Data Protection Impact Assessment - ICE 360 Retention

Document Name	ICE 360 Retention – DPIA
Author/Owner (name and job title)	Janice Milbourne - Project Manager & Jonathan Wren - Lead Development Coordinator
Department/Team	PMO
Document Status (draft, published or superseded)	Published
Version Number	v1.0
Release Date	24/02/23
Approver (if applicable)	N/A
Review Date	24/02/24
Distribution (internal or external)	Internal

Privacy by design at the ICO

Welcome to our privacy by design process. You should use this every time you want to implement or change a product or process at the ICO. It is essential to managing your own project risks but also to managing the corporate risks of the ICO.

Responsibilities

- It is your responsibility to ensure that data protection impact is taken into account during the design and build of your product or service. To do this successfully, you will need to be able to explain what your proposal is, and map out how data is used. This includes, amongst other things, where data might sit at any time geographically, but also the purpose of its use at different points in time.

- Remember the basics. Key to a good assessment is knowing at all points in the process: what data you are collecting and why, where it will be stored, for how long will you keep it, who will access it and for what purpose, how it will be kept secure and whether it's being transferred to any other country.

- Your Information Asset Owner (your Service Director) is ultimately responsible for managing any residual risk.

- The Information Management Service, working on behalf of our DPO, can help complete the paperwork, provide compliance advice and spot risks. It is not the Service's responsibility to own, manage or mitigate the risks identified during the process.

Getting advice

- You might also need advice from subject matter experts in other teams to make sure that you understand how something works or risks resulting from what you're proposing to do. This is particularly likely if it involves new, or changing, technologies. Getting this advice will help to provide your IAO with assurance that you have understood and identified the risks.

- You might well be working on a contract or agreement and a Security Opinion Report at the same time – these are also ways that you can mitigate risks and should be viewed as part of the overall assessment process.

The paperwork

- You should think of this as a live document. You might change your plans or new information might come to light that changes the risk profile of your proposal. If that’s the case, you should revisit the paperwork and update it to reflect any changes. You might also need to inform your IAO of new or changed risks.

The DPIA process

- You should review our internal DPIA Process and allow time for this process in your project plans. Start early! How long it takes will depend on what you’re proposing, and how well you can explain it and identify risks. It can take several weeks to get the right advice and risk assessment in place.

Guidance for completing this template – please read.

- You only need to complete this Data Protection Impact Assessment (DPIA) template if you have completed a Screening assessment - do I need to do a DPIA?

- If you're unsure whether you need to complete a DPIA use the screening assessment first to help you decide.

- Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you won't be able to continue with your plans without changing them, or at all.

- Guidance notes are included within this template to help you – just hover your mouse over any blue text for further information. In some sections links are provided to ICO guidance for further information.

- It is recommended that you fill out each section of this template in order as each subsequent section builds upon the last. You will not be able to complete later sections correctly if you skip ahead.

- If you are struggling with any sections of this template the Information Management and Compliance Service is available to provide advice and support. Please keep in mind their service standards if you require help.

1. Process/system overview

1.1 Ownership

Guidance Link: Controllers and processors | ICO

Project Title:	BDG200 – Retention and Deletion – ICE 360 Workstream
Project Manager:	Janice Milbourne
Information Asset Owner:	Mike Fitzgerald - Director of Digital, IT and Business Services
Controller(s)	ICO
Data processor(s)	Microsoft

1.2 Describe your new service or process

This DPIA covers the functionality that will enable deletions within the ICE 360 casework system that comply with the time spans set out in the ICO's retention schedule.

There are a number of different scenarios that are covered under the proposed functionality but as ICE 360 is predominantly used for casework processes, then it will mainly focus on the requirements around the retention of cases. Within the system cases are linked to a number of different entities and therefore the retention job rules refined will delete a case from the system, when required, and also cascade the deletion to the relevant associated entities. There are also a number of 'housekeeping' rules that are included which will delete those records which are no longer linked to cases in line with agreed retention time limits.

In order to create the list of retention rules for ICE, the project team has consulted the ICO's retention schedule and sought technical advice from staff who have experience of developing and managing the system. Additionally, where necessary further guidance has been sought from, the Information Management team and the MI team in addition to LIMO's in specific departments and teams. A full list of the rules is accessible in the project folder, and where possible we have linked each rule to either the relevant section of the ICO retention schedule, or the decision received from the relevant team/department: https://edrm/sites/corp/ICEProg/_layouts/15/DocIdRedir.aspx?ID=CORP-825150718-34

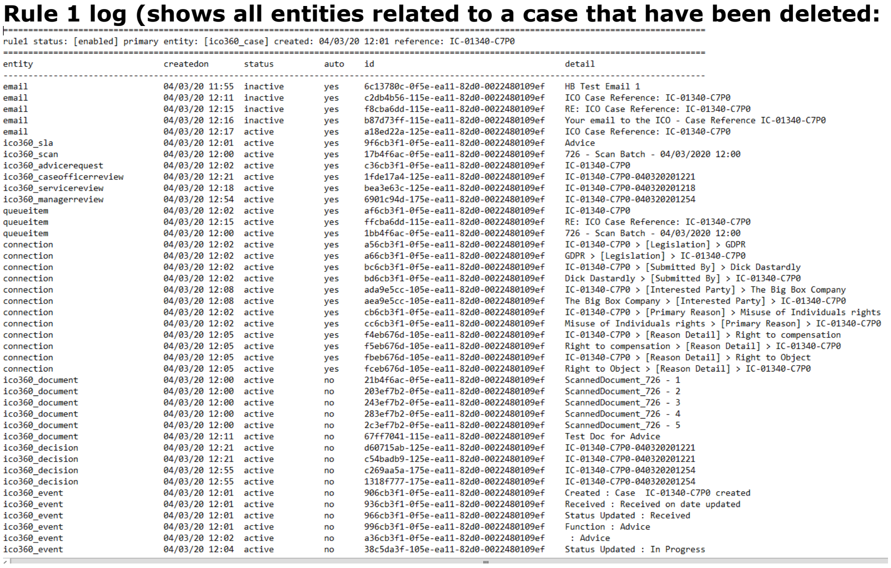
Technical Details:
The Retention and Disposal function will run as a standalone console application so that it can be scheduled to run out of hours, thereby minimising the impact on performance and user experience. After initial burn-in, it will run every evening after close of business.

