WIRRAL

Audit and Risk Management Committee

Tuesday, 22 November 2016

REPORT TITLE:	**General Data Protection Regulation (GDPR) Implementation Update**
REPORT OF:	**Assistant Director: Law & Governance (Monitoring Officer)**

REPORT SUMMARY

The report seeks to provide assurance to the Committee on the implementation of the Council's GDPR project plan.

The GDPR project is working to achieve the following agreed objectives:

- Create a framework and environment for the Council to become GDPR compliant by 25 May 2018
- Build GDPR compliance into policies and procedures,
- Continually assess the Council's compliance with the GDPR
- Manage the training and awareness for staff on data protection, in line with the GDPR
- Create Data Protection Officer (DPO) job description and role
- Implement all identified requirements for change in high risk areas within the Council.

The project is at a key phase of its implementation, where it will inform and seek involvement from all Council departments to implement actions to meet the 25th May 2018 deadline.

Current Position

The Council appointed a GDPR Project Manager in November 2017. A project plan was designed and approved by the Information Governance Delivery Group (IGDG) who additionally acts as the project board.

The project plan is progressing, with contributions from the IGDG and the Working Group members.

Regular reports are prepared for the IGDG and the Senior Leadership Team (SLT).

Supporting the project is a communications and training strategy, which also provides evidence of compliance with GDPR. This is a rolling strategy which will provide more information both general and specific as the project progresses

External training for SLT has been arranged for 13/03/2018 and a new online training module is currently being reviewed.

A number of key tools and processes have been developed and will soon be implemented across the Council's departments.

RECOMMENDATION/S

That the Audit and Risk Management Committee:

(1) Notes the GDPR project update.

(2) Support the GDPR project.

SUPPORTING INFORMATION

1.0 REASON/S FOR RECOMMENDATION/S

1.1 The Audit and Risk Committee has responsibility as part of the risk management framework for assuring that important risks to the Council are monitored and reviewed. Failure to comply with the GDPR and UK Data Protection legislation (once it incorporates GDPR and agreed derogations) have both financial and reputational implications.

2.0 OTHER OPTIONS CONSIDERED

2.1 No other options were considered.

3.0 BACKGROUND INFORMATION

3.1 The GDPR replaces the EU Data Protection Directive and will govern how personal data should be held and processed by all 28 EU member states.

3.2 The Data Protection Act 1998 will no longer apply after 25th May 2018.

3.3 The GDPR will apply to any data controller or processor offering goods or services to data subjects located within the EU. The effects of the GDPR will also extend well beyond Europe. All organisations and businesses that hold data on EU citizens, whether they are located within the EU or not will be affected.

3.4 Both controllers and processors of personal data will be subject to the GDPR. The European Data Protection Board will have oversight of the GDPR with individual EU states having their own data protection authority.

Data Protection Bill

3.5 The GDPR has direct effect across all EU member states and has already been passed but comes into force on the 25th May 2018.

3.6 However, the GDPR gives member states a number of derogations to make provisions for how it applies in their country.

3.7 The GDPR, and the derogations (which have yet to be finally agreed by Parliament) are incorporated into the Data Protection Bill which is set to have final approval in early May 2018.

3.8 If the Bill is not passed, UK organisations will still have to comply with GDPR requirements which have already been passed.

Key Features of the GDPR

3.9 Appointment of a Data Protection Officer

As a public authority, the Council will be required to designate a person as its Data Protection Officer (DPO) (Article 37).

Article 3 (5) provides that the DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.

The DPO can be an employee or a named contractor.

Article 38 (3) provides protection against dismissal of the DPO for performing their tasks and they "shall directly report to the highest management level of the controller or the processor" (Article 38 (3)).

The DPO must ensure that all requirements under the GDPR are adhered to, including the following:

- Advising the organisation on regulation obligations
- Monitoring compliance, policies and training
- Advising on data protection impact assessments
- Communicating with the ICO

3.10 Information, Notification and Consent

The Council will be required to notify individuals if they process their personal data.

