PREPARING FOR GENERAL DATA PROTECTION REGULATION (GDPR)

OrbitTech Limited

WHAT IS IT?

- REVISED REGULATIONS GOVERNING COLLECTION, STORAGE & USAGE OF PERSONAL DATA
- MOVES BALANCE OF CONTROL BACK TO ORDINARY PEOPLE
- GIVES CITIZENS RIGHTS TO ACCESS, EDIT, TRANSFER THEIR DATA FROM COMPANY SYSTEMS
- CAN REQUIRE EXPLICIT CONSENT TO BE OBTAINED AND ARCHIVED
- NOTIFICATION OF BREACHES NECESSARY WITH 72 HOURS
- MILLIONS DOLLARS PENALTIES
- EFFECTIVE MAY 2018

THINGS TO CONSIDER

1. EDUCATE
2. STAY ACCOUNTABLE
3. MAKE SURE YOU'RE LEGAL
4. GET THE RIGHT CONSENT
5. PSEUDONYMISATION
6. GET YOUR COMMUNICATIONS SORTED
7. MAKE SURE YOU UNDERSTAND THE RIGHTS THAT GDPR AFFORDS INVIDUALS
8. DATA CONTROLLERS & DATA PROCESSORS
9. DATA BREACHES
10. DESIGN & PRIVACY IMPACT ASSESSMENTS
11. DATA PROTECTION OFFICERS
12. INTERNATIONAL IMPLICATIONS

EDUCATE

- Raise awareness across all relevant departments of your business
- Applicable to all companies in the EU
- Find out more information from the ICO – Information Commissioner's Office

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

STAY ACCOUNTABLE

- Accountability is a key driver
- Document what personal data you hold and identify areas of risk
- Understand data sources and distribution
- Consider an information audit

MAKE SURE YOU'RE LEGAL

Six Privacy Principles

- Consent
- Contracts
- Legal compliance (with another law)
- Protecting the vital interests of a person
- Public interest
- Legitimate interest

GET THE RIGHT CONSENT

- Consent strengthens existing rules.
- Consent must be freely given, specific, informed & unambiguous with a positive action from the individual.
- Sensitive data requires explicit consent.

PSEUDONYMISATION

- Pseudonymisation is introduced as a process applied to data to ensure it is no longer directly linked to an individual

- Personal data without any directly identifying details could also be pseudonymised at the point of collection. For example, a randomised cookie ID allowing a user to be recognised but not directly identified.

GET YOUR COMMUNICATIONS SORTED

- Transparency is another requirement which requires different levels of detail depending on whether you obtain the data directly from the individual or not
- The associated notice has to be concise, easily accessible and written in clear and plain language.
- It must include the legal basis and explain the legitimate interest in processing the data
- Review existing privacy notices and analyse what needs changing

MAKE SURE YOU UNDERSTAND INVIDUALS' RIGHTS

The right

- to be informed
- of access
- to rectification
- to erasure
- to restrict processing
- to data portability
- to object
- not to be subject to automated decision making, including profiling

Ensure you can adequately respond to requests from individuals.

DATA CONTROLLERS & DATA PROCESSORS

- The notions of ‘data controller’ and ‘data processor’ are retained
- Data controllers are organisations. Data processors act on behalf of the data controller. Statutory obligations for compliance are now extended to data processors.
- Review your precise role. Renew contracts with partners to ensure compliance.
- You may have to pay a fee to ICO if you are processing personal data as a controller. Check exemptions - https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf

DATA BREACHES

- Develop processes to detect, report and investigate a breach.
- Identify those types of data that trigger the notification requirement.
- To report a breach, call the ICO helpline – on 0303 123 1113

DESIGN & PRIVACY IMPACT ASSESSMENTS

- Privacy Impact Assessments (PIA) and Data Protection Impact Assessments (DPIA) are specifically defined.
- A PIA has to be run in high-risk situations.
- Understand processes and impact on new products or services brought to market.

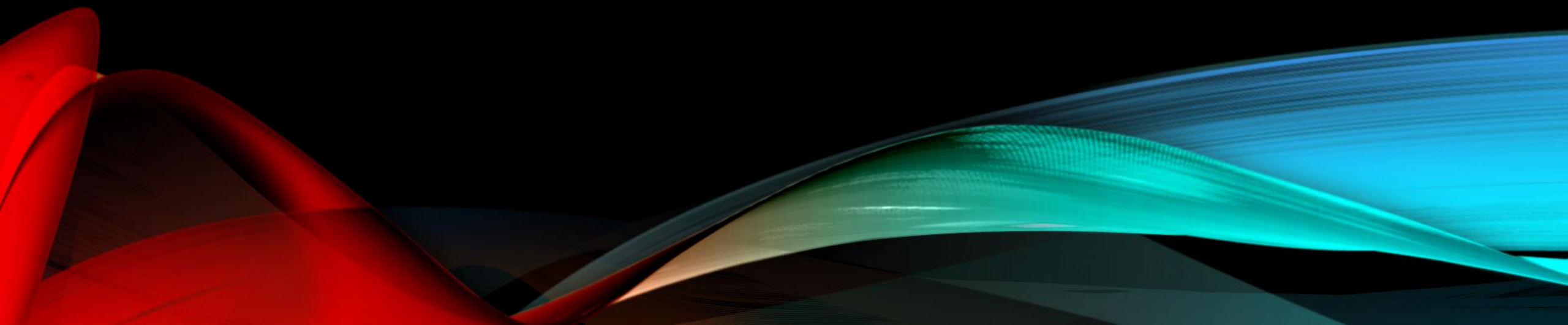
DATA PROTECTION OFFICERS

- A Data Protection Officer (DPO) must be appointed when 'the core activities of the controller or the processor consist of processing operations … which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring … of data subjects on a large scale'.

- Understand requirements for appointment and decide where to include in the business structure and governance.

INTERNATIONAL IMPLICATIONS

- A lead Data Protection Authority must be specified for cross border businesses.
- Consider options for transferring data to countries outside the EU.



PREPARING FOR GENERAL DATA PROTECTION REGULATION (GDPR)