The console application implements 2 phases, identification and deletion. The identification phase identifies all CRM entities that should be deleted based on a set of known retention rules. Identification metrics are reported to log files in the implementation folder, which may be retained for the system audit trail as required by section 3.11 of the retention schedule. The reports will not contain the contents of the entities that have been deleted but will include a list of the records deleted, a line of description which is normally the subject of the activity and detail of the specific retention rule which triggered the deletion.

The deletion phase will then delete the identified entities. The console application is driven by configuration, which allows each rule to be enabled or disabled, and within each rule, for the deletions to be throttled by maximum processed or duration - so that we can effectively manage the throughput of the deletions according to business need and backlogs.

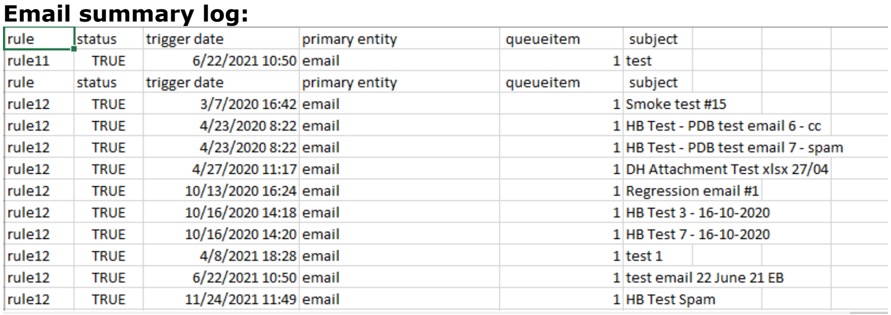
Over the page we have included some screenshots of the deletion logs from our test environment for reference:

Rule 1 log (shows all entities related to a case that have been deleted:



