(GDPR) SERVICE DEVELOPMENT WITH DATA PROTECTION BY DESIGN AND BY DEFAULT

John Timney (MVP)

REGULATION CONFUSION

- The General Data Protection Regulation (GDPR) was adopted as Regulation (EU) 2016/679 of the European Parliament and of the Council on April 27, 2016.
  - In contrast to the Data Protection Directive, the GDPR is intended to apply directly in each EU Member State without the need for implementing legislation, and to create a framework within which more detailed rules can be made. This harmonizes the legislation across Europe [see Territorial scope]. For example, the requirement to notify the DPA [see DPA] of new processing will be abolished (except in a limited number of cases) and be replaced by an obligation to document all processes. Controllers [see Data controller] and processors [see Data processor] must agree on the responsibilities between them; otherwise, they will be jointly and severely liable. The Regulation can be found online: http://eur-lex.europa.eu/legal-content/EN/TXT/
- **e-Privacy Directive**
  - The e-Privacy Directive was first adopted as Directive 2002/58/EC of the European Parliament and of the Council. It is currently controlling the privacy rights applied to electronic communications technology and content. The Directive can be found online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do
- **e-Privacy Regulation**
  - Following the adoption of the GDPR, the e-Privacy Directive will be revised to comply with the GDPR and address the technological innovations created since the Directive's last amendment in 2009. A draft proposal of the Regulation titled "Regulation on Privacy and Electronic Communications" was released on January 10, 2017. The Regulation will be applicable to any provider of electronic communications services or to any entity that processes electronic communications data. It will impact the way organizations interact electronically with EU citizens, including user tracking, data collection in user devices, and direct marketing.
- **UK Data Protection Act 2018**
  - The first draft of the Data Protection Bill (DPB) was released on 13 September 2017, following its second reading in the House of Lords. This bill is designed to bring the UK's data protection laws in line with the European Union's (EU) General Data Protection Regulation (GDPR).
- **Council of Europe Convention 108**
  - Equivalency guidance from the EU for non EU countries to ratifyt a level privacy law in their own country, to hel getting equivalency agreements in place for non-EU countries

CROSS SECTOR / FUNCTION – GDPR HAS DIFFERENCES BY SECTOR/BUSINESS FUNCTION AND HAS OTHER INDUSTRY REGULATION WHICH MAY OVERRIDE

Banking

- GDPR Lawful basis (LI, Consent, Contract, Legal Obligation)
- UK DPA 2018
- PECR
- Finance Act 2018

Government

- GDPR Lawful Basis (LI, Vital Interest, Public Task, Special category)
- UK DPA 2018
- Digital Economy Act 2017

Police

- GDPR Lawful Basis (LI, Vital Interest, Public Task, Criminal Offence)
- UK DPA 2018
- EU Law Enforcement Directive
- Policing and Crime Act 2017

Only GDPR cover Privacy by Design as an mandatory provable activity, but its not the only law with privacy expectations

GLOSSARY

- Privacy by Design = Data Protection by Design and Default
- Personally Identifiable Information
- Data Subject = a person or Citizen
- Controller
- Processor
- Software Development and services are interchangeable

JOHN TIMNEY

- Microsoft Office Services MVP
- 27 years+ of ugly IT
- 18 Years as an MVP
- Primarily worked in large organisations, on large projects
  - **IT Services Agency, Syntegra, BT PLC, Capgemini**
  - **Hewlett Packard Enterprise**
  - **DXC Technology**
  - **IBM**
- Specialise in Privacy, HYBRID CLOUD Advisory, Transformation at Scale, Hybrid 365/Azure Stack/Pack Strategy, Assurance and Governance
- Co- authored a few books on various SharePoint, JAVA and .NET subjects
- North East Administrator for the SharePoint UK User Group
- Co-Administrator for NEBytes (a Microsoft DEV and I.T Pro Group)

AUDIENCE

- GDPR took effect May 2018
- Developers, software architects, project managers, testers, operators, data protection officers and security advisors must adopt “Privacy by Design”
- It is an adaptive process
- It is unique to each business
- It never ends!

Its all about RISK to Citizen Data and you will be judged

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY

- **EU law** requires that controllers put in place measures to effectively implement data protection principles and to integrate the necessary safeguards to meet the requirements of the regulation and protect the rights of data subjects. These measures should be implemented both at the time of processing and when determining the means for processing. In implementing these measures, the controller needs to take into account the state of the art, the costs of implementation, the nature, scope and purposes of personal data processing and the risks and severity for the rights and freedoms of the data subject.

- https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

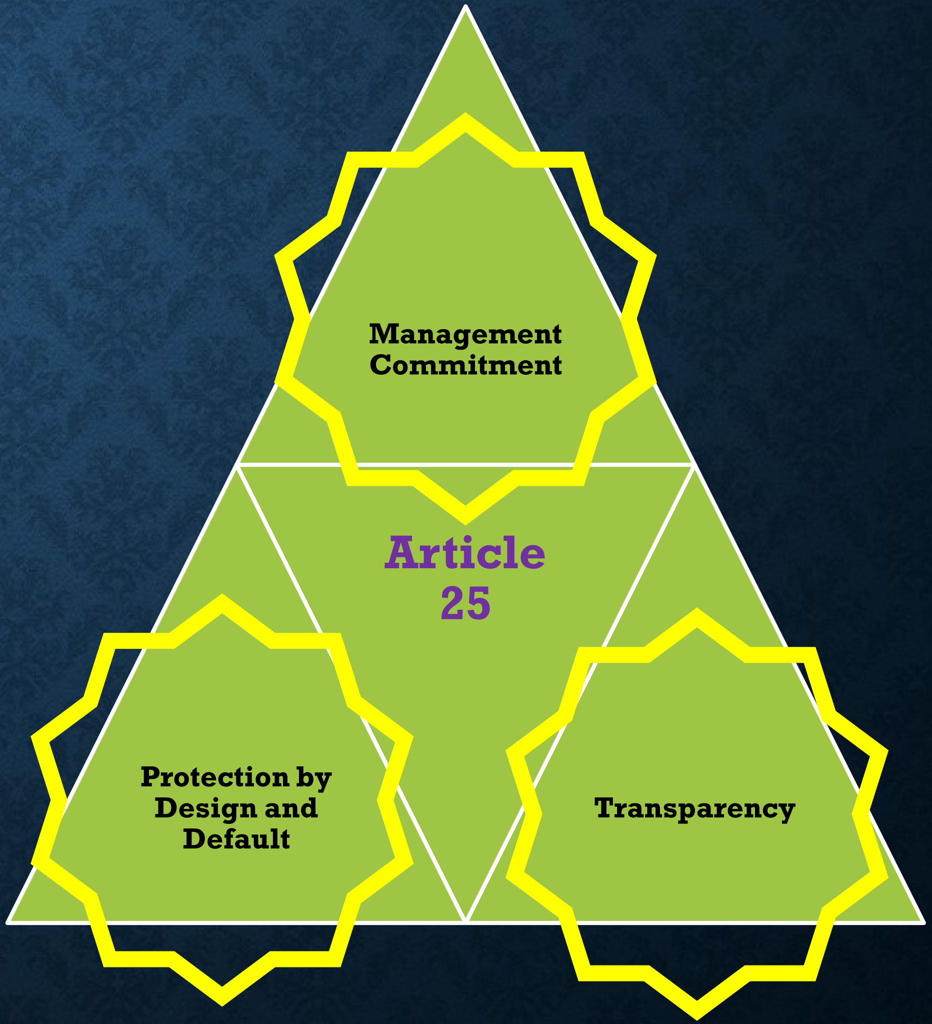
GDPR MANDATORY ARTICLE 25

- **Recital 78 Appropriate technical and organisational measures**
- "When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications"

Crafting a development or services BUILD process that works for your organisation, and protects citizen data

WHAT IS DATA PROTECTION BY DESIGN?