Any individual, whose data is going to be collected and / or processed, must be informed in unambiguous terms of the action, as well as for what specific purpose (or multiple purposes) the data will be used. It will be the Council's responsibility to document this process.

Under the GDPR the definition of "consent" has been significantly restricted. The GDPR requires the data subject to signal agreement by "a statement of or clear affirmative action". Consent must be "given unambiguously by any appropriate method enabling a freely given, specific and informed indication of the data subject's wishes". Explicit consent will be required for the processing of sensitive personal data. Organisations must be able to demonstrate consent. Special regard and sensitivity is needed when gaining consent from children

The Council will need to redesign its processes so that these requirements can be incorporated, when it processes personal data.

3.11 The right to erasure

Individuals will be able to withdraw their consent to having their personal data processed and the Council will be required to erase the personal data of data subjects if requested, unless the retention of data is necessary for the

performance of a contract or for compliance with a legal obligation. The data can be kept as long as necessary for that purpose.

If data is published by the Council, the recipient to whom the data has been passed must be notified if the data subject requests that links to or copies of this data be erased.

3.12 **Subject Access Requests**

The Council will be required to respond to all requests (under articles 15 to 20) without undue delay and, at the latest within one month of receipt of the request (rather than the current 40 day time limit).

The deadline can be extended for a maximum of two further months, when necessary taking into account the complexity and number of requests.

The data subject has to be informed of the reasons for the delay and right of appeal.

Requests will be free of charge.

Councils will be expected to have IT systems which will enable personal data to be retrieved.

3.13 **Security**

This is a key element of the GDPR.

A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The Council will be required to notify the ICO within 72 hours after 'becoming aware' of a personal data breach. In any report to the ICO, the Council will be required to provide the following details:

- Nature of incident
- Identity of organisation contact
- Likely consequences for data subjects
- Measures taken/proposed to be taken
- Mitigation

The Council will need to ensure that it has the right procedures in place to detect, report and investigate a personal data breach.

3.14 **Penalties**

Two levels:

- 10,000,000 Euros or 2% of turnover (whichever is higher for the private sector) relating to various organisational provisions including security retention;

- 20,000,000 Euros or 4% of turnover for breaches of principles, conditions, consent, protected data conditions, rights including fair processing, breaching ICO order.

The fines are based on the specific articles of the Regulation that the organisation has breached. Infringements of the organisation's obligations, including data security breaches, will be subject to the lower level, whereas infringements of an individual's privacy rights will be subject to the higher level.

When deciding whether to impose a fine and the level, the ICO must consider:

- The nature, gravity and duration of the infringement;
- The intentional or negligent character of the infringement;
- Any action taken by the organisation to mitigate the damage suffered by individuals;
- Technical and organisational measures that have been implemented by the organisation;
- Any previous infringements by the organisation or data processor;
- The degree of cooperation with the regulator to remedy the infringement;
- The types of personal data involved;
- The way the regulator found out about the infringement;
- The manner in which the infringement became known to the supervisory authority, in particular whether and to what extent the organisation notified the infringement;
- Whether, and, if so, to what extent, the controller or processor notified the infringement; and
- Adherence to approved codes of conduct or certification schemes.

The Data Protection Act (DPA) is the current legislation that holds organisations to account for data breaches. Below are two recent examples of ICO fines awarded under the DPA:

1. A GP practice was fined £40,000 for revealing confidential details about a woman and her family to her estranged ex-partner.
2. Islington Council was fined £70,000 following a fault in one of their I.T. systems potentially allowed public access to 89,000 individual's personal information.

3.15 **GDPR Governance Structure**

The project has a Project Board (IGDG)) and a Working Group which is made up of workstream Leads linked to key deliverable areas. The stakeholders meet and work on the following basis:

<u>Project Board (IGDG)</u>
Frequency: Monthly
Last Meeting: 26/01/2018
Next Meeting: 01/03/2018

Working Group with Working Group Leads
Frequency: Fortnightly
Last Meeting: 13/01/2018
Next Meeting: 28/02/2018

Reports on the project have regularly been presented to the Corporate Governance Group and a communication and training strategy briefing was presented to the Senior Leadership Team 06/02/2018.

3.16 **Risk Management**

Integral to the project is managing the potential risk and ensuring the implementation meets the expected legal and best practice requirements enforced by the Information Commissioner's Office (ICO). Therefore included on the Project Board and Working Group are representatives from Risk and Insurance (Mike Lane) and Internal Audit (Kelly Lacy).

The GDPR Project Risk is included on the Corporate Risk Register (Corporate Risk No. 8 – Governance (including information governance)) first presented to ARMC in September 2017 (See Appendix 1) and included in the SLT report in December 2017.

The project plan includes its own assessment of the project risk (See Appendix 2) and an important requirement is support from all departments. The project is broken down into 10 key areas, with a number of deliverables for each area. The areas are interrelated and there is a dependence on all department's information asset owners and administrators to respond to requests for information or assistance in a timely manner.

3.17 **Next Steps**

A GDPR User Guide is being developed for each department's information asset owners and administrators who have an important function in the Council meeting its objectives.

The guide will inform them of changes needed to meet the new legislative requirements and how personal data will need to be processed in their department.

The guide will also include a list of actions of what will be expected from officers with access to the tools and processes they will need to meet those requirements. Support will be provided for officers during the implementation period.

There will be close liaison with Internal Audit to provide assurance that the Council is meeting its requirements using the ISO guide: Preparing for the General Data Protection Regulation (GDPR) "12 steps to take now"' as the focus of the plan moves into the detailed implementation stage.

4 FINANCIAL IMPLICATIONS

4.1 There are no such implications arising

5 LEGAL IMPLICATIONS

5.1 The Council is required to comply with the GDPR and derogations agreed in the Data Protection Bill (when approved by parliament) and comes into force on the 25th May 2018.

6 RESOURCE IMPLICATIONS: ICT, STAFFING AND ASSETS

6.1 The Council is required to appoint a Data Protection Officer as per section - 3.9 "Appointment of a Data Protection Officer". A process is taking place to resource this role internally.

7 RELEVANT RISKS

7.1 The Council is open to fines from the ICO; claims by individual's for loss of data and harm caused; reduction in confidence in the ability of the Council to securely process sensitive and personal data; and loss of reputation.

8 ENGAGEMENT/CONSULTATION

8.1 Consultation with members of the IGDG, Corporate Governance Group and Internal Audit.

9 EQUALITY IMPLICATIONS

9.1 There are no such direct implications arising.

REPORT AUTHOR: ***Gareth Webb***
GDPR Project Manager
telephone: (0151) 666 4035
email: garethwebb@wirral.gov

APPENDICES

Appendix 1 **Corporate Risk No. 8 – Governance (including information governance)**
Appendix 2 **Project Plan Risk and Controls**

REFERENCE MATERIAL

The ICO's: Guide to the GDPR

The ICO's: Preparing for the General Data Protection Regulation (GDPR) "12 steps to take now"

SUBJECT HISTORY (last 3 years)

Council Meeting	Date
Audit and Risk Management Committee	**25th September 2017**
Council Cabinet	**6th November 2017**
Senior Leadership Team	**7th December 2017**
Corporate Governance Group	**20th December 2017**
Senior Leadership Team	**6th February 2018**

Appendix 1: Corporate Risk No. 8 – Governance (including information governance)

Risk Description	Lead Responsibility
Major acts of non-compliance with internal and external governance requirements could result in poor decision-making, malpractice and breach of legislation, leading to regulatory intervention and significant cost, both in financial terms and to the reputation of the Council and its partners.	Assistant Director – Law and Governance

Pledges affected	Impacts
Effective governance impacts on the delivery of all the Pledges.	• Legal challenge to decisions. • Financial penalties for non-compliance *(e.g. for information governance incidents or breaches of procurement legislation)*. • Loss of confidence by the public and other stakeholders in the Council's decision-making and governance arrangements. • Potential loss of inward investment in the borough from damage to the reputation of the Council and the wider Wirral Partnership in the eyes of potential investors.

