gdprcourse.com

General Data Protection Regulation

iacp

David Sumner
EU GDPR P CISM

Powered by OLIVE GROUP

In association with HFW

Certified by AoFA Qualifications

Accredited by The Insurance Institute

General Data Protection Regulation (GDPR)

gdprcourse.com OLIVE GROUP

Why?

- Supports a single digital market place
- Protect privacy & security of EU citizens in the digital age

When?

- 25th May 2018

Who?

- Controllers & Processors of personal data of EU data subjects

Where?

- Inside the EU
- Outside the EU
- Restrictions on transfer of personal data outside the EU

GDPR Deadline:

25th May 2018

What?

Personal Data

Fines

Rights

Principles

Responsibilities

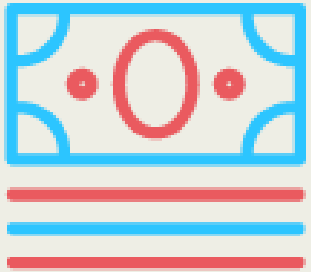
Personal Data

- **Any information relating to a living person that directly or indirectly identifies them**
- E.g name, an identification number, location data, an online identifier, biometric data
- **So who does GDPR apply to ?**
- **Everyone!?!**

Fines

gdprcourse.com OLIVE GROUP

- **Current DPC highest fine is €100K**
- Fines are intended to be proportionate, effective and dissuasive
- **€10M or 2% Global Group Turnover** for breach of controller/processor duties e.g. failure to notify a breach of personal data
- **€20M or 4% Global Group Turnover** for breach of GDPR requirements failure to uphold data subjects right or observe GDPR principles



DPC - Helen Dixon

Adrian Weckler (AW): Are you willing to go the full distance in fining companies €20m?

Helen Dixon (HD): Yes. We have to be willing to. The legislature in Europe provided for fines up to that level because they believe in certain cases it may arise. Presumably, it would involve many users. But it's absolutely the case that we will be imposing fines against big and small entities based on the issues that come across our desk and the areas of risk we identify. There's nothing surer than this.

AW: Will there by any leeway to ease companies into the new, stricter punishment regime?

HD: No. There's not going to be any amnesty or first or second chances. On the other hand, the GDPR does set out criteria when we go to look at the [level] of fine we might impose.

General Data Protection Regulation (GDPR)

- ICO International Strategy – clear statement of intent for a law of GDPR standards or higher for a post Brexit UK.

- "We will seek to explore the concept of the UK as a 'global data protection gateway' – a country with a high standard of data protection law which is effectively interoperable with different legal systems that protect international flows of personal data."

- The Data Protection Bill

Rights

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling.

Principles

- Lawfully, Fairly, Transparently
- Specified, Explicit, Legitimate Purpose
- Data Minimisation
- Accuracy
- Storage Limitation
- Security
- Accountability

Lawful Basis for Processing

- **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless outweighed by the data subject's interests. It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

Special Categories of Personal Data

- Racial or Ethnic Origin
- Political Opinions
- Religious or Philosophical Beliefs
- Trade Union Membership
- Biometric and Genetic Data
- Criminal Convictions
- Health
- Sex Life, or sex Orientation

Lawful Basis for Processing Special category Data

- The data subject has given explicit consent to the processing of their personal data for one or more specified purposes.
- Processing is necessary for the purposes of exercising specific rights of the controller or data subject in the field of employment and social security and social protection law.
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- Processing is carried out by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- Processing relates to personal data which are manifestly made public by the data subject;
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest.
- Processing is necessary for the purposes of preventive or occupational medicine,

Responsibilities

Controller

- Determines the purposes and means of processing
- In other words…What, Why and How?

Processor

- Processes on behalf of the Controller
- They can determine How but not What or Why
- They become a Controller by default if they do

Article 28

- A Controller shall only use Processors providing sufficient guarantees of technical and organisational measures to protect data subject rights

- Processing shall be governed by a contract that stipulates (inter alia) –
  - Documented instructions of the controller
  - Nature and Purpose of processing
  - Type of data processed
  - Confidentiality and Security requirements
  - And much more

- Consequences of no controller / processor contract =

RISK

Data Protection Impact Assessment (DPIA)

- DPIA is a risk assessment in respect of data subjects' freedoms
- Helps identify an effective way to be complaint and protect privacy
- Supports data protection by design and default
- Required for high risk processing e.g. Large scale processing involving profiling or sensitive data

Data Protection Officer (DPO)

- Required for public authorities and organisations performing large scale processing involving monitoring data subjects or sensitive personal data.

- Role
  - Advise
  - Monitor compliance
  - Staff Awareness
  - Point of contact with regulator and data subjects

- Independent role reporting and answering at Board level

Breach Notification

- Personal Data Breach of security leading to:
  - Destruction
  - Loss
  - Alteration
  - Unauthorised disclosure or Access
- Supervisory Authority notification required where risk to rights and freedoms of individual is likely i.e. detrimental effect
- Individual notification required where a high risk to rights and freedoms of individuals is likely
- 72 hours from becoming aware to notification

To Comply or Not to Comply and if so Why?

- What is your rationale?
  - Legal
  - Fines
  - Owners will exercise their new extensive rights with you
  - Market Positioning
  - Reputation
  - Opportunity

- It is simply too late to become fully compliant by **25th May 2018**

- It is not too late to be compliant enough to:
  - Protect your business and your customers
  - Gain competitive advantage
  - Exploit opportunity
  - Gain protection from harsher fines etc. etc.

How to Tackle It

- Record and Analyse all Personal Data Processing
- Compliance Gap Analysis
- Risk Assess (Dpia Lite)
- Staff Awareness Training
- Implement Based On Rationale And Risk Appetite

GDPR Project Tools

gdprcourse.com OLIVE GROUP

- ICO Self Assessment
- Running A GDPR Project A Practical step by step guide
- Preparing your organisation for GDPR- A guide to help SME
- The GDPR and Microenterprises – A Readiness Guide
- GDPR and You Resource page
- https://gdpr-info.eu
- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- https://ico.org.uk/for-organisations/health/
- https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/data-protection-impact-assessments-dpias-guidance/
- Rregistration with the DPC

gdprcourse.com OLIVE GROUP

Thank You

Powered by OLIVE GROUP

In association with HFW

Certified by AoFA Qualifications

Accredited by The Insurance Institute