Agenda Item: FC 124/17

General Data Protection Regulation (GDPR)

SUMMARY

What is it?
New piece of legislation that was adopted in April 2016 and comes into force May 2018 however, public sector are only now trying to interpret what it means for us and still they don’t have all the answers.

It builds on existing Data Protection Legislation.
Significant change for organisations that hold and process personal data, both hard copy and digital (basically any two pieces of data/info that can be used to identify a person, including photos).

SUPERVISORY AUTHORITY IS THE INFORMATION COMMISSION OFFICE (ICO)

KEY STEPS

1. **Awareness.**
   a. Give Councillors an update on where we are.
   b. Make sure all processors are aware.

2. **Information**
   a. Carry out an information audit; document all personal data you hold, where it came from and who you share it with.

3. **Look at Privacy Notices** (need to be clear).
a. Do we have privacy notices, if so then they should be reviewed?
b. If we don’t then need to identify where they are required.

4. **Individuals’ Rights**
   a. How would you delete personal data?
   b. How would you provide data electronically?
   c. Can you identify personal data easily, both physical and digitally?

5. **Review Procedures**.
   a. Map out all end to end workflows.

<table>
<thead>
<tr>
<th>Process</th>
<th>Subject</th>
<th>Record</th>
<th>Type</th>
<th>Source</th>
<th>Legal Retention</th>
<th>Transfer</th>
<th>Location</th>
</tr>
</thead>
</table>

6. **Legal basis for Processing**.
   a. Data Controller to determine the purpose and means of the processing of personal data.
   b. Liability is now shared between the Data Controller and Data Processor (50/50).
   c. Is the data we keep adequate & relevant?
   d. Is the personal data we hold accurate and up to date?
      i. Personnel (Employee (Data))
      ii. Allotment Tenants
      iii. Bank details for suppliers/contractors
   e. Make sure a Data Retention plan is in place.

7. **Consent**.
   a. Do we have the necessary consent protocol in place for keeping data, both physical and digital?
   b. How do we seek, record and manage consent?

8. **Privacy by Design**.
   a. Consult with Legal on all privacy notices.
   b. Carry out Privacy Impact Assessments (PIA)-Article 29

9. **Data Protection Officer (DPO)**.
   a. Parish Council to agree who the DPO will be and has to be in place by May 2018 (Article 37, 38).
   b. DPO to be fully trained on all legal aspects of the legislation.
   c. DPO informs and advises the Parish Council and its employees about their obligations to comply with the GDPR.
d. DPO monitors compliance with the GDPR including managing internal data protection activities, advice on data protection impact assessments, train staff and conduct internal audits.

e. DPO is the first point of contact for the regulator and for individuals whose data is processed.

10. Supply Chain.
   a. Due diligence to be carried out on all suppliers/contractor who work on our behalf to ensure they are fully conversant and compliant with GDPR.

11. Technology.
   a. Make sure adequate controls are in place regarding confidentiality, integrity, availability and resilience (look at ISMS-ISO 27001 for good practice).
   b. Encryption is not a requirement however, will be less exposed.

**Data Breaches**
Have to notify the ICO within 72 hours of any data breach that is of high risk.
If IT encryption is in place then just report to the ICO but don't have to report to the Data Subject.

**Fines**
Up to 4% of turnover or up to £20MIO (level requested by ICO for worst case scenario).

**Data Subject Rights**
1. Subject access request, have to process within 30 days.
2. Not allowed to charge, only if repeated requests.
3. Could ask for any electronic data (eg CD)
4. Make sure person asking for data is qualified as the actual person.

**NEXT STEPS**
1. Appoint a DPO, likely to be the Clerk/RFO as fixed employee. Councillors are elected and therefore change from time to time.

2. DPO to put together a Project Plan and present at November meeting.

3. Review and update further actions required in monthly Parish Council meetings.
Article 37 EU GDPR
"Designation of the data protection officer"

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) 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; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

=> Article: 39

**Article 38 - EU GDPR**

"Position of the data protection officer"

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

5. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.
1. The data protection officer shall have at least the following tasks:

(a) to **inform and advise** the controller or the processor and the employees who carry out processing of their **obligations** pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to **monitor compliance** with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to **Article 35**;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in **Article 36**, and to consult, where appropriate, with regard to any other matter.
Article 35 - EU GDPR
"Data protection impact assessment"

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. => Recital: 75, 84, 89

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

   (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

   (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

   (c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.
7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

=> Article: 58

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

12. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.
1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards.
safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller’s or the processor’s representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

=> Recital: 13