
A hospital could be responsible for a personal data breach if a patient's health record is inappropriately accessed due to a lack of appropriate internal controls.

"technical and organisational measures" 21 Instances in the GDPR.

Presentation Only

6 GDPR Principles

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	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
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR



Breach will happen

Understand the classifications

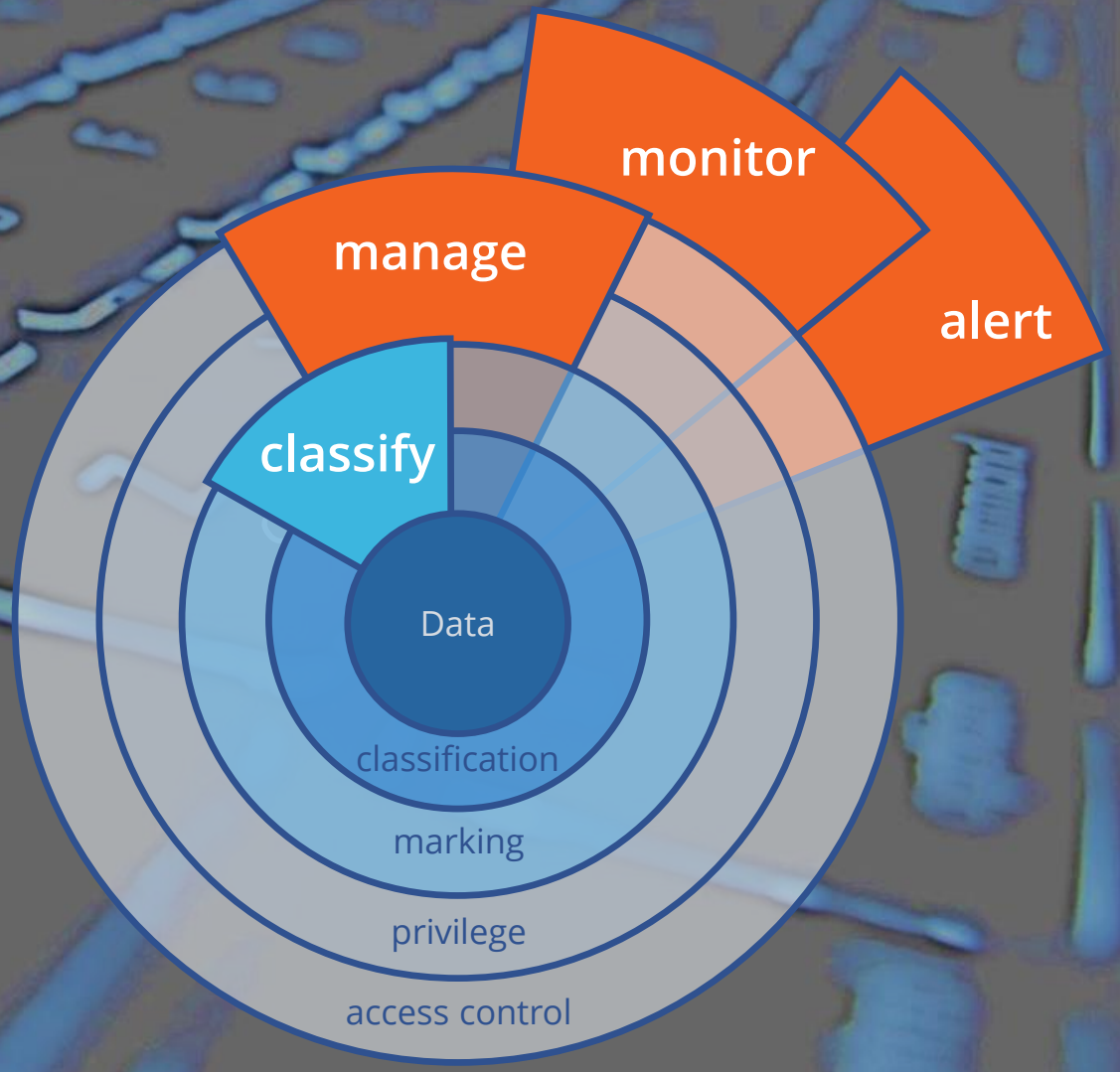
1. Access
2. Disclosure
3. Destruction
4. Loss
5. Alteration

Either Malicious or Inadvertent

Securing the data/information You Hold

Cyber Impact Assessment

- Identify PI Data
- Classify
- Retention Policy
- Marking
- Privilege
- Access Control



