AGENDA ITEM 13

Data Protection/GDPR Update

Agenda Item 13

Falkirk Council

Title: **Data Protection/GDPR update**
Meeting: **Executive**
Date: **15 May 2018**
Submitted By: **Director of Corporate and Housing Services**

1. Purpose of Report

1.1. The purpose of the report is to update the Committee on preparations for the implementation of the General Data Protection Regulation (**GDPR**) and to seek approval of an updated Data Protection Policy.

2. Recommendations

2.1. **The Executive is asked to:-**

(`) note the update provided on GDPR preparations; and

(2) approve the updated Data Protection Policy to take effect from 25th May 2018.

3. Background

3.1. The GDPR will come into force on 25th May 2018. It will be implemented in the UK by a new Data Protection Act, which is still at Bill stage but expected to be in place by 25th May 2018. This will replace the Data Protection Act 1998. The GDPR strengthens protection for individuals in relation to their personal information, and introduces greater requirements for data controllers in relation to accountability. The Council, as a data controller, must be able to evidence compliance with the legislation.

4. Update on GDPR preparations

Governance

4.1. The Information Governance Manager has taken the lead on the Council's preparations for the GDPR, which have been overseen by the Information Management Working Group (chaired by the Chief Governance Officer). The Group reports on GDPR-compliance to the Corporate Risk Management Group.

Register of Data Processing Activities

4.2. The GDPR requires the Council to hold a register of its data processing activities (**Register**) which must be produced to the Information Commissioner's Office on request. The requirements for the content of the Register are prescribed by statute and are stringent. Services are carrying out an audit of personal data processed which will form the basis of the Register.

Privacy Notices

4.3. Under the GDPR, individuals must be given fuller information about how their personal data is used, including the legal basis for processing and the length of time it will be kept. This is usually called a privacy notice. The personal data audit will identify where and how information is collected, and therefore when privacy notices should be given (whether on paper or electronic forms, in leaflets, on the Council's website or in person). Work is underway in Services to ensure that privacy notices are in place by 25th May 2018.

Data Protection by Design and by Default

4.4. The GDPR requires data protection to be considered by data controllers "*by design and by default*". This means that we must consider compliance with the data protection principles at the outset of any project or introduction of a new system or policy which may impact on personal data. To date, this has been best practice, rather than mandatory. We will now undertake data protection impact assessments to assess privacy risks.

Data Breaches

4.5. Under GDPR, serious data protection breaches will have to be notified to the Information Commissioner within 72 hours. Data breach reporting procedures are already in place and working well and it is anticipated that we can comply with this timeframe.

4.6. The level of fines for data protection breaches is increased by the GDPR. Currently, the maximum level of fine which can be imposed by the Information Commissioner is £500,000, with levels usually being less for local authorities (Glasgow City Council was fined £150,000 in 2013 for the loss of 2 unencrypted laptops containing details of 20,000 individuals. Kensington and Chelsea Borough Council was fined £120,000 in April 2018 for unlawfully identifying 943 people who owned vacant properties in the borough, by failing to properly redact information from an Excel spreadsheet in response to an FOI request arising out of the Grenfell Tower tragedy).

4.7. The fines under GDPR will be up to 4% of annual turnover which for a public authority is likely to be interpreted as its annual revenue budget.

Data Protection Officer

4.8. The GPDR requires public authorities to designate a Data Protection Officer (**DPO**) "*on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices*" and who "*shall directly report to the highest management level*". It is likely that the Council's DPO will be the Information Governance Manager.

4.9. As public authorities, the Falkirk Integration Joint Board, the Falkirk Council Licensing Board and Falkirk Community Trust will also require to designate DPOs.

Training

4.10. All staff who handle personal data must complete data protection training annually. The online training has been updated for 2018 to reflect the changes made by GDPR. The Information Governance Manager also has a programme of face-to-face training sessions in place which has been well-attended and well-received.

4.11. A session will be held for elected members. Elected members are currently data controllers in their own right for most purposes and this will not change with the GDPR.

5. Updated Data Protection Policy

5.1. On 7th June 2016, the Committee approved the Council's first data protection policy. This has been updated in light of the forthcoming legislative changes. The proposed new policy is attached as an appendix to this report (tracked and clean versions). The policy sets out 10 high level commitments, and includes a glossary and a summary of the data protection principles.

5.2. The main changes are that:

- a commitment is added to consider data protection by design and default;
- a commitment is added to ensure the designation of a data protection officer with appropriate resources;
- the data protection principles have been updated; and
- definitions have been added for key GDPR terms.

