Report to:	QSMTM Q3 2021-22
Report by:	Helen Gardner-Swift, Head of Corporate Services (HOCS)
Meeting Date:	3 February 2022
Subject/ Title: (and VC no)	UK GDPR Update Q3 2021-22 VC164269
Attached Papers (title and VC no)	None

Purpose of report

1. The purpose of this Committee Report (CR) is to update the Senior Management Team (SMT) on the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 requirements within the organisation and actions taken in Q3 2021-22.

Recommendation and actions

2. I recommend:

   (i) the SMT notes the contents of this report

   (ii) the publication of the report is agreed as set out in paragraph 47.

Executive summary

Background

3. Data protection requirements changed from 25 May 2018 when the EU GDPR and Data Protection Act 2018 came into force.

4. In order to be able to ensure that the Commissioner complies with the relevant requirements, an implementation project was assigned to the HOCS for which was in two parts:

   - the development of an implementation plan
   - the delivery of the implementation plan

5. The GDPR Implementation Plan 2019-20 (VC116199) was agreed by QSMTM on 9 May 2019. As the majority of the steps in the GDPR Implementation Plan 2019-20 were completed, implementation plans for 2020-21 or 2021-22 were not put in place

6. To assist with the delivery of the implementation plan, an internal GDPR Working Party consisting of myself (Chair), Margaret Keyse (SMT), Euan McCulloch (Enforcement), Lorraine Currie (Policy and Information) and Liz Brown (CST) was established.

7. The following matters have been carried forward into 2021-22:

   - review of personal data audit
   - finalisation of consent log
   - review of general policies and procedures
   - review of retention periods

8. From July 2019, the GDPR Working Party facilitated by the Scottish Parliament Corporate Body (SPCB), changed to the DPO Network Group, meets every two months and continues to be made up of Officeholders' representatives. The purpose of these meetings is to

discuss general UK GDPR/data protection requirements and receive general updates from the DPO. Myself and Liz Brown, the Finance and Administration Manager, attend the bi-monthly meetings. An update on the matters discussed is provided to the GDPR Working Party. The SMT is also updated by email.

9. Meetings of the DPO Network Group take place by video conference.

COVID –19 pandemic

10. As a result of the impact of the COVID-19 pandemic, the following actions have been taken:

- the office premises have been closed temporarily since 23 March 2020 and remain closed
- the DPO has been informed of the temporary closure of the office premises and is updated following each SMT review of this decision
- office security and IT security measures are in place whilst the office premises are temporarily closed
- in accordance with ICO guidance, we are taking a proportionate approach to adapting the way we work and sharing information
- all members of staff are working remotely (with remote access to the office systems) using laptops and mobile phones provided by us and this includes the Commissioner and all members of the SMT
- updated guidance has been issued to staff working remotely covering:
    - security of information, including data protection
    - records management - staff working remotely must comply with our information and records management procedures including ensuring that our records are trustworthy, complete, accessible, legally admissible in court and robust
    - data incident procedures
    - how to use Microsoft Teams and guidance on use

GDPR Working Party (internal)

11. The GDPR Working party met approximately every 4 weeks by video conference.

12. Throughout Q3, Erin Gray, Head of Policy and Information (HOPI) was the Policy and Information representative on the Working Party. Erin Gray left the organisation in January 2022 and a new Acting HOPI will be in post form 1 February 2022. I will discuss with the Acting HOPI who will be the representative going forward. The other members of the Working Party remain as set out in paragraph 6 above. If there are any further changes these will be reported in the Q4 update.

13. Although the GDPR is now referred to as the UK GDPR, for the time being, the name of the GDPR Working Party will remain the same as a number of policy and procedures contain reference to this.

Data Protection Officer (DPO)

14. The SPCB has provided a shared DPO service and the MOU for this was signed on 24 May 2018. Euan McCulloch has agreed to act as DPO if a conflict of interest arises in the operation of the shared service DPO.

15. The annual HOCS meeting with the DPO took place on 15 September 2021.

16. The MOU has been reviewed and signed by The Commissioner. It is now intended that the MOU will cover 2020-21 and 2021-22.

17. Robin Davidson has been confirmed as the new Head of Information Management and Governance at the Scottish Parliament and is now our DPO. An update has been provided to staff and the Privacy Notice, C5 Data Protection Policy and Handbook and ICO certification has been updated.

18. The DPO has been invited to attend a SMT meeting and a GDPR Working Party meeting in February or March 2022 and the All Staff Meeting in April 2022.

Data Protection Policy and Handbook

19. The updated and revised Key Document C5 Data Protection Policy and Handbook (VC1490830) was approved in March 2021 and has now been published. All members of staff have been advised that the update and revised document and templates are in place.