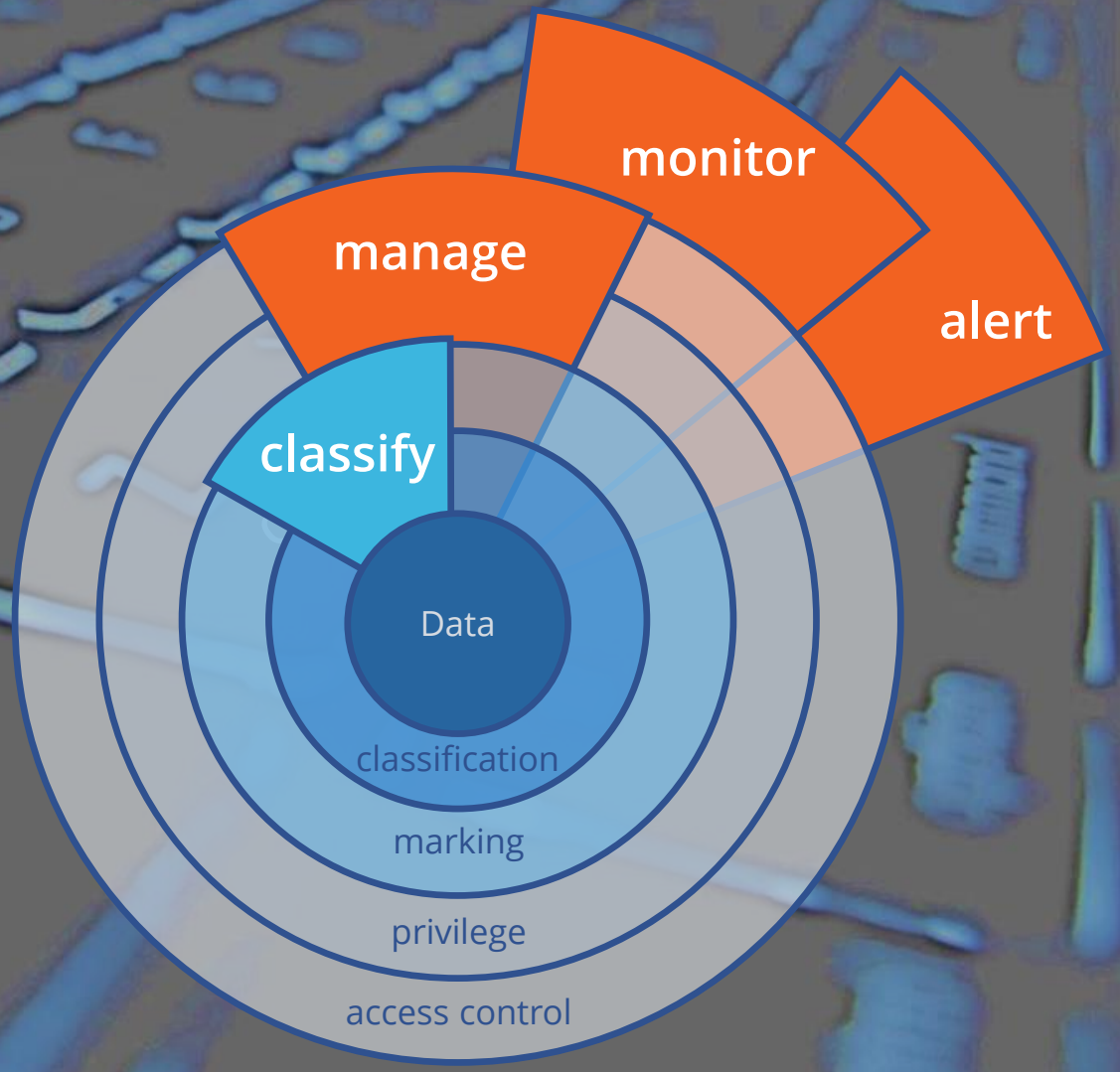
GDPR 6 Principles

Demonstrate Accountability

Once Classified, Marked, Privileged, Retention, Manage, Monitor, Alert

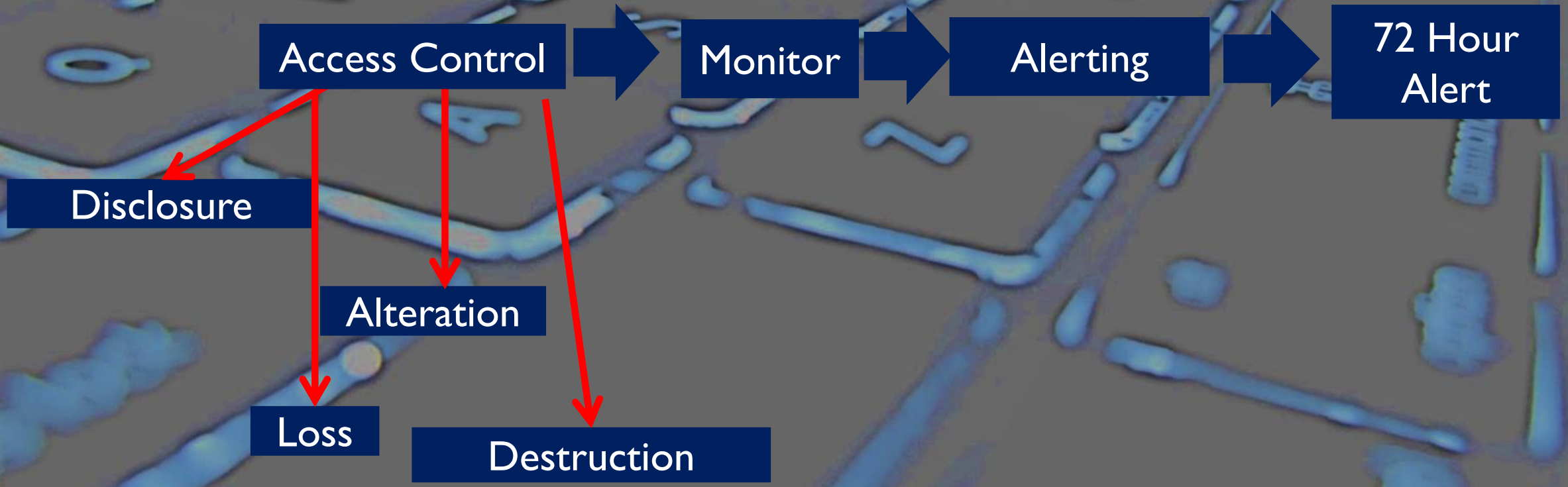
- ✓ Data Minimisation
- ✓ Storage Limitation
- ✓ Accuracy
- ✓ Purpose Limitation
- ✓ Integrity and Confidentiality
- ✓ Lawfulness , Fairness Transparency

