DATA PROTECTION ACT 2018 (GDPR)

OWASP EVENT

APRIL 2019

V1.0

WHAT IS THE DPA 2018 ALL ABOUT?

- Changes to consent requirements
- Changes to security requirements
- Introduces the Privacy by Design concept – the protection of **C**, **I** & **A**
- Changes to geographical reach and responsibilities
- Introduces the need for Data Protection Officers
- Gives control to the data subject (the 7 + 1 rights)
- Changes the definition of personal data
- Huge fines and possible criminal offences

CONTROLLERS VS PROCESSORS

The Controller is the Organisation or Person who:

- Defines the legal basis for collecting data
- Decides which items of personal data to collect, i.e. the content of the data
- Decides the purpose or purposes the data are to be used for
- Decides which individuals to collect data about
- Decides whether to disclose the data, and if so, who to
- Decides whether subject access and other individuals' rights apply

CONTROLLERS VS PROCESSORS

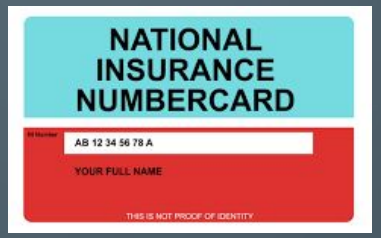
The Processor is the person or Organisation who:

- does not have overall control of the data
- are told what they can do with the Personal Data via contracts and agreements with the Controller
- Processors often decide the security arrangements for the data
- Stepping outside of the terms of a contract could amount to an infringement of Data Subjects rights and subsequently, the law

IMPORTANT!

If you use data for any other purpose than that stated in the privacy notice – you may be stepping into controller realms and this could be in contravention of DPA requirements

PERSONAL DATA REDEFINED



"Any information relating to an identified or identifiable natural person, whether directly or indirectly"

