

A close-up photograph of a person's hand holding a smartphone. The phone's screen is lit up and shows a blurred interface. In the background, a laptop screen is also visible, displaying a blurred webpage. The lighting is warm and focused on the hand and phone.

PHILIP<sup>LEE</sup>

3 months to go -  
your path to  
GDPR  
compliance



# Your presenter

---



**Terry McAdam**

**Management Consulting Partner, RSM Ireland**

[tmcadam@rsmireland.ie](mailto:tmcadam@rsmireland.ie)

Mobile: +353 (86) 0474002

[www.rsmireland.ie](http://www.rsmireland.ie)

# Agenda

---

- Welcome, introduction to GDPR and operational insights - Terry McAdam
- Key legal insights and practical tips - Eoghan Doyle
- The view of the regulator: areas of focus - John Keyes
- How technology can help you achieve compliance - Declan Timmons
- Questions and Answers

# RSM Ireland

Our firm's history goes back to **1987** and since then we have grown to become a top **8** professional services firms in Ireland specialising in providing advice to **mid-market businesses and government agencies**.

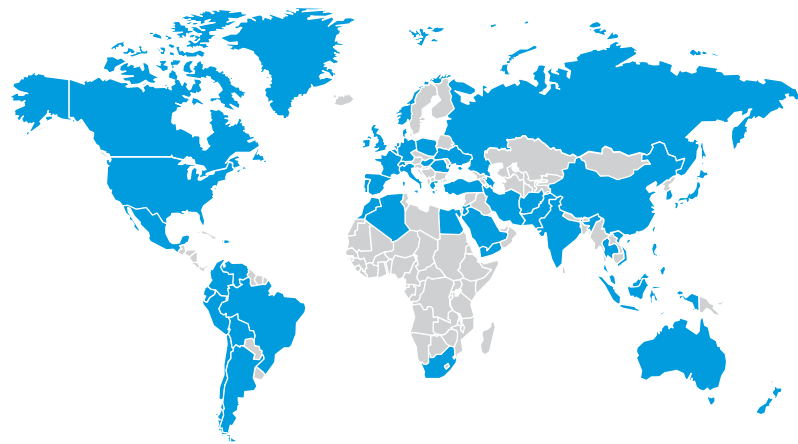
Our **150 people**, across all areas of the practice, provide clients with pragmatic, expert led, personalised advice and insight that helps them succeed, grow and prosper. Our firm is ideally placed to offer an unparalleled level of experience and expertise to our business partners in Ireland.

## About RSM International:

RSM International is one of the fastest growing networks of audit, tax and consulting firms in the world –

- ✓ We are the **sixth largest** with combined revenues of **\$5bn+**;
- ✓ Our member firms operate out of more than **800 offices**
- ✓ We are located in over **120 countries**; and
- ✓ We have over **43,000 staff worldwide**.

## Network coverage map:



# OUR PARTNERS



**John Glennon**  
Managing Partner



**Áine Farrelly**  
Management Consulting



**Catherine Corcoran**  
Management Consulting



**Aidan Byrne**  
International Tax



**George Maloney**  
Transaction Advisory Services



**Suzanne O'Neill**  
Tax



**Damien O'Sullivan**  
Audit



**Pat Keegan**  
Audit



**Brian Hyland**  
Transaction Advisory Services



**Niall May**  
Audit



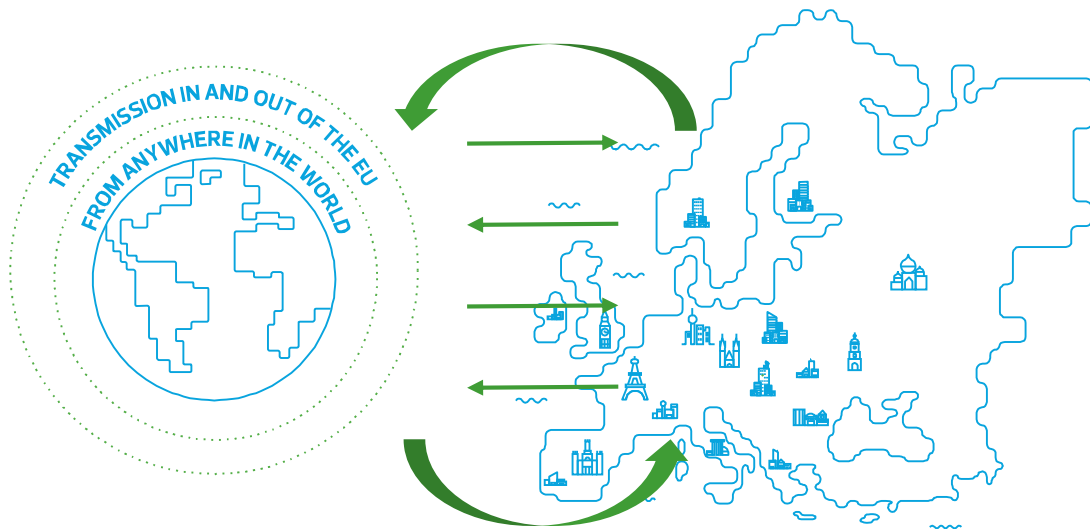
**Julian Caplin**  
Transaction Advisory Services



