

Report of the Data Protection Officer

Report to Corporate Governance and Audit Committee

Date: 8th February 2021

Subject: International Transfers Following the UK's Exit From the European Union

Are specific electoral wards affected? If yes, name(s) of ward(s):	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Are there implications for equality and diversity and cohesion and integration?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Is the decision eligible for call-in?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Does the report contain confidential or exempt information? If relevant, access to information procedure rule number: Appendix number:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Summary of main issues

The Council's international transfers of personal data have been impacted by the UK's exit from the European Union (EU) Transition Period as the EU-UK Trade Agreement does not contain an adequacy agreement.

Recommendations

Corporate Governance and Audit Committee are asked to

- consider the assurance provided in this report and invite the Data Protection Officer to provide a further update report at the next meeting;
- note the outstanding risk in relation to the provision of an adequacy agreement by the EU for the international transfer of personal data.

1. Purpose of this report

- 1.1 To provide an update to the Corporate Governance and Audit Committee with regard to international transfers of personal data following the UK's exit from the EU;
- 1.2 Provide assurances as to the sensitivity and impact of the relevant data and the arrangements being put in place to mitigate the risks and responses in relation to data adequacy in respect of Brexit.

2. Background information

- 2.1. Personal data is defined as any information relating to an identified or identifiable person including name, address, bank details, health records, photographs and video footage.
- 2.2. Since May 2018, personal data within the EU has been protected through the General Data Protection Regulation (GDPR). The UK, upon exiting the EU, has implemented the GDPR into UK law. This is known as the 'UK GDPR'. The legislation has removed references to Member States but maintains the same principles and requirements as the EU GDPR.
- 2.3. Where data is sent to another country it is known as an 'international transfer'. This can include (but is not limited to) emailing or uploading data to an organisation or supplier outside the UK or cloud-based hosting on servers outside the UK.
- 2.4. As of 1st January 2021, the UK is outside of the EU/EEA. As such, any transfers of data to the EU/EEA are considered as an international transfer; as is any data flowing from the EU/EEA to the UK. The EEA provides for the free movement of personal data within the EU in addition to Iceland, Liechtenstein and Norway.
- 2.5. Data adequacy is a status granted to countries who provide a level of personal data protection comparable to that provided in the GDPR. When a country has been awarded the status, personal information can pass freely between it and the EU/ EEA without further safeguards being required.
- 2.6. Decisions on adequacy for the UK are made by the Secretary of State for Culture, Media and Sport. Decisions on adequacy for the EU are made by the European Commission.
- 2.7. The UK Government has already previously stated that it recognises the EU/EEA as 'adequate' for the purposes of data transfers from the UK to the EU/EEA and that, as such, it considers a legal basis to exist for these transfers.

3. Main issues

- 3.1. The UK and the EU agreed the EU-UK Trade and Cooperation Agreement on 24th December 2020. This agreement did not resolve International Data Transfers. Instead it contains a temporary bridging mechanism that allows the continued free flow of personal data from the EU/EEA to the UK for up to 6 months from 1st January 2021.
- 3.2. It must be noted that the Agreement does not however state that the EU views the UK as 'adequate'. Such an adequacy decision is a separate process to a trade deal and has been under consideration by the Commission throughout 2020. Nor is it a certainty that the EU will grant adequacy, as a recent decision by the Court of Justice of the EU (CJEU) has raised concerns regarding whether the UK's legislation

permitting the retention and transmission of bulk data for national security purposes is compatible with EU law.

- 3.3. The Agreement does, however, state that the EU and UK both commit to uphold high standards of data protection, and it is hoped that that an adequacy decision will, consequently, be achievable within this six-month interim period.
- 3.4. Without an adequacy decision from the European Commission, European Data Protection Regulators could prohibit personal data transfers to the UK unless arrangements have been made to put in place one or other of the “appropriate safeguards” required by the GDPR and the UK GDPR, or unless a derogation specified in that legislation applies.
- 3.5. The Council currently processes some personal data within the EU where we have EU based contractors (or contractors who use EU-based servers). If a European Data Protection Regulator prohibited the return of this data to the UK, the Council would not be able to access it. This could have an impact upon service delivery and alternative business continuity arrangements would need to be implemented for such an eventuality.

