UNIVERSITY OF CAMBRIDGE
Governance and Compliance Division

Information Compliance Office

Data protection: personal data transfers and Brexit – a factsheet for departments and Principal Investigators

Version control

This factsheet was first issued on 10 December 2020. This updated version was issued on 7 January 2021 to reflect the data protection provisions contained within the EU-UK Trade and Cooperation Agreement announced on 24 December 2020, and to adjust phrasing to reflect the fact that the Brexit transition period has now ended.

Key points

- Since 1 January 2021, data protection law has remained essentially the same.
- In due course, there may be some changes to the arrangements for transfers of personal data from EEA-based organisations/businesses to the University – these would involve contractual amendments/supplements, though these should create no new ongoing practical burdens or obligations.
- Departments and PIs should be prepared to receive requests to enter into these contractual amendments/supplements, but need not do anything proactively.
- 'Bridging' provisions within the EU-UK Trade and Cooperation Agreement announced on 24 December 2020 mean that transfers of personal data from EEA-based organisations/businesses to the University remain unaffected for up to six months (i.e. until the end of June 2021), so the likelihood of receiving requests in the immediate term is significantly reduced.

Data protection law in the UK since 1 January 2021

1. Since 1 January 2021, data protection law has changed in the UK following the end of the transition period marking the UK's departure from the EU.

2. Data protection law sets out rules and standards for organisations to follow when handling information about living identifiable individuals. Until 31 December 2020, the law was the EU-wide General Data Protection Regulation (GDPR) as supplemented by the UK Data Protection Act 2018 (DPA 2018).

3. **Since 1 January 2021, all the substantive provisions of the GDPR, as detailed on the University's webpages about data protection, have continued to apply because the GDPR has been incorporated into UK law as the 'UK GDPR'**. The DPA 2018 continues to supplement the UK GDPR.

4. A number of technical/linguistic changes have been implemented to allow the UK GDPR to work in a domestic context, and to amend some of the DPA 2018's cross-references to it, but most of these are irrelevant to day-to-day University activity.

How UK data protection law has related to EU data protection law since 1 January 2021

5. Brexit negotiations between the UK and the EU concluded on 24 December 2020 with the EU-UK Trade and Cooperation Agreement. As part of this, the UK has committed to maintain high data protection standards. The EU has committed to promptly progress an 'adequacy finding' from the European Commission (EC) for the UK – this is a declaration by the EU that it regards the data protection laws in a non-EU country to be essentially equivalent to those within the EU.

6. An adequacy finding matters in data protection terms because, without one, the UK will simply be another 'third country' based outside the European Economic Area (i.e. the EU plus Iceland, Liechtenstein and Norway) without any special data protection arrangements with the EU.

7. Adequacy findings mainly are relevant to personal data transfers, whereby an organisation/business based within the EEA (the 'data exporter') transfers personal data to an organisation/business based outside the EEA (the 'data importer'). If the data importer is within a country that has an adequacy finding, no further measures are required to render the personal data transfer lawful.

Personal data transfers from the EEA to the UK since 1 January 2021

8. While an adequacy finding for the UK was not issued by 31 December 2020, the EU-UK Trade and Cooperation Agreement contains a 'bridging' provision that means that transfers of personal data from EEA-based data exporters to UK-based data importers remain unaffected for up to six months (i.e. until the end of June 2021). If an adequacy finding is *not* granted to the UK by the EC within this 'bridging' period, transfers of personal data *from* EEA-based data exporters *to* the University will be affected.[1] The affected transfers of personal data to the University might arise, for example, in the context of research collaborations, student placements in European universities or businesses, or external data storage/hosting arrangements. It is stressed that only transfers of *personal* data will be affected.

9. In order for the personal data transfers lawfully to continue if no adequacy finding is granted, it will be necessary for the EEA-based data exporter to ensure that the personal data it transfers will be 'appropriately safeguarded' by the University, as the UK-based data importer. There are some 'derogations' (exceptions) to this for occasional and limited transfers, but in general the simplest way for the data exporter to safeguard the

[1] Transfers of personal data from EEA-based *individuals* to the University – such as student/job applicants or conference attendees – are not affected. The mechanisms for transfers of personal data *from* the University *to* organisations/businesses based in the EEA and beyond similarly are unaffected, at least in the short term.

personal data will be for it to enter into a contract/contract variation with the University on the basis of the EC's Standard Contractual Clauses (SCCs) for personal data transfers.

10. Currently, there are two versions of the SCCs:[2]

    a) Where the data importer receives the personal data and uses it for its own purposes (this is known as a 'controller-to-controller' transfer).
    b) Where the data importer receives the personal data and uses it only on the instructions of the exporter (this is known as a 'controller-to-processor' transfer).

11. Incoming controller-to-processor transfers will apply rarely in a University context; that set of SCCs is principally aimed at situations where the data importer is a service provider for the data exporter (e.g. a mailing house based in a different country).

Practical implications for University departments and PIs

12. **University departments and PIs should be prepared to receive requests to sign the SCCs from EEA-based data exporters that transfer personal data to the University**. Such requests are less likely in the immediate term because of the 'bridging' provisions mentioned in paragraph 8 above, but some requests may still arrive. These requests might ask you to sign the full legal text (as published on the official webpage referred to in paragraph 9 above) or a simple declaration that you will abide by the SCCs as issued by the EC. The text of the SCCs cannot be amended and so there is no room for negotiation, though the inclusion of some factual information about the personal data being transferred in any particular instance may be required (coupled with, in some circumstances, information about the measures the University will take to keep the personal data secure).

13. If you are asked to sign the SCCs, you should do so according to normal University signatory processes as follows:

    a) SCCs covering personal data transfers in the context of research collaborations and agreements should be passed to the Research Operations Office.
    b) SCCs covering personal data transfers in other contexts (e.g. student overseas placements) may be signed by a Head of Department/Division.

    If in doubt, please contact the Information Compliance Office for advice.

14. **The SCCs should create no new ongoing practical burdens or obligations** as UK organisations continue to operate to high data protection standards. (It is recognised that administrative effort will be required to get them agreed and signed.)

---

[2] The EC, in a separate policy development unconnected to Brexit, has recently issued draft new versions of the SCCs, which work in a 'modular' way and for which there are four variants instead of two. However, these have not yet been approved for use. Any SCCs executed on the basis of the current versions may, in due course (and in all likelihood within about a year), need to be updated to reflect the new versions.

15. Prior to signing the SCCs, it is possible that the EEA-based data exporter might ask some 'due diligence' questions about the University's policy frameworks to ensure the security of the personal data being transferred. This is because EEA-based data exporters are being encouraged to supplement the SCCs with such due diligence checks.[3] If you are in doubt about how to answer any such questions, please check the University's webpages about data protection and contact the Information Compliance Office for advice where necessary.

16. **Other than familiarising themselves with this factsheet, University departments and PIs are not expected to take any proactive steps to prepare for the possible changes to personal data transfers over the next few months**.

Information Compliance Office
Governance and Compliance Division
University of Cambridge
10 December 2020 (updated 7 January 2021)

[3] These due diligence checks are not related to Brexit and are not unique to UK-based personal data importers. They have been triggered by a recent decision of the Court of Justice of the European Union which rendered the Privacy Shield invalid (the Privacy Shield was the adequacy finding from the EC for the USA). This decision also questioned the effectiveness of the SCCs in isolation, and suggested that extra measures should be considered to ensure the appropriate safeguarding of personal data when transferred outside the EEA under the SCCs.