**John Marks**  
Private Clients

# What is the GDPR?

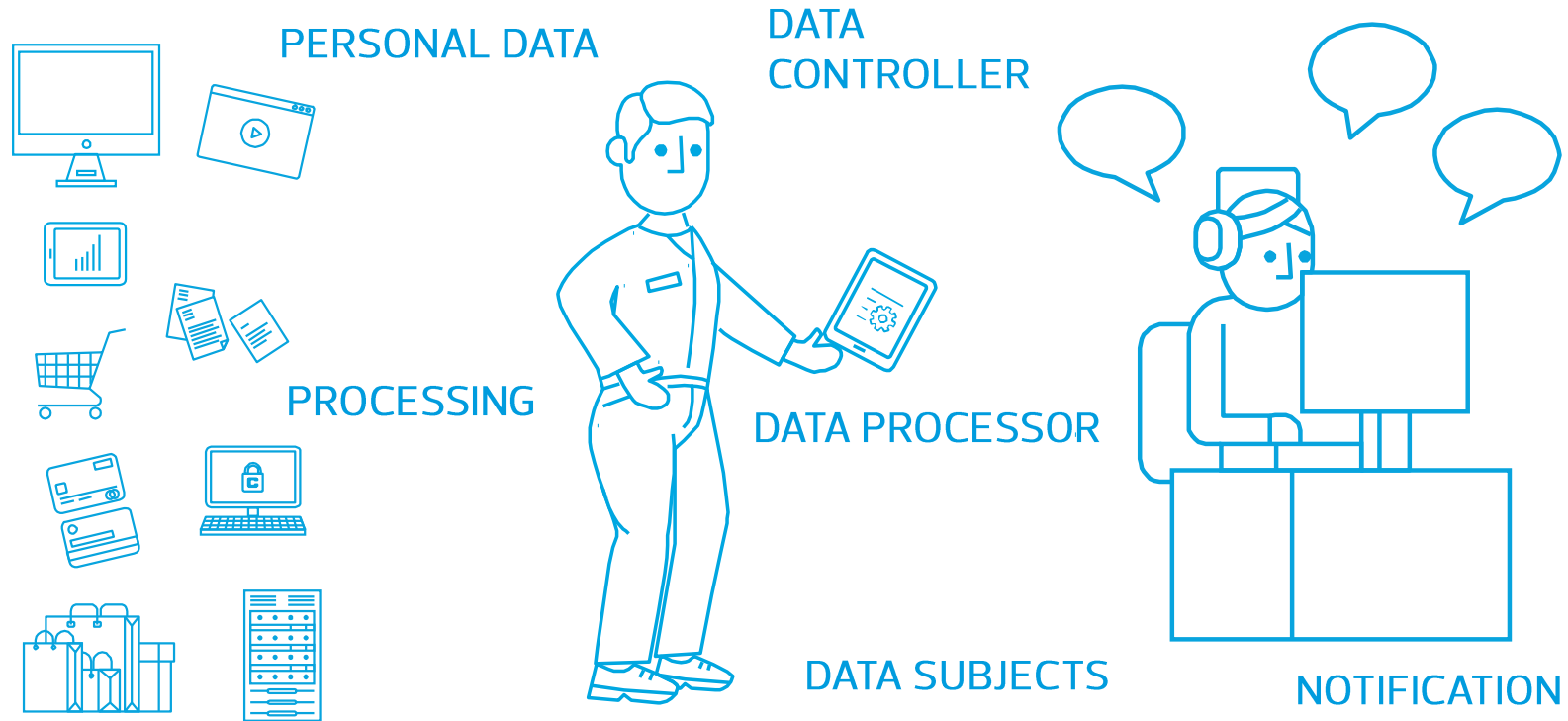
- European Union General Data Protection Regulation – “EU GDPR.”
- New data protection law adopted by the EU in **April 2016**
- Intended to enhance/align data privacy protections for EU residents
- Companies, government agencies and non-profit organisations who interact with **personal identifiable data** of EU citizens have until **25 May 2018** to comply



# What is the GDPR? (cont.)

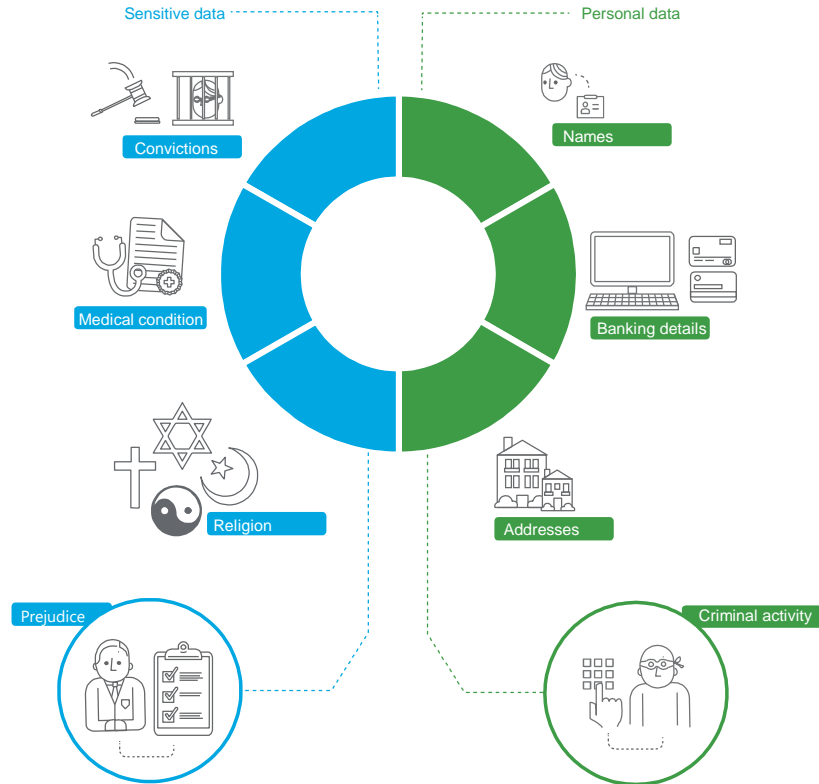
- Applies to organisations who interact with EU residents (consumers), primarily a B2C issue, **or**
- Organisations with EU-based employees.
- To determine if the GDPR affects your organisation, you need to ask questions such as:
  - Do you offer goods and services to EU residents?
  - Do you rely on third parties that store or transmit data to/from the EU?
  - Do you collect, transmit, or process data pertaining to EU residents?

# Key GDPR terms





# Sensitive and personal data



Sensitive personal data is a special category of personal data.

The GDPR requires a higher standard of care be applied to such data.

# So who has to comply?

---

Compliance is **mandatory** if either of the following statements are true:

You have controllers or processors of personal data based in the EU

You control or process the personal data of EU residents (regardless of where you are based)

# Penalties for non-compliance

If organisations do not comply, they face a maximum fine of:

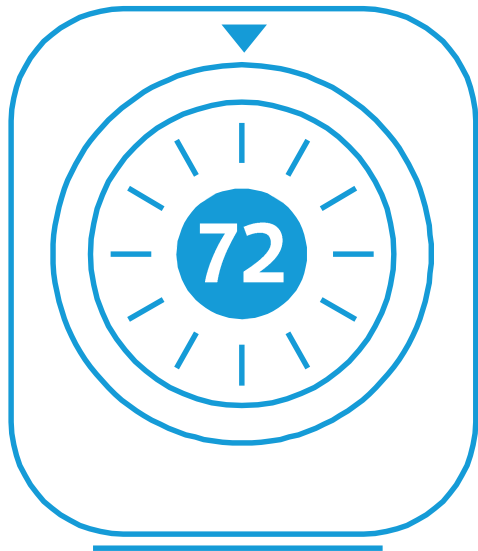
FAILURE TO COMPLY?

**4%** **OR** **€20** **WHICHEVER**  
**OF GLOBAL** **MILLION** **IS HIGHER**  
**REVENUE**

Other consequences – reputational damage, financial loss, **litigation** etc.

