THE NEW EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

Dr Peter Tobin

6 March 2018

BDO

AGENDA

What is the GDPR – an overview in 5 minutes

GDPR Health Check – 20 questions in 10 minutes

WHAT IS THE EU GDPR

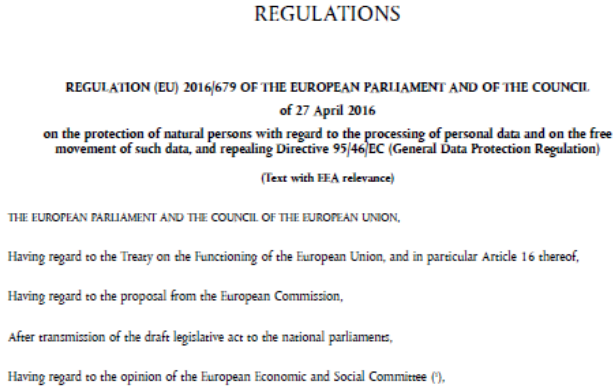
GDPR Overview: To find out more http://www.eugdpr.org/

- Single Regulation automatically applies to all current and future EU members
- Including UK post-BREXIT
- 173 introductory clauses
- Eleven chapters
- 99 Articles with multiple paragraphs
- Works in conjunction with other EU directives and regulations

WHAT IS THE EU GDPR

GDPR structure

- Chapter 1 – General Provisions
- ***Chapter 2 – Principles***
- ***Chapter 3 – Rights of the Data Subject***
- ***Chapter 4 – Controller and Processor***
- ***Chapter 5 – Transfer of Personal Data to 3rd Countries or International Organizations***



REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

WHAT IS THE EU GDPR

GDPR structure

- Chapter 6 – Independent Supervisory Authorities
- Chapter 7 – Cooperation and Consistency
- ***Chapter 8 – Remedies, Liability and Penalties***
- ***Chapter 9 – Provisions Relating to Specific Processing Situations***
- Chapter 10 – Delegated Acts and Implementing Acts
- Chapter 11 – Final Provisions

WHAT IS THE EU GDPR

Key changes https://www.eugdpr.org/key-changes.html

- Increased Territorial Scope (extra-territorial applicability)
- Penalties
- Consent
- Breach Notification
- Right to Access
- Right to be Forgotten
- Data Portability
- Privacy by Design
- Data Protection Officers

WHAT IS THE EU GDPR

Article 29 DPWP is planning the following guidance:

- Consent
- Transparency
- Profiling
- High risk processing
- Certification
- Administrative fines
- Breach notification
- Data transfers

GDPR HEALTH CHECK

In this short session we will have a quick review of some of the key considerations when preparing for compliance with the European Union General Data Protection Regulation (GDPR)

There are 20 questions

We will use a simple Yes/No scale, you could use a more granular assurance point scale (e.g. 1 to 5)

Let’s see how we do!

GDPR HEALTH CHECK (Q1 TO Q4): CAN YOU PROVE…

1. You comply with the 6 principles relating to personal data processing?
   Article 5: Principles relating to personal data processing
2. You comply with the lawfulness of processing rules?
   Article 6: Lawfulness of processing
3. You have records of consent that meet the required conditions?
   Article 7: Conditions for consent
4. You have records of consent for special categories of personal data that meet the required conditions?
   Article 9: Processing of special categories of personal data

GDPR HEALTH CHECK (Q5 TO Q8): CAN YOU PROVE…

5. You have provided all necessary information at point of collection?
   Article 13: Information to be provided
6. You have a policy, process and procedures to ensure a) right of access; b) to rectification; c) to erasure; d) to restriction of processing; by the data subject?
   Article 15 - 18: Right of access; to rectification; to erasure; to restriction of processing
7. You have a policy, process and procedures to ensure to data portability?
   Article 20: Right to data portability
8. You are meeting all the responsibilities of the controller?
   Article 24: Responsibility of the controller

GDPR HEALTH CHECK (Q9 TO Q12): CAN YOU PROVE…

9. You have data protection by design and by default?
   Article 25: Data protection by design and by default
10. You have a representative in the EU?
    Article 27: Representatives of controllers not established in the Union
11. You have adequate records of processing?
    Article 30: Records of processing activities
12. You have adequate security of processing?
    Article 32: Security of processing

GDPR HEALTH CHECK (Q13 TO Q16): CAN YOU PROVE…

13. You have a policy, process and procedures for data breach notification to the supervisory authority?
    Article 33: Notification of a personal data breach to the supervisory authority
14. You have a policy, process and procedures for data breach notification to the data subject?
    Article 34: Communication of a personal data breach to the data subject
15. You have conducted data protection impact assessments where necessary according to the screening rules?
    Article 35: Data protection impact assessment
16. You have appointed an appropriate data protection officer following the EU requirements?
    Article 39: Tasks of the data protection officer

GDPR HEALTH CHECK (Q17 TO Q20): CAN YOU PROVE…

17. You have appropriate safeguards for cross-border transfers?
    Article 46: Transfers subject to appropriate safeguards
18. Your processing complies with freedom of expression and information?
    Article 85: Processing and freedom of expression and information
19. Your processing complies with the context of employment rules?
    Article 88: Processing in the context of employment
20. You have trained your staff in all of the above aspects and more
    Article 39: Tasks of the data protection officer; Article 47: Binding Corporate Rules

THE NEW EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

THANK YOU. QUESTIONS?

BDO IT Consulting Ltd
10, Frère Félix de Valois Street
Port Louis

Office +230 202 9897
bdo.it.consulting@bdo.mu
www.bdo.mu/bdo-it-consulting

BDO