Privacy impact assessment screening questions

Will the project involve the collection of new information about individuals?

No

Will the project compel individuals to provide information about themselves?

No

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Yes. This information will be routinely proactively published on our website and therefore in the public domain and available to everybody. Information relating to individuals will be included only where it is in their capacity as data controllers operating in a non domestic context.

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

No, but it is routine proactive publication rather than providing a reactive response to information requests. Responses to information requests are published in the disclosure log on our website anyway. We are not disclosing any additional information that we would not already provide were it requested from us.

Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

No

Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

No

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

We hold information relating to all types of concern or investigation undertaken in our capacity as regulator of information rights laws. Some of these are about sensitive matters. Of particular note, there are records of criminal investigations, investigations brought to us by whistleblowers or concerns raised about domestic CCTV users. In these circumstances, disclosure of the fact of the case and the complained about party might associate identifiable individuals with issues in a way that would be unfair or unlawful.

Will the project require you to contact individuals in ways which they may find intrusive?

No

Privacy impact assessment

Step one: Identify the need for a PIA

The aim of this project is to proactively disclose our biggest dataset in a reusable format and increase transparency around the regulatory work that we do. The dataset is information about public concerns and self reported incidents reported that we have dealt with and where there is an outcome. We regularly receive requests for this information from individuals and organisations to the extent that there is clearly interest in it being available from a range of parties. We acknowledge that there is a legitimate public interest in the information being proactively available, reusable and regularly updated. We also acknowledge that there is a legitimate public interest in individuals easily having access to the outcomes of concerns raised about specific organisations.

We identified the need for a PIA because we know that some data controllers are householder domestic sole traders, some investigations are criminal in nature and some were brought to us by whistleblowers. We're also aware of not disclosing names of individual employees (other than sole traders) rather than the name of the organisation itself.

We also considered whether there was an impact on organisations as sa result of this project and although this is not a privacy or data protection risk, it was a consideration for us. We are aware that some organisations consider that publication of this type of information might adversely affect their interests. Although we acknowledge this view, we have concluded that the overriding public interest lies in us being transparent about the work that we have completed and in there being open public access to the information. We will publish the information alongside an explanatory note to provide the context of the disclosure.

Step two: Describe the information flows

The information contained in the dataset is generated during our casework process either by staff selecting from predefined options within our casework management system or recorded automatically by the system. The information is then extracted directly from our casework management system and held in a data warehouse. We run reports on this information which will form the published datasets. Individuals will only be included in their capacity as a data controller.

Consultation requirements

We will check the dataset before publication for inclusion of any case types that should be excluded or for clear inaccuracies in party records and ensure that stakeholders who are likely to feel that greater transparency might jeopardise their interests are informed. We consulted internally with relevant IAO's and the Senior Management Team.

Step three: identify the privacy and related risks

Privacy issue	**Risk to individuals**	**Compliance risk**	**Associated organisation/ corporate risk**
Disclosure of cases brought by whistleblowers.	Risk that disclosure of just the reference number or name of data controller could lead to identification of whistleblower with further risk of potential detriment.	Risk of disclosing personal information in contravention of the first data protection principle and whistleblower legislation and policy.	Risk of prejudicing investigations. Risk of reputational damage and potential complaints to ICO in regulatory capacity.
Disclosure of cases relating to criminal investigations.	Risk that disclosure of just reference number or name of data controller could identify individuals under criminal investigation with further risk of potential detriment.	Risk of disclosing personal information in contravention of the first data protection principle.	Risk of prejudicing investigations. Risk of reputational damage and potential complaints to ICO in regulatory capacity.
Disclosure of cases relating to domestic householder data controllers, in relation to use of CCTV.	Risk that disclosure of data controller name would lead to identification of individual domestic householder data	Risk of disclosing personal information in contravention of the first data protection principle. These individuals are	Risk of prejudicing investigations. Risk of reputational damage and potential complaints to

	controllers who are not operating in a business capacity with further risk of potential detriment.	given the choice about whether identifying detail appears on the public register.	ICO in regulatory capacity.
Disclosure of names of individual employees (other than sole traders) rather than organisational name.	Risk that disclosure of employee names would lead to their identification and might make them appear responsible when the responsibility lies with the data controller. Minimal risk of potential detriment.	Risk of disclosing personal information in contravention of the first data protection principle.	Risk of reputational damage and potential complaints to ICO in regulatory capacity.

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary
(e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Disclosure of cases brought by whistleblowers.	Case type removed from disclosure.	Eliminated	This is a proportionate solution as it enables us to proactively publish as much information as possible without risk to individuals.
Disclosure of cases relating to criminal investigations.	Case type removed from disclosure.	Eliminated	This is a proportionate solution as it enables us to proactively publish as much information as possible without risk to individuals.
Disclosure of cases relating to domestic householder data controllers, in relation to use of CCTV.	Case type removed from disclosure.	Eliminated	This is a proportionate solution as it enables us to proactively publish as much information as possible without risk to individuals.
Disclosure of names of	Dataset checked for individual names,	Eliminated	This is a proportionate

individual employees (other than sole traders) rather than organisational name.	where these are found in this context, the entry is corrected to reflect the data controller.		solution as it enables us to proactively publish as much information as possible without risk to individuals.

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project?

Head of Customer and Business Services, Paul Arnold

Step six: Integrate the PIA outcomes back into the project Plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork?

Senior Business Development and Analysis Officer, Anna Feetam
Group Manager, Records and Information Management, Helen Ward

Who is responsible for implementing the solutions that have been approved?

IAOs for casework teams
Senior Business Development and Analysis Officer, Anna Feetam
Group Manager, Records and Information Management, Helen Ward

Who is the contact for any privacy concerns which may arise in the future?

Head of Customer and Business Services, Paul Arnold