- Profiling, automated decision-making, and personalised services have become part of our day-to-day lives.
- These trends often involve processing of personal data on a large scale.
- Users expect services to both be secure and safeguard their privacy in an effective manner.
- Businesses that take data protection issues seriously, build trust. Thus, strong data protection measures can be a competitive advantage.



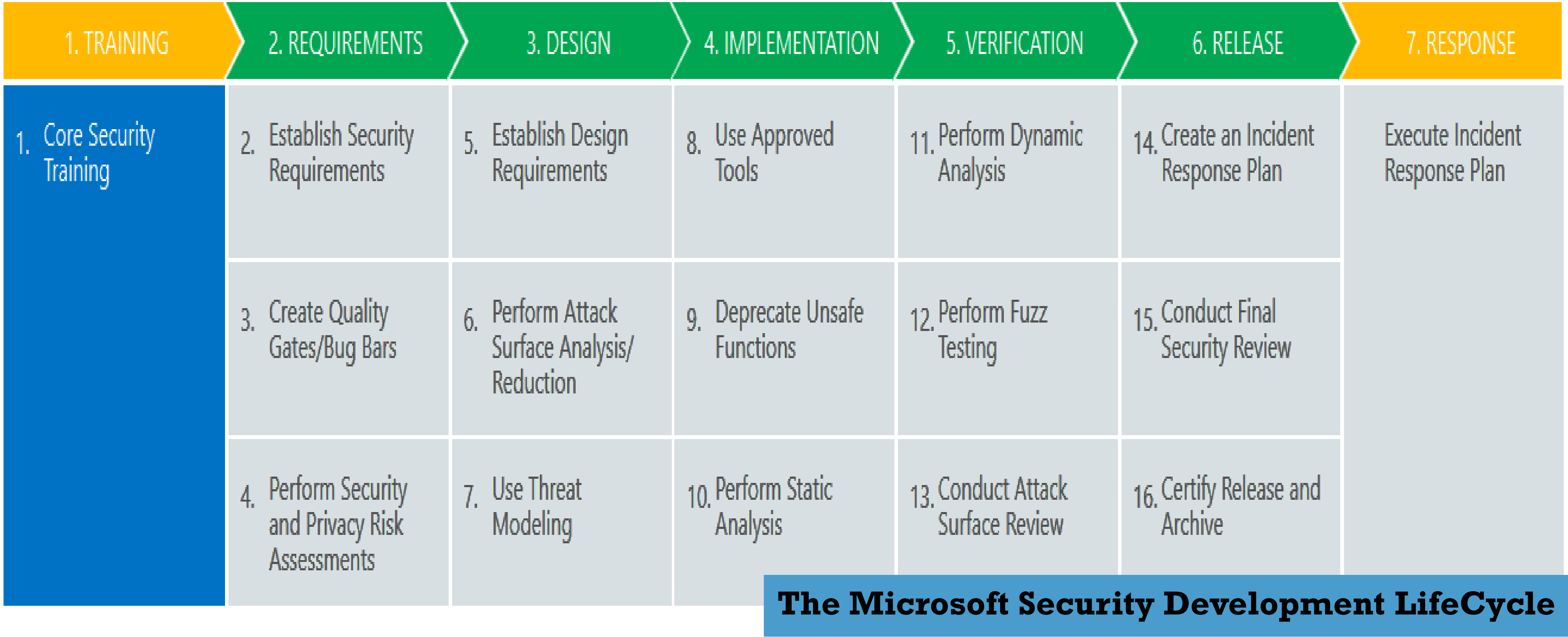
THE SDLC PROCESS

- SHOULD Follow a methodology with key activities to ensure that the final product is BREACH robust

  - Microsoft Security Development Lifecycle (SDL), (https://www.microsoft.com/en-us/SDL)
  - The *Open Web Application Security Project* Secure Software Development Life Cycle (S-SDLC) (https://www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project)
  - ENISA; (European Union Agency for Network and Information Security)
  - https://www.enisa.europa.eu/)

- Privacy and Data Protection by Design – from policy to engineering, as a starting point, and explored how to incorporate data protection principles, subject rights, and the requirements of the GDPR into every step of the process.

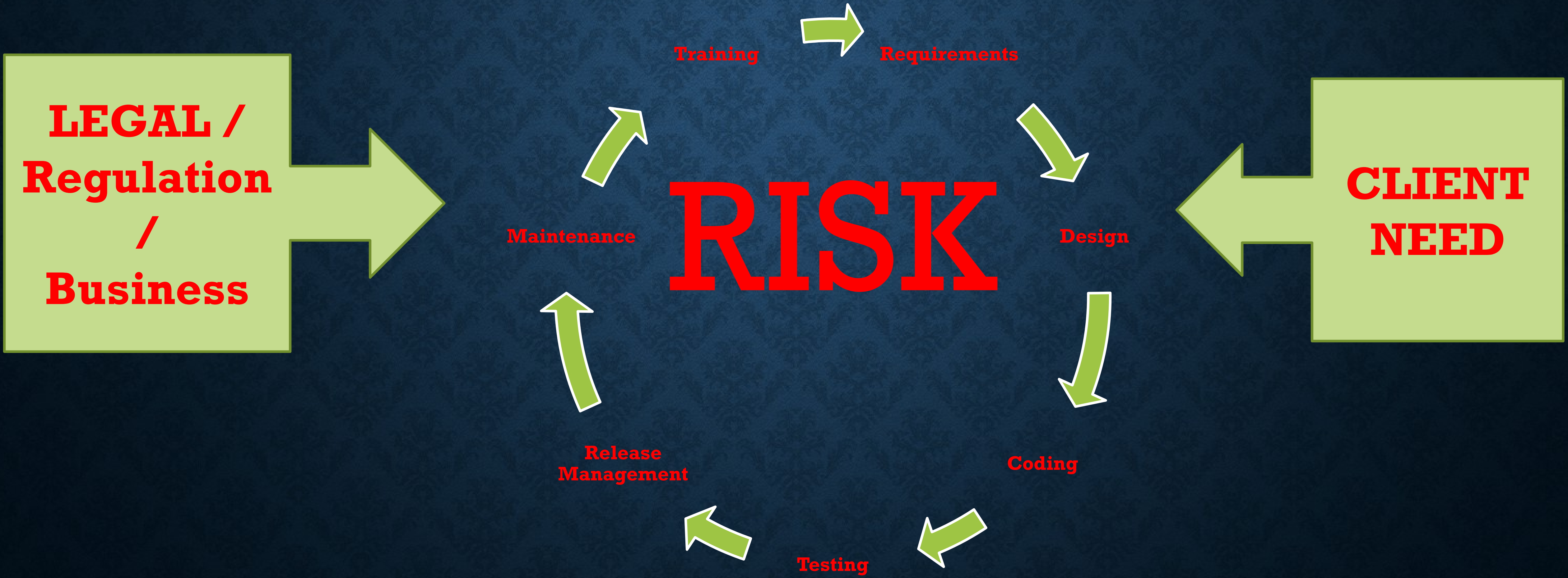
THE MICROSOFT SDL



1. TRAINING	2. REQUIREMENTS	3. DESIGN	4. IMPLEMENTATION	5. VERIFICATION	6. RELEASE	7. RESPONSE
1. Core Security Training	2. Establish Security Requirements	5. Establish Design Requirements	8. Use Approved Tools	11. Perform Dynamic Analysis	14. Create an Incident Response Plan	Execute Incident Response Plan
	3. Create Quality Gates/Bug Bars	6. Perform Attack Surface Analysis/ Reduction	9. Deprecate Unsafe Functions	12. Perform Fuzz Testing	15. Conduct Final Security Review	
	4. Perform Security and Privacy Risk Assessments	7. Use Threat Modeling	10. Perform Static Analysis	13. Conduct Attack Surface Review	16. Certify Release and Archive	

The Microsoft Security Development LifeCycle

ACTIVITIES



LEGAL / Regulation / Business

Training

Requirements

Design

Coding

Testing

Release Management

Maintenance

RISK

CLIENT NEED

TRAINING

Ensuring **that everyone in the organisation** understands the risks associated with data protection and security.

