Report to:	QSMTM Q4
Report by:	Helen Gardner-Swift, Head of Corporate Services (HOCS)
Meeting Date:	29 April 2021
Subject/ Title: (and VC no)	UK GDPR Update Q4 2020-21 VC148575
Attached Papers (title and VC no)	None

Purpose of report

1. 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 Q4 2020-21.

Recommendation and actions

2. I recommend:

   - the SMT notes the contents of this report
   - the publication of the report is agreed as set out in paragraph 49.

Executive summary

Background

3. As you will be aware, 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.

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. Of the steps set out in the GDPR Implementation Plan 2019 -20, 66 have been completed and 7 are ongoing.

8. The completed steps include:

   - personal data audit
   - identification of the types of processing of personal data and determining the legal basis for processing personal data
   - review of arrangements for the processing of personal data and update of arrangements
   - privacy notice

- subject access request procedures
- consent procedures
- data incident/breach procedures
- staff training and updates
- review of supplier and services contracts
- appointment of Data Protection Officer
- update of Committee Report templates
- review of Data Protection Policy and Handbook (to be finalised for publication)
- privacy by design guidance, DPIA procedures and templates
- revised contracting guidance and model terms and conditions

9. The remaining steps include:

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

10. These matters have also been commenced and have been carried forward into 2020-21.

11. As the majority of the steps in the GDPR Implementation Plan 2019-20 have been completed, an implementation plan for 2020-21 has not be put in place. The remaining steps are kept under review by the HOCS and the GDPR Working Party.

12. 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 GDPR/data protection requirements and receive general updates from the DPO. I attend the bi-monthly meetings and update the GDPR Working Group on the matters discussed. The SMT is also updated by email.

13. Following the closure of a number of Officeholder's office premises (due to the impact of the COVID-19 pandemic), the DPO Network Group continued via the provision of email updates. However, since 20 August 2020, meetings of the DPO Network Group have resumed and take place by video conference.

COVID –19 pandemic

14. 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)

15. Up and until the temporary closure of our office premises, the GDPR Working Party met every 3 weeks. These meetings resumed on 22 September 2020 and are now held every 4 weeks by video conference. Erin Gray, Head of Policy and Information (HOPI) will be the Policy and Information representative on the Working Party from 23 February 2021. The other members of the Working Party remain as set out in paragraph 6 above.

16. Although the GDPR is now referred to as the UK GDPR, 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)

17. 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.

18. The annual HOCS meeting with the DPO took place on 16 July 2020 and this was held by video conference.

19. The MOU has been reviewed, we have been consulted and provided our comments on the revised document and are awaiting details for the signing of the document from the Scottish Parliamentary Corporate Body (SPCB). It is now intended that the MOU will cover 2020-21 and 2021-22.

20. The DPO attended the monthly meeting of the SMT on 24 February 2021 and is due to attend a meeting of the GDPR Working Party in Q1 2021-22.

Data Protection Policy and Handbook

21. 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 is in place.

Privacy Notice

22. The Key Document C5 Privacy Notice (VC102891) has been kept under review throughout 2020-21 and updated when required.

Staff training

23. The annual all staff UK GDPR training/update took place remotely on 8 and 9 December 2020.

24. The online data protection/UK GDPR training provided by the Scottish Parliament has been rolled out to all members of staff.

Budget

25. There was no specific budget allocated for data protection/UK GDPR requirements in the approved budget for 2020-21.

Cyber resilience

26. 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.

27. 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.

28. The Commissioner was re-accredited with Cyber Essentials in December 2020 and re-accredited with Cyber Essentials Plus in March 2021.

Data Incidents

29. In 2020-21 there were a total of 6 data incidents, only one of which was reported to the ICO. The other 5 incidents Q1 were minor and did not need to be reported to the ICO.

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

31. 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	Yes
Q2	1	Yes	No
Q3	2	Yes	No
Q4	2	Yes	No
Total	**6**		

Data protection at the end of the EU transition period

32. The HOCS attends the regular meetings of the Scottish Government's Public Bodies Forum managed by the Information Assurance and Data Privacy Branch. This forum provides advice to Scottish public bodies on data protection following the UK's exit from the EU. The HOCS provides updates to the SMT and the GDPR Working Party on the advice and guidance received from this forum.

33. The UK left the EU on 31 January 2020 and the transition period ended on 31 December 2020. The Trade and Co-operation agreement concluded between the EU and the UK on 24 December 2020 sets out preferential arrangements in areas such as trade in goods and in services, digital trade, intellectual property, public procurement, aviation and road transport, energy, fisheries, social security coordination, law enforcement and judicial cooperation in criminal matters, thematic cooperation and participation in EU programmes. The agreement also includes some references to data protection.

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 adequacy decision is expected within the first half of 2021 and, in the meantime, a bridging mechanism is in place which:

- is intended to protect data flows during adequacy gap
- will last for 4 months, with the possibility of a 2 month extension
- will fall away when data adequacy is granted

36. A draft MOU has also been published by the UKG and ICO that lays out the relationship on the role of the ICO in relation to new UK adequacy assessments Memorandum of Understanding (MoU) on the role of the ICO in relation to new UK adequacy assessments - GOV.UK (www.gov.uk)

37. At the present time, legacy data is covered by Article 7(1) of the Withdrawal Agreement and, generally:

- at present, EU and UK aligned
- this may change going forward
- public bodies need to consider this as regards data and metadata held in systems, both in the UK and the EU

38. The continuing steps for public bodies are:

- understand data flows
- ensure correct assurance from data processors is in place should the bridging mechanism collapse for any reason
- consider the arrangements that need to be in place so that continue to get access to data and, in particular, legacy data

39. The HOCS and the GDPR Working Party are keeping the above under review to ensure that any required organisational changes are put in place.

Schrems II

40. 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.

41. New draft SCCs have been published by the European Data Protection Board and are going through the process of being ratified. It is anticipated that the UK Government will also produce a similar set of SCCs that would work to UK GDPR requirements and, if so, it is likely that these will have to be formally approved through UK legislation.

Risk impact

42. 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

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

Privacy impact

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

Resources impact

45. 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

46. None at present.

Records management impact (including any key documents actions)

47. None at present.

Consultation and Communication

48. MSMTM minute and HOCS email update to staff.

Publication

49. This committee report 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.