BANK OF ENGLAND

Privacy and data protection

Data Protection Impact Assessment

[*Insert name of project*]

SPD-Privacy

A Data Protection Impact Assessment ('DPIA') is required when a new project or procedure will materially affect how the Bank processes information that relates to individuals. The purpose of this assessment is to identify possible risk sources to individuals' privacy, to put forward mitigating actions to reduce or eliminate this risk, and to record how these have been taken forward.

A DPIA is required in high risk circumstances prescribed by the General Data Protection Regulation (Article 35) and associated guidance. Where risks cannot be mitigated, it may be necessary to engage the Information Commissioner's Office.

1. EXECUTIVE SUMMARY

Drafting note:

- *Include a summary sentence or two on the project*
- *Explain important aspects of the risk view*
- *Explain recommendations*
- *Propose next steps*
- *Summarise why you identified the need for a PIA and refer/link to supporting documents as needed*
- *Outline your recommendations*

2. PROJECT BACKGROUND

Explain broadly the project aims and what type of processing of personal data it involves, referring/linking to supporting documents as needed.

Drafting note: issues to cover

(i) Consider the following:

- *What is the source of the personal data?*
- *Is the processing novel in any way?*
- *How much personal data will you be collecting and how often?*
- *What geographical area does it cover?*
- *Does the data include special category or criminal offence data?*
- *Does the data include vulnerable individuals' data (e.g. children's data)?*
- *What is the current state of technology in this area?*
- *Are there any current issues of public concern re your proposal/processing that you should factor in?*
- *What are the benefits of the processing for you and more broadly?*
- *Is there another way to achieve the same outcome?*

(ii) Risks to individuals

- *What is the nature of the Bank's relationship with individuals?*
- *What is the intended effect on individuals?*
- *How much control will individuals have over their personal data? (especially children)*
- *Describe how you will consult with individuals or why it is not appropriate to do so*

3. SCOPE

This assessment is limited in scope to the [*PROJECT*], which covers the [*DESCRIPTION (SPECIFY BUSINESS AREAS AFFECTED, HOW)*]. This PIA should be read in conjunction with documents related to this project.

This document is based on information provided by the project owners as at [*DATE*] and the actions and conclusions included may no longer be valid should any part of the process materially change.

The following are outside the scope:

Drafting note: *Include any Code of Conduct/Certification Scheme that the Bank has signed up to which is relevant to the project scope.*

4. INFORMATION FLOWS

5. PRIVACY RISKS

5.1 Risk: EMPOWER

Risk description	Risk observations	Extant risk	Proposed mitigation	Residual risk
The risk that individuals' information is used in a manner that differs from what they have been told, or otherwise from what they would reasonably expect		Choose an item.		Choose an item.

Risk description	Risk observations	Extant risk	Proposed mitigation	Residual risk
Individuals are not able to exercise their rights of access, rectification, blocking, erasure in respect of information held about them Individuals are impacted by automated decision making or profiling		Choose an item.		Choose an item.

5.2 Risk: MANAGE

Risk description	Risk observations	Extant risk	Proposed mitigation	Residual risk
The risk that individuals' information is used in a way that is unlawful. *[SPD to flag if children's or other vulnerable individuals' data is used.]*		Choose an item.		Choose an item.

Risk description	Risk observations	Extant risk	Proposed mitigation	Residual risk
The risk that the purpose for which an individuals' information is used does not have an appropriate basis		Choose an item.		Choose an item.

Risk description	Risk observations	Extant risk	Proposed mitigation	Residual risk
The risk that individuals' information is used for a purpose that is different to and incompatible with the purpose for which they provided it		Choose an item.		Choose an item.

Risk description	Risk observations	Extant risk	Proposed mitigation	Residual risk
The risk that an excessive amount of individuals' information is processed for the identified purpose		Choose an item.		Choose an item.

Risk description	Risk observations	Extant risk	Proposed mitigation	Residual risk
The risk that decisions are made using information about individuals that is not sufficiently complete to fulfil the identified purpose, or is not of sufficient quality, or is not up to date		Choose an item.		Choose an item.

Risk description	Risk observations	Extant risk	Proposed mitigation	Residual risk
The risk that individuals' information is retained for longer than is required for the identified purpose		Choose an item.		Choose an item.