WHERE DO WE START

- Article 5 the lawfulness of processing,
- Article 6 conditions for consent,
- Articles 7 and 8 processing of special categories of personal data, and criminal offences,
- Articles 9 and 10 Chapter III concerning data subjects' rights
- Articles 12 - 23 Chapter IV on the duties of data controllers and data handlers,
- Articles 24-43, particularly privacy by design, and privacy by default, Records of data processing activity , Security of personal data, notification of personal data and information security breaches to the supervisory authority,and notification of data breach to the data subject
- data protection impact assessment and prior consultation
- data protection officer appointment, job descriptions, overview of tasks
- codes of conduct and certification
- laws and regulations related to the subject area of the software to be developed (e.g. patient record law, Privacy and Electronic Communications Regulation
- (ePrivacy), ICT regulation) mandatory business / sector / industry requirements and code of conduct
- the organisation's own information security requirements and guidelines
- the organisation's own internal security protocols
- roles and organization in the organisation relating to privacy and information security
- Information Security Framework (e.g. ISO27001, Standard of Good Practice (SoGP))
- Framework for software development (e.g. Microsoft Security Development Lifecycle (SDL), ISO27034 security testing (e.g.OWASP Top 10, OWASP Testing Guide, OWASP ASVS walkthrough)
- threat and risk assessment (e.g.STRIDE, DREAD, Microsoft Threat Modelling Tool)
- documentation requirements

WHAT IS IMPORTANT FOR EMPLOYEES TO LEARN

- An understanding of data protection and information security
- Regulation
- What data needs protecting in the tools that they use
- What they should look out for
- Creating a more communicative culture
- which methodology and security practices should be followed
- To contribute to the training plan

WHICH TRAINING REQUIREMENTS APPLY FOR THE ORGANISATION?

- Relevant internal and external requirements

- Data protection, information security, internal control, and resource management
- Regulatory and mandatory requirements
- Best practices, standards, code of conducts
- Permitted tooling (Collaboration, Storage, IDEs, Security Testing)
- OWASP Application Security Verification Standard Project (OWASP ASVS)
- OWASP Top 10
- OWASP Testing Project

The *Open Web Application Security Project* (*OWASP*)

INTERNAL/EXTERNAL REGULATION

Examples of these include the Freedom of Information Act, the Patient Records Act, the pending ePrivacy Regulation, the Regulations on the Use of Information and Communications Technology (ICT), the framework for information security (for example ISO27001, and the ISF Standard of Good Practice for Information Security (SoGP).

CORE TOOLS FOR PRIVACY IM

- Microsoft Trust Centre
- https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx
- https://servicetrust.microsoft.com/
- Compliance Manager

- Code of Conduct (Article 40) Guidance
- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct

REQUIREMENTS

- Requirements for data protection and information security
  - Data protection and information security
  - Exist in the project plan.

- Try and Identify the requirements for data protection, security, tolerance levels, data protection impacts, and security risks early in the lifecycle
- Service Development then know which privacy requirements they need to meet, and which risks to mitigate associated with data protection and information security across the SDLC.

CRAFT REQUIREMENTS AROUND DATA PROTECTION PRINCIPLES

- The processing shall be lawful, fair and transparent.
- Processing of personal data shall be carried out for specified, explicit and legitimate purposes
- Only data that is necessary for the software to function shall be collected
- How the personal data will be used
- Be Concise
- Ensure protection of data subject’s rights
- Encryption and access control are examples of measures that can be used to help ensure security.
- https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/?q=security

- Read Up On:
    - OWASP ASVS
    - ISO27001
    - The ISF Standard of Good Practice for Information Security (SoGP)

KNOW YOUR RISK TOLERANCE LEVELS

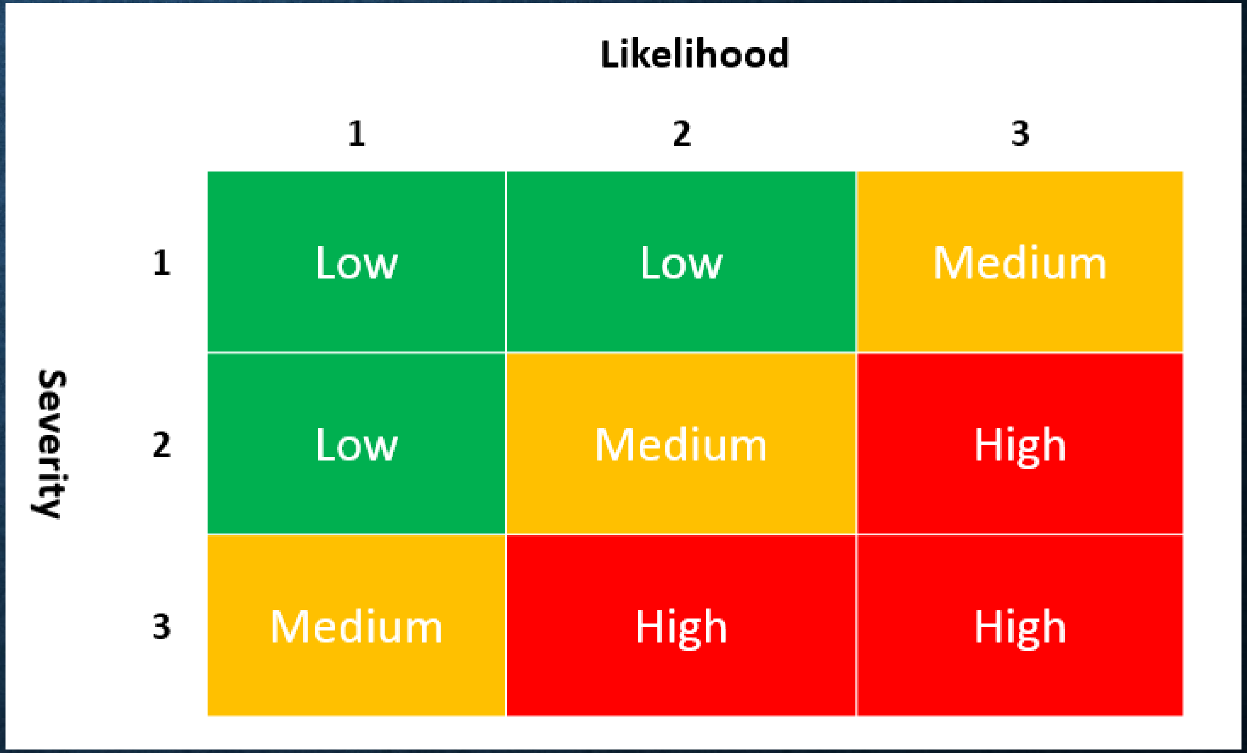
- Identify the impact of different incidents or scenarios
  - how likely or easy it is that something horrible occurs.
    - accidental alteration of personal data,
    - unauthorised disclosure of personal data
    - lack of access that could significantly affect life and health
    - losing control over his/her personal data
    - being subjected to discrimination based on profiling
    - being re-identified from anonymised data.

