How to prepare for Brexit (research activities)

This guidance is for PIs who handle personal data and/or oversee data sharing with organisations in Europe and/or the United States other than for the purposes of research projects

Where are we now?

After months of negotiations, the UK and EU agreed a Brexit deal which means the UK will leave the EU on 31 January 2020. It comes in two parts: (i) a legally binding withdrawal agreement and (ii) a non-legally binding short statement on future relations.

Following the UK’s exit, there will be an 11 month transition period until at least 31 December 2020 during which time the UK / EU will begin negotiations that includes the issue of data protection and the potential to complete / pass the assessment to gain an ‘Adequacy Decision’ for the UK.

However, whilst it has been stated that the UK / EU will attempt to complete the process, there is no guarantee it will occur and if no extension to the transition period is made then 1 January 2021 the flow of personal data to the UK will be affected and include;

1. organisations in the EU/EEA will not automatically be able to continue to lawfully share personal data with the College;
2. the College may not be able to continue to share lawfully personal data with organisations in the United States.

The inability to continue to share personal data lawfully with US and EU counterparties may impact negatively ongoing research, collaborations and/or other research projects. Given the current political uncertainty, it is up to each PI to decide, in the context of their own projects, on whether to take immediate mitigation action to protect current data sharing arrangements or to wait until there is greater certainty as to what will happen and therefore accept the risk of potential disruption of EU —— UK and UK —— US personal data flows.

The next page contains a diagram with questions and steps PIs need to ask and take to address this risk.

Further information on Brexit and personal data sharing is available on this website which will be updated as and when things change:
http://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/brexit/
Cross-Border Personal Data Sharing in Research and Brexit Impact Questionnaire

Are you sharing any personal data* with organisations in the EU/EEA? (note not domestically within the UK)

- No
- Yes
  - Are you solely sending the personal data to the EU/EEA (i.e. not receiving any personal data)?
    - No – (also) sending personal data
    - Yes
      - Has the US organisation signed up to the EU – US Privacy Shield?
        - Yes
        - No
          - Has the US organisation updated its commitment to compliance with the Privacy Shield to cover both the EU and, expressly, the UK?**
            - Yes
            - No
              - Have the College and the organisation signed the EU Standard Contractual Clauses (SCCs)?
                - Yes
                - No
                  - Contact the DPO or Deputy DPO to check if any exemptions apply or whether you need to engage with the organisation to enter into the SCCs***

Please see the notes on the next page
* **Personal data** - any information relating to an identified or identifiable natural person i.e. one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

**Note that** personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable is not personal data within the meaning of the GDPR and therefore anonymisation of personal data before any sharing can be a viable solution to the cross-border sharing issues a no deal Brexit presents.

**You will need to check that the relevant US organisation has made the necessary update to its commitment to compliance with the Privacy Shield to cover both the EU and the UK (this should be an easy and quick step for US organisations to take).** Confirmation of the update should usually be possible simply by checking the US organisation’s publicly available privacy policy. More information about the Privacy Shield arrangements can be found on the Privacy Shield website.

***The table on the next page describes the available templates that can be used (they are also accessible here: [http://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/internal-guidance/templates/](http://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/internal-guidance/templates/).***

**Note that** the templates in column 3 have been provided by the ICO – they satisfy the GDPR requirements but have a different layout, they also contain helpful completion notes and may therefore be more user friendly for completion by College in some respects but our counterparties may find them more difficult to accept because of the unusual format.

*How to determine if the College is a controller or a processor?* If the College, alone or jointly with others, determines the purposes and means of the processing of personal data, then the College will be a **controller** in respect of that personal data. If the College is processing personal data on behalf of (i.e. on instructions from) another person, then, the College will be a **processor**.
### Templates

<table>
<thead>
<tr>
<th>(1) College &amp; EC Commission Templates for use with EU/EEA counterparties</th>
<th>(2) College &amp; EC Commission Templates for use with US counterparties</th>
<th>(3) Alternative ICO Templates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Template EU1</strong> – where College is a controller and the EU/EEA counterparty is also a controller</td>
<td><strong>Template US1</strong> - where College is a controller and the US counterparty is also a controller</td>
<td><strong>Template A1</strong> - where College is a controller and the counterparty (EU or US) is also a controller</td>
</tr>
<tr>
<td><strong>Template EU2</strong> – where College is a processor and the EU/EEA counterparty is the controller</td>
<td><strong>Template US2</strong> – where College is a processor and the US counterparty is the controller</td>
<td><strong>Template A2</strong> – where College is a processor and the EU counterparty is the controller</td>
</tr>
<tr>
<td><strong>Template EU3</strong> - where College is a controller and the EU/EEA counterparty is a processor (which transfers personal data back to the College)</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>