PERTH AND KINROSS COUNCIL

Strategic Policy & Resources Committee

18 April 2018

IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION

Report by Head of Legal and Governance Services

PURPOSE OF REPORT
This report provides an update on progress towards implementing the General Data Protection Regulation in the Council.

1. BACKGROUND / MAIN ISSUES

1.1 The General Data Protection Regulation ("the GDPR") will come into force on 25 May 2018 and will affect virtually all of the processing of personal data undertaken by the Council. The GDPR will remain law even following the UK's exit from the European Union. From a Council perspective therefore, all of our personal data processing must be compliant with the requirements of the GDPR from 25 May this year.

1.2 There is a separate Data Protection Bill currently progressing through parliament which will provide the amendments to the GDPR necessary for the UK's implementation. This includes specific provision for law enforcement functions which will affect Trading Standards and Criminal Justice. The content and detail of this legislation is still not finalised and the delay creates a significant handicap in preparing for a live date some 2 months away.

1.3 Whilst the GDPR was approved in May 2016, very little guidance has been available until relatively recently. This is partly due to the need to reflect the UK legislation correctly. This has caused delay in developing revised policies and procedures, but a significant amount of preparatory work has been undertaken including awareness raising sessions and process-mapping within Services. This work has been led by the Council's Information Compliance Manager, supported by a cross-Service working group.

1.4 Local authorities in Scotland have been collaborating wherever possible or practical and have relied heavily on work being undertaken by Edinburgh and Glasgow Councils. The Information Commissioner's Office is preparing material for communicating the changes to customers, service users, etc. but this will not be available until later in March.

2. SIGNIFICANT CHANGES

2.1 The Data Protection Act requires compliance with the legislation, but the GDPR introduces a new requirement to maintain evidence of compliance. This includes creating and maintaining a register of our data processing

activities and providing significantly more information to individuals in our privacy notices.

2.2 Liabilities also change under the GDPR.

- Data processors become separately liable for their actions, but contracts with processors must now explicitly state a number of requirements.
- Data breaches must be reported within a 72 hour period
- Individuals are entitled to compensation for any breach of the GDPR that affects them.
- The maximum fine for a breach of the legislation by the Council increases from £500,000 to £20m.

2.3 Further requirements include the following:-

- A public authority is required to appoint a statutory Data Protection Officer (DPO).
- Data protection must be included in the design of any new process
- Privacy impact assessments become mandatory and the lawful basis has to be identified before starting processing any personal information. The use of consent and the 'legitimate interest' condition for processing personal data is restricted for a public authority.
- The timescale for a subject access request reduces from 40 days to 28 days and the ability to charge a fee is completely removed.
- The annual registration fee will increase; the UK draft regulations currently indicate that the Council's annual fee will be £2,900.

3. PROGRESS TO DATE

3.1 The major task prior to the implementation date is creating a register of all activities involving the processing of personal data across the Council. This has been in progress since September 2017 and it is hoped to complete this by the end of March 2018. The information collected will require considerable review and updating by the Information Governance team.

3.2 In conjunction with this there is work in progress to identify all our existing privacy notices so that they can be amended to suit the new and extensive legislative requirements. This work will be informed by the register of processing activities.

3.3 A successful series of Learn Innovate Grow sessions was completed prior to Christmas and a new series is running from February through to June 2018. Tailored briefings have also been provided to a number of specific teams.

3.4 A general overview in booklet form has been prepared based on work done by City of Edinburgh Council and specific topic guidance is being prepared and will be published on ***eric*** as time and knowledge permit.

3.5 An e-learning module, based on work done by Glasgow City Council, has been developed and will be available shortly.

3.6 Some guidance has been given to the Council's ALEOs about the GDPR, but they are generally working independently on implementation. The situation in relation to the GDPR of several other bodies closely associated with the Council has also been given consideration (Integrated Joint Board, TACTRAN, Tayside Joint Valuation Board, and the Returning Officer).

4. OUTSTANDING IMPLEMENTATION WORK

4.1 The following is work that is ongoing/ still to be completed :-

- the register of processing activities
- development of a new privacy notice template(s) and revision of all privacy notices
- ensuring that there are compliant standard contract terms and amending standard ITT clauses and the associated tender evaluation criteria
- once the UK Act is approved, we will require to develop a suite of policies, specific procedures and a wide range of guidance material to support staff and ensure compliance with the new requirements
- revision of the documentation for privacy impact assessments and privacy notices
- development of specific guidance and targeted training regarding the use of consent and reporting data breaches
- once known, provide specific awareness training sessions and develop guidance for Trading Standards / Criminal Justice on the law enforcement provisions
- specific awareness sessions for outlying sections of staff and for schools
- brief elected members regarding their individual responsibilities as data controllers
- prepare awareness materials for Community Councils
- prepare and publish appropriate communications to services users, citizens and staff

5. POST IMPLEMENTATION DATE

5.1 Once the GDPR is implemented and the UK legislation is enacted the following programme of further and ongoing work will be required:-