- Security Tolerance
- Data Protection Tolerance

Management OWN the tolerance levels, i.e. risk appetite

RISK ASSESSMENTS

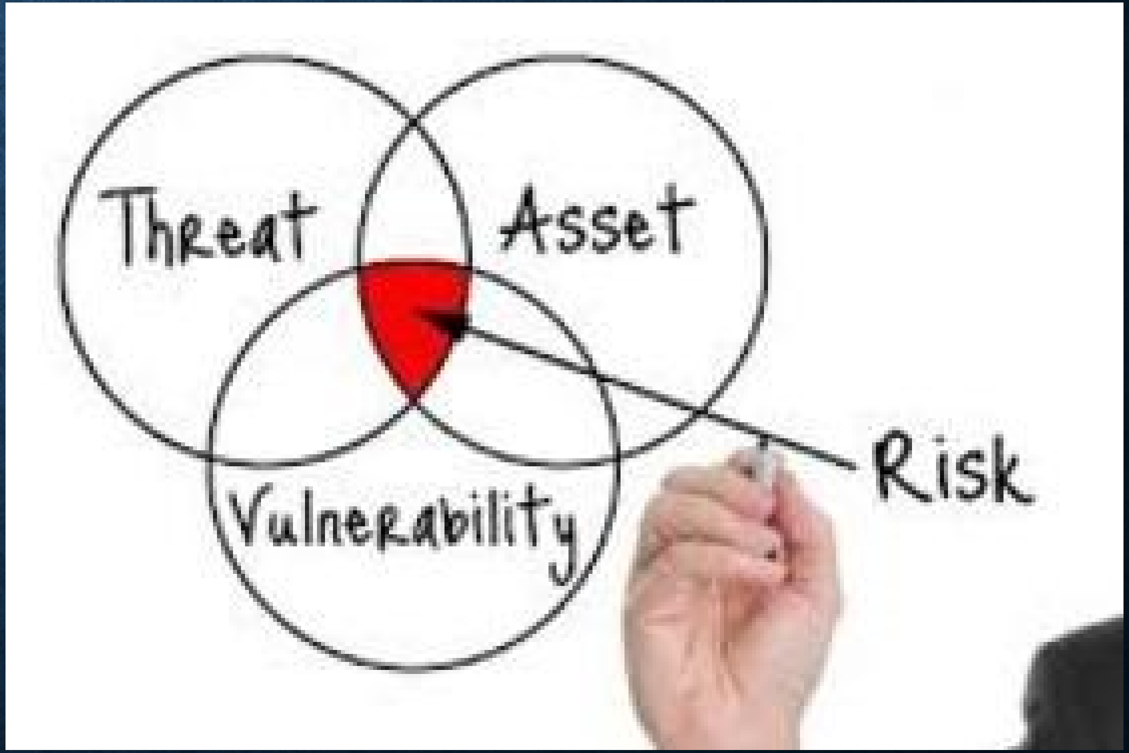
- Contains:
  - Security Risk Assessment
    - Threat assessment
    - Industry Specific Regulatory guidance
  - DPIA (official evidence Term in GDPR)



		Likelihood		
		1	2	3
Severity	1	Low	Low	Medium
	2	Low	Medium	High
	3	Medium	High	High

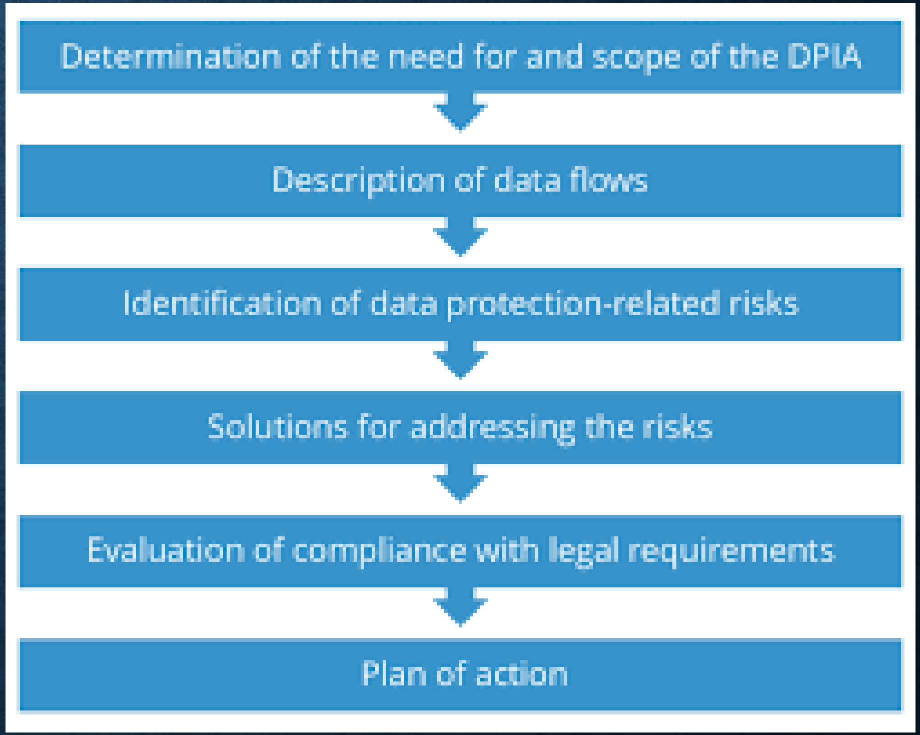
THREAT ASSESSMENT

- identify which actors could be interested
- Seek attack vectors
- detect vulnerabilities
- Reinforce security tolerance levels
- Identify Owners
- Identify Deadlines



DATA PROTECTION IMPACT ASSESSMENT

- be lawful, fair, and transparent
- Identify automated decision-making
- Identify the legitimate interest
- Show measures to address risks
- Define what to do for unmitigated risk