6. Consultation

6.1. The Information Management Working Group has reviewed the proposed new policy.

7. Implications

Financial

7.1 No financial implications arise from the report's recommendations.

Resources

7.2 The Data Protection Officer will need to be appropriately resourced. Further work is required on assessing this, and whether it can be managed from existing staff resource.

Legal

7.3 The Council, as a data controller, must comply with the GDPR. Failure to comply may result in financial penalties and/or reputational damage.

Risk

7.4 The Corporate Risk Register includes two risks relating to information. Compliance with GDPR is fundamental to mitigation of these risks.

Equalities

7.5 No equality and poverty impact assessment is required.

Sustainability/Environmental Impact

7.6 No sustainability assessment is required.

8. Conclusions

8.1 The Council remains committed to protecting personal data and ensuring that it is compliant with data protection legislation. Preparations for changes to data protection legislation on 25th May 2018 are underway. An updated policy is required.

Director of Corporate and Housing Services

Author – Wendy Barber, Information Governance Manager, 01324 506124,
wendy.barber@falkirk.gov.uk
Date: 1 May 2018

Appendices

Appendix 1 - Revised Data Protection Policy
Appendix 2 - Revised Data Protection Policy (tracked changes)

List of Background Papers:

The following papers were relied on in the preparation of this report in terms of the Local Government (Scotland) Act 1973:

- None

DATA PROTECTION POLICY

We process personal data in order to carry out our statutory functions. We are registered with the Information Commissioner's Office (ICO) as a data controller.

We are committed to protecting personal data and complying with data protection legislation as defined by the Data Protection Act 2018 (the Act) and the 6 data protection principles.

In terms of our Financial Regulations, the Director of Corporate and Housing Services, in consultation with the Chief Governance Officer, is responsible for ensuring that the requirements of the Act are complied with. Each Service Director is responsible for compliance with the Act by employees within their Service.

Our 10 core commitments

1. We will ensure that proper policies and procedures are in place to ensure compliance with data protection legislation, in particular in the areas of Information Security and Records Management.
2. We will ensure that all staff who handle personal data understand their responsibilities under data protection legislation and receive appropriate training annually.
3. We will ensure that our information technology systems protect the availability, integrity and confidentiality of personal data.
4. We will ensure that we consider data protection by design and default, in particular by the use of data protection impact assessments where any processing is likely to result in a high risk to the rights and freedoms of individuals.
5. We will ensure that we tell data subjects what we will do with their personal data, by the use of privacy notices.
6. We will ensure that we designate a data protection officer and provide the resources necessary to enable that officer to carry out their statutory tasks.
7. We will ensure that procedures are in place to deal with subject access requests in line with the data protection legislation, and that we uphold other rights of data subjects.
8. We will ensure that we only share personal data with other organisations when appropriate and that it is shared safely and securely. Information sharing agreements will be put in place where regular sharing takes place.
9. We will ensure that we include appropriate clauses in contracts with third parties where they process personal data on our behalf.
10. We will ensure that any data breaches are handled in line with the ICO's guidance on data security breach management. All breaches will be recorded in a central log maintained by the Chief Governance Officer. Any serious breaches will be reported to the ICO.

Compliance with this policy, and related policies and procedures, is a condition of employment.

This policy will be reviewed every 3 years.

Summary of data protection principles

1. Personal data must be processed fairly and lawfully.
2. Personal data must be processed for specified, explicit and legitimate purposes.
3. Personal data must be adequate, relevant and not excessive.
4. Personal data must be accurate and up-to-date.
5. Personal data must not be kept for longer than is necessary.
6. Personal data must be processed in a secure manner.

Glossary

Data
Recorded information of any kind, including information held in a form which can be processed by computer

Personal data
Data which relates to a living individual who can be identified (a) from that data or (b) from that data and other information in the possession of the data controller. This includes an expression of opinion about the individual.

Data controller
A person who determines the purpose for which, and the manner in which, any personal data are, or are to be, processed.

Processing
Includes obtaining, recording, holding, using, adapting, altering, disclosing, deleting or erasing.

Data subject
An individual who is the subject of personal data.

Subject access request
A written request by an individual to a data controller under the Act, usually for any personal data processed by the data controller of which s/he is the data subject.

Data protection by design and default
A privacy-focused approach - data controllers design appropriate technical and organisational measures (a) to implement the data protection principles in an effective manner, and (b) to integrate into the processing itself the safeguards necessary for that purpose.

Data protection impact assessment
A documenting process to systematically describe and analyse intended processing of personal data, helping to identify and minimise data protection risks at an early stage.