- review and revise all current data sharing agreements, as necessary
- review and revise all contracts involving the processing of personal data, as necessary
- devise and implement appropriate procedures to monitor and report on the Council's compliance with the legislation
- investigate data breaches and liaise with the Information Commissioner's Office as and when required
- develop the register of processing activities, and the relevant procedures, to ensure it can be maintained appropriately
- integrate the new process with the Data Protection Impact Assessment process and the creation of privacy notices
- publicise the role of the DPO both internally and externally

- review project governance processes to ensure that the DPO is appropriately involved in every project involving the processing of personal data
- provide appropriate advice to the Council on all aspects of data protection.
- maintain and further develop the required knowledge and expertise in data protection law and practice to ensure continuing compliance and best practice

6. DATA PROTECTION OFFICER

6.1 Taking into consideration both the statutory tasks of a Data Protection Officer and the qualities required in a DPO, the Executive Officer Team agreed to designate an appropriate officer as the Council's DPO and the current Information Compliance Manager has been confirmed in this role.

6.2 The Council's Scheme of Administration will be amended to take account of this.

7. CONCLUSION AND RECOMMENDATION(S)

7.1 Implementation of the GDPR is a major challenge for an organisation as complex as the Council that relies on the processing of personal data for the majority of its activities. The Council has made reasonable progress towards implementation within the resources available and will continue to treat compliance with the legislation as a priority. The delay in finalising the UK legislation is a considerable handicap, but the Council is no worse off in this regard than all other organisations in the UK.

7.2 The scale of the requirements and the potential scale of the sanctions present a significant new risk to the Council. The Data Protection Officer will have a critical role in monitoring the state of the Council's compliance and advising on areas for improvement.

7.3 The Committee is asked to: -

a) Note the content of the report and highlight any areas of concern
b) Note the appointment of the Data Protection Officer and approve the amendment to the Scheme of Administration

Author(s)

Name	Designation	Contact Details
Lisa Simpson	Head of Legal and Governance Services	01738 475000

Approved

Name	Designation	Date
Jim Valentine	Depute Chief Executive (Chief Operating Officer)	4 April 2018

If you or someone you know would like a copy of this document in another language or format, (on occasion, only a summary of the document will be provided in translation), this can be arranged by contacting the Customer Service Centre on 01738 475000.

You can also send us a text message on 07824 498145.

All Council Services can offer a telephone translation facility.

ANNEX

1. IMPLICATIONS, ASSESSMENTS, CONSULTATION AND COMMUNICATION

Strategic Implications	**Yes / None**
Community Plan / Single Outcome Agreement	**N**
Corporate Plan	**N**
Resource Implications	
Financial	**N**
Workforce	**N**
Asset Management (land, property, IST)	**N**
Assessments	
Equality Impact Assessment	**N**
Strategic Environmental Assessment	**N**
Sustainability (community, economic, environmental)	**N**
Legal and Governance	**Y**
Risk	**Y**
Consultation	
Internal	**N**
External	**N**
Communication	
Communications Plan	**Y**

1. Strategic Implications

Community Plan/Single Outcome Agreement

1.1 Not applicable.

Corporate Plan

1.2 Not applicable.

2. Resource Implications

Financial

2.1 Not applicable.

Workforce

2.2 Not applicable.

Asset Management (land, property, IT)

2.3 Not applicable.

3. Assessments

Equality Impact Assessment

3.1 Not applicable.

Strategic Environmental Assessment

3.2 Not applicable.

Sustainability

3.3 Not applicable.

Legal and Governance

3.4 Not applicable.

Risk

	Risk	Impact	Prob.	Action
1	Failure to adequately document our processing activities	High	High	Senior management support is sought to prioritise and resource this activity in services which are struggling to complete the task in the timescale.
2	Failure to develop all the necessary procedures, guidance, etc.	Medium	High	Best endeavours – this risk has been exacerbated by the extremely late publication of guidance and the as yet draft UK legislation
3	Lack of staff awareness and engagement	Medium	High	Senior management support is sought to encourage all staff and where required mandate key staff to engage in training.
4	Due to other demands, GDPR is not given the appropriate strategic prioritisation within the organisation	High	Medium	Regular updates to EOT/CMG Elected Member briefings Organisation wide communiations

	Risk	Impact	Prob.	Action
5	Insufficient resources to complete all tasks required for implementation date	High	Medium	Prioritise activity based on risk. Continue to engage with other authorities to see where work can be shared. Seek management support to target barriers/ pressures
6	Lack of appropriate contractual terms with all suppliers	Medium	Medium	Prioritise contract amendment in terms of risk related to personal data

4. Consultation

Internal

4.1 Not applicable.

External

4.2 Not applicable.

5. Communication

5.1 The Council's Communication Team have been a key participant in the Implementation Group and the GDPR implementation has been included in the Council's corporate communications plan.

2. BACKGROUND PAPERS

None.

3. APPENDICES

None.