Demonstrate Accountability

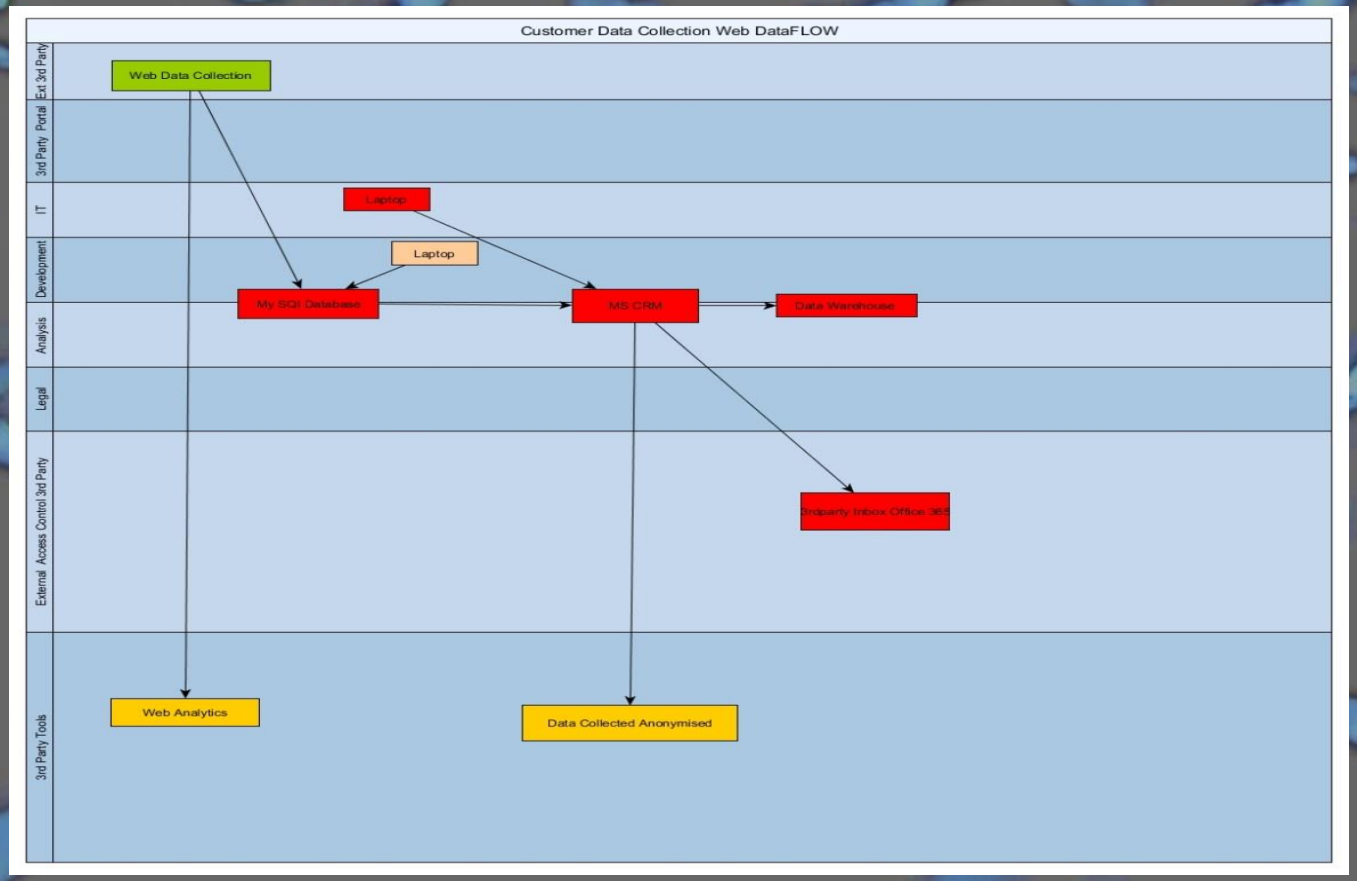


GDPR Cyber Security Control Tower

