Cabinet Office

# Personal Data Risk Assessment

**Completing this assessment enables the Cabinet Office to meet its legal obligations under UK GDPR and the UK Data Protection Act. Failure to complete this risk assessment could result in a data breach which may need to be reported to the Information Commissioner's Office.**

This Risk Assessment must be completed in any instance where personal data is processed either via a new activity (e.g. new system, new process, new third party relationship) or via a material change to an existing activity.

The Personal Data Protection Questionnaire, also found on the CO Intranet, will help you understand whether you need to complete this assessment.

For any questions, or processing of personal data, contact your BU GDPR lead, your BU privacy team, or the CDIO Data Privacy & Compliance Team (DPC team).

---

The assessment is split into 3 sections, as detailed below:

Section 1 - Key Information

- To be completed by the Business Unit
- All questions are mandatory
- Once completed you should move on and complete Section 2

Section 2 - Initial Assessment

- To be completed by the Business Unit
- You may reach out to your BU GDPR Lead, your BU Privacy resources or the CDIO DPC team dataprivacy@cabinetoffice.gov.uk for help in completing this assessment
- All questions are mandatory
- To be submitted to your BU privacy team, or the CDIO DPC team for advice on how to proceed

**You MUST NOT proceed with processing the personal data until you have received advice on how to proceed.**

Section 3 - Data Protection Impact Assessment (DPIA) (if applicable)

- Section 3 needs to be completed if there is a potentially high risk of processing the personal data
- If you are aware that a DPIA needs to be completed you may complete this immediately after completing the Initial Assessment; otherwise you should complete this assessment once you receive advice from your BU Privacy resources or CDIO DPC team that the DPIA must be completed
- To be completed by the Business Unit

- You should reach out to your BU Privacy resources or the CDIO DPC team dataprivacy@cabinetoffice.gov.uk for help in completing this assessment
- The BU privacy team or CDIO DPC team will advise which, if any SME teams should be consulted in completing the DPIA
- All questions are mandatory.
- To be submitted to your BU privacy team, or the CDIO DPC team once complete
- The BU Privacy resources or the CDIO DPC team will review the DPIA and submit to the (DPO)
- The DPO will review all the materials and provide advice as to whether the processing activity should proceed

**You MUST NOT proceed with processing the personal data until you have received advice from the DPO.**

Cabinet Office

# Section 1 – Key Information

**All questions in this section are mandatory.**

**If you are unsure how to complete this section, please seek advice from your Business Unit's GDPR lead, the CDIO Data Privacy and Compliance Team (DPC team) or your local BU Privacy resources.**

**Once you have completed this section you should move on to Section 2.**

1) **Please provide your contact details and the name of the senior responsible owner**

| | |
|---|---|
| **Name** | Myles Lester |
| **Telephone** | 07393 780 641 |
| **Email** | myles.lester@cabinetoffice.gov.uk |
| **BU** | Beyond Boundaries, Fast Stream and Emerging Talent, Government People Group |
| **Senior Responsible Owner** | Andrew Key |

2) **For what purpose or purposes will personal data be collected, used, held or disclosed? Please cover all intended purposes (you may not be able to use the data for new purposes later).**

The Beyond Boundaries programme is a talent development programme for AA to SEO staff across the Civil Service. Departments bid each year for a flexible number of places on the programme and they also inform FSET as to whether they require ring fencing of any places for individuals with various protected characteristics under the equality act. There must always be places open to mainstream candidates. Departments must provide "reasonable" evidence to FSET to demonstrate the need for ringfencing (if any) and that the positive action is justified. The processing will involve the collection of applicant and developmental personal data, which will - for successful candidates - then be held for the duration of their time on the programme. A subset of that personal data will then be held for a longer period, subject to the data subject's consent. We will hold the data for approx 600 successful applicants - this may vary year to year depending on how many successful applications we have that year. This will be used to make comparisons year on year and

to assess if the programme is meeting the needs of the Depts in terms of ring fencing of bids. The contact data will be held post programme so that we can contact learners post programme to assess the impact the programme has had after it has completed.