5.3 Risk: PROTECT

Risk description	Risk observations	Extant risk	Proposed mitigation	Residual risk
The risk that appropriate organisational and technical measures are not applied to protect individuals' information against unauthorised access, use, disclosure or loss		Choose an item.		Choose an item.

Risk description	Risk observations	Extant risk	Proposed mitigation	Residual risk
Third-parties processing information about individuals on behalf of the Bank do not appropriately protect this, or handle it outside the agreed terms of their engagement		Choose an item.		Choose an item.

Risk description	Risk observations	Extant risk	Proposed mitigation	Residual risk
Individuals' information is transferred to a jurisdiction outside the EEA that does not provide an equivalent degree of protection, without one of the mechanisms in place and not in reliance on one of the derogations		Choose an item.		Choose an item.

6. INTEGRATION OF OUTCOMES INTO PROJECT PLAN

Proposed mitigation	Owner	Accepted	Target date

Has the ICO been consulted in light of any residual high risks? ○ YES ◉ NO

Reason(s):

7. SIGN OFF AND RECORD OF OUTCOMES

Item	Name	Date	Notes
Measures approved by:			*[Integrate actions back into project plan, with date and responsibility for completion]*
Residual risks approved by:			*[If accepting any residual high risk, consult the ICO before going ahead]*
DPO advice provided:			*[DPO should advise on compliance, measures and whether processing can proceed]*
Summary of DPO advice:			
DPO advice accepted or overruled by:			*[If overruled, you must explain your reasons]*
Comments:			
Consultation responses reviewed by:			*[If your decision departs from individuals' views, you must explain your reasons]*
Comments:			
This PIA will be tracked and kept under review by the business area:			*[The DPO should also review ongoing compliance with DPIA]*

8. LEGAL DIRECTORATE

DPIA reviewed by:	
Date reviewed:	
Comments:	*Legal Directorate views should be sought on all PIAs. The Legal Directorate contact should complete this box, even if only to confirm that Legal Directorate have no comments or that their views have been reflected in the PIA.* *Where Legal Directorate disagrees with a proposal, or where there are significant legal issues, a summary of its views must be included.*

9. REFERENCES

European Data Protection Board Guidelines on Data Protection Impact Assessment and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679

ICO Guide to the General Data Protection Regulation – Data Protection Impact Assessments https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-carry-out-a-dpia/

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Data Protection Act 2018 UK http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Version History

Version	Date	Author	Description/Change Summary

Review History

Version	Date	Reviewer	Department/Role	Comments

Privacy issues checklist

This checklist is to identify whether there are any material privacy impacts for a new proposal. It helps SPD-Privacy triage issues, for more detailed consideration. Please submit descriptive project documentation (e.g. the Working Business Case, Statement of Business Need and the High Level Plan) to 'SPD-Privacy' and answer the following checklist.

It focuses on ***personal data***, which is information about an identifiable, living individual.

PROJECT NAME		Yes	No	?
Is this a process or change that could require a privacy review?				
1.	Will the proposal involve a ***new collection*** of personal data? Or require individuals to provide information about themselves?	☐	☐	☐
2.	Does the proposal envisage ***a new use*** for personal data that is already held?	☐	☐	☐
3.	Is the proposal for a ***purchase of data*** that includes personal data?	☐	☐	☐
4.	Does the proposal involve any other ***material change to the way we store, process, secure or retain*** personal data?	☐	☐	☐
5.	Will the proposal involve ***sharing*** of personal data within the Bank with business areas or people who have not previously had routine access to the information?	☐	☐	☐
6.	Will the proposal change or create any system of ***regular disclosure*** of personal , data whether to another public sector entity (ONS, ECB, SFO), to the private sector, or by broad publication?	☐	☐	☐
7.	Is any ***surveillance*** or other ***potentially intrusive technology*** proposed?	☐	☐	☐
8.	Will the proposal create or leverage an ***identification system***, eg using a biometric signature like a fingerscan, or use of personal questions for password reset? Will it require existing ID, such as a driver's licence or passport?	☐	☐	☐
9.	Is it proposed to ***link or match*** personal data with other Bank data, or externally sourced datasets?	☐	☐	☐
How high risk is the process, and how detailed will the review need to be?				
10.	Is any of the personal information particularly ***sensitive or private***? *Eg. relating to one of the following topics: racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health; sexual life; the commission or alleged commission by the data subject of any offences.*	☐	☐	☐
11.	Please provide a Confidentiality rating for the information			

