General Data Protection Regulation

Local Councils Liaison Committee
12 March 2018

Epping Forest District Council

What is the General Data Protection Regulation?

Arising from EU legislation, the GDPR is the biggest change in data privacy laws for 20 years.

GDPR will come into effect on 25 May 2018 and Brexit will have no impact.

Organisations must be able to demonstrate compliance with the Regulation.

Epping Forest District Council

General Data Protection Regulation

- Same basic principles as the Data Protection Act 1998, but strengthened;
- Accountability;
- New rights for individuals and strengthening of existing rights;
- Mandatory breach reporting;
- Data Protection Impact Assessment/Data Protection By Design; and
- Higher penalties for non-compliance.

Epping Forest District Council

Demonstrating Compliance

Data controllers will have to demonstrate compliance with the GDPR:

- technical and organisational security measures;
- maintaining records of processing activities;
- appointment of a Data Protection Officer;
- data protection impact assessment and data protection by design/default.

Epping Forest District Council

Lawful Basis

There must be a lawful basis for the processing of personal data and the GDPR places a higher threshold on the processing of data by consent:

- review how consent is sought, obtained and recorded;
- consent must be freely given;
- consent must be specific, informed and unambiguous and a positive affirmation of the individual's agreement.

This is a high standard!

Epping Forest District Council

Privacy Notices

The GDPR specifies matters that people will need to know about the processing of their personal data:

- the lawful basis for processing the data;
- data retention periods; and
- internal/ICO complaints processes.

This information must be provided in concise, easy to understand and clear language.

Epping Forest District Council

Rights of Individuals

The main rights for individuals under the GDPR:

- subject access;
- to have inaccuracies corrected;
- to have information erased;
- to prevent direct marketing;
- to prevent automated decision-making and profiling;
- data portability.

Epping Forest District Council

Subject Access

Rules for subject access will change:

- in most cases, no charge will be able to be made;
- the period for compliance will be a month, rather than the current 40 days;
- there will be different grounds for refusing to comply with subject access request – manifestly unfounded or excessive requests can be charged for or refused; and
- policies and procedures must be in place to demonstrate why requests meet these criteria.

Epping Forest District Council

Data Breaches

- Procedures must be in place to detect, report and investigate personal data breaches;
- GDPR introduces a breach notification duty for all organisations;
- Not all breaches will have to be notified to the ICO, only those where the individual is likely to suffer some form of damage; and
- Breach reporting within 72 hours of the breach being discovered.

Epping Forest District Council

Data Protection Impact Assessment

It has always been good practice to adopt a privacy by design approach and the ICO has recommended organisations use privacy impact assessments for some time.

The GDPR will make this a legal requirement for some projects.

Epping Forest District Council

Data Protection by Design

When personal data is to be used data in new and innovative ways, it is currently good practice to ensure that data protection is considered as part of service design.

In some circumstances the GDPR will make this a legal requirement.

Epping Forest District Council

Enforcement

The GDPR introduces increased administrative fines for non-compliance.

Not all infringements of the GDPR will lead to serious fines.

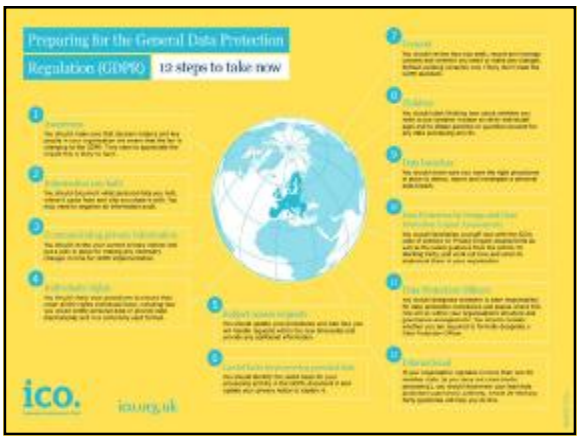
As well as the power to impose fines, the ICO has other sanctions to enforce the GDPR, including warnings and reprimands; a temporary or permanent ban on data processing; and requiring the rectification or erasure of data.

Epping Forest District Council

What next?

- identify <u>all</u> personal data processing activities;
- identify the purposes for which the data is processed;
- identify the legal basis for each processing activity;
- identify who personal data may be shared with;
- implement the principles of Data Protection Impact Assessment and Data Protection by Design/Default; and
- review privacy notices.

Epping Forest District Council



GDPR Guidance

The Information Commissioner has published a Guide to the GDPR, to help those who have day-to-day responsibility for data protection to ensure that organisations comply with its requirements.

The Guide includes links to relevant sections of the GDPR and to ICO and other guidance.

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

Epping Forest District Council

General Data Protection Regulation

Stephen Tautz
Data Protection Officer
(01992) 564180
stautz@eppingforestdc.go.uk

Simon Hill
Monitoring Officer
(01992) 564249
shill@eppingforestdc.go.uk

Epping Forest District Council