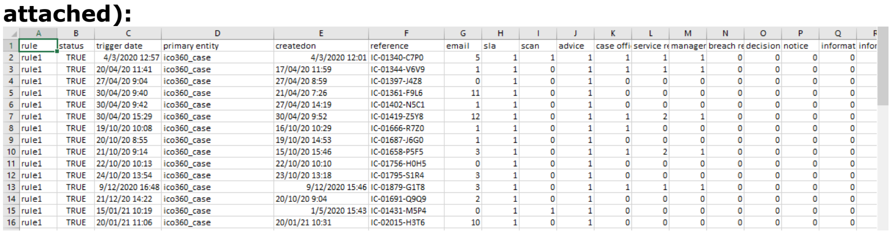
```
==============================================================================================================
rule1 status: [enabled] primary entity: [ico360_case] created: 04/03/20 12:01 reference: IC-01340-C7P0
==============================================================================================================
entity                    createdon       status      auto   id                                    detail
--------------------------------------------------------------------------------------------------------------
email                     04/03/20 11:55  inactive    yes    6c13780c-0f5e-ea11-82d0-0022480109ef   HB Test Email 1
email                     04/03/20 12:11  inactive    yes    c2db4b56-115e-ea11-82d0-0022480109ef   ICO Case Reference: IC-01340-C7P0
email                     04/03/20 12:15  inactive    yes    f8cba6dd-115e-ea11-82d0-0022480109ef   RE: ICO Case Reference: IC-01340-C7P0
email                     04/03/20 12:16  inactive    yes    b87d73ff-115e-ea11-82d0-0022480109ef   Your email to the ICO - Case Reference IC-01340-C7P0
email                     04/03/20 12:17  active      yes    a18ed22a-125e-ea11-82d0-0022480109ef   ICO Case Reference: IC-01340-C7P0
ico360_sla                04/03/20 12:01  active      yes    9f6cb3f1-0f5e-ea11-82d0-0022480109ef   Advice
ico360_scan               04/03/20 12:00  active      yes    17b4f6ac-0f5e-ea11-82d0-0022480109ef   726 - Scan Batch - 04/03/2020 12:00
ico360_advicerequest      04/03/20 12:02  active      yes    c36cb3f1-0f5e-ea11-82d0-0022480109ef   IC-01340-C7P0
ico360_caseofficerreview  04/03/20 12:21  active      yes    1fde17a4-125e-ea11-82d0-0022480109ef   IC-01340-C7P0-040320201221
ico360_servicereview      04/03/20 12:18  active      yes    bea3e63c-125e-ea11-82d0-0022480109ef   IC-01340-C7P0-040320201218
ico360_managerreview      04/03/20 12:54  active      yes    6901c94d-175e-ea11-82d0-0022480109ef   IC-01340-C7P0-040320201254
queueitem                 04/03/20 12:02  active      yes    af6cb3f1-0f5e-ea11-82d0-0022480109ef   IC-01340-C7P0
queueitem                 04/03/20 12:15  active      yes    ffcba6dd-115e-ea11-82d0-0022480109ef   RE: ICO Case Reference: IC-01340-C7P0
queueitem                 04/03/20 12:00  active      yes    1bb4f6ac-0f5e-ea11-82d0-0022480109ef   726 - Scan Batch - 04/03/2020 12:00
connection                04/03/20 12:02  active      yes    a56cb3f1-0f5e-ea11-82d0-0022480109ef   IC-01340-C7P0 > [Legislation] > GDPR
connection                04/03/20 12:02  active      yes    a66cb3f1-0f5e-ea11-82d0-0022480109ef   GDPR > [Legislation] > IC-01340-C7P0
connection                04/03/20 12:02  active      yes    bc6cb3f1-0f5e-ea11-82d0-0022480109ef   IC-01340-C7P0 > [Submitted By] > Dick Dastardly
connection                04/03/20 12:02  active      yes    bd6cb3f1-0f5e-ea11-82d0-0022480109ef   Dick Dastardly > [Submitted By] > IC-01340-C7P0
connection                04/03/20 12:08  active      yes    ada9e5cc-105e-ea11-82d0-0022480109ef   IC-01340-C7P0 > [Interested Party] > The Big Box Company
connection                04/03/20 12:08  active      yes    aea9e5cc-105e-ea11-82d0-0022480109ef   The Big Box Company > [Interested Party] > IC-01340-C7P0
connection                04/03/20 12:02  active      yes    cb6cb3f1-0f5e-ea11-82d0-0022480109ef   IC-01340-C7P0 > [Primary Reason] > Misuse of Individuals rights
connection                04/03/20 12:02  active      yes    cc6cb3f1-0f5e-ea11-82d0-0022480109ef   Misuse of Individuals rights > [Primary Reason] > IC-01340-C7P0
connection                04/03/20 12:05  active      yes    f4eb676d-105e-ea11-82d0-0022480109ef   IC-01340-C7P0 > [Reason Detail] > Right to compensation
connection                04/03/20 12:05  active      yes    f5eb676d-105e-ea11-82d0-0022480109ef   Right to compensation > [Reason Detail] > IC-01340-C7P0
connection                04/03/20 12:05  active      yes    fbeb676d-105e-ea11-82d0-0022480109ef   IC-01340-C7P0 > [Reason Detail] > Right to Object
connection                04/03/20 12:05  active      yes    fceb676d-105e-ea11-82d0-0022480109ef   Right to Object > [Reason Detail] > IC-01340-C7P0
ico360_document           04/03/20 12:00  active      no     21b4f6ac-0f5e-ea11-82d0-0022480109ef   ScannedDocument_726 - 1
ico360_document           04/03/20 12:00  active      no     203ef7b2-0f5e-ea11-82d0-0022480109ef   ScannedDocument_726 - 2
ico360_document           04/03/20 12:00  active      no     243ef7b2-0f5e-ea11-82d0-0022480109ef   ScannedDocument_726 - 3
ico360_document           04/03/20 12:00  active      no     283ef7b2-0f5e-ea11-82d0-0022480109ef   ScannedDocument_726 - 4
ico360_document           04/03/20 12:00  active      no     2c3ef7b2-0f5e-ea11-82d0-0022480109ef   ScannedDocument_726 - 5
ico360_document           04/03/20 12:11  active      no     67ff7041-115e-ea11-82d0-0022480109ef   Test Doc for Advice
ico360_decision           04/03/20 12:21  active      no     d60715ab-125e-ea11-82d0-0022480109ef   IC-01340-C7P0-040320201221
ico360_decision           04/03/20 12:21  active      no     c54badb9-125e-ea11-82d0-0022480109ef   IC-01340-C7P0-040320201221
ico360_decision           04/03/20 12:55  active      no     c269aa5a-175e-ea11-82d0-0022480109ef   IC-01340-C7P0-040320201254
ico360_decision           04/03/20 12:55  active      no     1318f777-175e-ea11-82d0-0022480109ef   IC-01340-C7P0-040320201254
ico360_event              04/03/20 12:01  active      no     906cb3f1-0f5e-ea11-82d0-0022480109ef   Created : Case  IC-01340-C7P0 created
ico360_event              04/03/20 12:01  active      no     936cb3f1-0f5e-ea11-82d0-0022480109ef   Received : Received on date updated
ico360_event              04/03/20 12:01  active      no     966cb3f1-0f5e-ea11-82d0-0022480109ef   Status Updated : Received
ico360_event              04/03/20 12:01  active      no     996cb3f1-0f5e-ea11-82d0-0022480109ef   Function : Advice
ico360_event              04/03/20 12:02  active      no     a36cb3f1-0f5e-ea11-82d0-0022480109ef    : Advice
ico360_event              04/03/20 12:04  active      no     38c5da3f-105e-ea11-82d0-0022480109ef   Status Updated : In Progress
```

Email summary log:



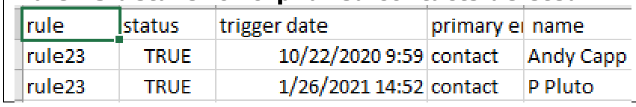
rule	status	trigger date	primary entity	queueitem	subject
rule11	TRUE	6/22/2021 10:50	email	1	test
rule	status	trigger date	primary entity	queueitem	subject
rule12	TRUE	3/7/2020 16:42	email	1	Smoke test #15
rule12	TRUE	4/23/2020 8:22	email	1	HB Test - PDB test email 6 - cc
rule12	TRUE	4/23/2020 8:22	email	1	HB Test - PDB test email 7 - spam
rule12	TRUE	4/27/2020 11:17	email	1	DH Attachment Test xlsx 27/04
rule12	TRUE	10/13/2020 16:24	email	1	Regression email #1
rule12	TRUE	10/16/2020 14:18	email	1	HB Test 3 - 16-10-2020
rule12	TRUE	10/16/2020 14:20	email	1	HB Test 7 - 16-10-2020
rule12	TRUE	4/8/2021 18:28	email	1	test 1
rule12	TRUE	6/22/2021 10:50	email	1	test email 22 June 21 EB
rule12	TRUE	11/24/2021 11:49	email	1	HB Test Spam

Summary of deleted cases under rule 1 (shows number of entities attached):