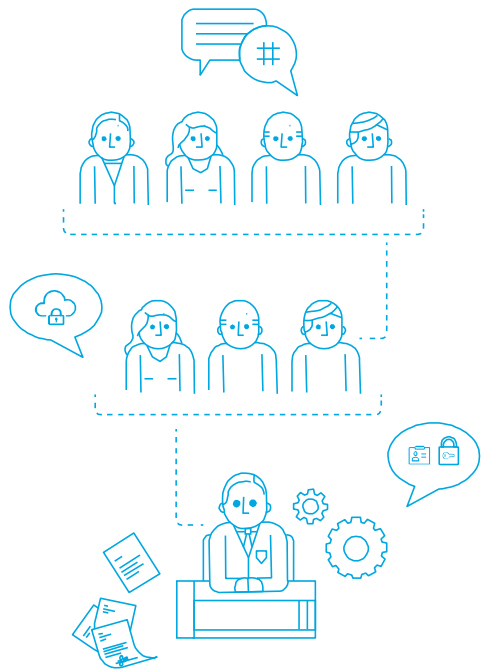
# KEY OPERATIONAL INSIGHTS

# Breach notifications



- Organisations are now under legal obligation to **notify their local regulator within 72 hours** if EU resident data is lost
  - only exception is if data is encrypted
  - organisations required to inform affected individuals if an “adverse impact” is determined from the breach
- Need to create rapid and robust process to support internal identification, reporting, triage and documentation of potential breach leading to notification, if required.

# Data Protection Officer



- DPO obligatory if entity involved in significant processing of personal data
- Office holder is operational lead re initial and ongoing compliance with GDPR
- Governance: unfettered access to Board, no conflict of interest
- Signal to market place re priority given to data protection within your organisation

# Privacy Impact Assessments



- PIAs represent key tool in helping organisations to assess risk that data subject's privacy may be impacted by current or proposed practice
- Deployed when change proposed in process or technology (subject to threshold test)
- Process walkthrough will identify risks to data privacy present in current or target operating model and allow planned mitigation

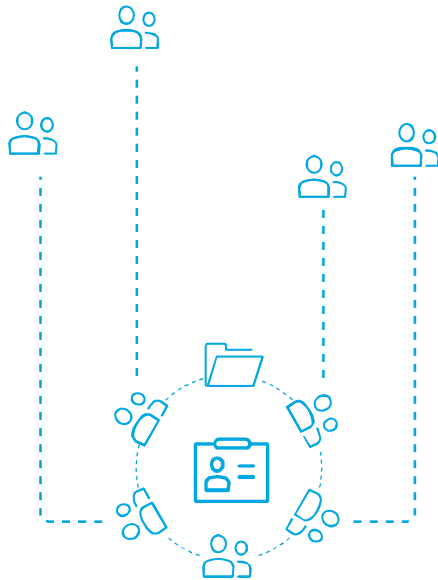
# Data discovery/mapping



- Ability to respond to Subject Access Requests (SARs) in timely fashion dependent on understanding of data held
- Need to be able to accurately search structured and unstructured data
- Organisations can reduce challenges by maintaining information asset register, restricting users' ability to email/copy/download data and making investment in search tools

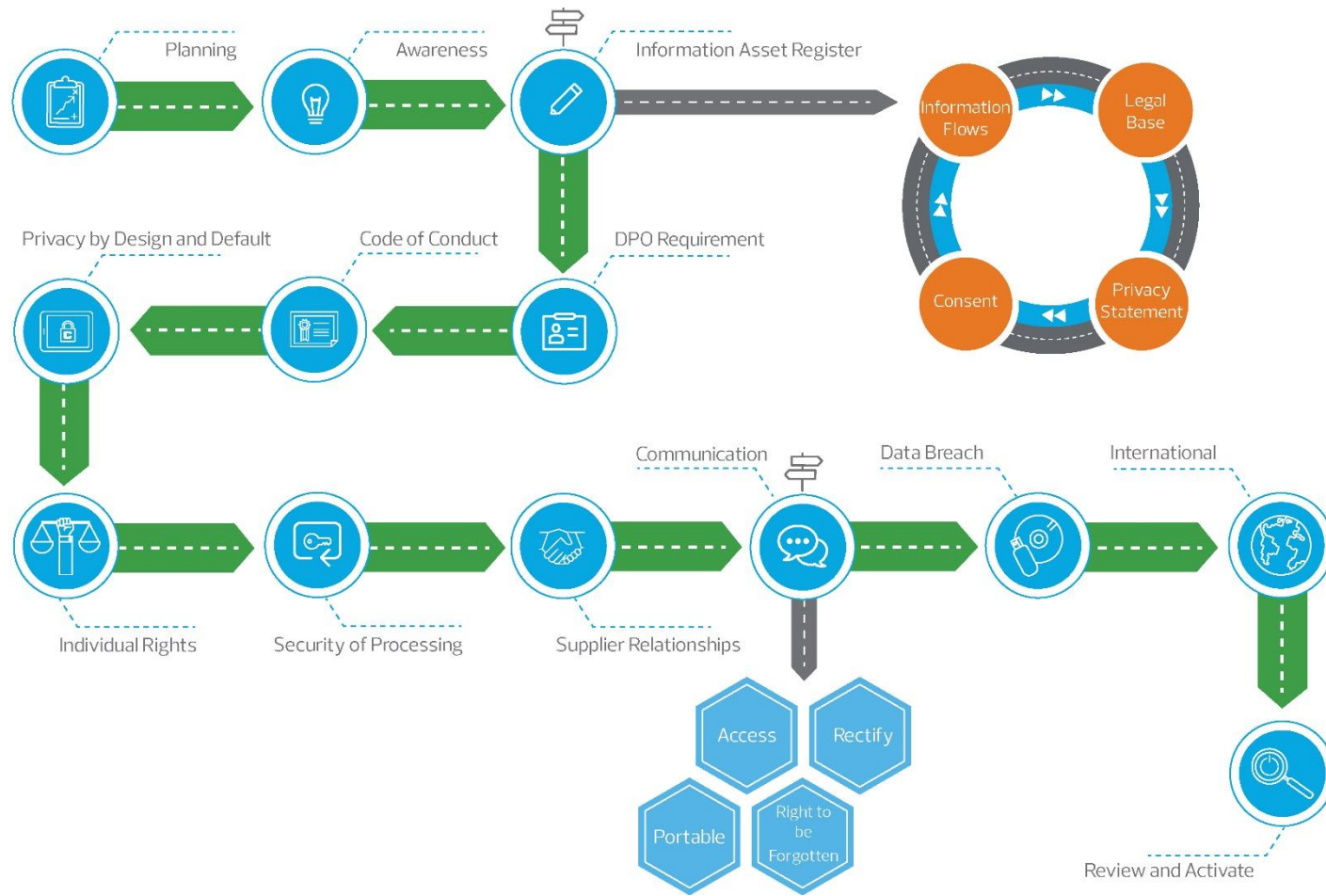


# Sustaining compliance



- Ongoing GDPR compliance cannot remain consultant-led as change will be constant
- Compliance projects must focus on knowledge transfer to and upskilling of internal personnel
- Project should enable internal DPO, or other personnel, to undertake PIAs, manage SARs and assess potential breaches, notifying as appropriate

# ROADMAP TO COMPLIANCE



# GDPR

## ROADMAP TO COMPLIANCE

# Polling questions



Thank you for your time  
and attention.