PROJECT NAME		Yes	No	?
12.	Could the proposal affect a very extensive number of individuals, or otherwise be ***high impact*****?** *Eg. by nature of geographical extent of the processing activity, large number of data items being processed, the duration or permanence of the activity etc.*	☐	☐	☐
13.	Could the processing involve evaluation or scoring of individuals (including profiling or predicting behaviour)?	☐	☐	☐
14.	Are any decisions made about individuals without human validation or interaction that could lead to their exclusion or discrimination?	☐	☐	☐
15.	Does the process observe, monitor or control individuals, including systematic monitoring of a publicly accessible area (eg. CCTV)?	☐	☐	☐
16.	Will the proposal result in the Bank making decisions or taking action against individuals in ways which can have a significant impact on them (for example, preventing them from exercising a right or using a service or a contract)?	☐	☐	☐
17.	Could the information relate to vulnerable individuals? (e.g. children)	☐	☐	☐

Personal data is:

any information relating to an identifiable living person who can be identified either from that information on its own, or in combination with other information.

What counts as personal data?

A wide range of personal identifiers can constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. Personal data can include opinions and any indication of intentions towards an individual. It does not include information that is only about a firm or entity though.

What types of personal data require extra care?

Some types of personal data require special care, because they are more sensitive. The GDPR sets out certain types of information that require extra care, which it calls **special category data**. That includes:

- information relating to one of the following special categories: racial or ethnic origin; political opinions; religious beliefs or philosophical beliefs; trade union membership; physical or mental health; biometric or genetic data; sexual life or orientation
- information about criminal convictions or offences or alleged offence

Even where information isn't special category data, it will still sometimes be more 'sensitive'. Things like negative opinions, financial information (eg. customer data) or certain location information have the potential to cause greater harm to individuals, so the standards we have to apply to protect them are higher. An intrusive method of collection may also mean extra care is required.

Does the format in which the information is held matter?

The GDPR says that information will only be personal data when:

- It's held in an electronic format; or
- It's held as part of manual filing systems, where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

The principles set out in the GDPR for how to handle personal data only apply in a more limited way to information that is held manually, such as unstructured notes in a notebook.

If it doesn't have a name, does that mean it isn't personal data?

Information that has been 'pseudonymised' (eg key-coded) can still be personal data depending on the ability of any party to re-identify the particular individuals. It is only when data is truly anonymised (ie. where there is no means by which to re-identify the individuals) that information would not be considered to be personal data.

What about if it's already public?

Whether or not something is published or otherwise access ble doesn't change whether or not it counts as 'personal data', though it may affect how the data protection principles should apply. Where individuals have clearly taken deliberate steps to make information public, it is l kely to be more reasonable to conclude that their expectations of privacy in respect of that will be more limited. If further uses could be unexpected, however, extra care may be required.

INITIAL ASSESSMENT OF PIC BY SPD PRIVACY

C Rating is 5	Presumed DPIA required
If C Rating is 4 or above + 12 is checked	Presumed DPIA required
C Rating is 3 or above and 9 is checked	Presumed DPIA required
If 13 + 16 are checked	Presumed DPIA required
If 14 is checked	Presumed DPIA required
C Rating is 3 or above and 17 is checked	Presumed DPIA required
17 is checked	Optional, for review in the circumstances
15 is checked	Optional, for review in the circumstances (eg. Staff, non-staff and expectations of CCTV use)
If C Rating is 4 or above	Optional, for review in the circumstances
If C Rating is 3 or above + 12 is checked	Optional, for review in the circumstances
C Rating is 3 or above +16 is checked	Optional, for review in the circumstances
Any of 1-9 is checked and the C Rating is 1 or 2	Privacy review or compliance advice (unless DPIA also triggered)
Any of 1-9 is checked and the C rating is 3	Discretion with privacy team as to whether a privacy review or a PIA (unless DPIA also triggered)
Any of 1-9 is checked and the C rating is 4 or above	PIA required (unless a DPIA is also triggered)

Is a full PIA or DPIA required? ○ YES ○ NO

Summarise why you identified the need for a PIA:

Confirmation by SPD-Privacy:

Date: