PAPER G

Purpose: For Noting

Committee report

Committee	**AUDIT COMMITTEE**
Date	**16 MARCH 2020**
Title	**GDPR AND DATA PROTECTION - UPDATE REPORT**
Report of	**DIRECTOR OF CORPORATE SERVICES**

EXECUTIVE SUMMARY

1. This is a further update report to outline the progress made against the General Data Protection Regulation (GDPR) audit action plan to date since the last audit committee report dated 30 September 2019. The action plan originally arose to address issues identified within an internal audit report into the council's arrangements for compliance with the GDPR and the Data Protection Act 2018, presented to members on 20 May 2019.

2. Members are asked to note the progress made to date.

BACKGROUND

3. On 20 May 2019 Audit Committee received an internal audit report on the council's arrangements for compliance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018. This report identified ten risks arising, three of which were judged as being high risk.

4. The three high risks were identified as:

   (a) the proper completion of information asset registers (IARs);
   (b) ensuring contractual arrangements are in place with data processors;
   (c) ICT systems register.

5. This paper provides a summary of the council's progress in delivering the agreed action plan.

STRATEGIC CONTEXT

6. Compliance with GDPR is an identified strategic risk and as such is one that can affect our successful delivery of our corporate plan.

FINANCIAL / BUDGET IMPLICATIONS

7. The internal audit report recognised that the council had devolved responsibility for meeting a number of duties to service managers and this had impacted upon the standard of compliance with GDPR requirements. Therefore, the delivery of the action plan has required the temporary appointment of a data protection advisor (DPA) for 12 months to enable the council to deliver the required actions. The post has been funded by a carry forward of an underspend from a corporate services budget.

LEGAL IMPLICATIONS

8. The council has a statutory duty to comply with data protection legislation, including the General Data Protection Regulation and the Data Protection Act 2018.

9. Legislation requires the council to have appropriate documentation in place to demonstrate that there are adequate organisational and technical measures in place to properly process personal information that the council holds.

10. The legislation also requires the council to hold a record of processing activities, have appropriate contractual arrangements with commissioned providers that process the personal information the council holds and to document how we safely manage our information.

11. Legislation does not however specifically require an information asset register to be developed. However, this is a matter of good practice as part of the council's records management arrangements.

PROGRESS TO DATE

12. The data protection advisor, in conjunction with the services leads from ICT and Procurement and Contract Monitoring, has been progressing the findings and associated tasks assigned, as defined in the internal audit report generated in May 2019.

INFORMATION ASSET REGISTERS (IARs)

13. A new template has been devised in accordance with the recommended action. This was formally agreed by the council's internal Information Governance Group (IGG) at its meeting of 4 September 2019. The template has been prepopulated with the information from previous IARs that are held and were not too historic. Additional columns for information on retention and data protection policies have been included. Additional instructions were included in the template to assist in their completion. Thirty-six services were requested to complete an IAR. All 36 have been completed, reviewed and filed.

CONTRACTS

14. The Procurement and Contracts Monitoring Team identified 77 contracts that have a value exceeding £25,000, and which required appropriate revision to the contracts that are in place. Of these 77, 32 were due to expire and were therefore discounted from required action. The remaining contracts in the list were risk assessed and those adjudged to be above low risk (based upon data processed and contracting

period) were dealt with by way of unilateral notice to each of the contracting partners. 35 contracts are now deemed to be amended with 13 contract holders still in compliance negotiation. Work continues to bring these matters to successful conclusion.

15. Those contracts with a value of under £25,000 These contracts rest with the individual commissioning services and as such are not overseen by the Procurement and Contract Monitoring Team. A GDPR letter was prepared for individual services to issue to their service providers. Contact was made with the 49 services, all of whom have confirmed, where necessary, compliance to the revision of contracts by use of the template letter.

ICT SYSTEMS REGISTER

16. Meetings have been held between the data protection advisor (DPA) and head of ICT to address the need to design and implement a central GDPR systems register for the council and to address the issue regarding the council email system being used for case management purposes. An interim GDPR systems register has been developed from the information contained in the information asset registers (IARs), which will be utilised in the longer term generation of a full change management database (CMDB). Confirmation has been obtained that the email system is no longer being used for case management.

In relation to the other lower risks identified:

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

17. The Organisational Intelligence Team (which provides project management support to directorates), the Procurement and Contract Monitoring Team, and ICT are now providing a gatekeeping service to identify the potential need for DPIAs, when services are considering service redesigns or introduction of new systems. The Corporate Information Unit (CIU) is also providing central support to review and advise departments on the completion of the DPIAs.

OVERSIGHT

18. The terms of reference of the Information Governance Group (IGG) was reviewed and updated. Changes made include; invitation for membership by the contract and procurement team, the newly designated data protection officer (director of corporate services) who chairs the meeting, and the newly appointed senior information risk officer (head of ICT), and routine monthly reporting of the progress being made in completing the action plan is provided to the group to provide further oversight that the risks are adequately addressed and actions completed.

CORE DOCUMENTATION

19. All related GDPR and data protection policy documents, listed in a policy table, located at page 2 of the new IAR template, have now been reviewed and relevant amendments made. All relevant policy documents are now published on the Intranet.

OVERALL PLAN

20. An overall plan has been drafted to address all issues arising from the internal audit report and was endorsed by the IGG on 4 September 2019. The plan continues to be updated regularly and a copy is appended to this report.

RECORD OF PROCESSING ACTIVITIES (ROPA)

21. Although the Isle of Wight ROPA was considered to be as sufficient and compliant to GDPR article 30, as the information commissioner's office (ICO) template, the head of legal services authorised the amendment of the document, in line with the recommendations from the internal audit report, to ensure the document is fully compliant

DATA EXCHANGE AGREEMENTS (DEAs)

22. All redundant DEAs have been removed from the council's intranet site.

STRATEGIC RISK REGISTER

23. GDPR has been added to the strategic risk register, and is regularly updated and reviewed by the corporate management team.

RISK MANAGEMENT

24. It is important that the council manages its risks especially those identified as a strategic risk. The specific recommendations of the audit of the council's GDPR compliance will assist the council manage the risk.

RECOMMENDATION

25. Members are asked to note the progress made to date and the proposed next steps identified in the report above.

APPENDICES ATTACHED

26. Appendix 1 - Action plan timetable

Contact Point: Justin Thorne, Strategic Manager of Legal Services,
☎ 821000 e-mail justin.thorne@*iow.gov.uk*

CLAIRE SHAND
Director of Corporate Services

CLLR GARY PEACE
Cabinet Member for Community Safety and Digital Transformation