# PHILIP LEE

---

## 3 MONTHS TO GO – YOUR PATH TO GDPR COMPLIANCE

---

Presented by Eoghan Doyle, Partner, Philip Lee  
27 February 2018

---

# Outline

1. Applicability – the scope of GDPR
2. Legal basis – focus on consent
3. Controllers and processors
4. Data subject rights

# Applicability – scope of GDPR

- Applicability = Step 1!
- Directive (95/46/EC) Vs GDPR
- Article 2 material scope
- Article 3 geographical scope
- What should businesses do?



# Consent

- “Freely given, specific, informed and unambiguous....”
- Cannot be conditional or “tied”
- Detriment
- Granularity / unbundled
- Balance of power is relevant

# Consent

- Consent via electronic means
- Ability to withdraw consent
- Children and information society services
- Relevance to data subject rights

# Consent for marketing

- Review the consents you hold
- Do they comply with GDPR?
- If not, look at refreshing consents
- Provide detailed information notice
- Keep records of all consents going forward

# Controllers and processor contracts

- Previous practice Vs Art. 28
- Higher stakes for both now
- Controllers must assess suitability of data processors
- Data processing agreement must set out specific provisions

# Controllers and processor contracts

- Process on basis of **documented instructions**, including **data transfers**
- **Staff** bound by **confidentiality**
- Take all **security measures** required under Art. 32
- Follow **sub-processing** rules
- Assisting controller with **data subject rights**
- Assist controller to **demonstrate compliance** with security
- Provide information to **show compliance** with Art. 28 – **audits and inspections**
- **Deletion and return of data**

# Controllers and processor contracts

- Warranties and indemnities
- Who is responsible to initiate change?
- How to approach in practice?

# Data subject rights

- Information and access
- Rectification
- Erasure (right to be forgotten)
- Restriction of processing
- Data portability
- Profiling rights
- Objection

# In summary

- Review applicability of GDPR
- What is our legal basis for processing?
- Is consent appropriate in future?
- Consider approach to contracts and implement change
- Data subject rights and practices



# PHILIPLEE

philiplee.ie  
info@philiplee.ie



**DUBLIN**  
7/8 Wilton Terrace  
Dublin 2  
Ireland  
T: +353 (0)1 237 3700  
F: +353 (0)1 678 7794

**BRUSSELS**  
39 Rue des Deux  
Eglises  
1000 Brussels,  
Belgium  
T: +353 (0)1 237 3700  
F: +353 (0)1 678 7794

**SAN FRANCISCO**  
201 Spear Street, Suite  
1100 CA 94105,  
United States  
T: +353 (0)1 237 3700  
F: +353 (0)1 678 7794

An Coimisinéir  
Cosanta Sonraí



Data Protection  
Commissioner

# “Insights on Data Protection Supervision for 2018 and beyond”

John Keyes LLB, BL  
Assistant Commissioner - Investigations  
Office of the Data Protection Commissioner



@DPCireland

Philip Lee and RSM  
Dublin – 27<sup>th</sup> February 2018

Countdown  
to

G

D

P

R



25<sup>th</sup> May 2018

# Irish SME Association (ISME) GDPR Survey

- ☐ Action to date on GDPR compliance by 507 SMEs
- ☐ Only 7% have completed GDPR plan
- ☐ 76% are concerned about GDPR
- ☐ 62% couldn't name any change GDPR will bring
- ☐ 70% have not identified steps/actions needed
- ☐ 59% have no staff member responsible for overseeing compliance and preparing for GDPR



# European Data Protection Legal Framework

- General Data Protection Regulation (GDPR) effective in law from 25<sup>th</sup> May 2018
- Data Protection Bill 2018 published by Government on 01 February 2018 – an important piece of the jigsaw
- Draft e-Privacy Regulation still under negotiation. Council, Parliament and Commission positions appear to have some ongoing distance between them. Unlikely to be implemented this year




# Focus of the GDPR

- Giving Data Subjects more control
- Making Data Controllers/Processors more accountable
- Making personal data processing more transparent
- Reducing personal data security vulnerabilities
- Co-operation between Supervisory Authorities on cross-border processing

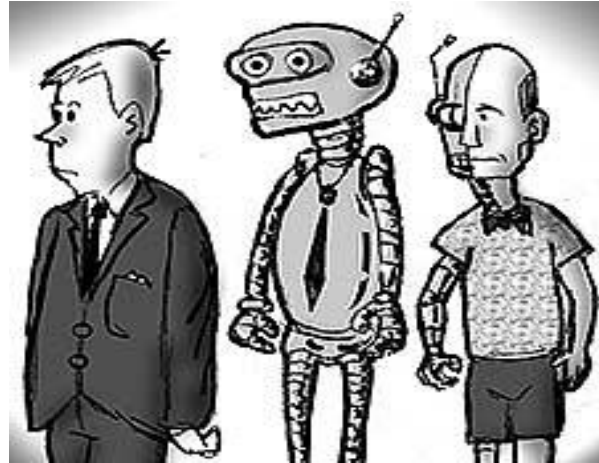


# What's largely unchanged in GDPR

- ❑ Concept of Personal Data
  - ❑ Acts of Processing
  - ❑ Data Protection Principles
  - ❑ Definitions of Data Controller/Processor
- 

# GDPR Definition of Personal Data (Article 4.1)

- any information
- relating to
- an identified or identifiable
- natural person






# Scope of Personal Data


- Article 29 Working Party Opinion 4/2007 on the concept of personal data
- *“data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated”*



# Data Protection Principles – Article 5(1)

- a) Processed lawfully, fairly and in a transparent manner...*
  - b) Collected for specified, explicit and legitimate purposes..*
  - c) Adequate, relevant and limited to what is necessary...*
  - d) Accurate and, where necessary, kept up to date....*
  - e) Kept in a form which permits identification for no longer than is necessary...*
  - f) Processed in a manner which ensures appropriate security...*
- 

# What's new in GDPR

- ❑ *Accountability – demonstrating compliance*
  - ❑ *Transparency – providing information pre-processing*
  - ❑ *Risk-based mandatory data breach reporting (72 hours)*
  - ❑ *Strengthened 'Consent' obligations*
  - ❑ *New and enhanced Data Subject rights*
  - ❑ *Administrative Fines*
  - ❑ *Data Protection Officer (DPO) for certain organisations*
- 

# Accountability

## Article 24.1

*“...the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation”*

## Article 24.3

*“Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller”*



# Transparency Requirements

At the time when personal data are obtained provide the data subject with information on;

- ☐ Identity of controller and DPO
- ☐ Purpose of processing and legal basis
- ☐ Source of the data
- ☐ Specific legitimate interest pursued, if applicable
- ☐ Recipients of the data
- ☐ Data transfer arrangements
- ☐ Retention period
- ☐ Right of access, rectification, erasure, objection
- ☐ Right to withdraw consent
- ☐ Right to lodge complaint with SA
- ☐ Details of the contractual or statutory basis
- ☐ Details of automated decision-making



