Director Decision Meeting – for decision

Meeting agenda title: Proactive disclosure of complaints and concerns datasets.

Meeting date: 11 November 2021

Time required: 30 minutes

Attendees: Louise Byers, Director of Corporate Planning, Risk & Governance, Joanne Butler, Head of Risk and Governance, Hannah Silk, Senior Information Access Officer

1. Objective and recommendation

1.1 The Information Access team is undertaking work to resume proactively publishing datasets which require updating (previous datasets were pre pandemic and were last published on the ICO webpages for September 2019). The work has identified a number of risks that need to balance the risk of publishing personal data, and in meeting our commitment to openness and transparency and obligations under the FOIA. These risks fall within the ICO's risk appetite areas of information governance which has a minimal appetite, legal compliance which has an averse appetite and reputational risk which has a cautious risk appetite.

1.2. Whilst recognising that ongoing publication is necessary, the Director of Planning, Risk and Governance is requested to consider the options proposed and to approve the recommendations made in order for the Information Access team to continue with the work on publishing datasets.

1.3. The Director is requested to consider and decide on the options and recommendations made on:-

a) whether to continue to proactively disclose datasets, with the recommended option being to publish but with additional measures to mitigate risk
b) the approach to publishing civil, cyber and criminal investigations cases, with the recommendation being to publish datasets from crimson of civil and cyber cases but to exclude criminal cases
c) the approach to publishing Personal Data Breach (PDB) cases due to ICE casework software technical issues, with the recommendation being to publish the PDB dataset but to

remove additional columns and retain the same level of detail as previously published.

2. History and dependencies

2.1 In 2016 a Privacy Impact Assessment was completed and recommended that datasets should be published.

2.2 A new DPIA will be required should we continue to publish personal data; this has been drafted but not yet finalised as it will need to take account of the recommendations and decisions made in this report.

3. Developing a common understanding

3.1 The migration of all casework to ICE 360 has prompted a review of publishing datasets. The datasets currently include personal data of sole traders and other non-corporate entities. The move of casework to ICE 360 also means differences in reporting capabilities which also need to be considered.

3.2 Consultation with the casework departments has identified further concerns around the operational challenges of publication but also around the sensitivity of some cases. We have also obtained legal advice which identified some concerns and made recommendations to ensure compliance with legislation.

4. Matters to consider to achieve objective

4.1 Due to the number of elements, three separate decisions need to be taken. More detailed discussion papers of the issues linked to the recommended options are available on request.

4.2 **Decision 1: Whether to continue to proactively disclose datasets**

FOIA s.42 - Legal professional privilege [redacted] Where personal data is concerned, Lawful Basis under the GDPR and Article 8 of the ECHR also need to be considered.

4.2.1 **Option 1**- cease publishing datasets

Benefits:

- Alleviates legal concerns around proactive disclosure

- Reduces work for casework departments in assisting with publication.

Risks:

- Undermines our commitment to openness and transparency.
- Would represent poor service to parties interested in the data (public, professionals etc).
- We would still need to disclose datasets reactively under s.1 of the FOIA which is more risky and less efficient.

If Information Access stop publishing datasets centrally, each department could have the option to publish their own. This is not recommended as it would lead to inconsistencies and reduce the benefit of the datasets.

If this option is decided upon then no further decisions are needed, and the next section can be disregarded.

4.2.2 **Option 2-** publish with additional measures to mitigate risk (recommended option)

Further information about each measure is attached in *Annex 1.*

Basic options:

- Modification to ICE to include mandatory field for case officers to indicate suitability for disclosure when completing a case.
- Enhanced notification to data controllers (DCs) and public authorities (Pas) about the datasets, explaining how they can object to publication and the process we would follow.
- Exclude personal data, anonymise the names of sole traders etc.

4.2.3 **Option 3-** publish with enhanced additional measures to mitigate risk.

Basic options (as above) plus:

- Cease to publish cases where the outcome is 'no further action'

Benefits:

- DCs and PAs would only find themselves included within the datasets if they have been found to be at fault under the laws the ICO regulates.
- This would further reduce intrusion and greater demonstrate proportionality.

- Easy to implement through the reporting system.

Risks:

- Reduced value of the datasets for the public and for request handlers.
- Datasets would not present a complete picture of the work the ICO has done, as large numbers of cases would be eliminated.

4.3 Decision 2: Approach to civil, cyber and criminal investigations cases

Under previous review we decided to publish civil and cyber cases from CMEH but not criminal cases. Now all investigations are managed on Crimson, they will be omitted if we only publish datasets from ICE.

4.3.1 **Option 1:** Publish datasets only from ICE and not Crimson- therefore publishing no investigations cases

4.3.2 **Option 2:** (Recommended)**:** Publish datasets from crimson of civil and cyber cases but exclude criminal cases

4.3.3 **Option 3:** Publish datasets from crimson of civil, cyber and criminal cases

Benefits of recommended option:

- Consistent with previous approach.
- Strong public interest in investigation cases.
- Better in line with our commitment to openness and transparency and the Communicating Regulatory Activity Policy (CREAP).
- Avoiding the increased risk associated with criminal cases.

Risks:

- Possible inappropriate disclosure of sensitive cases.
- Does not follow the recommendations of the civil and cyber teams who are not in favour of publication of their cases.

The recommended option is consistent with the decision made in the previous review and we think this is still correct and in line with the CREAP.

We also recommend that we exclude from ICE all PDB cases with the outcome 'investigation pursued' as this may relate to open investigations.