Privacy notice
Information made available or provided to individuals when information is collected about them, including why it is collected, how long it is kept and whether it is shared with anyone else.

Version Number	Purpose/Change	Author	Date
1.00	Approved by Executive	Information Governance Manager	07/06/16
1.01	Update for new Act	Information Governance Manager	03/04/18

DATA PROTECTION POLICY

We process personal data in order to carry out our statutory functions. We are registered with the Information Commissioner's Office (ICO) as a data controller.

We are committed to protecting personal data and complying with data protection legislation as defined by the Data Protection Act ~~1998~~ 2018 (the Act) and the 6~~8~~ data protection principles.

In terms of our Financial Regulations, the Director of Corporate and Housing Services, in consultation with the Chief Governance Officer, is responsible for ensuring that the requirements of the Act are complied with. Each Service Director is responsible for compliance with the Act by employees within their Service.

Our 10~~8~~ core commitments

1. We will ensure that proper policies and procedures are in place to ensure compliance with ~~the Act~~data protection legislation, in particular in the areas of Information Security and Records Management.
2. We will ensure that all staff who handle personal data understand their responsibilities under ~~the Act~~data protection legislation and receive appropriate training annually.
3. We will ensure that our information technology systems protect the availability, integrity and confidentiality of personal data.

~~3.~~4. We will ensure that we consider *data protection by design and default*, in particular by the use of *data protection impact assessments* where any processing is likely to result in a high risk to the rights and freedoms of individuals.

Formatted: Font: Italic

Formatted: Font: Not Italic

5. We will ensure that we tell data subjects what we will do with their personal data, by the use of ~~fair processing~~privacy notices.

~~4.~~6. We will ensure that we designate a data protection officer and provide the resources necessary to enable that officer to carry out their statutory tasks.

~~5.~~7. We will ensure that procedures are in place to deal with subject access requests in line with the ~~Act~~data protection legislation, and that we uphold other rights of data subjects ~~under the Act~~.

~~6.~~8. We will ensure that we only share personal data with other organisations when appropriate and that it is shared safely and securely. Information sharing agreements will be put in place where regular sharing takes place.

~~7.~~9. We will ensure that we include appropriate clauses in contracts with third parties where they process personal data on our behalf.

~~8.~~10. We will ensure that any data breaches are handled in line with the ICO's guidance on data security breach management. All breaches will be recorded in a central log maintained by the Chief Governance Officer. Any serious breaches will be reported to the ICO.

Compliance with this policy, and related policies and procedures, is a condition of employment.

This policy will be reviewed every 3 years.

Appendix 2

Summary of data protection principles

1. Personal data must be processed fairly and lawfully.
2. Personal data must be processed for specified, explicit and legitimate~~limited~~ purposes.
3. Personal data must be adequate, relevant and not excessive.
4. Personal data must be accurate and up-to-date.
5. Personal data must not be kept for longer than is necessary.
6. ~~Personal data must be processed in line with the data subject's rights.~~
7. ~~6.~~ Personal data must be processed in a secure manner.
8. ~~Personal data must not be transferred to other countries without adequate protection~~.

Glossary

Data
Recorded information of any kind, including information held in a form which can be processed by computer

Personal data
Data which relates to a living individual who can be identified (a) from that data or (b) from that data and other information in the possession of the data controller. This includes an expression of opinion about the individual.

Data controller
A person who determines the purpose for which, and the manner in which, any personal data are, or are to be, processed.

Processing
Includes obtaining, recording, holding, using, adapting, altering, disclosing, deleting or erasing.

Data subject
An individual who is the subject of personal data.

Subject access request
A written request by an individual to a data controller under ~~section 7 of~~ the Act, usually for any personal data processed by the data controller of which s/he is the data subject.

Data protection by design and default
A privacy-focused approach - data controllers design appropriate technical and organisational measures (a) to implement the data protection principles in an effective manner, and (b) to integrate into the processing itself the safeguards necessary for that purpose.

Formatted: Font: Bold, Italic

Data protection impact assessment
A documenting process to systematically describe and analyse intended processing of personal data, helping to identify and minimise data protection risks at an early stage.

Formatted: Font: Bold, Italic

Privacy notice

Formatted: Font: Bold, Italic

Appendix 2

Information made available or provided to individuals when information is collected about them, including why it is collected, how long it is kept and whether it is shared with anyone else.

Formatted: Font: Bold, Italic

Version Number	Purpose/Change	Author	Date
1.00	Approved by Executive	Information Governance Manager	07/06/16
1.01	Update for new Act	Information Governance Manager	03/04/18