PAPER E

Purpose: For Note

ISLE of WIGHT COUNCIL

Committee report

Committee	**AUDIT COMMITTEE**
Date	**28 SEPTEMBER 2019**
Title	**GDPR AND DATA PROTECTION - UPDATE REPORT**
Report of	**DIRECTOR OF CORPORATE SERVICES**

EXECUTIVE SUMMARY

1. To receive an update on the council's action plan to address issues identified within an internal audit report that was presented to members on 20 May 2019.

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

BACKGROUND

3. On 20 May 2019 Audit Committee received an internal audit report on the General Data Protection Regulation (GDPR) and data protection that identified ten risks arising from an internal audit of the council's GDPR compliance, three of which were judged 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.

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 Regulations and the Data Protection Act 2018.

9. The relevant legislation does require that we have appropriate documentation to show that we have adequate organisational and technical measures in place to properly process personal information that the council holds.

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

11. There is no specific requirement to hold an information asset register. This requirement is a matter of good practice under records management requirements as opposed to specific data protection requirements.

PROGRESS TO DATE

12. The data protection advisor started his appointment on 30 July 2019 and is underway with now progressing tasks that were assigned to the post in recognition of the lack of capacity to otherwise do so.

Information asset registers

13. In relation to information asset registers, the council has now agreed a template that requires completion. This has been agreed with relevant information governance colleagues, notably ICT. The template will now be prepopulated with the information from the current IAR's that are held and are not too historic. Additional information on retention and data protection policies have been included. The IAR template was agreed by the council's IIGG (Internal Information Governance Group) for approval on 4 September. Additional instructions have been included in the template to assist their completion. Initial contact has been made with 36 services to advise that the IAR will be circulated for completion once IIG approves the template.

Contracts

14. The Contracts and Procurement Team has initially identified 60 potential contracts that each has a value exceeding £25,000 that remain outstanding and may require appropriate revision to the contracts that are in place. It is now proposed that this list will be risk assessed and those that are judged to be above low risk (based upon data processed and contracting period) will be dealt with by way of unilateral notice to each of the contracting partners. This work is expected to be completed by 1 October 2019.

15. In relation to contracts with a value under £25,000, that sit with the service and not the Contracts and Procurement Team, a GDPR letter has been reviewed and updated. Initial contact has been made with 36 services to advise that the contracts will need revision by use of the template letter and support will be provided shortly to assist achieve this.

ICT

16. A meeting has been held between the DPA and head of ICT to address the updating of the ICT policies, the need to design and implement a central GDPR systems register, and the issue of the council email system content. All ICT related policies are now under review and a central GDPR systems register is being developed.

OTHER LOWER RISKS IDENTIFIED

Data protection impact assessments (DPIAs)

17. The Contracts and Procurement Team is now providing a gatekeeping service to identify potential need for DPIAs and the Corporate Information Unit is also providing central support to advise departments when they are considering service redesigns as to the need for DPIAs.

Oversight

18. The terms of reference of the IIG is being reviewed. While immediate changes, such as the Contract and Procurement Team attending the group, have been made a further review to assess regular report content, meeting regularity and meeting attendees is being completed.

Core Documentation

19. The broken link to 2018 Data Protection Policy on the council website has been corrected. The 2016 Protective Marking Policy has been updated and republished. All relevant policy documents have been listed in a policy table, currently located as page 2 of the new IAR template. All policies are currently being reviewed and relevant amendments being made.

Overall Plan

20. An overall plan has been drafted to address all issues arising from the Internal Audit report and was endorsed by the IIGG on 4 September. The plan is appended to this report.

Record of processing activities (ROPA)

21. The Information Commissioners Office's (ICO) ROPA template has been reviewed and compared with the council's current ROPA. Article 30 of GDPR, that governs the requirement for a ROPA has also been reviewed.

22. It is considered that the council's ROPA is as sufficient as the ICO template. It is also considered that the current template complies in the main with Article 30 but an amendment is to be made to ensure it is fully compliant.

23. In addition, the review has highlighted that it may be of benefit to combine our ROPA with the new IAR so as to provide a better operational document.

Data exchange agreements (DEAs)

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

Strategic risk register

25. GDPR has been added to the strategic risk register.

RISK MANAGEMENT

26. 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

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

APPENDICES ATTACHED

28. Appendix A - 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 STUART HUTCHINSON
Deputy Leader and Cabinet Member for Resources