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	rule	status	trigger date	primary entity	createdon	reference	email	sla	scan	advice	case offi	service re	manager	breach re	decision	notice	informat	infor
2	rule1	TRUE	4/3/2020 12:57	ico360_case	4/3/2020 12:01	IC-01340-C7P0	5	1	1	1	1	1	1	0	0	0	0	
3	rule1	TRUE	20/04/20 11:41	ico360_case	17/04/20 11:59	IC-01344-V6V9	1	1	0	1	1	1	1	0	0	0	0	
4	rule1	TRUE	27/04/20 9:04	ico360_case	27/04/20 8:59	IC-01397-J4Z8	0	1	0	1	0	0	0	0	0	0	0	
5	rule1	TRUE	30/04/20 9:40	ico360_case	21/04/20 7:26	IC-01361-F9L6	11	1	0	1	0	0	0	0	0	0	0	
6	rule1	TRUE	30/04/20 9:42	ico360_case	27/04/20 14:19	IC-01402-N5C1	1	1	0	1	0	0	0	0	0	0	0	
7	rule1	TRUE	30/04/20 15:29	ico360_case	30/04/20 9:52	IC-01419-Z5Y8	12	1	0	1	1	2	1	0	0	0	0	
8	rule1	TRUE	19/10/20 10:08	ico360_case	16/10/20 10:29	IC-01666-R7Z0	1	1	0	1	1	0	0	0	0	0	0	
9	rule1	TRUE	20/10/20 8:55	ico360_case	19/10/20 14:53	IC-01687-J6G0	1	1	0	1	0	0	0	0	0	0	0	
10	rule1	TRUE	21/10/20 9:14	ico360_case	15/10/20 15:46	IC-01658-P5F5	3	1	0	1	1	2	1	0	0	0	0	
11	rule1	TRUE	22/10/20 10:13	ico360_case	22/10/20 10:10	IC-01756-H0H5	0	1	0	1	0	0	0	0	0	0	0	
12	rule1	TRUE	24/10/20 13:54	ico360_case	23/10/20 13:18	IC-01795-S1R4	3	1	0	1	0	0	0	0	0	0	0	
13	rule1	TRUE	9/12/2020 16:48	ico360_case	9/12/2020 15:46	IC-01879-G1T8	3	1	0	1	1	1	1	0	0	0	0	
14	rule1	TRUE	21/12/20 14:22	ico360_case	20/10/20 9:04	IC-01691-Q9Q9	2	1	0	1	0	0	0	0	0	0	0	
15	rule1	TRUE	15/01/21 10:19	ico360_case	1/5/2020 15:43	IC-01431-M5P4	0	1	1	1	0	0	0	0	0	0	0	
16	rule1	TRUE	20/01/21 11:06	ico360_case	20/01/21 10:31	IC-02015-H3T6	10	1	0	1	0	0	0	0	0	0	0	

Rule 23 details for orphaned contacts deleted:



rule	status	trigger date	primary e	name
rule23	TRUE	10/22/2020 9:59	contact	Andy Capp
rule23	TRUE	1/26/2021 14:52	contact	P Pluto

Additionally, although none the contents will be kept please see a list below summarises the fields that will display in the deletion log (highlighted are the fields that could contain personal data:

- Case Summary/Detail Field (potentially PD),
- Contact name,
- Email Subject Line (potentially PD),
- Entity type,
- Created on dates,
- CRM Status,
- GUID,
- Case Detail/Summary Field,
- Trigger date,
- Contact name,
- Account name,
- Error Event name,
- Case event details,
- Processing restriction type.

1.3 Personal data inventory - explain what personal data is involved

Guidance Link: What is personal data? | ICO

Category of data	Data subjects	Recipients	Overseas transfers	Retention period
All information within our care relating to casework processed through ICE 360:– Contact details Contents of complaints, data breaches, advice and information requests to ICO containing personal data Special category data Data relating to criminal offences Staff user records, including user name, full name, work contact details and manager	Complainants Enquirers ICO Staff Staff at other organisations MPs Information relating to children	ICO: Access to casework system through CRM using role based privilege Access to document storage in SharePoint will be limited to ICO staff on a least privilege basis.	UK only	Specific retention rules have been defined as stated above. In each case the retention will either be in line with the ICO Retention Schedule or with a decision made by the relevant LIMO for a department.
Deletion logs (see above)	Complainants Enquirers ICO Staff Staff at other organisations	The deletion logs will then be moved to SharePoint Online by a	UK only	1 Year

	MPs Information relating to children	Windows Task which runs daily. Logs will be deleted on admin server when push into SharePoint is successful to prevent duplication. Access to this site in SharePoint can be restricted in line with business requirements but initially, access will only be granted to LIMOs, IT Help staff, and ICE admins & BAU support staff.		

1.4 Identify a lawful basis for your processing

Guidance Link: Lawful basis for processing & Lawful basis interactive guidance tool

The lawful basis for the majority of our processing is article 6(1)(e) of the GDPR – public task.

Where casework requires us to process special category information - lawful basis for processing is article 9(2)(g) of the GDPR – public interest.

The relevant DPA 2018 schedule 1 condition is paragraph 6 - statutory and government purposes.

Where the processing relates to the law enforcement purposes, separate considerations under DPA 2018 will apply.

The processing will be lawful under s.35 (2)(b) DPA 2018, i.e. it is 'based on law' and is 'necessary for the performance of a task carried out for that purpose [i.e. any of the law enforcement purposes] by a competent authority'.

So far as 'sensitive processing' is concerned, s. 35(5) DPA 2018 applies. The relevant schedule 8 condition is Schedule 8 paragraph 1 – statutory purposes and the ICO has an appropriate policy document in place.

1.5 Explain why it is both necessary and proportionate to process the personal data you've listed in your data inventory

We already collect the minimum possible personal data below in order to carry out the following business functions:

- Considering complaints received relating to the mishandling of personal data under the DP regulations;
- Processing breach reports from organisations, required under the GDPR;
- Handling requests for decisions made to the ICO under the FOI, EIR and RPSI;
- Responding to information requests received under the GDPR, FOI, EIR and RPSI; and
- Providing advice to members of the public and businesses about information rights, the legislation we oversee, the role of the ICO and other matters.

No further processing of information is proposed or anticipated during the phases of work outlined in this project. The functional proposed will delete this information in line with the ICO Retention Schedule.