4. Actions to date

- 4.1. A working group was established to review all international transfers which the Council currently undertakes.
- 4.2. The group conducted an audit to identify all international transfers, which have now been logged on a central register which is maintained by the Information Management and Governance service.
- 4.3. Where it has been identified that personal data is transferred to the EU/EEA and, therefore, may be affected if an adequacy agreement is not granted, the Council has ensured that robust business continuity plans are in place. These vary depending on the nature of the data and the service. Mitigating actions include:
 - 4.3.1. Contacting suppliers to identify alternative legal bases for transfers (these include: Standard Contractual Clauses, national derogations, explicit consent of the data subject)
 - 4.3.2. Where an alternative legal basis cannot be identified, working with those suppliers to relocate information to data centres within the UK.
 - 4.3.3. As a last resort, where neither of the above is possible, exporting data from systems into a new UK-based format.
- 4.4. The audit currently indicates in the region of 130 applications hosted overseas, not all of which are within the EU/EEA. This is a dynamic dataset which is subject to change as discussions with suppliers continue and suppliers select new sub-processors. In addition we currently have approximately 20 service areas sharing personal data overseas, but not via hosted applications.

- 4.5. Many of the larger companies that undertake data processing on the Council's behalf (for example Microsoft, Google and Amazon Web Services, who are the responsible data processors for well over half of our transfers) already have provisions in place to ensure that international transfers will still be able to continue in the event of there being a no adequacy decision. These will, essentially, involve the introduction of Standard Contractual Clauses (SCCs) as part of their Terms of Service. They have also provided assurances to the government that they are aware of the potential risks associated with a no adequacy decision and that they will continue to enable data transfers in the event of a challenge provided this is lawful under their relevant contract. As such, there is no further direct action that the Council need take in this regard.
- 4.6. Separately to these larger providers, however, the Council has also sought to directly agree SCCs with some companies directly. An example of such a case is Technogym (used by customers of the Sports service to track exercise activity), which has processing operations both in the EU and the US. In other cases, such as the DIS Remedy system (used by the DIS Service Desk), the Council has ensured business continuity by agreeing with the supplier that the information currently hosted in the EU will be transferred to UK-based servers in the event of a no alternative legal basis being available after the end of the transition period. Similarly, the Council has agreed that data from 'Tapestry' an application used by Children's Services to capture pre-school years attainment will, if necessary, be transferred to the Council in hard copy format should this be required.
- 4.7. New guidance has been drafted for DIS and Procurement staff to ensure that any new contracts or systems are rigorously checked from the start of procurement.
- 4.8. The current Council Data Protection Impact Assessment (DPIA) is being updated to include specific questions on international transfers so as to ensure relevant checks are undertaken.
- 4.9. Information Asset Owners will be questioned with regard to any additional international transfers they are aware of as part of the annual Information Asset Register review to ensure that no instances have been missed.

5. Corporate considerations

5.1 Consultation and engagement

- 5.1.1 Consultation and engagement has taken place with service areas, information management professionals and colleagues within the DIS service.

5.2 Equality and diversity / cohesion and integration

- 5.2.1 There are no issues in relation to Equality and Diversity or Cohesion and Integration.

5.3 Council policies and best council plan

- 5.3.1 The Council has a wide range of compliance programmes for the GDPR and successor legislation.

5.3.2 Non-compliance may affect the achievement of Best Council Plan objectives and the aims of council policies.

5.4 Resources and value for money

5.4.1 All DIS projects undergo a rigorous evaluation and impact assessment process to ensure value for money.

5.5 Legal implications, access to information, and call-in

5.5.1 Delegated authority sits with the Director of Resources and Housing and Senior Information Risk Owner and has been sub-delegated to the Chief Digital and Information Officer under the heading “Knowledge and information management” in the Director of Resources and Housing Sub-Delegation Scheme.

5.5.2 There are no restrictions on access to information contained in this report.

5.6 Risk management

5.6.1 There is a risk that, if the EU does not grant the UK an adequacy agreement, European Regulators could prohibit personal data transfers to the UK. This would cause an impact to service delivery if the mitigating actions taken above were not implemented.

6. Conclusions

6.1 International transfers of personal data from the UK to the EU/EEA and from the EU/EEA to the UK will remain legally compliant for 6 months from 1st January 2021.

6.2 It is envisaged that a formal adequacy agreement will be completed between the EU and the UK before this time period expires.

6.3 The Council has undertaken a review of its international transfers. In the event that an adequacy agreement is not completed, the Council will undertake mitigating actions to ensure that the impact on service delivery is minimised.

7. Recommendations

7.1 Corporate Governance and Audit Committee are asked to:

- consider the assurance provided in this report and invite the Data Protection Officer to provide a further update report at the next meeting;
- note the outstanding risk in relation to the provision of an adequacy agreement by the EU for the international transfer of personal data.

8. Background documents

N/A