AGENDA ITEM
17

Falkirk
Health and Social Care
Partnership

Title/Subject:	**The General Data Protection Regulation (GDPR)**
Meeting:	**Integration Joint Board**
Date:	**1 June 2018**
Submitted By:	**Chief Officer**
Action:	**For Decision**

1. INTRODUCTION

1.1. The purpose of the report is to highlight the key features of new legislation and set out considerations for Falkirk Joint Board (the IJB) in relation to its responsibilities under the new legislation.

1.2. A new European Regulation, the General Data Protection Regulation came into effect on 25 May 2018. That is supplemented by a new Data Protection Act in the UK, which replaces the 1998 Act. The new Data Protection legislation imposes new responsibilities on all organisations that process (or control the processing of) personal data, and introduces significantly higher monetary penalties for non-compliance.

1.3. For the most part, the new legislation has a much bigger impact on the Council and NHS Forth Valley than the IJB. However, there are some impacts on the IJB.

2. RECOMMENDATION

The Integration Joint Board is asked to:

2.1. note the requirements of new Data Protection legislation, and its significance for the work of the IJB

2.2. approve Deirdre Coyle, Head of Information Governance, NHS Forth Valley as the Data Protection Officer (DPO) for the Falkirk IJB

2.3. note that further work will be required by the IJB to review arrangements for processing of personal data by the IJB, to check that processes are compliant with GDPR

2.4. note that the IJB must document its arrangements for processing personal data, and have a privacy notice in place for the public, in line with the requirements of GDPR in relation to transparency and accountability.

Falkirk Council NHS Forth Valley

3. BACKGROUND

3.1. The GDPR is a new regulation which replaces existing data protection legislation across the European Union from 25 May 2018. Certain aspects of the regulation need to be put into effect or clarified by domestic legislation in each member state, and a new Data Protection Act is currently being considered by the UK Parliament.

3.2. Together, the GDPR and new Data Protection Act will modernise the approach to processing of personal data in the digital age. The legislation imposes new obligations on organisations and expands and strengthens the rights of individuals in relation to personal data.

3.3. The Information Commissioner's Office (ICO) will remain as the supervisory authority for data protection legislation within the UK. Under existing legislation, the Information Commissioner can issue Monetary Penalty Notices for breaches of data protection legislation of up to £0.5m. GDPR will allow significantly higher fines of up to 40m Euros (currently around £17.6m) depending on the nature of the breach.

4. GENERAL DATA PROTECTION REGULATION

4.1. This part of the report sets out the main features of the GDPR.

4.2. **Data Protection Officer (DPO)**
Falkirk Integration Joint Board is a **"**Data Controller" in terms of GDPR as it determines the purposes and means of processing personal data. The IJB holds minimal personal data in its own right. Falkirk Council, and NHS Forth Valley are also both Data Controllers in respect of service user/patient personal data.

4.3. The GDPR introduces a statutory role of Data Protection Officer which must be appointed by certain Data Controllers, and set out both the position and tasks of this role. The IJB, as a public authority, is required to appoint a DPO. The DPO is responsible for ensuring compliance with GDPR, and must have a direct reporting route to senior management. The DPO will be expected to have sufficient professional knowledge to inform and advise the organisation on data protection matters, and to act independently with sufficient authority to identify, report and rectify risks around the processing of personal data. The legislation allows for one person to act as DPO for more than one organisation.

4.4. The IJB are asked to approve Deirdre Coyle, Head of Information Governance, NHS Forth Valley as the DPO for the Falkirk IJB.

4.5. **Data Protection Principles**

GDPR is based on 6 Data Protection Principles which provide that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- accurate and, where necessary, kept up to date; ('accuracy')
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation')
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4.6. **Transparency and Accountability**

GDPR requires greater transparency about how Data Controllers comply with each of the Data Protection principles. It requires details to be provided to people in the form of a privacy notice at the point at which their personal data is collected. Privacy notices will need to ensure people are told about processing in sufficient detail, and include several mandatory elements, including the purpose of the processing, the lawful basis for processing, how long the data is kept, and who it is shared with.

4.7. In addition, GDPR requires data controllers to maintain documentation relating to processing activities, which could be made available to the Information Commissioner or members of the public on request. Organisations need to compile a register of data processing which documents in detail each process involving personal data.

4.8. The register of processing is an effective way of assessing compliance of each process against the requirements of data protection legislation. Typical actions arising might involve: revising privacy notices to ensure detailed information is given to people at the point at which their data is collected; making sure the lawful condition for processing has been identified and documented; ensuring there are agreements in place with other people and organisations to share personal data; and ensuring that there are retention rules in place for all personal data held, and that these rules are routinely implemented.

4.9. For the most part, this has a greater impact on Falkirk Council and NHS Forth Valley than the IJB. However, the IJB will need a simple register of data processing activities and privacy notices in place to comply with the new legislation

4.10. **Rights of Individuals**

GDPR creates some new rights for individuals as well as strengthening some of the rights that exist under current legislation. Changes to existing rights include a revised timescale for Subject Access Requests (where an individual request access to the personal data held about them) which have to be answered within 30 calendar days (but with the possibility of extending the deadline by a further 2 months) rather than 40 days under existing legislation.

4.11. **Impact Assessments**

GDPR will require organisations to implement "Privacy by Design" to consider privacy and data protection implications from the start of any initiatives, projects or new technology which use personal data. It will become mandatory to complete a Data Protection Impact Assessment (DPIA) for such projects which pose a high risk to individuals' privacy, to ensure that privacy issues are considered and documented. Under present legislation, such assessments are considered good practice, but are not mandatory.

4.12. **Breach Management**

GDPR introduces a legal duty for organisations to report certain types of data breaches to the ICO, within 72 hours of them occurring. Failure to do so could result in a financial penalty. Under present legislation, the ICO expects that "serious" breaches would be reported to the Commissioner, but there is currently no requirement to do so.

5. CONCLUSIONS

The IJB is a "Data Controller" in terms of data protection legislation, and will have responsibilities under the new GDPR. In particular, it will need to nominate a Data Protection Officer, document its arrangements for processing personal data (relating to any personal data about service users/patients and IJB members) and ensure that its processes comply with the requirements of the new legislation.

Resource Implications

Should there be any significant change to the responsibility of the IJB in the future, this role and its associated responsibilities would need to be reviewed.

Impact on Strategic Plan Priorities and Outcomes

This report and associated recommendations do not relate to the Falkirk Health and Social Care Partnership local outcomes and Strategic Plan priorities; however it supports the Board and Partnership to exercise their statutory duties.

Legal & Risk Implications

Failure to comply with new data protection legislation risks enforcement action by the Information Commissioner, and possible monetary penalties.

Consultation

Leads for governance across the two authorities have been consulted in the development of this report.

Equality and Human Rights Impact Assessment
The contents of this report do not require an EQIA because it relates to compliance with legislation.

_____
Approved for submission by: Patricia Cassidy, Chief Officer

Author: Suzanne Thomson, Programme Manager
Date: 14 May 2018

List of Background Papers: