

Cabinet (Performance Management) Panel

17 December 2018

| | | |
|--|---|--|
| Report title | Information Governance Quarter Two Performance and General Data Protection (GDPR) Update Report | |
| Decision designation | AMBER | |
| Cabinet member with lead responsibility | Councillor Val Gibson Governance | |
| Key decision | No | |
| In forward plan | Yes | |
| Wards affected | All Wards | |
| Accountable Director | Jennifer Brake, Service Director of Strategy and Change | |
| Originating service | Information Governance | |
| Accountable employee | Anna Zollino-Biscotti | Information Governance Manager & DPO |
| | Tel | 01902 555166 |
| | Email | Anna.zollino-biscotti@wolverhampton.gov.uk |
| Report to be/has been considered by | Corporate Leadership Team | 27 November 2018 |
| | Strategic Executive Board | 4 December 2018 |
| | Information Governance Board | 10 January 2018 |

Recommendations for decision:

The Cabinet (Performance Management) Panel is recommended to:

1. Review the quarterly progress update on the General Data Protection Regulation.
2. Review the quarter two performance for Information Governance.

1.0 Purpose

- 1.1 To provide an update on the Information Governance performance figures for quarter two 2018-2019.
- 1.2 To provide a quarterly update on the work currently being undertaken by the Information Governance (IG) team and directorates following the implementation of the General Data Protection Regulation (GDPR).

2.0 General Data Protection Regulation

Background and context

- 2.1 On 14 April 2016, the EU Parliament approved the General Data Protection Regulation. In the following October, the Government confirmed that it will implement the GDPR in the UK and that the UK's decision to leave the EU will not affect the commencement of the GDPR. The new regulations have replaced the Data Protection Act 1998 and the Information Commissioner's Office (ICO) will continue to be the supervisory authority for the UK.
- 2.2 In April 2017, the Government issued a consultation document to consider the derogations (exemptions) within the GDPR where the UK can exercise discretion over how certain provisions are applied.
- 2.3 In September 2017, the Data Protection Bill was published setting out new standards for protecting general data in accordance with GDPR and preserving certain other exemptions of the current Data Protection Act 1998.
- 2.4 The Data Protection Act 2018 was given Royal Assent on 23 May 2018. The General Data Protection Regulation came into force on 25 May 2018 and provides an accountability-based framework for data protection in Europe.
- 2.5 In preparation for the new regulation, a GDPR work programme was developed, drawing on regional collaborative work completed with other local authorities. This was approved in July 2017 and this report provides the fifth quarterly update to the Cabinet (Performance Management) Panel on progress to date.

Progress to date and next steps

- 2.6 The GDPR programme of work is now moving towards a business as usual status. GDPR training sessions have now been delivered across the Council and the demand for face to face general awareness training has further declined over the last three months. Where refresher or targeted training is requested, this will be delivered through the normal channels in addition to the GDPR e-learning training module that employees can access to further support their learning and understanding of the new Regulation.
- 2.7 The focus of teams over the last quarter has moved from training to the completion of key tasks aligned with the actions identified from the initial GDPR review and readiness audit conducted by Audit Services in May 2018. The audit's focus was on the Council's

preparations for the implementation of the new regulation in line with the ICO's 12 Steps to GDPR compliance. The main areas of work identified by the initial audit were the completion of individual Information Asset Registers and the completion of individual department/team GDPR matrices, the latter of which ensures that teams have carried out the various activities required to remain compliant with the new data protection laws. Work on the completion of these documents continues and updates are regularly provided to leadership teams and the Strategic Executive Board (SEB) on progress.

- 2.8 To follow on from the initial readiness audit and to ensure that changes have been applied, a further, more detailed audit will be scheduled in late Autumn/early Winter 2018.
- 2.9 The IG team continues to see an increase in the volume of general GDPR queries from teams in this last quarter; specifically requests from service areas requiring support with the completion of Data Privacy Impact Assessments (DPIAs), information sharing agreements and local privacy notices and consent forms. Work is also ongoing with Schools and Tenant Management Organisations (TMOs) who have purchased the Council's GDPR and IG support service under a paid for service level agreement.
- 2.10 No formal communications were scheduled this last quarter. Reminders and updates on GDPR and any other generic information governance related matters will continue to be published as and when required, either following a business need or following updates from the ICO.

3.0 Quarter two Information Governance performance reporting

Background and context

- 3.1 The ICO has been interacting with the Council on information governance matters for several years. Considerable improvements have been made since their consensual audits in 2011 and 2012, which focused on requests for personal data (Subject Access Requests - SAR) and Freedom of Information (FOI).
- 3.2 Work has continued since the conclusion of the audit and a strategic approach to Information Governance has been adopted to ensure that the Council appropriately manages its information assets. Considerable improvements have been made in terms of processing information requests and the Council's overall statutory response rates have improved dramatically over the last five years.
- 3.3 To ensure ongoing improvements with information governance this report outlines current performance.