Unmanaged Risk Rating	Impact	5	Likelihood	4	Total	20

Key Existing Controls	Responsibility
• Council Constitution	• Assistant Director – Law and Governance
• Code of Corporate Governance	• Assistant Director – Law and Governance
• Member / Officer Protocol	• Assistant Director – Law and Governance
• Staff Policies (e.g. Dignity at Work)	• Assistant Director: HR & OD
• Corporate Policies (e.g. Whistleblowing)	• Assistant Director – Law and Governance
• Operational policies (e.g. Information Governance, Gifts and Hospitality)	• Assistant Director – Law and Governance
• Ethical Framework for Members	• Assistant Director – Law and Governance
• Regulatory policies - Planning and Licensing	• Heads of Regen & Planning and Env. & Regulation
• Oversight provided by CGG and Information Governance Delivery Group	• Assistant Director – Law and Governance
• Annual Governance Statement	• Assistant Director – Law and Governance

Managed Risk Rating	Impact	3	Likelihood	3	Total	9

Planned Additional Controls	Responsibility
• Review the Constitution, Code of Corporate Governance and Members Code of Conduct.	Assistant Director – Law & Governance 2017/18
• Introduce the webcasting of Council Committee and Cabinet meetings.	Assistant Director – Law & Governance 17/18
• Review and enhance information governance arrangements (including delivery of action plan responding to the ICO report and ensuring delivery of the Council's GDPR Project	Assistant Director – Law & Governance and Senior Information Risk Officer – 2017/18

Appendix 2 Project Plan Risk and Controls

Risk Ref.	Risk Owner	Risk Category	Risk Description	Links to other Projects / Plans	Unmanaged Scores			Existing Controls	Current Scores			Planned Additional Controls	Control Owner	Target Date
					Likelihood	Impact	Total (LxI)		Likelihood	Impact	Total (LxI)			
01	SIRO	Corporate	Project cannot meet the required deadline and incurring fines, claims and loss of reputation.		5	4	20	Senior Management buy-in to the project. Resources allocated with a full time designated project lead. Defined compliance action plan. Prioritisation of deliverables with key milestones.	3	4	12	Work with Internal Audit during project timelines to provide ongoing assurance. Implement governance and reporting lines to Project Board and internal governance mechanisms	Gareth Webb	25/05/18
02	SIRO	Operational	The scope of the Project is increased without sufficient resources to meet new requirements.		4	4	16	Project Plan states current scope. Any changes will need additional resources provided and new scope approval from Project Board.	2	4	8	No further action required at this time.	Gareth Webb	25/05/18
03	SIRO	Operational	Internal knowledge and resources unavailable resulting in a delay to the project		5	3	15	Agreed prioritisation of resourcing. Leads allocated to assist Deliverables	3	3	9	Implement governance and reporting lines to Project Board and internal governance mechanisms	Gareth Webb	25/05/18
04	SIRO	Operational	Unidentified complex changes to IT Systems / Practices which may cause significant delay or consume resources.		5	3	15	Agreed prioritisation of resourcing. Leads allocated to assist Deliverables	3	3	9	Implement governance and reporting lines to Project Board and internal governance mechanisms	Gareth Webb	25/05/18
05	SIRO	Operational	Insufficient support or contribution from all WBC Departments to engage or implement changes.		4	3	12	Risk and Project Reporting to Corporate Governance Committee and IGDG.	3	3	9	Escalation procedure where lack of engagement is identified	Gareth Webb	25/05/18