Report of the Director
of Policy and Resources

Decision to be taken after:
24 March 2017

NORTH LINCOLNSHIRE COUNCIL

GOVERNANCE AND TRANSFORMATION CABINET MEMBER

GENERAL DATA PROTECTION REGULATION

1. OBJECT AND KEY POINTS IN THIS REPORT

1.1 This report sets out how the council will prepare for the introduction of the General Data Protection Regulation (GDPR).

1.2 The GDPR will automatically replace the Data Protection Act 1998 on 25 May 2018. It will be implemented in UK law before Article 50/Brexit is implemented.

1.3 Failure to comply with the requirements of GDPR may expose organisations to fines of up to 4% of turnover. GDPR is regarded as a significant new business risk.

2. BACKGROUND INFORMATION

2.1 The current Data Protection legislation is enshrined in the European Data Protection Directive 95/46 EC. European member states implemented this legislation by introducing domestic legislation. In the UK this was the Data Protection Act 1998 (DPA).

2.2 The DPA placed obligations on organisations processing (handling) personal information to comply with eight principles and to fulfil certain responsibilities as Data Controllers of personal information and it gave individuals certain rights. It also introduced corrective powers and administrative fines for noncompliance with the Act.

2.3 The General Data Protection Regulation (GDPR) became European law on 24 May 2016. On 25 May 2018 the GDPR will take effect in UK law following a two year transitional period. It will remain in force until the UK leaves the European Union and amends or repeals the legislation. It is highly likely that post-Brexit UK privacy legislation will retain significant elements of the GDPR.

2.4 Recent unprecedented and rapid advances in technology have brought about fundamental changes to the way people use and share information. A series of high profile security breaches, phone hacking scandals and globally reported whistle-blowing revelations have all served to increase public awareness of the impact of technological advances on their personal privacy.

2.5 The GDPR responds to these challenges and opportunities by introducing changes to strengthen individual's rights and build trust. Those processing personal data will face increased accountability and compliance obligations.

2.6 The overall themes of the GDPR are to:

- Harmonise data protection law across member states;
- Increase the importance of data protection within organisations;
- Widen the scope of what constitutes personal data and to introduce special categories of data e.g. Biometric data;
- Introduce legislation that applies to data processors as well as data controllers;
- Provide individuals with greater rights and powers over their personal information;
- Simplify the current DPA principles;
- Introduce greater sanctions, such as higher fines.

2.7 The current eight principles that organisations must comply with are being replaced by six, as follows:

1. Lawfulness, fairness and transparency;
2. Purpose limitation;
3. Data minimisation;
4. Accuracy;
5. Storage limitation;
6. Integrity and confidentiality.

2.8 The principles in some cases place similar obligations on organisations but there are some differences, such as the obligation to be transparent and greater emphasis on only processing personal information for the specified purpose and only collecting the minimum amount of data. Appendix 1 provides further detail on the differences.

2.9 In summary the GDPR retains the fundamental principles of current data protection law. Any organisation which can demonstrate good compliance with the DPA and the NHS IG Toolkit (or any successor framework) will be well-positioned for compliance with the new regulation.

2.10 The ICO will remain the UK regulator. Existing data protection case law and subsequent rulings under the new regulation prior to the UK's departure from the EU, will continue as a binding part of UK law. The Human Rights Act and European Convention on Human Rights will remain an important element of privacy and information law in the UK, in particular the right to a private and family life.

2.11 The ICO have issued initial guidance for preparing for the introduction of the GDPR, 'GDPR – 12 Steps to Compliance' which can be seen in Appendix 2. This has been followed by their Overview of the GDPR in January 2017, which will be regularly reviewed and updated. In addition the ICO is providing updates on its website on the DP Reform page and is providing updates in the monthly newsletter.

2.12 The ICO have stated that compliance with the current Data Protection Act is seen as a good starting point for compliance with the GDPR.

2.13 The next steps for the Council are to:

a) Produce an Implementation Action Plan based on the GDPR 12 Steps to Compliance document including any associated costs;

b) Ensure awareness of the GDPR is raised and maintained with decision makers and key people, through regular reports and briefings;

c) Identify all Council information assets to ensure processing of personal information is documented and in accordance with the GDPR. This will link to the Information Asset Owner register and role, and inform the development of Privacy Notices; and

d) Ensure existing and future contracts are reviewed and amended as appropriate to comply with GDPR requirements.