Progress for quarter two

- 3.4 The IG performance figures for quarter two are contained in appendix 1
- 3.5 Freedom of Information and Environmental Information (FOI/EIR) – 329 requests were received for Freedom of Information and Environmental Information, which is slightly less

than the volumes received last quarter (340). 327 requests were responded to within the statutory 20-day timeframe, which equates to a response rate of 99% for this quarter.

- 3.6 The number of requests received this quarter may indicate a break in the trend of volumes received for the last four quarters; this is the first quarter in more than 12 months where the volumes received within a three-month period have not increased.
- 3.7 Data Protection (DP/SAR) – 115 requests for personal data were received this quarter. All but two requests (113) were responded to within the shorter 30 calendar-day statutory timeframe, which again demonstrates a stable 98% response rate for the quarter.
- 3.8 Information Incidents – the number of incidents reported for the quarter remains almost the same as the numbers reported in the previous three months. 22 information incidents were reported in this quarter, which is just short (eight) of the total number of incidents reported in the whole of the period 2017-18. This may be indicative of the fact that employees are now more aware of what constitutes a breach and of the channels to report them following the GDPR training and awareness programme that has run for the last 12 months. All incidents reported, with the exception of one, were of the low risk category.

4.0 Financial implications

- 4.1 There are no financial implications associated with this report as Councillors are requested to review the information governance performance figures and note the progress made on the GDPR programme of work. All work associated with delivery of training and meeting information governance requirements is covered through existing budgets.
- 4.2 It is worth noting, however, that a failure to effectively manage information governance carries a financial risk. Inaccurate and out of date information can lead to poor decision making and a potential waste of financial resources. Following the implementation of GDPR, a two-tiered sanction regime with higher financial penalties will be adopted. Lesser information incidents will be subject to a maximum fine of either €10 million or 2% of an organisation's global turnover, whichever is greater. More serious violations could result in fines of up to €20 million or 4% of turnover.
[ES/22112018/X]

5.0 Legal implications

- 5.1 The Council has a legal duty under the current Data Protection Act 2018, GPDR 2016/679, Freedom of Information Act 2000 and Environmental Information Regulations 2004 to appropriately manage and protect information assets.
- 5.2 The integration of Public Health into the Council in April 2012 required the Council to provide assurance to the NHS that it had in place suitable Information Governance policies, procedures and processes.

5.3 Failure to effectively manage information governance could increase risk of exposure to fraud and malicious acts, reputational damage, an inability to recover from major incidents and potential harm to individuals or groups due to inappropriate disclosure of information.

5.4 The Information Commissioner has the legal authority to:

- Fine organisations for breaches of Data Protection 2018 or Privacy & Electronic Communication Regulations. With the implementation of the GDPR on 25 May 2018, a two-tiered sanction regime has been introduced and higher financial penalties will be adopted by the ICO. Lesser information incidents could be subject to a maximum fine of either €10 million or 2% of an organisation's global turnover, whichever is greater. More serious violations could result in fines of up to €20 million or 4% of turnover.
- Conduct assessments to check organisations are complying with the Act.
- Serve Enforcement Notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps to ensure they comply with the law.
- Prosecute those who commit criminal offences under section 170 of the DPA 2018 (previously section 55 of the 1998 Act.)
- Conduct audits to assess whether organisations processing of personal data follows good practice.
- Report issues of concern to Parliament.

5.5 Demonstration of the Council's compliance with the current Data Protection Law protects it from legal challenges for alleged breaches of individuals' rights.
[JSM 20/11/2018/ DP]

6.0 Equalities implications

6.1 Having considered the equalities issues presented under the new legislation - Data Protection Act 2018 and GDPR 2016/679 and the previous Data Protection Act 1998, no new implications have been identified from associated actions or recommendations of this report.

6.2 Any new equalities issues that become apparent as the programme of work progresses will undergo an initial screening and if appropriate will be followed by a full equalities analysis.

7.0 Environmental implications

7.1 There are no environmental implications identified.

8.0 Human resources implications

8.1 Working practices to support the adoption of GDPR controls and measures will be incorporated into existing Information Governance and HR policies.

9.0 Corporate landlord implications

9.1 There are no direct corporate landlord implications identified.

10.0 Health and Wellbeing implications

10.1 There are no direct health and wellbeing implications identified in this report.

11.0 Schedule of background papers

11.1 Strategic Executive Board – Briefing note on GDPR – July 2017

11.2 Strategic Executive Board Report – Approach to GDPR – January 2017

12.0 Appendices

12.1 Appendix 1 – Quarter two 2018-19 info-graph