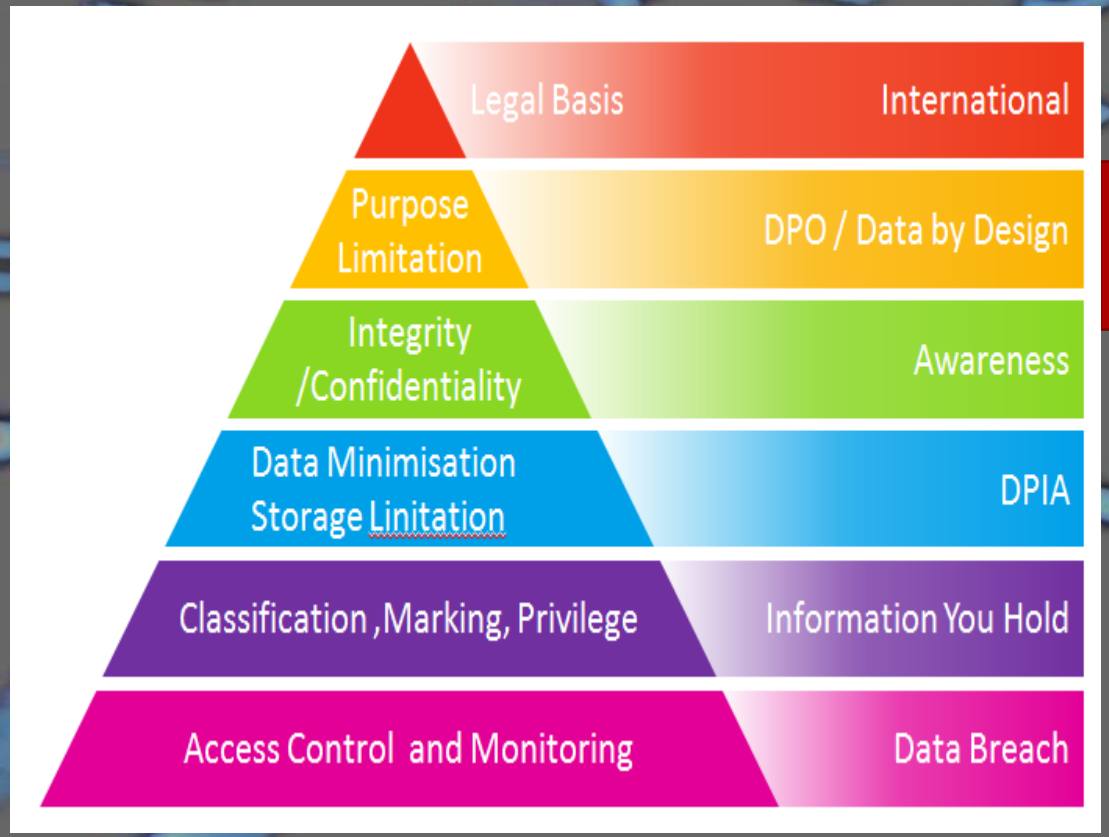
Access Control >Monitor > 72 Hour Notification