**3) What specific items of personal data will be processed?**

The following personal data will be collected during the application stage:

- Name
- Email address
- Department
- Grade
- Location
- Diversity details relating to characteristics which are protected under the Equality Act with the addition of Lower Socio Economic Background (which is not protected under the Equality Act).

When on the scheme, the additional items will be processed:

- Learning agility baselines and progression data
- Line manager evaluation baselines and progression data
- Personal job satisfaction and confidence monitoring
- Transitions in roles, such as sideways role moves or promotions

The purpose of these additional items is to ensure that we can monitor how well the programme is doing and whether it is supporting employees in securing progression/providing the skills required to progress and develop. We also seek out Line Manager evaluation to make sure the programme is fit for purpose from a managers perspective and to ensure we take Line Manager feedback into consideration for continuous improvement of the programme.

When applicants leave the scheme, we will retain the following data:

- All of the above for baseline and comparable data sets

**4) Will you be processing any of the following 'special categories' of personal data? (Y/N)**

| | |
|---|---|
| **Y** | Racial or ethnic origin |
| **N** | Political opinions |

| | |
|---|---|
| **Y** | Religious or philosophical beliefs |
| **N** | Trade union membership |
| **Y** | Health (including disability and dietary requirements) |
| **Y** | Sexual orientation |
| **N** | Data concerning a person's sex life |
| **N** | Genetic data |
| **N** | Biometric data (where used for identification purposes) |

5) **Will any personal data relating to criminal conviction or offences of individuals be processed?**
*If yes, provide details e.g. volume of data*

No

6) **Are you intending to enter into any third party agreement / contract?**
*If yes, provide details.*

No.

7) **Please explain which categories of data subject the processing relates to. For example, staff, children, members of the public, users of a particular website, etc**

Existing civil servants, from AA to SEO grades, who apply for the development programme.

Existing staff working in NDPBs/ALBs.

8) **If you are collecting personal data from somewhere other than directly from the individual concerned, where are you obtaining that data from?**

| |
|---|
| *N/A* |

**9) Which of the following will you be doing?**

| | |
|---|---|
| **X** | Collecting personal data |
| **X** | Holding personal data |
| **X** | Using personal data |
| **X** | Disclosing personal data |
| **X** | Deleting personal data |

## Next Steps

Thank you for completing the Key Information section of the Personal Data Risk Assessment.

**You should now complete Section 2. Once completed, you should send it to the CDIO Data & Compliance Team (DPC team) [dataprivacy@cabinetoffice.gov.uk] or your local BU Privacy resources. If you are unsure how to answer any of the questions in Section 2 they will be able to support you.**

Cabinet Office

# Section 2 – Initial Assessment

**All questions in this section are mandatory.**

**Complete this section as far as possible and reach out to your Business Unit's GDPR Lead, the CDIO DPC team or BU Privacy resources if you need support. Once you have completed this section as best you can, share this document with the Data Privacy and Compliance team (dataprivacy@cabinetoffice.gov.uk) or your BU Privacy resources.**

**Note. You MUST NOT proceed with processing the personal data until you have received advice from the DPC team or BU Privacy resources.**

1) **What is the legal basis (or bases) for processing the personal data?**
*This will normally be a public task, contract or legal obligation. There may be limited circumstances in which consent or legitimate interests is the appropriate basis. Further guidance is available here.*

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller. In this case that is the successful running of the Beyond Boundaries development programme.

For when applicants complete the programme, we will continue to hold their data in order to assess the effectiveness of the programme. We will conduct a final evaluation with them 6 months post programme which we will analyse. All data will be partly anonymised during analysis and looked at from a programme level. There may be instances where very low numbers mean data is not fully anonymised.

In instances where there are very low numbers used in analysis and it may therefore be theoretically possible to identify individuals, the lawful basis for processing the non-special category parts of this data will be legitimate interests. In this case, the interest is analysis of the programme.

