MUNICIPAL YEAR 2017/2018 REPORT NO. **132**

MEETING TITLE AND DATE:

Audit & Risk Management Committee
11th January 2018
REPORT OF:
Head of Legal Services/ Chair of IGB

Agenda – Part:	**Item: 6**
Subject: Update on work of IGB **Wards: all** **Key Decision No:**	
Cabinet Member consulted:	**n/a**

Contact officer and telephone number:

Jayne Middleton-Albooye 0208379 6431

E mail: Jayne.Middleton-Albooye@enfield.gov.uk

1. EXECUTIVE SUMMARY

This report updates Audit Committee on the work of the Information Governance Board (IGB) and explains the changes to data protection rights and obligations which will be introduced by the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR). The report seeks to provide assurance that the Council is adequately prepared for the implementation of the GDPR, and attaches at Appendix 1, the implementation plan.

The report also updates Audit Committee on the work done by IGB to prepare for an audit carried out by NHS digital at the end of November. No final report of the audit has been received by the Council so the findings will be reported to a future Audit Committee.

The report also updates Audit Committee on the internal review of the National Audit Office Guidance *Cyber and Information Security Risk Guidance for Audit Committees* as requested by previous meeting.

IGB is also responsible for considering any Data Protection breaches or Information Commissioner's Office (ICO) referrals, and this report summarises matters that have come to IGB in this financial year.

2. RECOMMENDATIONS

Audit Committee is asked to note:

1. An overview of the changes which will be brought about by the GDPR and the Data Protection Bill.

2. The progress of the IGB to date, and any deadlines, contained within the implementation plan, to implement the GDPR.

3. To note the inspection of the NHS auditors.

4. To note the comments on the National Audit Office Guidance

3. BACKGROUND

Changes to Data Protection Legislation

The GDPR was adopted by the EU in April 2016 and will replace the current EU Data Protection Directive 95/46/EC on 25th May 2018. The GDPR introduces new obligations to data processors and data controllers, including those based outside the EU. Given that infringement can lead to fines of up to 4% of annual worldwide turnover or €20 million, it is important for companies/ organisations to assess how the GDPR will affect them and prioritise preparations to comply by May 2018. The Data Protection Bill, currently going through Parliament, will bring the GDPR into UK law, helping Britain prepare for a successful Brexit.

Many of the principles in the GDPR are much the same as in the current Data Protection Act 2000 (DPA). If an organisation is already complying with the current DPA, then it has a strong starting point to build from. There are some important new elements, and some things will need to be done differently.

- Greater harmonisation between member states. GDPR introduces a single legal framework that applies across all EU member states. This means that businesses will face a more consistent set of data protection compliance obligations from one EU member state to the next.
- Expanded territorial scope. Many non-EU businesses will be required to comply if they offer goods or services to data subjects in the EU.
- The GDPR imposes a significant burden for demonstrating compliance with the data protection regime not only on the controller but also on the processor, which contributes to the overall principle of accountability.
- The GDPR adopts a risk-based approach to compliance, under which businesses bear responsibility for assessing the degree of risk that processing activities pose to data subjects. This may involve substantial changes to existing compliance strategies. Preparatory steps will include creating awareness among senior decision-makers; audit and document personal data held, recording where it came from and who it is shared with; reviewing the legal basis for the various types of processing which are carried out, and documenting this; reviewing privacy notices.
- Organisations will need to maintain detailed documentation recording their processing activities and the GDPR specifies the information this record must contain. Organisations need to ensure they have clear records of all processing activities and that such records are available to be provided on request.
- Mandatory privacy impact assessments where this is likely to result in a high risk to data subjects.

- Organisations are required to appoint a data protection officer with expert knowledge of data protection. That officer may have protected status and must be independent with no potential for conflict of interest.
- Organisations will need to identify processor agreements early on so that these can be reviewed and amended if necessary. Increased compliance obligations for processors may mean increased cost of data processing services. Negotiating agreements may become more difficult. Some processors may wish to review their existing agreements to ensure compliance.
- The GDPR continues the approach under the previous regime requiring a data controller to justify the processing of personal data before it will be considered lawful.
- Consent, as a legal basis for processing will be harder to obtain. The DPA distinguished between ordinary consent and explicit consent for sensitive data. **The GDPR requires a very high standard of consent**, which must be given by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to the personal data being processed. Where the Council relies on consent as a legal basis for processing personal data, we will need to carefully review our existing practices to ensure that any consent we obtain indicates affirmative agreement from the data subject. Mere acquiescence (for example, failing to untick a pre-ticked box) does not constitute valid consent under the GDPR. We must also ensure that we have the processes in place so that an individual can withdraw their consent at any time.
- In general, the rights of data subjects are expanded under the GDPR. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processes. This represents a tightening of the principle in the DPA that the data must not be 'excessive'. A right to request that businesses delete their personal data in certain circumstances. A new right to obtain a copy of their personal data. Additionally organisations must reply within one month from the data of receipt of the request (currently 40 Calendar days), and provide more information than was required under the DPA.
- Data subjects have a right to object to processing for public interest purposes. It will be for the data controller to demonstrate compelling legitimate grounds for the processing which overrides the data subjects' rights and freedoms. This represents a different burden of proof from the approach under the DPA, where the data subject had to establish compelling legitimate grounds that would override the data controller's right to process the data for public interest purposes.
- Increased enforcement powers. Current fines are comparatively low and the GDPR will significantly increase the maximum fines up to 20 million euros for data controllers and data processors. Also introduces new investigative powers to carry out audits and require information and access to be provided.
- Strict data protection breach notification rules. Organisations must make a notification of breach within 72 hours, unless the breach is unlikely to result in risk to individuals. Organisations must inform data

subjects if there is a high risk to individuals. The Council will need to develop and implement a data breach response plan, including designating specific roles and responsibilities, training employees and preparing template notifications enabling them to act promptly in the event of a breach.

Data Protection Bill

The Data Protection Bill had its first reading in the House of Lords on 13 September. The Bill serves a number of functions as, once it receives Royal Assent, it will:

- Repeal and replace the DPA.
- Fill in the gaps (the derogations) in the GDPR.
- Go further than the GDPR as it will address data processing in law enforcement and the intelligence services (which are covered by the Law Enforcement Directive).
- Attempt to ensure that on leaving the EU the UK has an "adequate" data protection regime to that of the EU.

Work of IGB

The IGB meets monthly and the new membership has met 4 times. The aim is to expand the membership to cover all departments of the Council. The focus of IGB for these 4 months has been preparation for the implementation of GDPR, and to ensure that the Council was prepared for the NHS digital audit at the end of November, focusing on the action plan to prepare for this.

One of the first actions of IGB was to review and approve policies and procedures to ensure they are GDPR compliant. IGB has thus far approved all 23 policies and procedures, needed to ensure compliance with GDPR, and is in the process of uploading these on to the intranet to replace old policies and procedures. The policies include: subject access policy and procedure; third party access and management policy; security incident reporting procedure and cyber security policy. Several of the policies and procedures were either deleted, as they were no longer relevant, or were amalgamated. On-going consideration is being given by IGB as to whether further consolidation of the policies can be undertaken. IGB will be raising awareness across the Council of the new policies and procedures.

The board receives reports from the Council's IT Capital Programme and Security Consultant on the operational implementation of the GDPR. He has set up a project board with representatives from across the Council.

The Council has now recruited 2 data analysts specifically for GDPR who will undertake assessments of the extent to which personal data is required to achieve processing purposes as part of the Information Governance Privacy Impact Assessments and within data sharing agreements. This will also provide the documentation required for the council to evidence its data

holding, its legal basis or consents for processing and to ensure that compliance gaps are surfaced and can be dealt with.