Data Breach ,Crisis Management Alignment



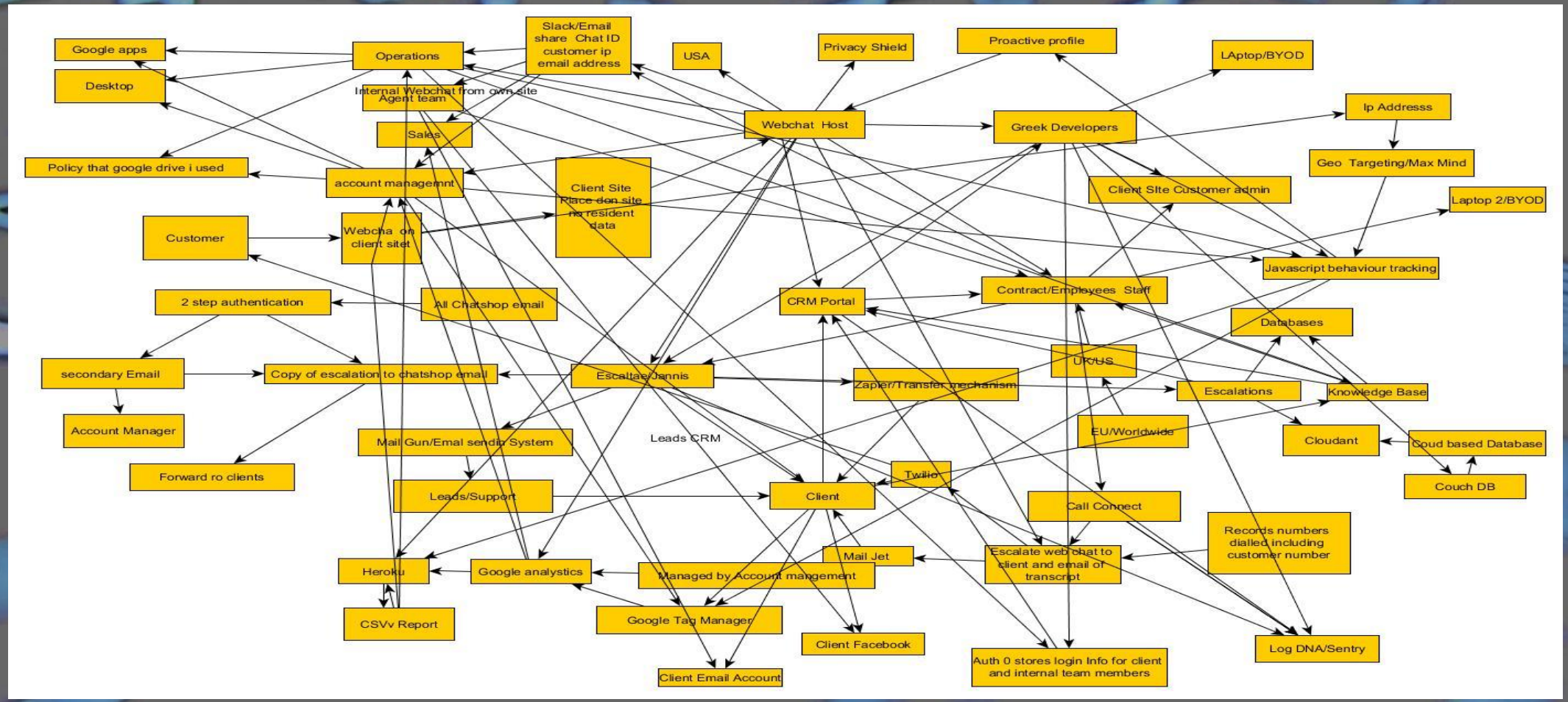
Cyber Security and GDPR Together



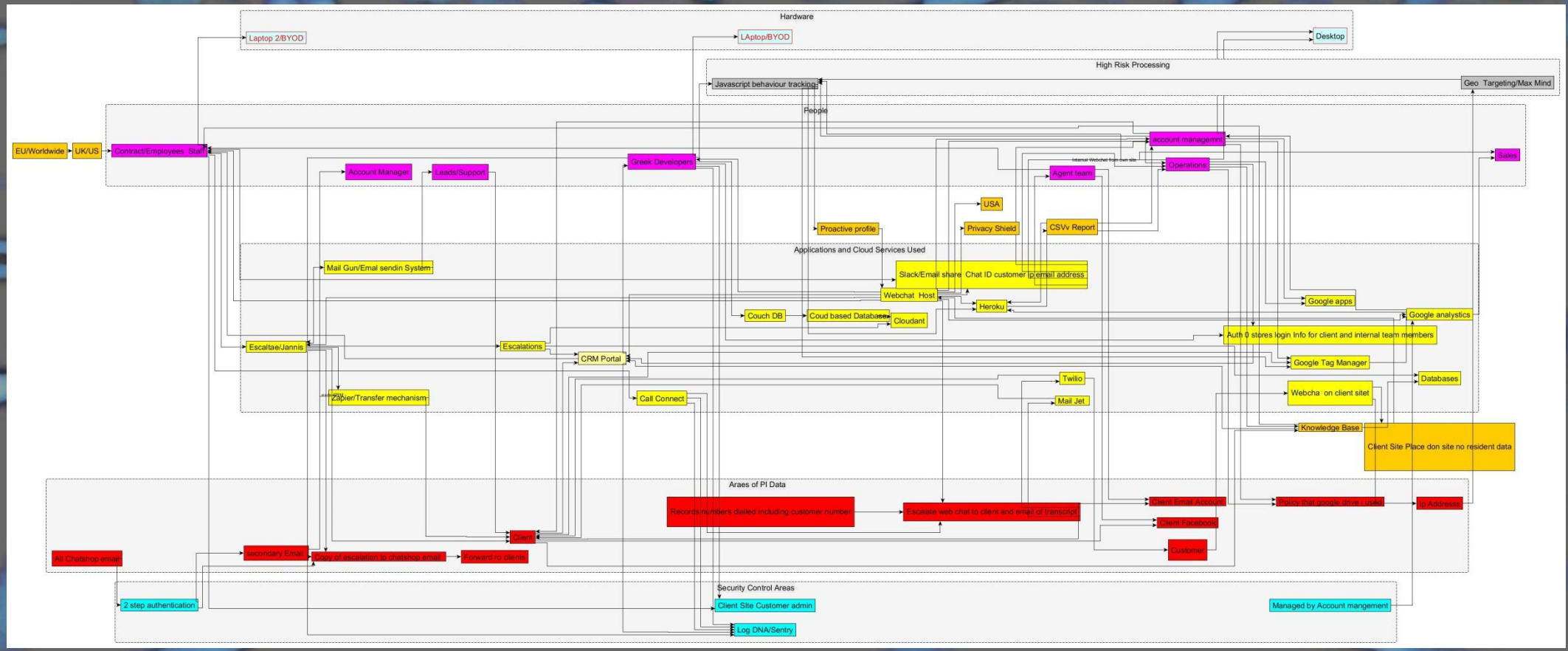
Assists with 5 of the 6 principles

Data Minimisation
Storage Limitation
Accuracy
Purpose Limitation
Integrity and Confidentiality