20. As Responsible Manager, I will be reviewing the key document in Q4.

Privacy Notice

21. The Key Document C5 Privacy Notice (VC102891) has been kept under review throughout Q1 2021-22 and has been updated when required.

Staff training

22. The annual all staff UK GDPR/data protection training/update was undertaken in Q3.

23. The online data protection/UK GDPR training provided by the Scottish Parliament was undertaken by staff prior to the annual all staff training.

Accountability Framework Self-Assessment Report

24. The HOCS completed the accountability self-assessment on the ICO's website to assess the extent to which our organisation is currently meeting the ICO's expectations in relation to accountability.

25. Based on the answers provided, we are meeting more than 75% of the ICO's expectations. The areas where we did not meet expectations related to:

- making information about the purpose of the processing and the lawful basis publicly available and easy to locate, access and read – the HOCS and the GDPR Working party are considering how this can be done
- the carrying out of an external audit - this is planned for Q4

Budget

26. There is no specific budget allocated for data protection/UK GDPR requirements in the approved budget for 2021-22.

Cyber resilience

27. Any element of a cyber security issue resulting in the loss of or harm to personal data is likely to be treated as a data breach.

28. Although not required to do so, the Commissioner follows the Scottish Government guidance on cyber security and is participating, as far as possible, in the Public Sector Action Plan as part of the Cyber Resilience Strategy issued by the Scottish Government. Appropriate action has been taken in response to early warning notices (Crew Notices) that have been sent to us by the Scottish Government's Cyber Resilience Unit.

29. The Commissioner was re-accredited with Cyber Essentials in December 2021 and is aiming for Cyber Essentials Plus re-accreditation in Q4.

Data Incidents

30. In Q3 there were three data incidents and none of these needed to be reported to the ICO.

31. The DPO has been consulted on all data incidents and the SMT has approved the recommended actions.

32. The table below provides a summary, for each quarter, of the number of data incidents and the action taken.

Data Incidents 2020-21			
	Number	DPO consulted	Reported to ICO
Q1	1	Yes	No
Q2	2	Yes	No
Q3	3	Yes	No
Q4			
Total	**6**		

Data protection at the end of the EU transition period

33. The UK left the EU on 31 January 2020 and the transition period ended on 31 December 2020.

34. As regards relevant terminology, we now operate under the "UK GDPR" with references to the EU's version being the "EU GDPR". Our contracts, policies, correspondence and relevant documentation should now refer to "UK GDPR", where appropriate, to distinguish the difference between these regimes.

35. A positive EU-UK adequacy agreement is in place and this means the free flow of personal data between the EU and the UK can continue. The agreement is due to be reviewed again in five years.

Schrems II

36. The HOCS and the GDPR Working Party are also keeping under review the implications of the European Court of Justice decision in Schrems II (July 2020) which struck down the EU-US Privacy Shield scheme and emphasised the additional steps that organisations need to take when relying on the EU Standard Contractual Clauses (SCCs) for international data transfers and other transfer mechanisms. This decision also has a potential impact on EU/UK data transfers following the expiry of the transition period referred to above.

37. Any use of the SCCs (either current or new) will need to comply with the Schrems II decision - this means EEA-based controllers are going to need to understand UK surveillance laws and assess the risk of any proposed transfer to the UK.

38. SCCs have also been published by the European Data Protection Board.

39. The ICO has published UK versions of the SCCs (with guidance), consulted on these and intends to publish them in 2022. The ICO has also explained that the ICO and the Secretary of State must keep the transitional arrangements for SCCs under review and that it may be

that at some point the EU SCCs will cease to be valid, for new and/or existing restricted transfers from the UK. The ICO will provide more information about this when this situation arises.

Risk impact

40. The effective implementation of UK GDPR and data protection requirements ensures that there are relevant policies and procedures in place, including policies and procedures relating to information governance, data incidents, subject access, HR governance and privacy by design. In turn, this ensures that operational risks are mitigated as far as possible.

Equalities impact

41. There is no direct impact arising from this report. Equality and diversity matters will be considered in data protection requirements.

Privacy impact

42. There are no direct privacy implications arising from this report.

Resources impact

43. Additional staff resource is required to enable work to continue on the steps carried forward from the GDPR Implementation Plan 2019-20 and this will be met from within current resources.

Operational/ strategic plan impact

44. None at present.

Records management impact (including any key documents actions)

45. None at present.

Consultation and Communication

46. QSMTM minute.

Publication

47. This CR should be published in full but the GDPR Implementation Plan 2019-20 (VC116199) referred to within the report should be withheld on the basis that the exemptions in Sections 30(b)(ii), 30(c) and 39(1) of the Freedom of Information (Scotland) Act 2002 would apply if a request were, at this stage, to be made for the information.