1.6 Outline your approach to completing this DPIA

This DPIA has been completed on the basis that we currently have approval for the enhancement of ICE Reg and Casework to a safe and stable platform (as part of phase 1 and 2 of the ICE Infrastructure project work. Please see below links to relevant DPIAs and SOR:

DPIA Phase 1: DPIA - ICE Infrastructure - Safe and Stable - v.1.docx ICE Registration Infrastructure upgrade – DPIA Release date – 05/06/2022

DPIA Phase 2: Updated DPIA - ICE Infrastructure - Safe and Stable - V.2 - Casework.docx ICE 360 Casework Infrastructure upgrade – DPIA release date – 08/12/2022

SOR Ref: 000067 – ICE Stabilisation V2.0, approved on 19/05/22. As agreed, a refreshed SOR submission was provided to cyber security on – 25/02/22 to cover updates in design.

In order to design the retention rules, the project team has consulted the wider organisation and the ICO retention schedule in order to refine specific requirements.

If there are any changes suggested to the retention periods specified then we will consider and update this DPIA form if necessary.

2.0 Personal Data Lifecycle

Guidance Note:

- You must provide a systematic description of your processing from the point that personal data is first collected through to its disposal.

- You should explain the source of the data, how it is obtained, what technology is used to process is, who has access to it, where it is stored and how and when it is disposed of.

- If your plans involve the use of any new technology you should explain how this technology works and outline any 'privacy friendly' features that are available.

- You can use the headings provided below to help you construct your lifecycle. Also include a flow diagram if it helps your explanation.

Data source and collection:
The information is collected via the ICE 360 casework system. Information is received by the ICO usually either via post or email. In some limited circumstances the data will be collected over the phone or by others means (eg a breach report taken by phone, an information request received by phone or reasonable adjustment for a case creation).

Despite the method by which the information is received, it will be stored in the ICE 360 system. Some information will only be kept in the queues (i.e. spam, cc'd emails or quick reply responses); whilst the majority of information will be added to a case (either a new or existing one).

At each stage the information held will be reviewed an considered by case officers in line with the specific casework processes for their department.

Technology used for the processing:
A C# console app that connects to the CRM database and uses SQL queries for the identification of result sets for each rule, and CRM SDK API for deleting them

Storage location:
The only information that will be stored as part of this functionality is the deletion logs kept for 12 months in line with requirement 3.11 in the ICO retention schedule (see example logs above).
The file location for R&D files is \\csw-crm-da01\f$\Retention & Disposal\
Access controls and data sharing:
Configuration of the retention console app and access to the retention logs will be limited to staff responsible for admin of ICE 360. If the team receive specific request concerning the deletion of certain records, then information from the retention records could be supplied on a case by case basis.

Disposal:
The functionality covered under this project facilitates the disposal of information contain the ICE 360 casework system in line with ICO requirements.

The console app will run and identify the relevant records for deletion daily (eg cases and associated records, emails, contact, records, org records, documents) and produce a log. An overnight job also ran by the console will then delete these records.

Retention logs will be kept for 12 months in line with requirement 3.11 in ICO retention schedule relating to system audit logs.

If the retention rule has an outcome of review (rather than delete) the log produce can be used to identify relevant cases and report these to the relevant teams. The console will not automatically delete cases unless we specific configured it to do so, therefore these cases would need a manual deletion once they have been review and agreed for deletion with relevant departments/teams.

3.0 Key GDPR principles and requirements

Purpose & Transparency

1. Will you need to update our privacy notices?

Yes ☐ No ☒

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

The retention schedule is linked to from the PN already so PN requires no update.

3. If consent is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

Guidance Link: Consent

Yes ☐ No ☐ N/a ☒

4. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

Yes ☐ No ☐ N/a ☒

If applicable please provide a link to your completed assessment.

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes ☒ No ☐

6. How will you ensure the personal data remains accurate for the duration of your processing?

The console app identification process will use metadata from ICE 360 which has been input and managed by cases officers in teams relevant to specific business functions. Data can easily/quickly be updated as required and reflected immediately within the ICE applications.

7. If the personal data isn't being obtained directly from the data subject what steps will you take to verify accuracy?

The data that the retention rules we be applied is held in the ICE 360 Casework system, therefore the steps concerning accuracy are held within the corresponding DPIA.

For reference, here are the steps contain in that DPIA:

"Where appropriate, controls in place to prevent inaccuracy of data including:

1. Email validation - double entry of email addresses and copy and paste functionality only available in the first email field;
2. We have implemented duplicate detection based on certain criteria such as name and address. Duplicate searches have also been incorporated into data entry processes (such as case creation);
3. Prompts to remind staff to check and confirm data on entry;
4. Usage of Data8 plugin, in order to verify postal addresses of organisations and individuals;
5. Reminders for users to check case information and metadata upon case closure;
6. Fields required during data entry configured with specific parameters, to avoid human error (i.e. validation on registration no. field);
7. Where we have initially had input, business processes were tailored so that information is crossed referenced (i.e. between ICE Reg and Casework, or against Companies House information); and
8. Checks within dialogs sending correspondence prompting users to check accuracy of information prior to sending.

Notably the specific changes being suggested under this project should not alter the existing measures already in place in ICE to protect the accuracy of data."

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes ☒ No ☐

9. How will you ensure the personal data are deleted at the end of the retention period?

Testing of the retention rules will be undertaken by the project team prior to live deployment.

Testing will work on identifying whether the identification process ran by the console app is identifying the correct cases for deletion based upon the rules stated.

Information contained in the retention logs provides an extensive record of exactly which entities have been deleted that will be useful for testing purposes and after deployment for auditing purposes.

Process to be agreed for the storage of the retention log to be agreed in line with current IT practices and in line with requirements under 3.11 of ICO retention schedule.

10. Will you need to update the retention and disposal schedule?

Yes ☐ No ☒

Integrity and confidentiality

11. Where will the personal data be stored?

ICO systems: The information that will be deleted is held in ICE 360 and in SharePoint Online.

The deletion logs will contain minimal personal information, likely to be either contact names, email subject headers or information entered into the case summary field by the case officer.