Mapping Data Touch Points

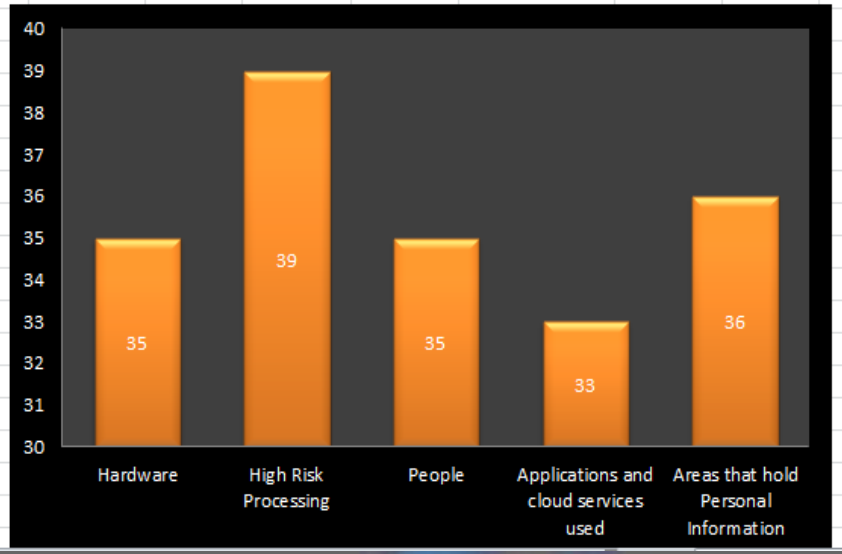


Aligning the Touch Points



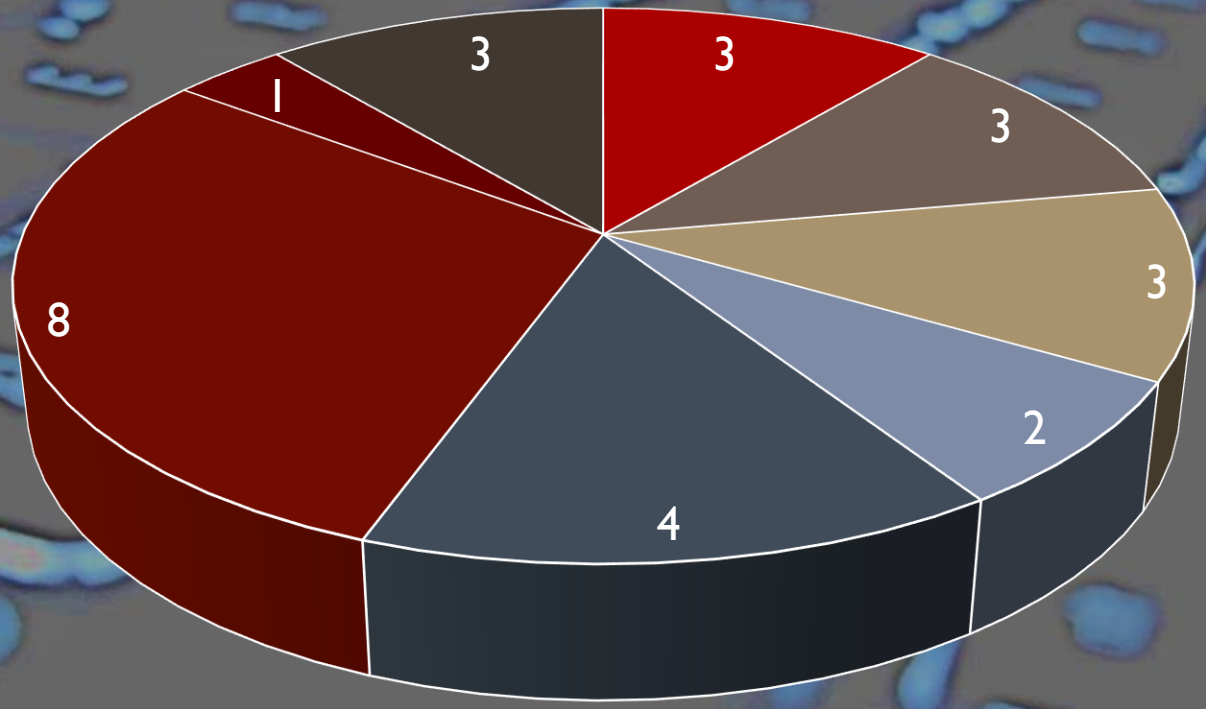
Managing the Cyber Risk

Description	Lawfulness, fairness and transparency	Purpose limitation	Data minimisation	Accuracy	Storage limitation	Integrity and confidentiality	Accountability	Disclosure	Loss	Destruction	Alteration	Access	Awareness	Total
Hardware	1	3	3	3	3	3	2	3	3	3	3	3	2	35
High Risk Processing	3	3	3	3	3	3	3	3	3	3	3	3	3	39
People	3	3	3	2	2	2	2	3	3	3	3	3	3	35
Applications and cloud services used	2	3	3	3	3	3	3	2	1	3	2	3	2	33
Areas that hold Personal Information	3	3	3	3	3	2	2	3	3	3	3	3	2	36