# GDPR

- ☐ Personal Data Breach Risk Evaluation
  - ☐ Data Security
  - ☐ Transparency
  - ☐ Administrative Fines
  - ☐ Data Protection Bill 2018
  - ☐ Article 29 Working Party Guidance
- 

# Personal data breach risk evaluation

## Recital 75 GDPR

*“The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymisation, or any other significant economic or social disadvantage”*



# Data Integrity & Security

- DPC has noted countless cases of organisations simply not patching and keeping systems up to date
- Most current Breach notifications arise from preventable human errors and process deficiencies
- Mandatory breach reporting may open up potentially shocking vista





# Sources of Data Security Threats

## Internal Threats;

- ☐ Social engineering
- ☐ Physical theft
- ☐ Privilege abuse
- ☐ Copying to personal accounts or drives
- ☐ Unintentional data leaks
- ☐ Loss of company property

## External Threats;

- ☐ Social engineering
- ☐ Hacking
- ☐ Malware/Ransomware
- ☐ Malicious USB drops
- ☐ Physical theft



# Transparency

- 250 hours or 30 full working days would be required to read the privacy notices of the websites we typically visit each year (Source: Lorrie Cranor of the Federal Trade Commission)
- 30 hours would be required to read the 900 pages of user terms and conditions of the 33 apps typically found on a Norwegian smartphone (Source: The Norwegian Readathon)



# Transparency

- “Growing up Digital” taskforce of the Children’s Commissioner for England
- Social networking platform long privacy policy deemed ‘boring’ and not understood by group of teenagers
- *“Officially you own any original pictures and videos you post but we are allowed to use them and we can let others see them as well, anywhere around the world. Other people might pay us to use them and we will not pay you for that. We can share with other companies any personal information about you such as your birthday or who you are chatting with, including in private messages”*
- ‘Shocked’, less likely to engage and more likely to delete their accounts



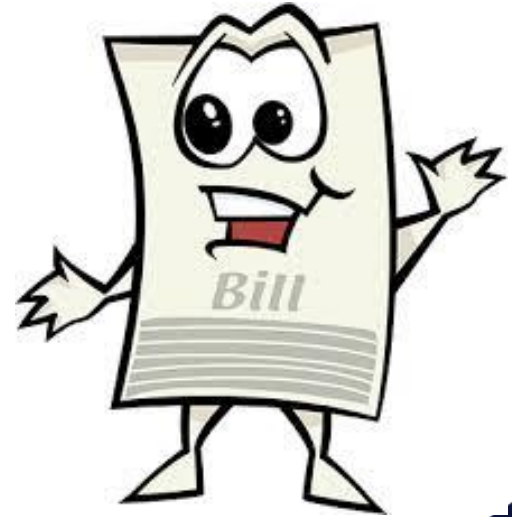
# Administrative Fines

- Article 83 GDPR and Sections 136-138 Data Protection Bill 2018)
- Section 136(3) – *The commission may decide to impose an administrative fine on a controller or processor that is a public authority or body only where the authority or body acts as an undertaking within the meaning of the Competition Act 2002*
- *Appeal to Circuit Court (up to €75,000) or the High Court in any other case*
- *Fine to be confirmed by the Circuit Court even if not appealed by the Controller*



# Data Protection Bill 2018

- 162 Sections in 8 Parts
- No repeal of 1988 and 2003 Acts
- No separate Law Enforcement Bill
- Many Sections require enactment of further Statutory Instruments (Regulations) to have full effect e.g. Section 54 general public interest provisions



# Article 29 Working Party Guidelines

- Data Portability
- Consent
- Transparency
- Personal Data Breach notification
- Profiling and Automated Decision Making
- Data Protection Officer (DPO)
- Lead Supervisory Authority
- Data Protection Impact Assessment (DPIA)



**ARTICLE 29**

Data Protection Working Party

**An Coimisinéir  
Cosanta Sonraí**



**Data Protection  
Commissioner**

[www.dataprotection.ie](http://www.dataprotection.ie)



@DPCireland

[info@dataprotection.ie](mailto:info@dataprotection.ie)

Thank You



WardSolutions

Assess | Protect | Detect | Respond

# GDPR Organisational and Technical Controls

## Agenda

- GDPR Key Benefits
- GDPR Organisational and Technical Controls
- GDPR Challenges

27th Feb 2018, Hilton Dublin

**Declan Timmons, Msc FCCI, Msc IS, Bsc IT**

CISM | NUIX Specialist Investigator | EnCE Forensics | ISO-27001 | Law Society Data Protection |



**Disclaimer:** This presentation does not represent legal advice or purport to be a legal interpretation of legislation, regulation or standard rules. Whilst every effort is made to ensure the information is accurate, responsibility cannot be accepted for any liability incurred or loss suffered as a consequence of relying on any material published herein. Appropriate professional advice should be taken before acting or refraining to act on the basis of this presentation.

# Company Overview – Who are we?

Founded	1998 - Reputation for Excellence
Markets	Information Security, System & Application Design, Integration & Management
Location	Dublin, Belfast and Limerick
Growth	65+ Staff and Hiring - Profitable, Growing 20% per annum
Sample Customers	
Key Partnerships	



Ward Solutions

Assess | Protect | Detect | Respond

Operation Centre

Network Operation Centre

Cyber Security Operations Centre



Ward Solutions

# GDPR – Key Benefits



# GDPR Benefits

- Harmonised approach to Data Protection in EU
- Opportunity to increase efficiency through a critical review of current business processes
- Cost savings from reduced storage requirements
- Brand Opportunity - “Safe Organisation” to share personal information with”
- Increase Consumer Confidence in e-Commerce

# Security Incidents Real life examples

What are the odds of ...



(Global average 28%)

# Passwords – Data Breaches

DATA BREACH (2012)