The deletion logs will be held in the file system in the location \\csw-crm-da01\f$\Retention & Disposal\ and will be deleted in line with the requirement for the deletion of system audit logs after 12 months (ICO retention schedule 3.11)

12. Are there appropriate access controls to keep the personal data secure?

Yes ☒ No ☐

13. Have you contacted the cyber security team for a security assessment of your plans?

Yes ☒ No ☐ N/a ☐

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

No change to policies required. Staff (eg users) will not be interacting with this system other than to provide technical oversight of automated processes.

Therefore access will be limited to only a small pool of system admins.

Accountability

15. Who will be the Information Asset Owner for this personal data?

Mike Fitzgerald - Director of Digital, IT and Business Services

16. Will you need to update our Article 30 record of processing activities?

Yes ☐ No ☒

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes ☒ No ☐ N/a ☐

Individual Rights

Guidance Note:

- UK GDPR provides a number of rights to data subjects where their personal data is being processed.
- As some rights are not absolute and only apply in limited circumstances we may have grounds to refuse a specific request from an individual data subject. But you need to be sure your new service or process can facilitate the exercise of these rights and it should be technically feasible for us to action a request if required.

Guidance Link: Individual rights

18. Is there a means of providing the data subjects with access to the personal data being processed?

Yes ☒ No ☐

19. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes ☒ No ☐

20. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐

21. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐ N/a ☐

22. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes ☒ No ☐ N/a ☐

23. Can we erase the personal data on receipt of a request from the data subject?

Yes ☒ No ☐

4.0 Risk assessment

Risk Description		**Response to Risk**	**Risk Mitigation**	**Expected Risk Score**		
				I	**P**	**Total**
				See Appendix 1 – Risk Assessment Criteria		
Example: *Access controls are not implemented correctly and personal data is accessible to an unauthorised third party.*		*Reduce*	*Existing mitigation: We have checked that the system we intend to procure allows us to set access permissions for different users.* *Expected mitigation: We will appoint and train a system administrator who will be responsible for implementing access controls and monitoring access. The system administrator will also audit the system periodically to review access permissions.*	*3*	*1*	*3 - low*
1.	Defined retention rules to apply do not accurately reflect ICO retention standards.	Reduce	Advice sought from relevant stakeholders to define retention rules. The rules to be applied are documented in detail from a technical perspective and, where able have either been linked to a relevant section of the ICO Retention schedule or business decision. A full list of the rules is accessible in the project folder, and where possible we have linked each rule to either the relevant section of the ICO retention	3	1	3 – low

			schedule, or the decision received from the relevant team/department: https://edrm/sites/corp/ICEProg/_layouts/15/DocIdRedir.aspx?ID=CORP-825150718-34			
2.	Retention rules applied do not function correctly, resulting in cases being deleted either too soon, longer than is necessary.	Reduce	Comprehensive testing of rules carried out in test environment, to ensure that criteria are applied correctly. Identification job of console app has been run in reporting only mode against the live environment. Manual checks conducted against log of cases identified for deletion and higher level cross reference checks have been carried out in conjunction with estimates given by MI Team. The part of on the console app which applies the deletion job is configurable and will only be applied in Live environment once all checks are complete and we are satisfied that only the required cases will be picked up for deletion.	3	1	3 - low
3.	As stated in ICO retention schedule, some requirements are for deletion of cases whereas as others are around cases being flagged for review. Risk that cases which	Reduce	Testing carried out as stated above to check that identified cases for deletion match criteria (including those rules requiring review only).	3	1	3 – low

	require review are deleted early in error.					
4.	Risk of inappropriate disclosure (eg personal data, critical system, corporate information or information relating to ongoing investigations) if deletion logs are considered under access request.	Reduce	Deletion logs will be redactable as required by the consideration of the Information Access Team.	3	1	3 – low
5.	Console application job fail, resulting in data being held longer than necessary.	Reduce	Deletions job will be monitored by system admins and automated alerts will be configured to highlight when jobs fail.	2	1	2 – low

5.0 Consult the DPO

Guidance Note:

- Once you have completed all of the sections above you should submit your DPIA for consideration by the DPIA Forum who will provide you with recommendations on behalf of our Data Protection Officer (DPO). The process to follow is here.
- Any recommendations from the DPOs team will be recorded below and your DPIA will then be returned to you. You must then record your response to each recommendation and proceed with the rest of the template.

	Recommendation	**Date and project stage**	**Project Team Response**
1.	**DPIA section:** 1.2 **Recommendation**: The full list of retention and disposal rules has been reviewed by the DPO team and some queries were raised about a few of the rules being applied. We're conscious the ICO retention and disposal policy has recently been updated and we need to be certain rules applied align with recent business updates. The Information Management and Compliance (IMC) team will contact the project team to review the rules in more detail with a view to:	Planning	Meeting held with IMC Team on 31/01/23. Clarification concerning rule 5 received from Laura Middleton surround NIS requirements on 08/02/2023. See here for decision email: https://edrm/sites/corp/ICEProg/_layouts/15/DocIdRedir.aspx?ID=CORP-825150718-54 IM raised no more actions for project team. IM to consider whether further entries to Retention Schedule required to cover rules 11-24. (i.e. requirements that are not case led, such as CC'd correspondence & SPAM). Re. bullet point 3, we will create a business facing version of the retention rules and definition. On the go to spreadsheet will refer to other business systems that impact on rules (i.e. information held in Crimson) in a

Commented [JW1]: Need to add in link to Laura's email once received.