2) **If you are going to be processing either sensitive personal data or criminal convictions personal data, please give details of the data and the legal basis relied upon.**

*For awarding roles and diversity monitoring:*

Processing is of data concerning ethnicity, religious or philosophical belief, health including disability or sexual orientation, and it is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people with a view to enabling such equality to be promoted or maintained (para 8, sch.1, DPA 2018).

This data will be used to help inform the selection of successful candidates. Diversity data is used to ring fence certain categories of individuals.

**3) How long is it necessary to keep the personal data in an identifiable form?**

The data of applicants who are unsuccessful will be retained in an identifiable form only for the duration of that window. After two years, application data will be deleted or anonymised.

The Beyond Boundaries development scheme will last for 1 year and the personal data of data subjects will be retained for 1 year after that for monitoring purposes.

**4) Name any third party organisations (including IT suppliers) that the personal data has been/ will be shared with or disclosed to?**

The application for the scheme will be done via the Smart Survey - and so that provider, Smart Survey Ltd. , will hold the data.

Data will be shared with KPMG and their supply chain as part of the learning contract. Berkshire Consulting are contracted on our behalf by KPMG to deliver the facilitation and therefore will have access to this data.

Data stored on our corporate IT systems will be shared with our data processors Google/AODocs.

**5) What are the roles of any third party organisations with whom data will be shared, or from whom it is collected? Guidance is available here on the different roles.**

Cabinet Office is the data controller for this processing.

Google/AODocs are data processors.
Smart Survey are data processors.
KPMG are data processors.
Berkshire consulting: KPMG's subprocessor

**6) If a data processor will process personal data on behalf of CO, what type of contract will be in place to govern this?**
*Note: contracts with third party data processors must include the specific clauses required by Article 28 GDPR. Where applicable this should be listed as a key control in question 7.*

- Smart Survey processes data under their bespoke contract with CO.
- KPMG processes data under their bespoke contract with the Government Skills and Curriculum Unit (formerly known as Learning 2020) which is part of the CO.
- Google processes data under their bespoke contract with central Cabinet Office.

**7) If a data processor is processing personal data on your behalf does that contract or instrument include the specific processor clauses required by Article 28 GDPR?**
Broadly, these guarantee that personal data will be protected in line with GDPR, and that any subcontractors will be bound by the same terms. These provisions may also be in a separate "data processing agreement" that sits alongside terms and conditions or a contract. See the guidance here.

Yes applies to all data processors

**8) Will the personal data be transmitted out of the UK?**

| | | | |
|---|---|---|---|
| **X** | **Yes** | | **No** |

**9) If the answer to the previous question is 'yes', please specify where this will be transmitted to, and what legal gateway is relied on to make this lawful. Guidance is available here.**

Data held by Smart Survey, KPMG, and their respective supply chain (eg. Berkshire Consulting), will be limited to the UK.

Data stored on G-drive or Gmail may be transferred and stored securely outside the UK by Google. Where that is the case it will be subject to equivalent legal protection through an adequacy decision or the use of Standard Contract Clauses.

**10) Where it is possible, please describe the technical and organisational measures in place to protect the personal data. These include measures such as restricted access, staff training, pseudonymisation, encryption, etc.**

Data held on the Cabinet Office Google Drives will be held in a locked-down folder, with only GRS and the Beyond Boundaries team having access. That team will all be permanent civil servants, have completed their mandatory training on managing information, and will be made aware on joining the team of the need to look after the data.

When information is shared outside of this team/folder, it will be aggregated such that no individual is likely to be identifiable.

When information is shared with third parties in an identifiable manner, it will be sent via an encrypted attachment.

**11) Will the project or activity involve any of the following potential high risk activities? (Y/N)**

| | |
|---|---|
| **Y** | Large scale processing of sensitive (special category) or criminal conviction personal data |
| **N** | Profiling,automated decision making, or using special category data to determine individuals rights to access a service or contract |
| **N** | Monitoring of a publicly accessible place or the internet |

| | |
|---|---|
| **N** | Innovative technology (e.g. processing using artificial intelligence) |
| **N** | Processing biometric, genetic data or other highly personal or highly sensitive data |
| **N** | Combining, comparing or matching data from multiple sources |
| **N** | Processing data of children, or vulnerable people |
| **N** | Tracking individuals' online or offline location or behaviour |
| **N** | Inferring information on individuals |

If you have answered 'Y' to any of the above criteria, there is a potentially high risk involved in processing the personal data. You do not need to complete Q12. Go to the Next Steps.

If you have not answered 'Y' to any of the criteria in Q11, go to Q12.

**12) What are the risks involved in processing the data?**

*Consider if there are any risks to data subjects based on the sensitivity of the data being processed, and the type of individuals involved. Consider risks to the Cabinet Office, e.g. financial or reputational risks. Review the Personal Data Governance and Risk Management Policy section 5.5.2 for potential risks to the CO and the data subject.*

- 
- 

**13) What are the controls or measures that are in place or will be in place to safeguard the personal data?**

*These could be measures such as restricted access, staff training, encryption, etc.*
Link to controls library for examples

| **Controls in place** | **New or existing** |
|---|---|
| | |

| | |
|---|---|
| | |
| | |
| | |

## Next Steps

Thank you for completing the Initial Assessment.

Once you have completed the Initial Assessment, you must submit the assessment to your BU privacy resources (where applicable) or the CDIO DPC team (dataprivacy@cabinetoffice.gov.uk). **You must not begin to process personal data until you receive advice from the DPC team or your BU Privacy resources.**

If you responded with 'Y' of any of the criteria in Q11, a DPIA is required. You may start completing the next section and the DPC team/ BU Privacy resources will reach out to support you complete the section and consult with the DPO. Otherwise, you must wait for a response from the DPC team/ BU Privacy resources.

**<u>This section must be completed by the DPC team/ BU Privacy resources</u>**

The risk rating is HIGH/ MEDIUM/ LOW [delete as appropriate]

If HIGH, reach out to the BU to support completion of the DPIA.
If MEDIUM, assess the residual risk and complete the below:

The residual risk rating is MEDIUM/ LOW [delete as appropriate]

Cabinet Office

# Section 3 – Data Protection Impact Assessment (DPIA)

**All questions in this section are mandatory if a DPIA is required.**

**This section must be completed with the support of the CDIO Data Privacy and Compliance team (DPC team) or your BU Privacy resources. Once Section 3 is complete, the DPIA will be submitted to the DPO for review. The DPO will provide advice on whether the processing of the personal data should proceed.**

**Note. You MUST NOT proceed with processing the personal data until you have spoken to the Personal Data & Compliance Team/ BU Privacy resources or DPO.**

1) **Outline the personal data flows**
   *Where and how is the data collected; what systems is it stored in; which systems is the data transferred between; what third parties (if any) will receive the data and how (use a diagram if easier).*

Applicants will apply via the CS Jobs website which will provide a link to the Smart Survey Application. They will be presented with a specific privacy notice for the Beyond Boundaries programme before they are asked to provide any personal data.

That application data will then be downloaded from Smart Survey's systems to the Beyond Boundaries team (on Google). The data will be moved into locked-down folders.

As part of the development activities of the scheme, the Beyond Boundaries team will occasionally submit data of applicants to KPMG and their supply chain (specifically Berkshire Consulting contracted by KPMG) - this is subject to the existing contract in place with them.

Anonymous D&I data will be shared with departments.

2) **Please explain why it is necessary to use the personal data for this project. If the project could reasonably be completed in another way, then the processing will not be necessary.**

Processing of personal data is necessary for the successful operation of the development scheme. As places may be ringfenced by departments for people with protected characteristics, it is important that we have an understanding of an individual's diversity

data in order to know to select them on that basis if they are successful in being listed on the merit list.