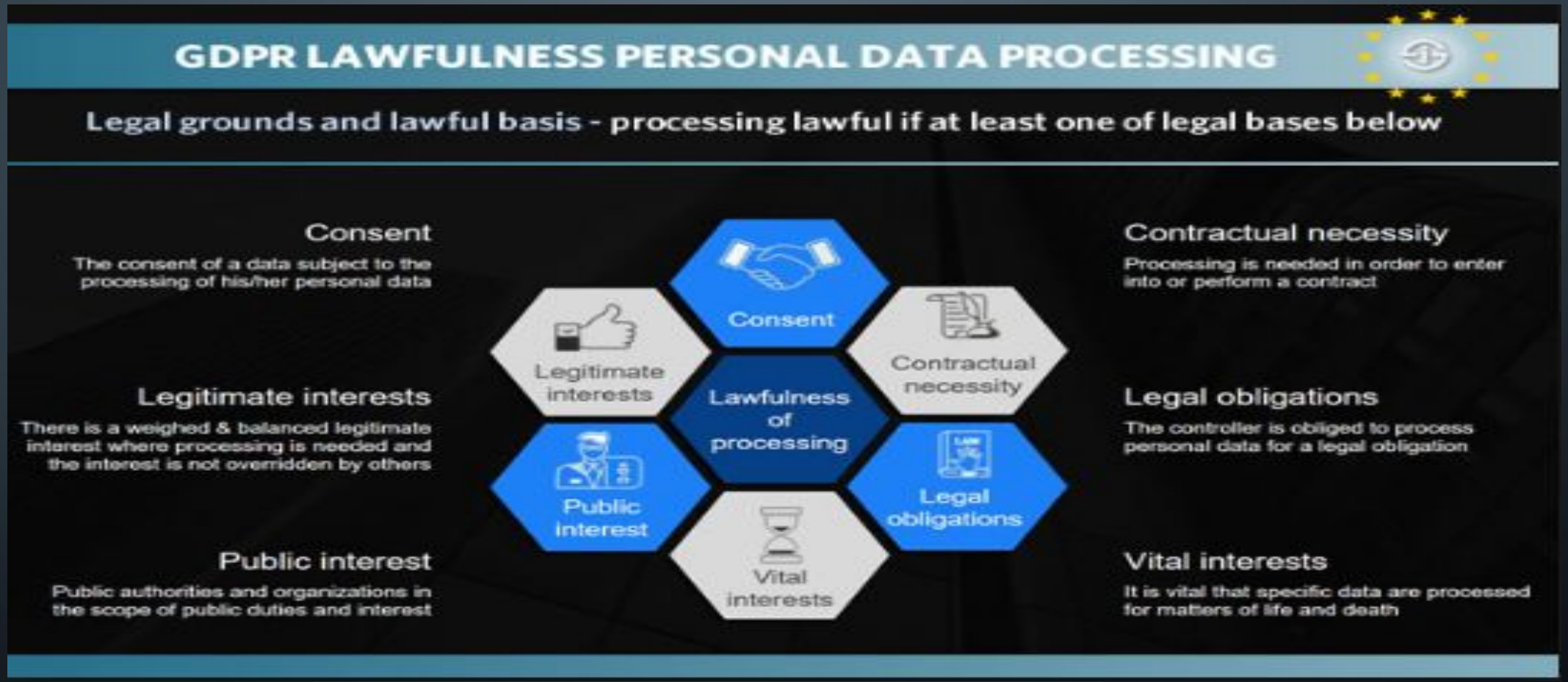
SPECIAL CATEGORIES OF PERSONAL DATA

RIGHTS OF THE DATA SUBJECT

The DPA 2018 has been designed to enhance protection of Personal Data and to enhance data subjects' 'rights and freedoms'. These rights are:

- The right to be informed
- The right of access (the only **GUARANTEED** right)
- The right to erasure (the right to be forgotten)
- The right to portability
- The right to rectification
- The right to restriction
- The right to object
- Rights in relation to automated decision making and profiling

LEGAL BASIS FOR PROCESSING



GEO – LOCATION

- The GDPR requires that the Personal Data of EU citizens is protected and not transferred outside of the EEA unless “adequacy” can be demonstrated
- Permission from the governing Data Protection Authority may be required before transfer of the data to a country outside of the EEA – this means you must consider the physical location of cloud servers to ensure we remain compliant
- Consider the use of cloud applications