**Link**

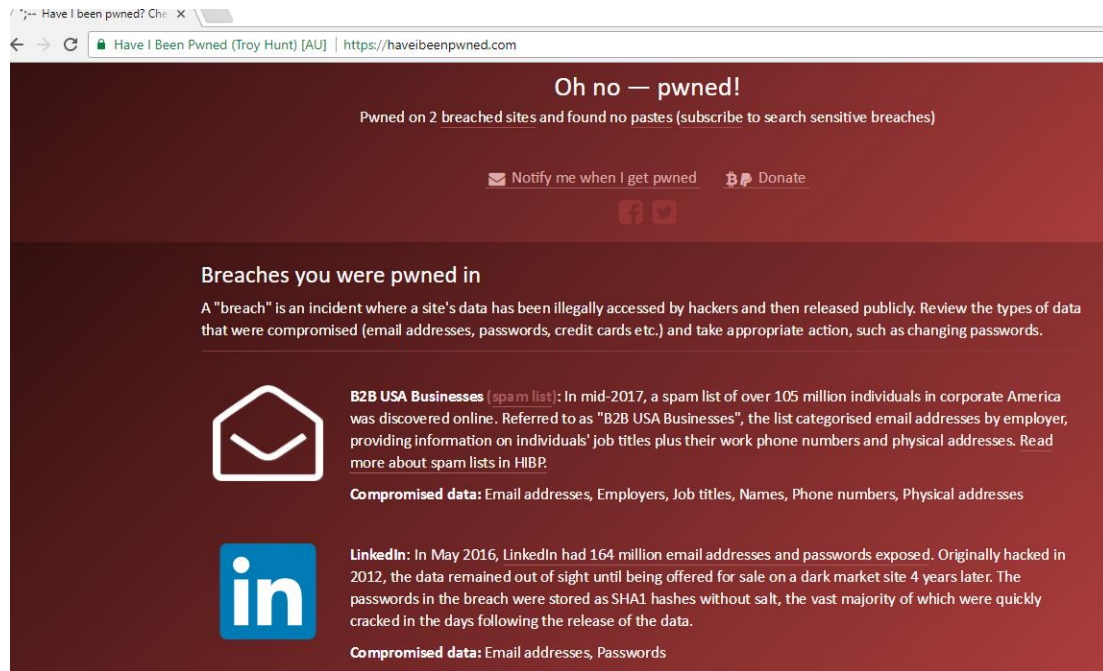
**HACKER A**

167 Million

**Linked in**

**Hacked** accounts on SALE!

# Passwords – Data Breaches



The screenshot shows a web browser window with the URL <https://haveibeenpwned.com>. The page has a dark red background and displays the message "Oh no — pwned!". Below this, it states "Pwned on 2 breached sites and found no pastes" with a link to "subscribe to search sensitive breaches". There are links for "Notify me when I get pwned" and "Donate". Social media icons for Facebook and Twitter are also present. The section "Breaches you were pwned in" explains that a "breach" is an incident where a site's data has been illegally accessed. It lists two breaches: "B2B USA Businesses (spam list)" and "LinkedIn".

Oh no — pwned!


Pwned on 2 [breached sites](#) and found no [pastes](#) ([subscribe to search sensitive breaches](#))

[Notify me when I get pwned](#) [Donate](#)

[Facebook](#) [Twitter](#)


### Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.



**B2B USA Businesses (spam list):** In mid-2017, a spam list of over 105 million individuals in corporate America was discovered online. Referred to as "B2B USA Businesses", the list categorised email addresses by employer, providing information on individuals' job titles plus their work phone numbers and physical addresses. [Read more about spam lists in HIBP.](#)

**Compromised data:** Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses

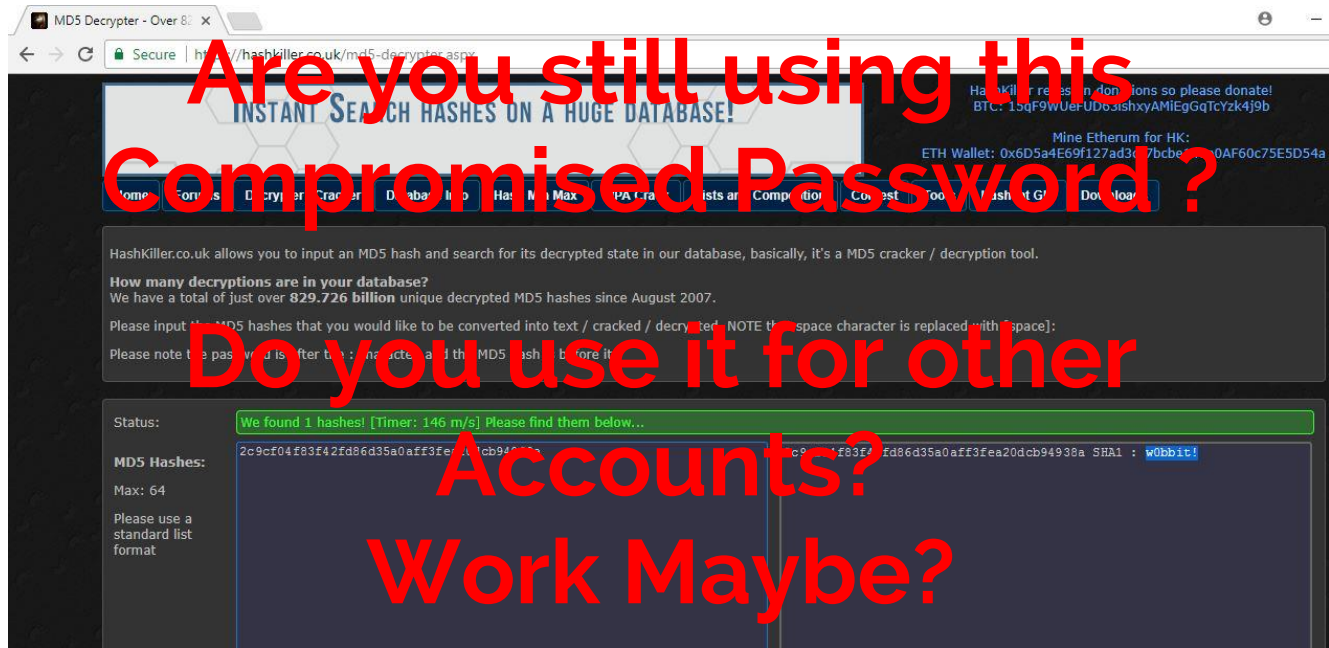


**LinkedIn:** In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

**Compromised data:** Email addresses, Passwords

<https://haveibeenpwned.com/>

# Passwords – Data Breaches



<https://hashkiller.co.uk/sha1-decrypter.aspx>





WardSolutions

Assess | Protect | Detect | Respond

Operation Centre

Network Operation Centre

Cyber Security Operations Centre



WardSolutions

# GDPR Organisational and Technical Controls

# Article 32 Security of Processing

## Article 32 EU GDPR "Security of processing"

=> Recital: [83, 74, 75, 76, 77](#)

=> administrative fine: [Art. 83 \(4\) lit a](#)

1. 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**, including inter alia as appropriate:

=> Article: [24](#)

=> Dossier: [Technical And Organisational Measures](#), [Obligation](#), [Risk For Rights And Freedoms](#)

(a) the pseudonymisation and encryption of personal data;

=> Article: [4](#)

=> Dossier: [Pseudonymisation](#), [Encryption](#)

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

=> Dossier: [Compliance](#)

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

=> Recital: [75](#)

=> Dossier: [Disclosure](#), [Risk For Rights And Freedoms](#), [Transmission](#)

3. Adherence to an approved code of conduct as referred to in [Article 40](#) or an approved certification mechanism as referred to in [Article 42](#) may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

=> Dossier: [Proof](#)

4. The controller and processor shall **take steps** to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them **except on instructions** from the controller, unless he or she is required to do so by Union or Member State law.