4.4 Decision 3: Ice technical issues and personal data breach (PDB) cases

Ice datasets include greater detail about PDB cases, such as number and type of data subject affected. They also differ from CMEH in that they are not fixed in time and there is potential for duplication of cases over time.

4.4.1 **Option 1:** Publish full PDB dataset with additional data

4.4.2 **Option 2:** Remove additional columns and keep the same level of detail as provided previously (Recommended)

Benefits:

- Consistent with the previous approach.
- Risk averse approach in line with corporate attitude to compliance risk.

Risks:

- Missed opportunity for making use of the additional data which many stakeholders may find useful.

The recommended approach is not to publish the additional data at this stage but keep it on review, particularly as the Breach Insights project progresses as that may be a better use of this data.

With regards to the live datasets, we suggest providing wording on the website to the effect that the datasets provide a snapshot and data will change over time and cannot necessarily be aggregated.

5. Areas for challenge

5.1 With regards to the suggested measures for mitigation in option 2 for decision 1, we may be challenged about the operational practicalities of implementing the improved notification to DCs and PAs about the datasets and also the new ICE option. These will require significant work with the casework departments, however IA will lead and feel implementation is feasible based on the work we have already done.

5.2 Challenges about whether we should publish at all given some of the concerns raised in the legal advice. We do not believe that ceasing to publish is a realistic option. Disclosure would still be required under s.1 of the FOIA so it would not resolve the problem. Disclosing proactively is the only practical way to manage this so we need to find a balanced approach.

6 Next steps

6.1 For new ICE option: suggestion to be passed through Louise Byers to be collated and fed through the business planning process and quarterly updates between the Project Management Office and Heads of Service.

6.2 IA to draft updated guidance on the publication criteria and circulate to casework departments.

6.3 IA to draft template wording for enhanced notification to DCs and PAs and circulate to relevant departments- some standard wording is already in use in some departments which can be updated.

6.4 IA to continue the ongoing work of reviewing datasets for publication, assimilating the new processes. Datasets to be obtained from Crimson & ICE.

7 Author: Hannah Silk, Senior Information Access Officer

8 Consultees: A consultation process was completed with all affected departments and a summary of their responses is available at Annex 2.

9 List of Annexes:

Annex 1: Explanation of risk mitigation measures for Decision 2 (reading optional)

Annex 2 Consultation with departments

10 Publication decision:

- Report can be published internally only, with some redactions.

Contains references to privileged legal advice.

11 Outcome reached:

Director Decision Meeting held on 11/11/2021 with Louise Byers, Director of Planning, Risk and Governance, Joanne Butler, Head of Risk and Governance and Hannah Silk, Senior Information Access Officer.

Decision 1, Option 2 was agreed which was to continue to proactively disclose datasets and to publish but with additional measures to mitigate risk.

Decision 2, option 2 was agreed to publish datasets from crimson of civil and cyber cases but to exclude criminal cases.

Decision3, option 2 was agreed the approach to publish the PDB dataset but to remove additional columns and retain the same level of detail as previously published.

Annex 1: Explanation of risk mitigation measures for Decision 2

Option 2 measures:

- **ICE modification**

Add a section to the case completion page on ICE for all case officer which requires them to state whether or not the case is suitable for publication in the datasets.

This should allow for a better demonstration of lawful basis and necessity in terms of publishing each case by allowing for more nuanced consideration of the CREAP factors relating to each case and demonstrate a more targeted and proportionate approach.

Currently, cases inappropriate for disclosure are identified by each department checking the datasets when they are due for publication- eliminating them at the time of closure would be more efficient and less risky.

This can be achieved through the business planning process between the Project Management Office and the Heads of Service.

This would only assist with cases closed after the new option has been introduced, and until then we would need to continue checking for cases which are unsuitable for disclosure in line with the current process.

- **Better notification for PAs/ DCs**

Currently not all DCs/ PAs are notified that we investigating a matter concerning them, so they may be completely unaware of a matter about them which will then be included in the datasets.

This may occur where we have no cause to contact the DC/PA, because we cannot investigate for any reason or cases where we can make a decision without requiring further information from the DC/PA.

In addition to this, most casework departments do not draw DCs/PAs attention to the datasets when they are in contact with them, so they are likely to be unaware that the information is being published or that they can raise an objection which we will consider. Currently only civil investigations do this.

We therefore suggest improving on this to ensure fairness to organisations being included in datasets. This is particularly pertinent in respect of sole traders where personal data is involved (if we continue to publish personal data). Suggestions:

- Ask casework departments to include standard paragraph notifying about the datasets when they write to DCs/PAs about matters we are looking into

- Notifying all registered DCSs when they register/ renew their fee
- Notification to include an explanation of the process to follow if they object to publication
- If we decided not to publish cases with the outcome 'no further action', this would also eliminate the cases where we do not make any contact with the DC/PA

- **Anonymise personal data of sole traders etc:**

This would affect a small number of cases, estimate is 1% or less and ensure that we are not in breach of the GDPR/ ECHR. Would have a small negative impact on the usefulness of the datasets however withholding personal data is easily justifiable. Can be achieved through ICE as there is an option within case 'Account' record to confirm if it is a sole trader. This is not being used by case officers at the moment but we could build this into the training around the new case closure option- we could then identify DC names which need to be anonymised through this.

Additional measure for Option 3:

- **Do not publish cases with 'no further action'- either just for STs or all DCs**

These include cases where there was found to be no concern that the ICO could investigate which, makes up the majority of the cases where the DC/PA is not contacted. Also covers cases where there is found to be no wrongdoing. Can be achieved easily through the reporting system in ICE.