Determination of the need for and scope of the DPIA

Description of data flows

Identification of data protection-related risks

Solutions for addressing the risks

Evaluation of compliance with legal requirements

Plan of action

If you cannot mitigate risk, you should contact the ICO for a prior consultation

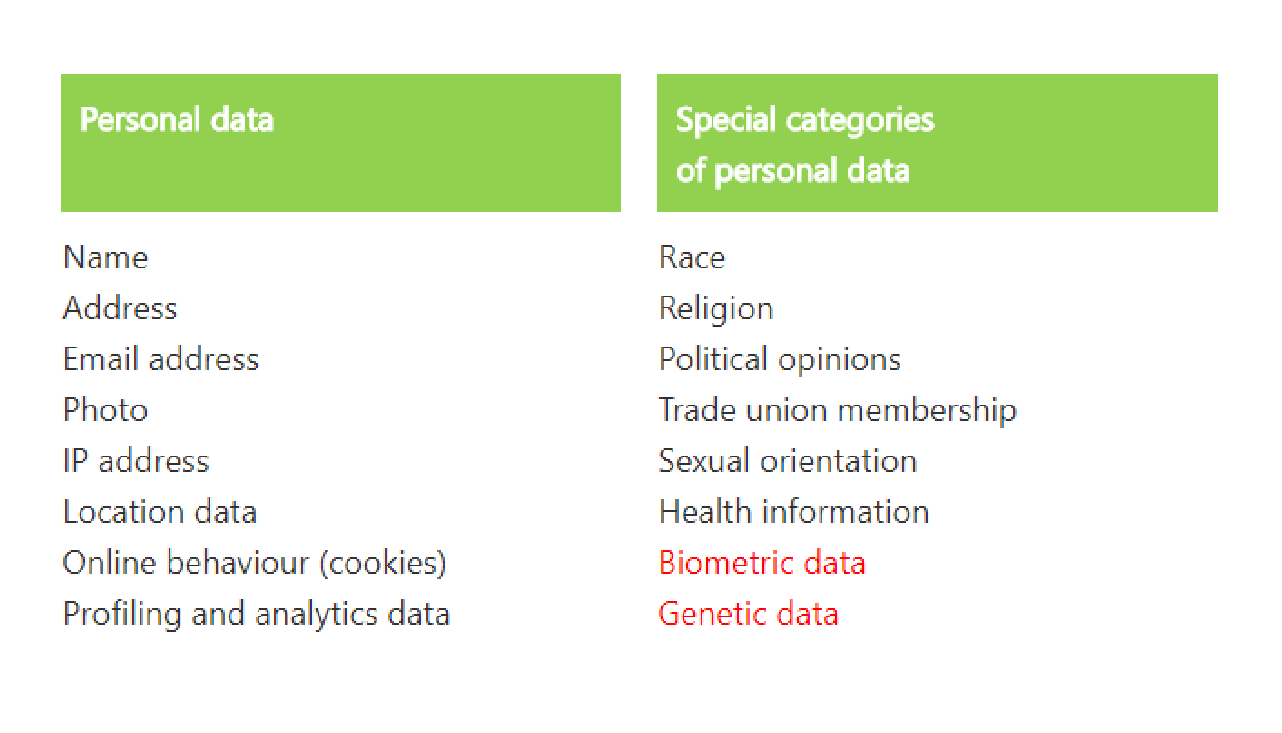
CRAFTING A DPIA

- Identify the need for a DPIA
- Describe the information flows
- Identify and assess the privacy risks
- Identify and approve controls
- Assign responsibility for implementing controls
- Re-assess and accept the risks.

- https://www.dur.ac.uk/ig/dp/dpia/

DESIGN

- It is "really" about designing to protect Personally Identifiable Information (PD)
- During this activity, you must ensure that requirements for data protection and information security are reflected in the design. The requirements identified during the requirements activity must be met, and requirements for the design must be defined.
- It is important to take into account the existence of threat actors that may attempt to obtain and gain access to personal data. To reduce the attack surface, it must be analysed, and the software modelled and designed to ensure a robust end product.



Personal data	Special categories of personal data
Name	Race
Address	Religion
Email address	Political opinions
Photo	Trade union membership
IP address	Sexual orientation
Location data	Health information
Online behaviour (cookies)	Biometric data
Profiling and analytics data	Genetic data

DATA ORIENTED DESIGN REQUIREMENTS (MANDATES)

- Minimise and limit (**Article 25** - **Article 5 (1) c**)
- Hide and protect **(Article 32) -** For example, personal data can be stored in separate databases, units, components and areas. Separation avoids linkability between different data sets.
- Separate and pseudonymize **(Article 3)**
- Aggregate (**Recital 162)** you can for example combine statistical data about large numbers of people without identifying individuals.

- Data protection by default **(Article 25)**

PROCESS ORIENTED DESIGN REQUIREMENTS (MANDATES)

- Inform – The software should be designed and configured so that the data subject is sufficiently informed on how the software works and how personal data is processed.
- Control – The data subject has the right to control their own personal data.
- Enforce – The software should be designed so that it may facilitate documenting how it safeguards the data subject's rights
- Demonstrate – The controller must be able to document compliance with the data protection regulation and security of processing.

REDUCE OPPORTUNITIES TO EXPLOIT VULNERABILITIES

- Analyse the attack surface of the designed software to reduce attack vectors and opportunities to exploit weak points and vulnerabilities..
- Use the assessments of both security risks and data protection impacts that were completed during the requirement activity to find Vulnerabilities
- Threat modelling involves the analysis of components, access points, data flow, and process flow within the software.
- Carry out a risk assessment of any vulnerabilities that remain, and which must be mitigated using other measures.

- RINSE AND REPEAT

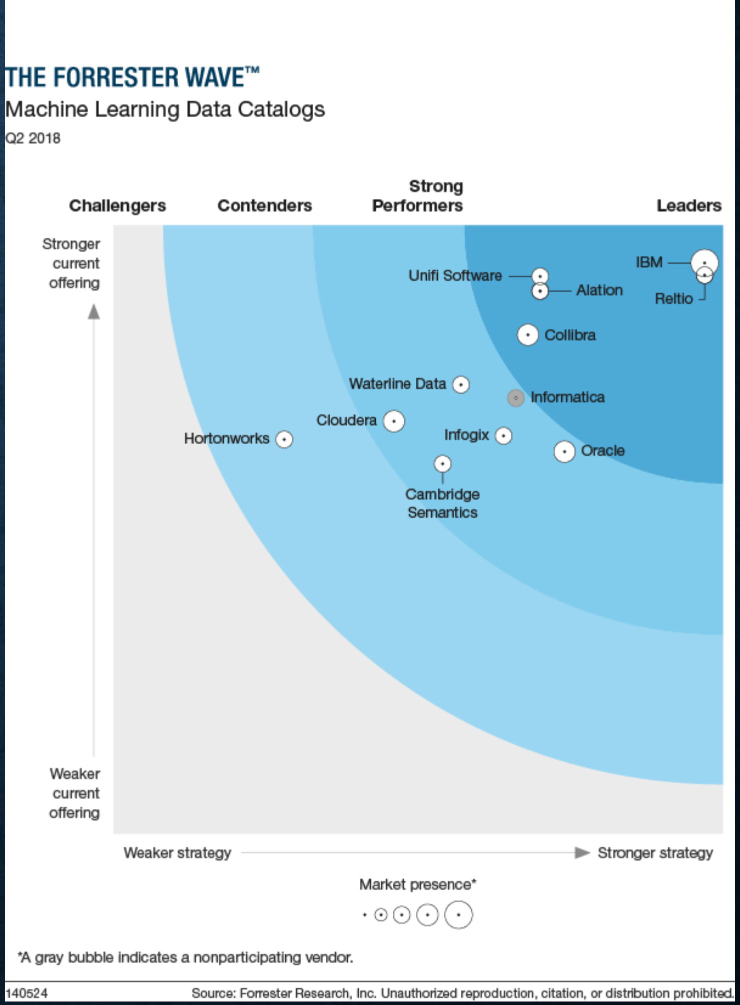
DON’T GET LOST IN THE COMPLEXITY

- Data cataloguing, and understanding personal data is then key
  - https://reprints.forrester.com/#/assets/2/600/RES140524/reports

- Look to Microsoft Compliance Manager and how you might use it
- Look to Azure Information Protection Scanner, to include services on-premise

- Catalogue Information like your business depends upon it

- Know what data needs to be protected, in what services and constantly evaluate and score for this



THE FORRESTER WAVE™

Machine Learning Data Catalogs

Q2 2018

*A gray bubble indicates a nonparticipating vendor.

140524

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

CODING

- This activity will enable developers to write secure code by implementing the requirements for data protection and security.
- It is important that the company choose a secure and common methodology, both for coding and for enabling the developers to detect and remove vulnerabilities from the code. Automated code analysis tools should be introduced, and the company must have established procedures for static code analysis and code review.
- Tools, support systems, and infrastructure should be “state of the art”; i.e. , the newest and most updated version of the technology, cf. Article 25.

USE APPROVED TOOLS AND FRAMEWORKS

- List approved and permitted tools, processes, and frameworks
- What the different tools can be used for
- Which components and development tools are permitted
- Risk-assessed and analysed for vulnerabilities
  - Also:
    - **Vulnerability Static Analysis for Containers (GITHUB)**
    - **Docker Security Scanning**
  - **/sdl (Enable Additional Security Checks)**

DISABLE UNSAFE FUNCTIONS AND MODULES

- Functions, APIs, third-party libraries and modules can be unsafe
- Analysis should be performed on all functions, APIs, third-party libraries and modules
- Replace blacklisted features with alternatives
- Deactivate unnecessary collection of personal data.