Council-Wide training is being built by the GDPR team to be rolled out in the New Year, and the legal team have organised free legal training at the end of January to ensure that legal, and key information governance staff are fully briefed on the new law. It is essential that when the training is available that EMT give full support to managers to ensure all staff undertake the training. In the event of a breach, well-trained staff will be viewed as a mitigating factor.

IGB has created a centrally held register of data sharing agreements. With management support, all data sharing agreements are being gathered from around the Council to be held on the central register.

The IT Capital Programme and Security Consultant has drafted a new Privacy Statement which is being considered by IGB.

IGB also has a standing item on Data Protection Act breaches and ICO referrals and decisions. IGB will receive a rolling list of breaches/ decisions at each meeting, these will be brought periodically to EMT. There have been 6 Data protection referrals and 7 FOIA referrals since the start of the financial year.

NHS Digital Audit

On 28th and 29th November 2017, NHS Digital undertook an audit of the Council's compliance to the data sharing agreement (DSA) with NHS Digital. Following the DSA breach incident in July 2017, IGB has developed and implemented an action plan to strengthen the Council's Information Governance and compliance to data sharing agreements. This included rejuvenating the IGB; establishing organisational process to support data sharing compliance including development and sign off, monitoring compliance and acting swiftly to any breaches; developing a central register of data sharing agreements to assist monitoring of compliance.. An audit report has been received in draft form and a copy of the report and its findings will be reported to a future Audit committee.

National Audit Office Guidelines

An assessment of the National Audit Office Guidelines *Cyber and Information Security Risk Guidance* was carried out by the IT Security Team.

The guidance is based on three high-level control areas, ten "more detail" areas for examination and two "additional questions". The questions do not map well onto the existing audits as existing audits follow far more detail in controls, so are not directly comparable. Overall the self-assessment rating was:

Area	Red	Amber	Green
High level questions	0	0	3
More detail questions	0	2	8

Additional questions	0	1	1

The Amber areas are as follows:

- Information Risk Management Regime (More detail) – impacted by the issues with data governance across the organisation leading to challenges with risk focus. Improvements in data governance from GDPR work will help, but there remain challenges with older, unsupported systems. Most of these are being replaced as part of various programmes, such as the Housing systems upgrade.
- Monitoring (More detail) – there is weakness in the ability to monitor system access in some areas. This is being examined with a view to bringing forward mitigations.
- Development of new services and technology (Additional Questions) – this was answered retrospectively for the last wave of development; security was not formally assessed early enough in development programmes, leading to challenges repairing gaps created by not initially performing "Data Privacy by Design". This is a legal requirement from 25 May, and the team working on the latest developments are aware of this. Security considerations for the new phase are already being discussed.

4. ALTERNATIVE OPTIONS CONSIDERED

To do nothing would put the Council at reputational and financial risk.

5. REASONS FOR RECOMMENDATIONS

The GDPR will mean huge changes for the Council in the way it processes data and the penalties for not implementing GDPR correctly are vastly increased. Member oversight of the implementation process will demonstrate the Council's commitment to protecting residents' data.

6. COMMENTS OF THE EXECUTIVE DIRECTOR OF FINANCE, RESOURCES AND CUSTOMER SERVICES AND OTHER DEPARTMENTS

6.1 Financial Implications

There are no financial implications arising from the recommendations in this report.

6.2 Legal Implications

There are no direct legal implications. It is good governance for Audit Committee to consider the work of the Information Governance Board and to consider the Council's readiness for the implementation of GDPR.

7. IMPACT ON COUNCIL PRIORITIES

7.1 Fairness for All

The thrust of GDPR and the Data Protection Bill is to give Data subjects greater rights in relation to their data and will ensure greater fairness in terms of individuals' means of controlling the use of their data.

7.2 Growth and Sustainability

A major breach, especially when GDPR comes into effect, could have a substantial effect on the Council's finances and therefore on its growth and sustainability.

7.3 Strong Communities

The implementation of the GDPR will assist the Council to be more open and accountable.

Background Papers

1. The Implementation plan