ICO Breach Notification Form

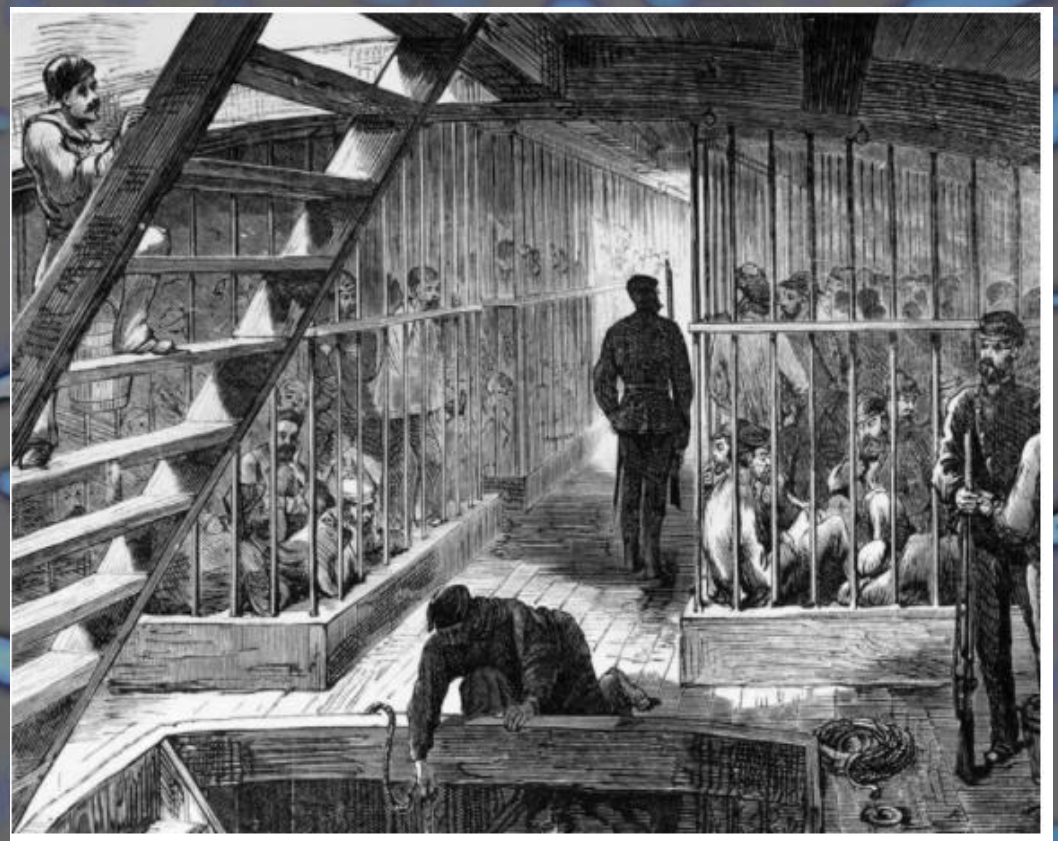
27 Questions, 8 Sections



What Cyber Compliance is Expected .....

If a way can be found to align the incentives, the processes and compliance will take care of themselves, “ Ron Baker

How Do You Stop Sea Captains From Killing Their Passengers? David Kestenbaum



Caged prisoners below deck on a transport ship bound for Australia.
Hulton Archive/Getty Images

Fines up to 4% of Global Revenue or 20,000,000 Euro whatever is higher

Accountability

Data Protection Officer for High Risk Processing

Subject Access Requests

Consent Management

Appropriate Technical and Organisational Controls and measures

Children's Data

International Transfers

Data Breach 72 Hour Breach

Data Protection is a matter for the board room. Farming out aspects of it to the IT department or fundraising arm will not work. You are accountable. You have the power to set the standards for your organisation

Denham ICO Commissioner

What is Covered "looking after the Data Subjects Rights where Social Interest Meets Self Interest

Situation Appraisal Convict Ships

Up To 33% Died on trip Australia

Force the captains to bring a doctor along. Require them to bring lemons to prevent scurvy. Have inspections. Raise captains' salaries. None of it worked.

Incentives matter.

Instead of paying for each prisoner that walked on the ship in Great Britain, the government only payed for each prisoner that walked off the ship in Australia in 1793 was adopted and implemented immediately, the survival rate shot to 99%.

GDPR

- Covers 750 Million People
- Comes into force 25/5/2018
- To provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors

If a business can't show that good data protection is a cornerstone of their practices, they're leaving themselves open to a fine or other enforcement action that could damage bank balance or business reputation

Elizabeth Denham ICO Commissioner

GDPR Benefits

No.	Benefit
1	Increased awareness and documentation of our internal data processing.
2	Tighter control over third party contracts and liabilities
3	Increase our organisational data maturity
4	Improved working relationships with third parties and service providers (reputational)
5	Improved documentation will lead to a smoother transition process.
6	Improved working practices for employees
7	Improved IT processes and associated security
8	Clear guidance for service providers (i.e. Contact Centre)
9	Ongoing cost saving…(less fines,less staff for rights ,)
10	Easier to do business with…
11	Market Advantage as others may not be ready in this industry.

For up to date information
LinkedIn Group GDPR
https://www.linkedin.com/groups/12017677
Daily GDPR News
http://paper.li/1DavidClarke/1477816063
Knowledge Base
http://gdpruk.eu/index.php/gdpr-knowledge

Thank you