- Regularly check vulnerabilities with **OWASP Dependency Check**

The *Open Web Application Security Project* (*OWASP*)

QUALITIES TO LOOK FOR IN A CODE ANALYSIS TOOL

- It should be designed for security
- It should support multiple levels
- It must be possible to expand.
- It must be useful to both security analysts and developers.
- It should support existing development processes.
- It should have value for Multiple Parties with ownership of the development

Adding Continuous Security Validation to your Microsoft CI/CD Pipeline
https://docs.microsoft.com/en-us/vsts/articles/security-validation-cicd-pipeline?view=vsts

RELEASE MANAGEMENT

- Planning for post-release incidents
- A final security review should be done before any major release.
- An incident response plan should be established
- Security reviews should be carried out upon each release.
- Archive all relevant data from the development process.

INCIDENT RESPONSE PLAN

- Resources and a contact point or response centre
- Relevant contact information for support and escalation, including the DPO
- Code from third-parties
- Response Time
- Communication channels
- The incident life cycle
- Log file handling
- Notification process for ICO / Subjects
- Llessons learned
- Patching regime

The plan should be updated and rehearsed regularly, as lessons are learned

SECURITY REVIEW OF THE SOFTWARE/SERVICE

- Based on previous reviews during the development process
- Seek deviations
- Use different groups of experts
- Seek and Document Release approvals
- Verify from the plan who has final approval to release the software
- Documentation from the entire development process should be archived

Archiving is important for customers and supervisory authorities – Audit Trail

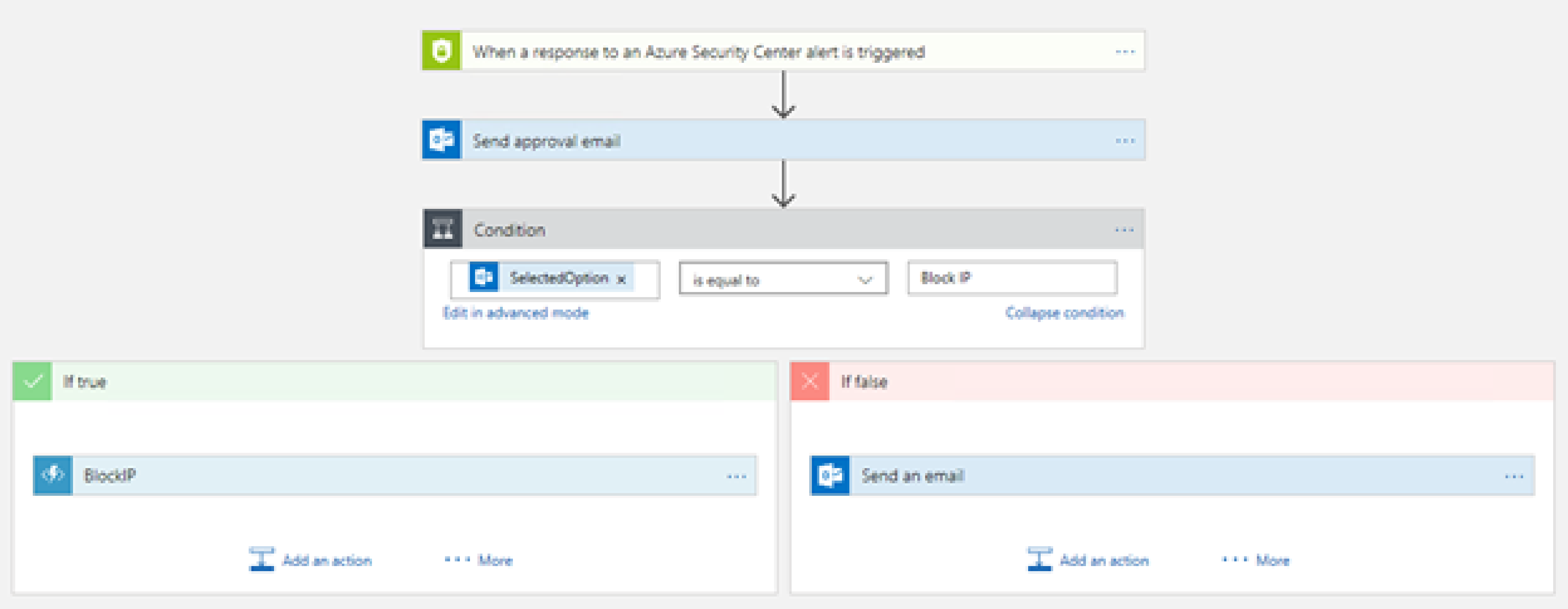
MAINTENANCE

- Implement a plan for incident response handling
- Be prepared to handle incidents, security breaches, and attacks
- Done via a response centre

HANDLING INCIDENTS AND DATA BREACHES

- Operate the plan – Period
- Stay calm and analyse the incident
- If you need to change the plan – invoke contacts and document
- Understand crisis management (https://www.local.gov.uk/our-support/guidance-and-resources/comms-hub-communications-support/cyber-attack-crisis)
- Invoke Reporting through defined channels
- If serious – inform the ICO via your DPO

AZURE SECURITY PLAYBOOKS



When a response to an Azure Security Center alert is triggered

Send approval email

Condition

SelectedOption is equal to Block IP

If true

BlockIP

If false

Send an email

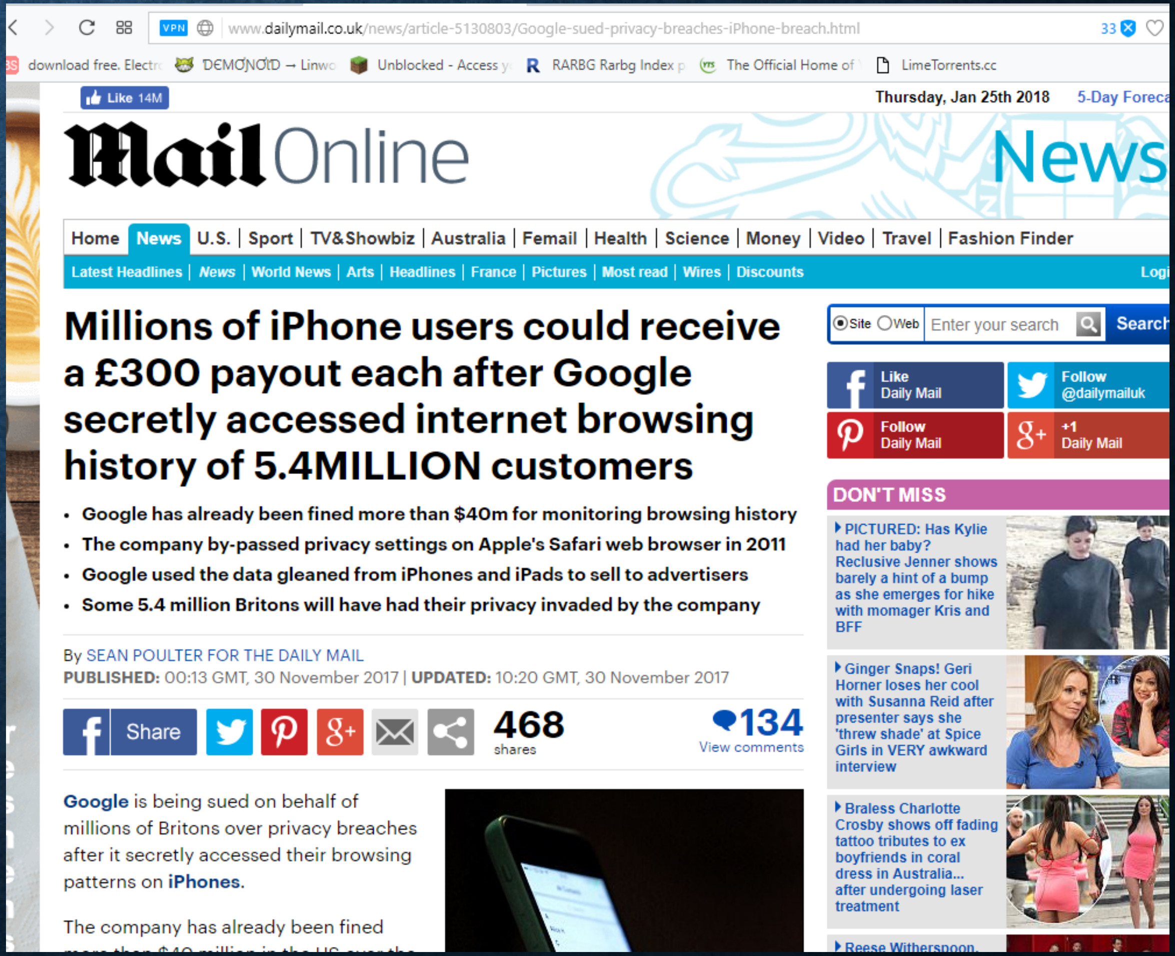
https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

MAINTENANCE, SERVICE AND OPERATION OF THE SOFTWARE

- Maintenance, service and operation of the software
- Continuous safeguarding of data protection and security
- Security testing
- Patching Schedules
- Log cleansing
- Validate you are not breaching the rules on TRANSPARENCY and approved USE
- Conduct regular external and internal audits

PRIVACY BREACH

- Understand Article 25
- Wrap your information management processes in GDPR
- Outline the processes, test them
- Have a response plan, test it
- Understand your risk
- Understand your cost
- Know who is at fault
- Notify


VPN
www.dailymail.co.uk/news/article-5130803/Google-sued-privacy-breaches-iPhone-breach.html
33
download free. Electr
DEMONOID – Linwo
Unblocked - Access y
RARBG Rarbg Index p
The Official Home of
LimeTorrents.cc
Like 14M
Thursday, Jan 25th 2018
5-Day Foreca
MailOnline
News
Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money | Video | Travel | Fashion Finder
Latest Headlines | News | World News | Arts | Headlines | France | Pictures | Most read | Wires | Discounts
Logi
○ Site ○ Web Enter your search Search
Like Daily Mail
Follow @dailymailuk
Follow Daily Mail
+1 Daily Mail
Share
468 shares
134 View comments

Millions of iPhone users could receive a £300 payout each after Google secretly accessed internet browsing history of 5.4MILLION customers

- Google has already been fined more than $40m for monitoring browsing history
- The company by-passed privacy settings on Apple's Safari web browser in 2011
- Google used the data gleaned from iPhones and iPads to sell to advertisers
- Some 5.4 million Britons will have had their privacy invaded by the company

By SEAN POULTER FOR THE DAILY MAIL

PUBLISHED: 00:13 GMT, 30 November 2017 | **UPDATED:** 10:20 GMT, 30 November 2017

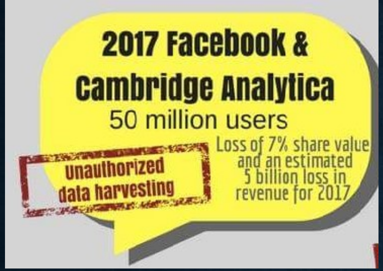
Google is being sued on behalf of millions of Britons over privacy breaches after it secretly accessed their browsing patterns on **iPhones**.

The company has already been fined

DON'T MISS

- PICTURED: Has Kylie had her baby? Reclusive Jenner shows barely a hint of a bump as she emerges for hike with momager Kris and BFF
- Ginger Snaps! Geri Horner loses her cool with Susanna Reid after presenter says she 'threw shade' at Spice Girls in VERY awkward interview
- Braless Charlotte Crosby shows off fading tattoo tributes to ex boyfriends in coral dress in Australia... after undergoing laser treatment
- Reese Witherspoon

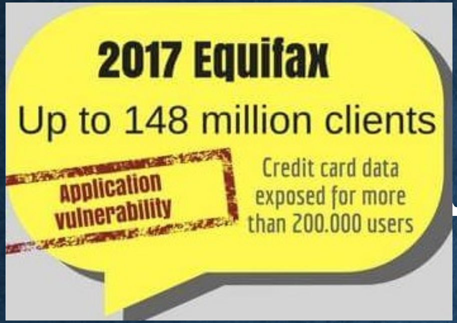
RT8


2017 Facebook & Cambridge Analytica

50 million users

Unauthorized data harvesting

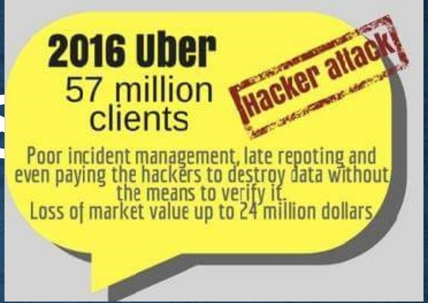
Loss of 7% share value and an estimated 5 billion loss in revenue for 2017


2017 Equifax

Up to 148 million clients

Application vulnerability

Credit card data exposed for more than 200.000 users


2016 Uber

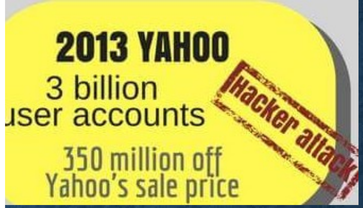
57 million clients

Hacker attack

Poor incident management, late repoting and even paying the hackers to destroy data without the means to verify it.

Loss of market value up to 24 million dollars

The result of the deliberate, criminal actions of a disgruntled former employee. He exploited his legitimate working access to Morrisons' databases to steal and post online the personal details of almost 100,000 Morrisons employees


2013 YAHOO

3 billion user accounts

Hacker attack

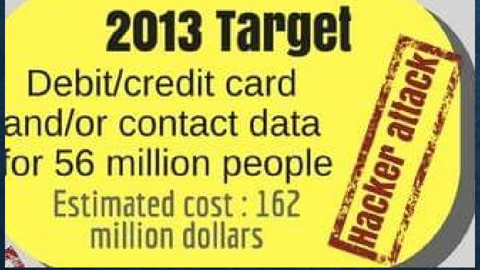
350 million off Yahoo's sale price

- Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

data for 56 million clients

Expenses over 160 million dollars for this breach

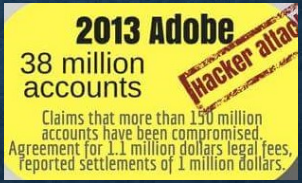
Malware


2013 Target

Debit/credit card and/or contact data for 56 million people

Estimated cost : 162 million dollars

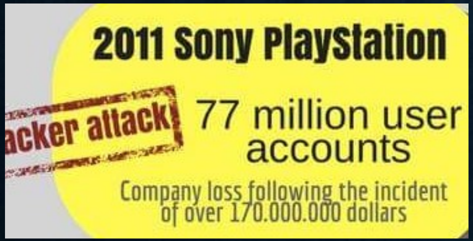
Hacker attack


2013 Adobe

38 million accounts

Hacker attack

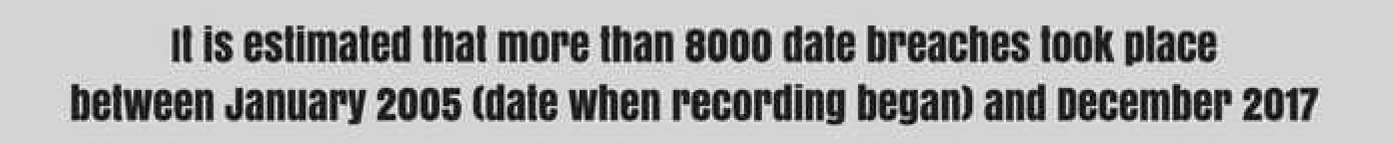
Claims that more than 150 million accounts have been compromised. Agreement for 1.1 million dollars legal fees, reported settlements of 1 million dollars.