	• Ensuring the correct retention rules are being applied from the recently updated ICO retention schedule • Ensuring the correct action is taken i.e. delete or mark for review when the retention period expires • Ensuring appropriate records are held of the business decision for the rule where the retention period is not being taken from the ICO R&D schedule • Updating the R&D schedule where considered necessary to reflect new retention and disposal rules that have been agreed with the business where these do not currently feature in the ICO schedule. **Suggested action:** IMC team to arrange meeting with project team for further discussion and to provide additional support.		notes section. Link to draft version: https://edrm/sites/corp/ICEProg/_layouts/15/DocIdRedir.aspx?ID=CORP-825150718-55
2.	**DPIA section:** 1.3 **Recommendation:** Deletion logs need adding to data inventory. An entry has been added by the DPOs team however project team to advise	Planning	Deletion logs will be generated on SQL box on admin server: CSW-CRM-DA01. This is where time scheduled jobs will be logged. Each day jobs are run, a new log folder is created. Only admins have access to this server (e.g. Product Owner, ICO Ops & ICE Support).

	on access controls in place to restrict access to these logs. **Suggested action:** Project team to add additional detail and ensure access to logs is appropriate		The deletion logs will then be moved to SharePoint Online by a Windows Task which runs daily. Logs will be deleted on admin server when push into SharePoint is successful to prevent duplication. Access to this site in SharePoint can be restricted in line with business requirements but initially, access will only be granted to LIMOs, IT Help staff, and ICE admins & BAU support staff.
3.	**DPIA section:** 1.5 **Recommendation:** There needs to be some consideration of necessity and proportionality of retaining personal data within audit logs after the substantive casework records have been deleted. **Suggested action:** Please add a few sentences to explain why retaining these logs is both necessary and proportionate.	Planning	The maintenance of the retention logs is necessary for auditing purposes on the retention and disposal of information held in ICE 360 (particularly cases). In order to maintain good information management practices the retention logs will hold minimal information about the records that have been deleted and the specific retention rules that they have been deleted under. Occasionally, requests are received from the business to check this information (i.e. if it is believed a case has been deleted inappropriately). The only personal information likely to be kept in the retention records are: • Contact names; • Subject lines of emails; and • Information held in the case summary field. This information has been specifically chosen to minimise the amount held whilst still being useful for the business, meaning we can identify which records have been deleted. Therefore there is likely a legitimate purpose for holding this information.

			If there were specific requests to delete personal data held in the retention logs (i.e. in respond to a right to erasure request) then steps could be taken to remove the relevant data from the log on a case by case basis. The logs will be kept for 12 months in line with 3.11 of the retention schedule and will be automatically deleted from SharePoint site 12 months after creation.
4.	**DPIA section:** 2.0 and 4.0 **Recommendation:** There needs to be some explanation in the DPIA about the review process for casework requiring review before it can be disposed of. There should be some further consideration of resulting risks to data subjects, in particular data being held longer than necessary whilst awaiting a review. Additionally, there should be some explanation about what happens to cases that are reviewed and the decision is then to retain - does it loop into another rule or fall outside the automation process altogether? **Suggested action:** Update DPIA with additional content.	Planning	Risk to be signed off: "There should be some further consideration of resulting risks to data subjects, in particular data being held longer than necessary whilst awaiting a review" Decision taken to not implement review functionality at this stage which would affect rules 4 & 5. At present: • There are no cases in live that would meet the criteria under rule 4 (PDB cases where Reg action is taken in ICE), as this is not current business process; and • only 1 case that the identification under rule 5 (NIS PDB cases, not handled in Crimson), this case is currently open (from January 23), so may still be moved to Crimson and completed with the investigation pursued outcome. Requirements around review processes would need more time and resources to refine before development and implementation can take place. A decision was taken on the basis that would substantially delay implementation of the automated deletion for the rest of the rules. This decision also took into consideration current risks regarding non-compliance.

			This decision has been signed off by project board. Further details: • The above decision will effect rules 4 & 5 on the ICE Casework retention rules (PDB action and PDB NIS): https://edrm/sites/corp/ICEProg/_layouts/15/DocIdRedir.aspx?ID=CORP-825150718-55 • As deletion settings are configurable for each rule, then we will not switch on the deletions for rules 4 & 5, to ensure that no cases are deleted in error. Although the identification job can still run, to highlight these cases. • Testing has been conducted to ensure that cases meeting the criteria for these rules should not be identified by other rules (potentially 3 & 6, which also refer to cases with the PDB function). • Further option that MI could report periodically on cases that meet these criteria under rule 4 & 5, to ensure that business processes have not changed. • If any cases were then identified a decision could be taken whether to mark them for preservation to prevent deletion.
5.	**DPIA section:** 2.0, 4.0 Risk 2 **Recommendation:** The DPIA be explicit about whether there is any	Planning	There is no recycle bin functionality with the retention and disposal rules. Back-ups of the data are held but

	ability to recover deleted cases (whether these are deleted in error or need to be recovered for some other reason.) For example is there a "recycle bin" where cases are further retained for a limited time period for recovery in case of error. Further are there any backups of data held. This will help inform risk scoring for risk of data being deleted in error and will provide some mitigation to this risk if there is the ability to recover data. **Suggested action:** Update DPIA with additional content.		would not be used for a retention scenario (only system recovery i.e. in event of catastrophic failure). The case deletion processes covered by the retention rules, rely upon the proactive marking of a case for deletion via the case completion dialog. The scenarios around this will depend upon the rule covered. a) For example rules 1 – 7 & 10, which cover the automated retention of cases completed with certain outcomes or legislations specific to each function, the deletion will only be triggered after the specified period has elapsed. This would be either 2 or 6 year from the date the case was completed with the relevant outcome for that rule. b) In the case of rule 25 which relates to user's ability to manually mark a case for deletion, this will also be added via the case completion dialog. This dialog has an information management reminder on, to ensure that users are inputting the correct data on the case. Additionally they will also (except on advice cases) have to specify whether the reason for deletion is "created in error" or "duplicate." If for either of these scenarios an outcome is logged incorrectly on a case, then in the first instance we would advise that users can edit this information by adding a case officer review, or manager review where available. If this is unavailable, then they would need to contact ICE