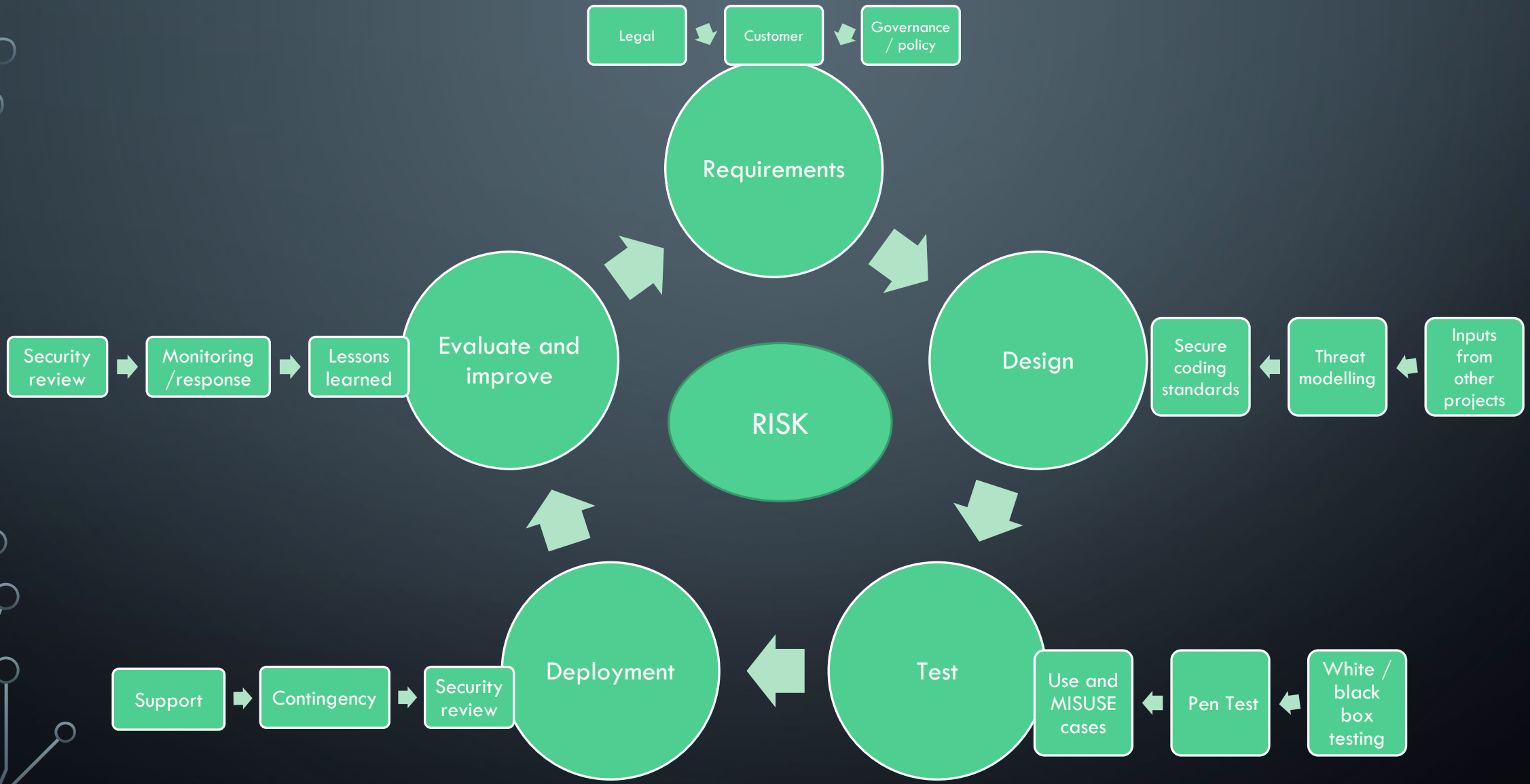
PRIVACY – BY – DESIGN

The Privacy by Design concept has been introduced by the GDPR, it should include the following:

- Security to be included in project risk assessments from project concept:
- Security objectives should be set
- Consideration common and not so common threats to Personal Data should be given – is your product unique
- Assign mitigations to reduce the risk
- Review security risks and objectives at project milestones – document the outcomes!

All security themed project documentation should be retained in the same way you retain your project notes, plans and meeting minutes.

SECURE DEVELOPMENT CYCLE



DATA PRIVACY IMPACT ASSESSMENTS

- Data privacy impact assessments (DPIAs) must be conducted where there is a risk to the rights and freedoms of data subjects
- DPIAs must be documented
- A DPIA is a risk based approach to identifying and mitigating data security risk
- It is sensible to create a written risk assessment procedure to ensure the process is repeatable
- DPIAs should be reviewed at regular intervals and updated where there are significant process changes or new technologies

COMMON SECURITY RISK - DEVELOPMENT

Common risks which should be considered as part of your Risk Assessment:

- Use of cloud – consider data types and location
- Lack of portability – can we move a data subjects' personal data from one place to another?
- Sharing of data with Third Party's – who are we giving it to? Are they secure?
- Protection of source code
- Control of mobile devices
- Lack of infrastructure control (e.g. use of Azure as controlled by Microsoft, or use of AWS as controlled by Amazon)
- Use of insecure protocols (e.g. Telnet, SNMPv1/2)
- Poor encryption key management (Crypto - cycle)