=> Article: [29](#)

2. The controller shall be responsible for, and be **able to demonstrate** compliance with, paragraph 1 ('accountability').

=> Article: [77, 82, 83](#)

=> Dossier: [Compliance](#), [Proof](#), [Obligation](#)

# Organisational and Technical Controls

## ***Security Accountability - Demonstrate Compliance***

Information Security Governance Framework (ISO27001)

## ***Determine as early as possible if you have been breached***

Managed SIEM/SOC Monitoring your Network

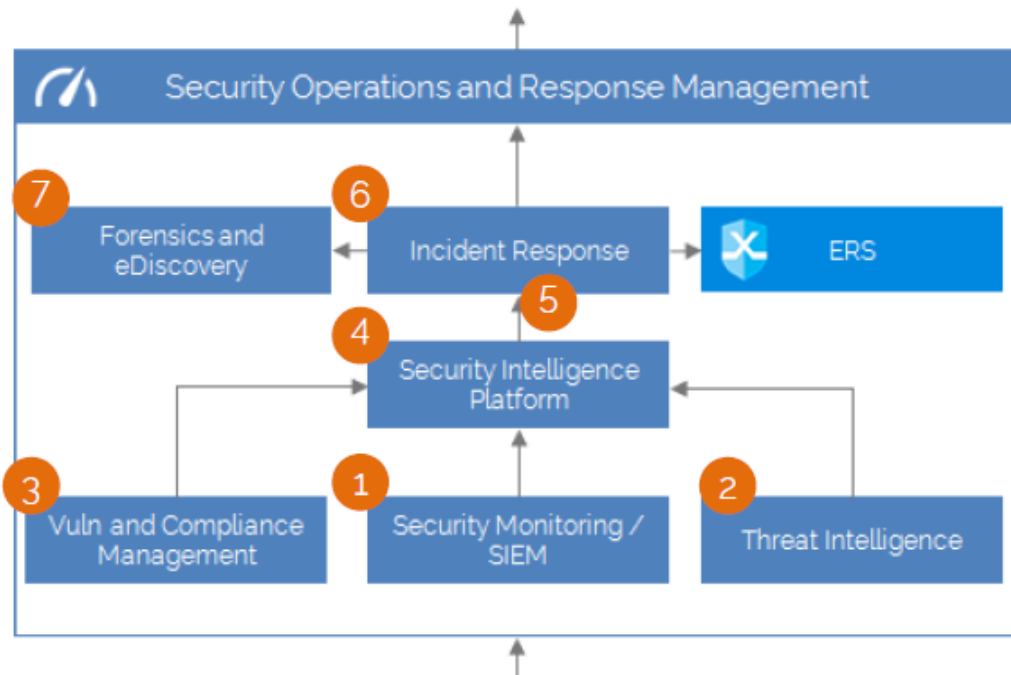
## ***Effective response to a Breach***

*Incident Response Management and Testing*

## ***Protect Data***

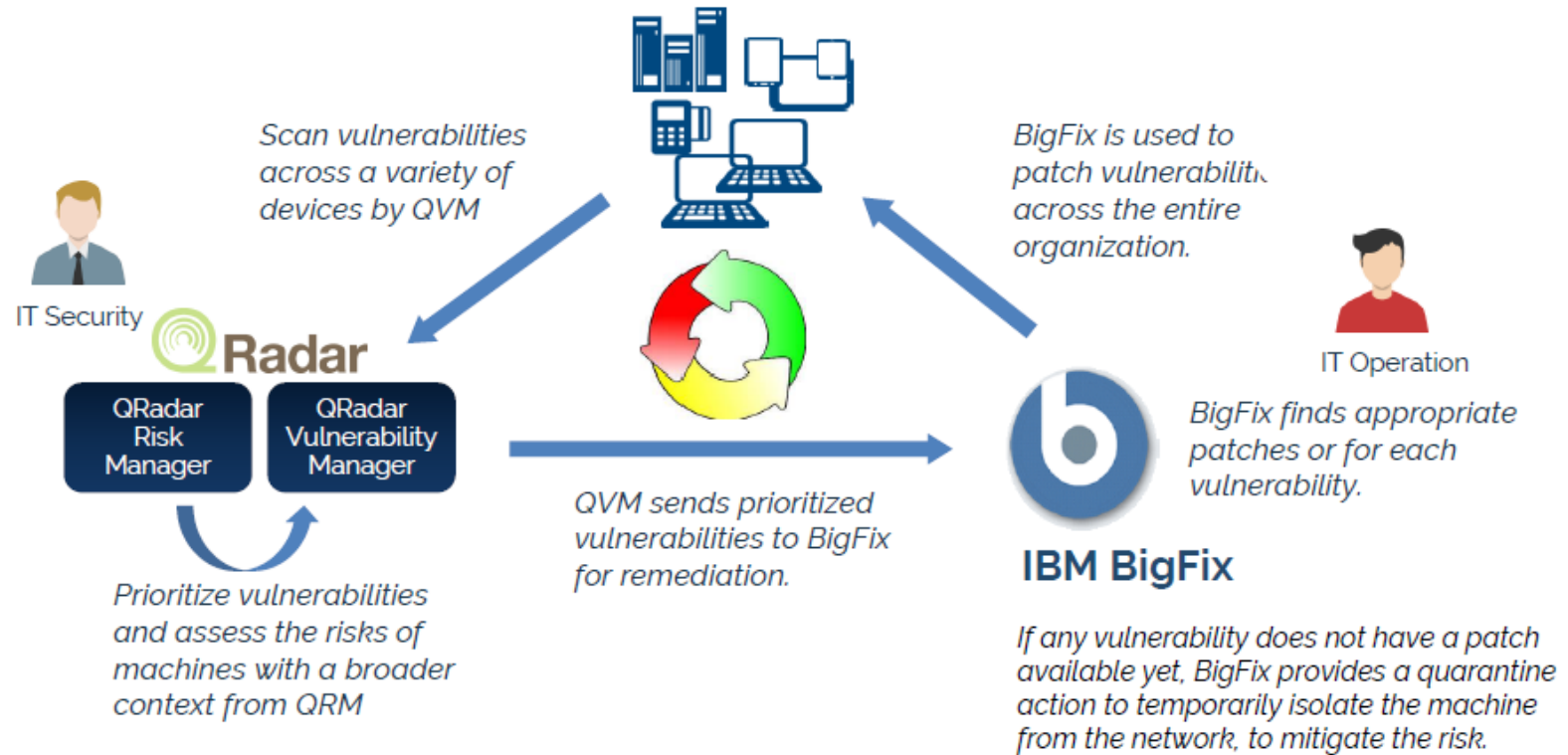
*Data Encryption or Data Pseudonymisation*

