Senior Leaders briefing on General Data Protection Regulations (GDPR)

Lauri Almond
IS Business Consultant IG Operations
July 2016

Essex County Council

What is it and why?

The final text for the General Data Protection Regulations (GDPR) was agreed and released on 12th March 2016.

The GDPR repeals Directive 95/46/EC on which our own Data Protection Act 1998 was built. By definition, an EU Directive sets ground rules, and member states must bring in national legislation to enable them to meet the requirements of the Directive, whereas an EU Regulation forms part of UK law without the need for national legislation, however there are some areas where member states are free to further define how elements will be implemented, and domestic law can be developed to support certain elements.

Essex County Council

When does it come into force?

- The GDPR comes into force on 25th May 2018
- We must comply with Data Protection Act 1998 (DPA) until then
- Information Commissioners Office (ICO) will be drip feeding guidance, starting with new areas previously not required under the DPA
- The ICO have created a microsite to assist organisations to prepare for GDPR
- The UK will need to implement the new law, regardless of Brexit. Firstly, it's unlikely we will have left the EU before 25 May 2018. Secondly, after the UK leave, EU countries won't be allowed to let data into the UK unless the UK implements something very like the GDPR.

Essex County Council

What is the key difference?

With the existing Data Protection Act 1998 organisations are considered complaint until they are challenged and found wanting by the ICO.

The GDPR brings in an ‘Accountability’ principle which requires us to document and evidence compliance.

The Controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)

Essex County Council

Key Legislative Changes

1. Data Processors (ie third party contractors like payroll providers) will now have specific legal obligations to maintain records of personal data and processing activities.
2. The 8 DPA principles are replaced by 7 GDPR principles which are broadly similar but more detailed and include the addition of the ‘Accountability’ principle
3. The conditions for processing remain broadly similar, however public authorities will no longer be able to use the Legitimate Interests condition for processing data, so where this has formed the legal basis for processing, post May 2018 an alternative condition will need to be identified
4. Consent must be verifiable and recorded

Essex County Council

Key Legislative Changes

5. Privacy Notices for children must be clear, plain and understandable by a child. All privacy notices must contain fuller information on processing
6. Data Subjects rights have been broadened to include:
   - The right to restrict processing
   - The right to data portability
   - Rights in relation to profiling (defined by ICO as any form of processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:
     - Performance at work;
     - Economic situation;
     - Health;
     - Personal preferences;
     - Reliability;
     - Behaviour;
     - Location; or
     - Movements)

Essex County Council

Key Legislative Changes – contd.

7. We will have to give people more information about what we are doing with their data than we currently required to
8. Privacy Impact Assessments will have to be undertaken in some circumstances.
9. Organisations must appoint a Data Protection Officer.
10. We must comply with any Code of Practice approved by the ICO
11. The ICO can provide an accreditation scheme
12. A new requirement to report ‘High risk’ breaches (as yet to be defined by the ICO) to the ICO and relevant data subjects within 72 hours – failure to notify a breach can result in a significant fine of up to 10 million euros
13. Serious breaches can result in monetary fines from the ICO of up to 20 million euros
14. More prescriptive regulations are imposed on the transfer of personal data outside of the EU.

Essex County Council

Domestic legislation

The GDPR does allow for some domestic legislation to support the GDPR in Member States in some areas, e.g.:

- UK Law can specify additional conditions when processing is allowed. UK law can give the Public the right to access official documents
- UK Law can broaden exemptions to reflect domestic expectations on processing of personal data for the purposes of :
  - Freedom of expression and information
  - National security & prevention and detection of crime
  - Historical and scientific research,
  - Statistical processing and archiving

Essex County Council

Preparation Activities

- An initial gap analysis has been completed by the Information Governance (IG) Team on the 12 key areas, and RAG rated with 7 areas in Amber and 5 areas in Green
- A work plan for GDPR readiness has been created to focus the IG team on areas of work for full compliance and forms part of their Supporting Success objectives
- Formation of a working group for the implementation of GDPR at ECC with a senior group for oversight including Margaret Lee, David Wilde & Paul Turner.
- Training on the GDPR will be delivered to the IG Team on 21st September 2016, with a condensed session planned for our Information Champions to support the wider business
- The creation of a Data Lifecycle Mapping/Information Asset Register by the IG team over the last 14 months has placed us in a positive position to build on this work to meet GDPR in terms of documented evidence of compliance.

Essex County Council

References

- EU-GDPR- Final Text for GDPR
- ICO Overview of GDPR
- GDPR headlines report
- Preparing for the GDPR-12-steps
- GDPR summary - Act Now

Essex County Council