3) **Please explain why it is proportionate to use the personal data for this project. How will you ensure that you are only processing the minimum possible personal data? Is your processing of personal data justified by your legitimate objectives?**

Diversity data is required to award places on the programme, to assess the fairness of the scheme, and to monitor for any inequalities that may arise.

We collect all data relating to the protected characteristics listed in the equality act plus Low-Socio Economic Background (LSEB) as departments can ring fence any of these characteristics. We will not have one advert for each department with only the characteristics (if any) that they are ring fencing, as this was trialled in 2022 and it resulted in an unmanageable number. We now have one advert per grade and in order to cover all possible areas of ringfencing possibilities we must ask for all the characteristics plus LSEB.

4) **What are the risks involved in processing the data?**
*Consider the risks to data subjects based on the sensitivity of the data being processed, and the type of individuals involved. Consider risks to the Cabinet Office, e.g. financial or reputational risks.*

*For each risk state whether there will be measures in place to protect the personal data. These could be measures such as restricted access, staff training, encryption, etc.*
*Review the Personal Data Governance and Risk Management Policy section 5.5.2 for potential risks to the CO and the data subject and* link to controls library for examples of controls

| No. | Potential risk | Risk rating (L/M/H) | Proposed Controls | Residual Risk (L/M/H) |
|---|---|---|---|---|
| | | | | |

| | | | | |
|---|---|---|---|---|
| 1 | Applicants may not know how their information will be processed/shared. | M | A specific privacy notice will be presented to them before they provide their personal data. | L |
| 2 | Smart Survey may inadvertently disclose applicant data with. | M | Smart Survey are bound by an existing contract, have specific technical and procedural controls in place, and are currently processing millions of surveys without incident. | L |
| 3 | The Beyond Boundaries team may inadvertently share personal data. | M | The information they download from Smart Survey will be placed in a locked-down folder in Google.<br>The team will be given clear processes to follow whenever they need to share data.<br>Large scale reporting of the scheme will include aggregated datasets that will be checked to ensure that individuals are highly unlikely to be identifiable. | L |
| 4 | The personal data of those on the scheme may be disclosed by KPMG or their supply chain. | M | A contract exists for the learning side, and controls are in place to protect personal data. | L |
| 5 | Applicant data may not be deleted in a timely manner / data retention dates may be missed. | M | The Beyond Boundaries team will have a clear and documented process for data deletion.<br>This will not include those applicants who have given consent that their data be retained for monitoring purposes. | L |
| 6 | Applicants may not realise that they have given consent for their data to be retained beyond their time on the scheme. | M | The Beyond Boundaries team will get explicit and genuine consent from applicants, and will retain copies of their consent forms in the locked-down folder. | L |

| | | | | |
|---|---|---|---|---|
| 7 | Data processing is ruled to be an unlawful discrimination or unfair processing. | H | A legal review of this exercise was carried out in late 2021, and an equality impact assessment completed. A second legal review has been carried out recently that confirmed this processing is legal but also recommended that departments also carry out equality impact assessments (which they have done). | L |
| 8 | Failure to refresh alumni consent every 2 years. | M | The team that will monitor this will embed into documentation and working processes that this consent needs to be refreshed. | L |

**5) State which teams were consulted in completing the DPIA**

| **Team** | **Date of review** |
|---|---|
| Beyond Boundaries team<br>GBS Information Assurance team | |

## Next Steps

Thank you for completing the DPIA. Please send this assessment to the DPC team (dataprivacy@cabinetoffice.gov.uk) or BU Privacy resources (as appropriate).

**You must not begin to process personal data until you receive advice from the DPC team or your BU Privacy resources or the DPO.**

---

**<u>This section must be completed by the DPC team/ BU Privacy resources</u>**

The residual risk rating is HIGH/ MEDIUM/ LOW [delete as appropriate]

**This section must be completed by the DPO**

**Once Section 3 is complete the DPC team will submit the DPIA to the DPO for review. The DPO will provide advice and inform you of the appropriate next steps.**

**DPO Comments**

| |
|---|
| |