MISCHIEF MANAGED – RISK MITIGATION

Once we have identified our risks, we must reduce the undesired effects. A number of mitigations can be considered:

- Security training for those on the project
- Contracts and agreements which include security stipulations
- Security testing of products and solutions
- Use of security controls such as encryption, anonymisation and psuedonymisation (KEY CONTROLS)
- Consider penetration tests and vulnerability scans – patch the holes!
- Contact, collaboration and monitoring of suppliers
- Access control (granted on the minimum level in order to complete a task or role, consider both physical and logical, reviewed upon changes to project or team)
- Policies, procedures and disaster recovery plans

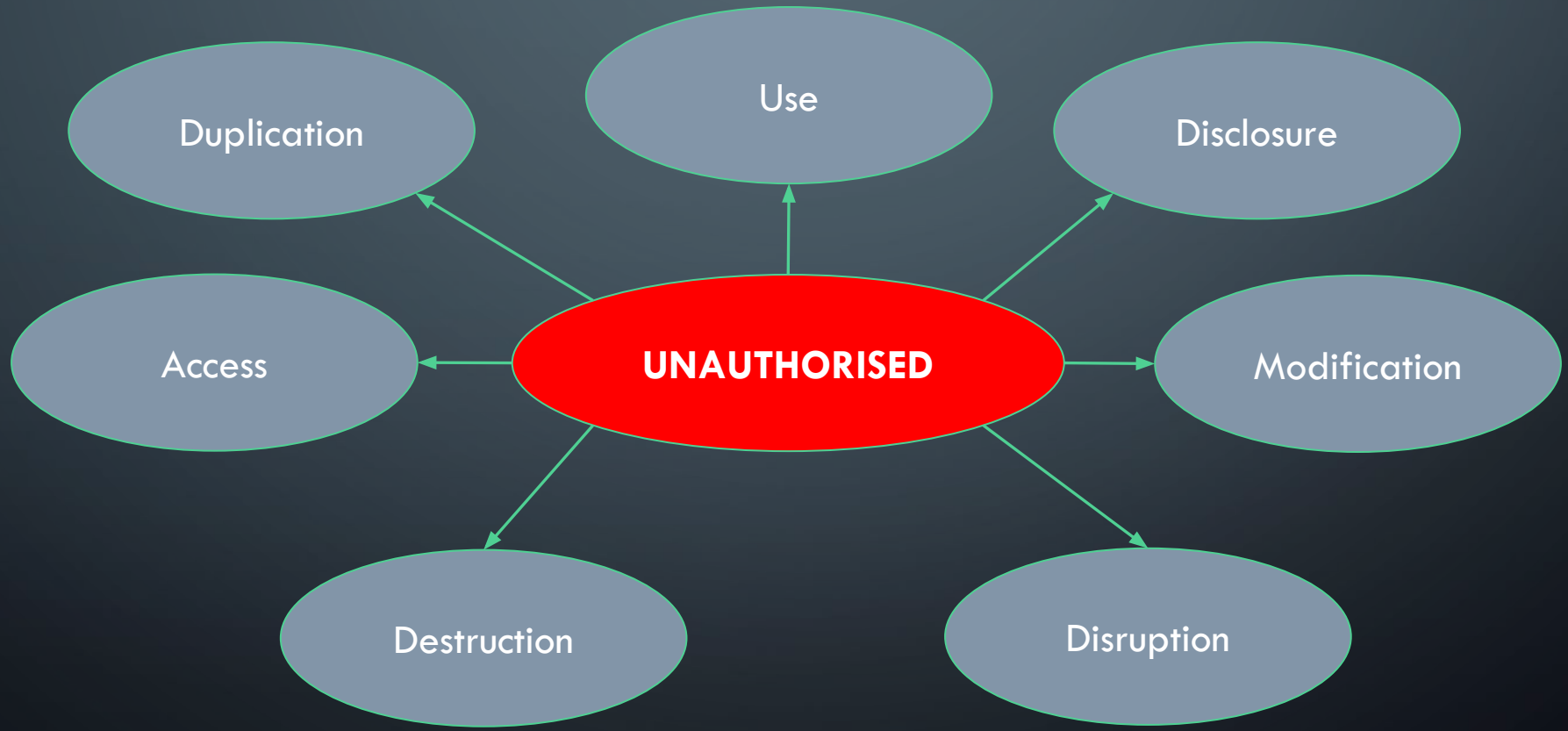
MOBILE DEVICE SECURITY

If you, the employees, trustees or volunteers use their personal devices to connect to company data – such as emails, you must ensure the control of mobile devices.

- Have a Bring Your Own Device Policy
- Insist that users use a lock to keep access to their devices secure
- Insist that mobile devices have anti – virus applications installed where possible
- Insist that all work related information is purged from mobile devices regularly
- Ensure your workforce are aware of incident reporting requirements

INCIDENTS – WHAT ARE THEY?

A security incident is where data has been subject to:



INCIDENT EXAMPLES

- Lost or stolen laptop
- Unauthorised access to a cloud platform
- Unauthorised access to project work space
- Confidential paperwork disposed of with no shredding
- Malicious code infection that has not been picked up and cleaned by Anti-Virus software
- Network disruptions
- A lost USB or external storage device
- Email sent to incorrect recipient
- Man in the Cloud vulnerability exploited
- Accidental disclosure or modification
- Disgruntled employee making unauthorised changes
- Plus more – if in doubt, report it!

INCIDENTS

- Reports to the ICO must be made within 72 hours of the incident being noticed
- If personal data was encrypted when it was lost – it does not need to be reported
- You should gather as much information about the incident as possible and preserve it
- The ICO website has a dedicated page for reporting incidents (data breaches) https://ico.org.uk/for-organisations/report-a-breach/
- Not all personal data breaches are reportable – the ICO guidance should be used to decide whether to make a report

Encryption, anonymisation and pseudonymisation are key security controls for Personal Data, consider these controls in your risk assessment!

SUBJECT ACCESS REQUESTS (SARS)

- Could come in any form – but written is encouraged
- Must be referred to the data protection officer (or similar) without delay
- 30 days to meet or reject the request
- SARs are a way of giving control to the data subject and help to uphold the 7 + 1 rights
- Access is the only absolute right

CONSEQUENCES

For the organisation

- Higher fines (up to 4% of annual, global turnover)
- Lower fines (up to 2% of annual, global turnover)
- Improvement notices
- Costs of repairing damage
- Possible criminal charges
- Possible civil action

For directors

- Possible criminal charges
- Bad press

FINES AND PROSECUTION

Facebook's recent data incident attracted the maximum fine under the old DPA. Under the new DPA that fine would have been £1.626 BILLION

The ICO found that Facebook had not made any effort to control the use of personal data its third parties had access to.

FINES AND PROSECUTION

Cambridge Analytica used personal data it had access to through Facebook, to perform illegal activities.

The ICO have confirmed they will be bringing criminal charges

IN THE NEWS…

NHS

TESCO

TalkTalk

Adobe

Heathrow

Dixons
Carphone Warehouse

BRITISH AIRWAYS

YAHOO!

ebay

EQUIFAX

THIRD PARTY CONTROL

- Contracts which detail data protection requirements should be in place with third parties who have access to personal data you control
- Assess those third parties to ensure they are managing personal data in a compliant way
- Use specific security agreements where necessary

SUMMARY

- Be mindful of your day to day use of data, keeping data secure is as important as health and safety
- Look after the data you and your employees have access to, make sure access is kept to a minimum
- Report all incidents and SARs to the designated person
- Implement security policies as part of your project
- Use ICO guidance to keep you on the right track

MORE INFORMATION

- Information Commissioners Office (ICO) https://ico.org.uk/
- National Cyber Security Centre https://www.ncsc.gov.uk/