2011 Sony PlayStation

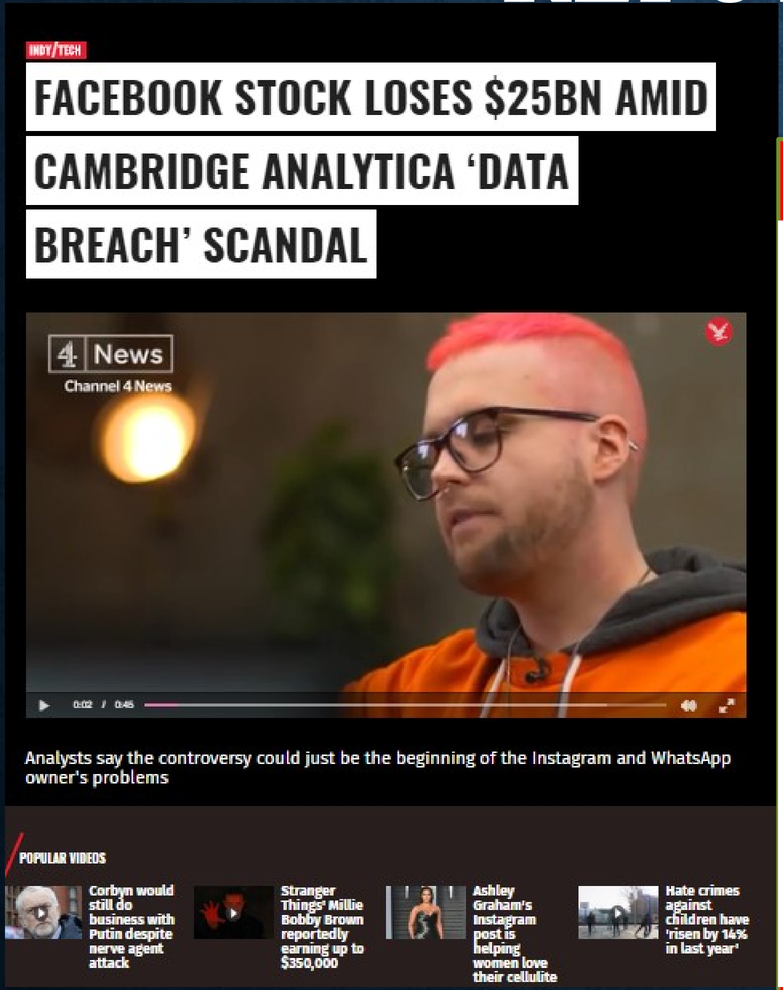
Hacker attack

77 million user accounts

Company loss following the incident of over 170.000.000 dollars


It is estimated that more than 8000 date breaches took place between January 2005 (date when recording began) and December 2017

REPUTATIONAL LOSS



INDY/TECH

FACEBOOK STOCK LOSES $25BN AMID CAMBRIDGE ANALYTICA 'DATA BREACH' SCANDAL

Analysts say the controversy could just be the beginning of the Instagram and WhatsApp owner's problems

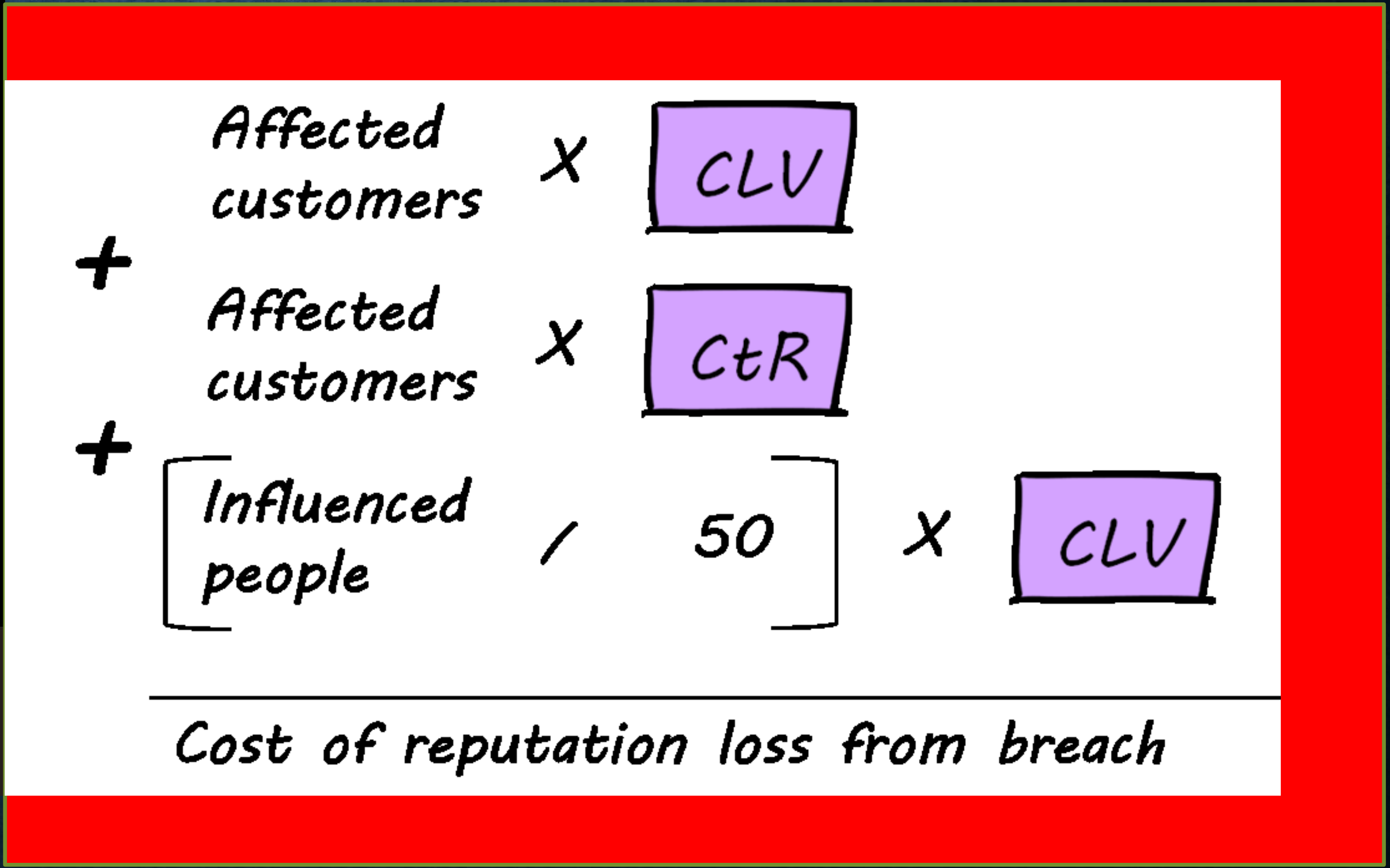
POPULAR VIDEOS

Corbyn would still do business with Putin despite nerve agent attack

Stranger Things' Millie Bobby Brown reportedly earning up to $350,000

Ashley Graham's Instagram post is helping women love their cellulite

Hate crimes against children have 'risen by 14% in last year'



Affected customers x CLV

+ Affected customers x CtR

+ [Influenced people / 50] x CLV

Cost of reputation loss from breach

FIN

- https://blogs.msdn.microsoft.com/microsoft_press/2016/04/19/free-ebook-the-security-development-lifecycle/
- https://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction%20to%20the%20Microsoft%20Security%20Development%20Lifecycle%20(SDL).ppsx
- https://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction_to_Threat_Modeling.ppsx

- **Any Questions?**

THANK YOU?

Here is my email address

DO YOU THNK THIS GIVES YOU CONSENT TO CONTACT ME?

ADD ME TO YOUR MAILING LIST AT YOUR PERIL!

John.Timney@IBM.COM
www.johntimney.com