3. OPTIONS FOR CONSIDERATION

3.1 OPTION 1 – Approve the suggested preparation arrangements for the introduction of the GDPR.

3.2 OPTION 2 – Amend or reject the preparation arrangements.

4. ANALYSIS OF OPTIONS

4.1 **Option 1** is our recommend approach to preparations for the implementation of the GDPR on the basis that it is following the ICO suggested approach to date and will easily allow the council to create future action plans as further ICO guidance is issued.

4.2 **Option 2** could result in the council not following the ICO approach making future action plans more difficult to align with the ICO.

5. RESOURCE IMPLICATIONS (FINANCIAL, STAFFING, PROPERTY, IT)

5.1 To be advised, as further ICO becomes available allowing for the preparation of more comprehensive action planning.

6. OUTCOMES OF INTEGRATED IMPACT ASSESSMENT (IF APPLICABLE)

6.1 N/A at this stage of the preparations.

7. OUTCOMES OF CONSULTATION AND CONFLICTS OF INTERESTS DECLARED

7.1 This has been consulted with the council's Senior Information Risk Owner (SIRO) and the wider Information Governance and ICT Security Function.

8. RECOMMENDATIONS

8.1 That the implications of the GDPR are noted;

8.2 That the initial high-level action plan set out in paragraph 2.13 is approved; and

8.3 That an update on progress with the implementation of GDPR is provided in September 2017

DIRECTOR OF POLICY AND RESOURCES

Civic Centre
Ashby Road
SCUNTHORPE
North Lincolnshire
DN16 1AB
Author: Phillipa Thornley/Paul Ellis/Jason Whaler
Date: 3 February 2017

Background Papers used in the preparation of this report:

APPENDIX 1

MAIN CHANGES INTRODUCED BY THE GDPR

Many of the changes from the GDPR will already be familiar to organisations in the UK, such as mandatory privacy impact assessments for high risk processing, the concept of pseudonymisation (data de-identification) and financial penalties.

Individuals will notice:

- Wider rights of subject access and information about processing
- Greater transparency about processing, and
- Stricter conditions for consent and the right to object.

For organisations there will be a focus on accountability and pro-active, evidence-based compliance:

- Thorough risk assessments, and the principles of 'privacy by design' and 'data protection by default'
- Requirement to maintain accurate records of all data processing activities,
- Increased regulatory enforcement powers and penalties, and
- Stricter breach notification requirements to both regulators and to the individuals affected.

A summary of the main changes and the requirements of the GDPR can be found below, and will be further explained when guidance has been issued by the ICO:

a) A wider and more detailed definition of what constitutes personal data;

b) A greater obligation on Data Controllers to demonstrate compliance with the GDPR, through:

   i) The maintaining of specified documents detailing the processing of personal information including clearly identifying the Data Controller and Processor if applicable;

   ii) A legal requirement to conducting impact assessments for 'higher risk' processing;

   iii) Implementing data protection by design and by default, i.e. data minimisation and de-identification to maintain and support privacy and confidentiality;

   iv) Appointing a designated Data Protection Officers with professional knowledge and experience who reports to the highest level of the organisation, and

   v) Contracts will need to be more explicit with Data Processors and sub-contractors.

c) New obligations on Data Processors acting on behalf of a Data Controller in relation to the processing of data,

d) Enhanced conditions to be met when data processing is on the basis of consent, and where possible processing will be underpinned by legislation or statutory duty,

e) Privacy Notices will need to be more comprehensive and set out the rights of the data subject,

f) New rights for the data subject including the right to be forgotten and data portability, which allows them to receive their data in a structured and commonly used format so it can be easily transferred to another data controller;

g) The timescales for dealing with a subject access request will be reduced to a calendar month and we will no longer be able to charge a fee (currently £10), unless the request is ‘manifestly unfounded or excessive’,

h) A requirement to notify the ICO of breaches within specified timescales, and to notify data subjects if there is a ‘high risk’ to their rights and freedoms, and

i) Increased financial penalties can be imposed by the ICO for breaches.

APPENDIX 2

GDPR – ICO 12 STEPS TO COMPLIANCE

Following is the Information Commissioner's Office (ICO) 12 GDPR 12 Steps to Compliance that will be used as a template for the councils' GDPR Action Plan as more guidance becomes available:

Step 01	You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.
Step 02	You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.
Step 03	You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.
Step 04	You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
Step 05	You should update your procedures and plan how you will handle requests within the new timescales and provide additional information.
Step 06	You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.
Step 07	You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.
Step 08	You should start thinking now about putting systems in place to verify individual's ages and to gather parental or guardian consent for the data processing activity.
Step 09	You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.
Step 10	You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.
Step 11	You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.
Step 12	If your organisation operates internationally, you should determine which data protection supervisory authority you come under.