# Security Operations and Response (not just SIEM)

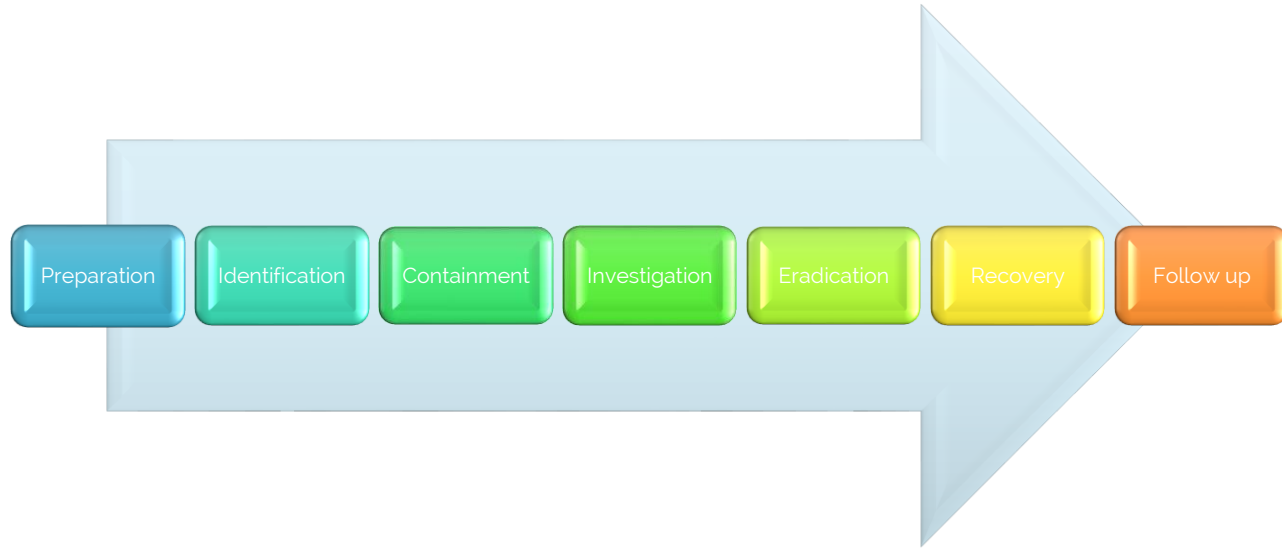


1. SIEM to generate offences
2. Enrich with threat intelligence.
3. Associate vulnerability data
4. Cognitive / AI / ML / Analysts
5. Offences become Incidents
6. Run IR playbooks.
7. Incident Forensics.

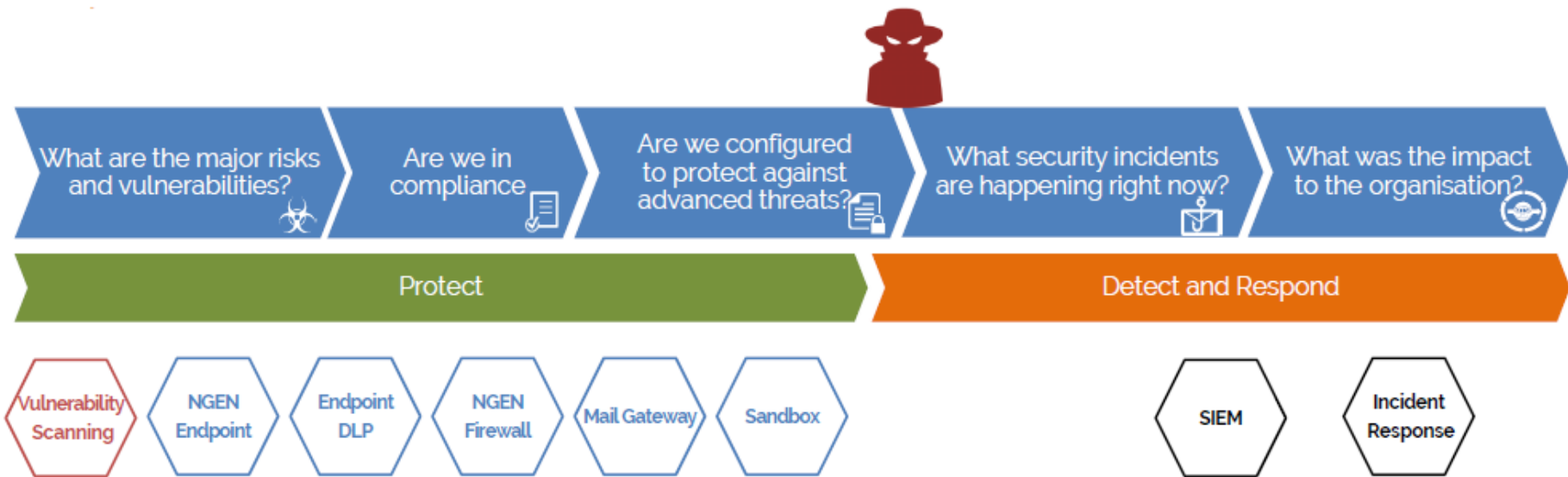
# Patch Management: IBM QVM



# Incident Management



# Incident Response



# Next Generation Endpoint

## Carbon Black

<https://www.carbonblack.com/>

SHARE



**How it works:** Carbon Black Endpoint Security Platform is another system that combines advanced analytics and behavior recognition to stop attacks. The platform incorporates three components: an advanced analytics, data science and behavior recognition core; a lightweight endpoint sensor that records all critical activity on the endpoint, flagging malicious activity for your security team; and an element that can thwart attacks by locking down critical systems using multiple levels of application control. Each of these elements is powered by Carbon Black's Collective Defense Cloud, which aggregates security data from more than 7 million endpoints to strengthen the entire customer base.

**What's unique:** Carbon Black's platform approach combines next-generation endpoint security with security policy controls, including the ability to whitelist applications. It also records all endpoint activity, and supports search so your team can gather security forensics and respond to attacks.

**Replace or supplement:** Carbon Black is a replacement for traditional anti-virus and other endpoint security solutions, but can integrate with existing SIEMs.

**Supports:** Windows, Mac and Linux

**Analytics:** Carbon Black has built-in analytics. It also integrates with existing SIEM, network security and threat intelligence solutions so you can perform user-behavioral analytics and other forms of analysis.

**Big brag:** Carbon Black was named "Best Endpoint Protection" in the SANS Institute's Best of 2014 Awards.





Ward Solutions

Assess | Protect | Detect | Respond

Operation Centre

Network Operation Centre

Cyber Security Operations Centre



# GDPR – Challenges



# Key Challenges for your organisation

- ✓ Managing Unstructured Data
- ✓ Migrating from Unstructured to Structured Data
- ✓ Data Minimization and Purge
- ✓ Data Retention and Purge
- ✓ Consolidation and Decommissioning
- ✓ Right to Access/Forgotten/Rectification
- ✓ Managing 3rd party Processors and Contracts



# Questions and Answers