			360 support, who should be able to update fields on case to prevent deletion if this is carried out on same working day. For the “housekeeping” rules that relate to entities which are not connected to cases, the rules have been defined specifically to only automate deletion once the record is no longer associated with a case, or a specific business decision has been sought (i.e. with SPAM & CC’d emails). Therefore the business has led on the appropriate period in which it is necessary to retain the information. Further suggestion: in meeting with IM, action taken away by the team responsible for updating the retention schedule whether some of these requirements need adding.
6.	**DPIA section: 3.0 Q9** **Recommendation:** As part of agreeing a process for the storage of the retention logs the project team also considers how disposal of personal data held in backup audit logs will work after 12 months. This should be automated if possible to avoid this personal data being retained beyond the 12 month period. **Suggested action:** establish disposal rules for ICE backup audit logs	Planning	See information contained in response to recommendation 2. Deletion logs will be held in SharePoint Online, the same site collection as the CRM documents and access to files will be restricted. Retention of site will be configured to automatically delete files older than 12 months since creation. This can be easily configured in SharePoint at site level.
7.	**DPIA section:** 2.0 **Recommendation:** Some explanation of how you intend to monitor and update ICE retention and	Planning	Product owner would need to annually carry out annual routine review of the DPIA.

	disposal rules should the ICO's retention and disposal schedule change is required to ensure implemented rules are reviewed. **Suggested action:** Update DPIA with additional content.		There needs to be consideration of how changes to the ICO retention schedule which affect the automated retention are communicated to the product owner to ensure that considerations can be made of how and when necessary changes can be made to retention & disposal jobs. (Bearing in mind this could also contain further development requirements for ICE casework system including new fields, or legislations). There needs to be a business process for communication between IM and product owner. As if this communication does not take place then there are potential risks to the implementation of future functionality. Product owner will need to consider: - The resources and time needed in order to implement changes to retention rules; - The feasibility of changes suggested (i.e. does trigger exist in ICE 360 system). This has been added to residual risk sign off below (see 7.0).
8.	**DPIA section:** 4.0 risk 5 **Recommendation:** Expand on mitigation for risk 5. If a job fails will the system catch up on itself or would failed jobs require manual deletion of records not disposed of due to failure? **Suggested action:** Further mitigation required to fully justify low risk score	Planning	Risk is that, for a period of time the information would be held for longer than is necessary until the technical issue is resolved. If jobs fail than an email alert will be created which will notify ICE support staff of the issue, which would then need to addressed in line with existing IT support processes.

			If the jobs fail, then once they are fixed they will automatically catch up by deleting information identified from previous days. In exceptional circumstances, then cases/entities could be deleted manually if necessary.

6.0 Integrate the DPIA outcomes back into your plans

Guidance Note:

- Completing sections 1 to 5 of your DPIA should have helped you identify a number of key actions that you now need to take to meet UK GDPR requirements and minimise risks to your data subjects. For example, you may now need to draft a privacy notice for your data subjects; or you could have risk mitigations that you need to go and implement.

- You should also consider whether any additional actions are required as a result of any recommendations you received from the DPO.

- Use the table below to list the actions you need to take and track your progress with implementation. Most actions will typically need to be completed *before* you can start your processing.

Action	**Date for completion**	**Responsibility for Action**	**Completed Date**
Meeting with IMC team to confirm correct application of R&D rules.		IMC team to arrange meeting	Follow up meeting held to review recommendations and responses with IM - 23/02/23

7.0 Expected residual risk and sign off by IAO

Guidance note:

- Summarise the expected residual risk below for the benefit of your IAO. This is any remaining risk ***after*** you implement all of your mitigation measures and complete all actions. It is never possible to remove all risk so this section shouldn't be omitted or blank.
- If the expected residual risk remains high (i.e. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

There are 3 main residual risks that we suggest will need singing off by the IAO:

1. **Review Requirements – see recommendation: 4**

A decision has been taken by the project board not to implement the review functionality at this time, as the effort involved seems to outweigh the benefits to the business. Including this functionality would increase the development time and testing time required and would greatly risk the project delivery.

Additionally those defined rules which refer to the need to "review" are highly unlikely to affect substantial volumes of live cases. At present:

- There are no cases in live that would meet the criteria under rule 4 (PDB cases where Reg action is taken in ICE), as this is not current business process; and
- only 1 case that the identification under rule 5 (NIS PDB cases, not handled in Crimson), this case is currently open (from January 23), so may still be moved to Crimson and completed with the investigation pursued outcome.

As specified above we believe this decision affects rules 4 & 5, which are PDB regulatory action cases, and PDB cases with the legislation NIS/eIDAS.

Due to current business processes, cases which are required for review are processes in Crimson and not ICE 360, so will be covered under the retention in that system. Additionally, MI support have confirmed that we only have 1 NIS/eIDAS case currently handled by PDB in ICE 360 and often those these would be processed by Investigations team.

The following mitigating steps will also be considered for this risk:

- As deletion settings are configurable for each rule, then we will not switch on the deletions for rules 4 & 5, to ensure that no cases are deleted in error. Although the identification job can still run, to highlight these cases.

- Testing has been conducted to ensure that cases meeting the criteria for these rules should not be identified by other rules (potentially 3 & 6, which also refer to cases with the PDB function).

- Further option that MI could report periodically on cases which meet criteria under rules 4 & 5, to ensure that business processes have not changed.

- If any cases were then identified a decision could be taken whether to mark them for preservation to prevent deletion.

We believe that this is a proportionate response to the risk, given the greater risks to the business around non-compliance. However, if substantial changes are made to ICO retention schedule or business process then this decision should be reviewed.

2. **Deletions made in error – see recommendation: 5.**

Following dialog with IM more information has been added to the DPIA around the residual risk that information marked for delete may be deleted in error; this is because there is no "recycle bin" functional included in the retention and disposal solution.

ICE 360 contains specific warnings for users when marking a case for deletion, additionally, all retention periods have been agreed with the business or defined as per the ICO retention schedule.

If a user marks a case for deletion in error, then they have until the end of the day to either correct this information by adding a case officer review, or manager review where available. If this is unavailable, then they would need to contact ICE 360 support, so that the relevant amends would be made.

We believe this to be a minimal residual risk given the mitigations already in place.

3. **Review process for ICO Retention Schedule – see recommendation: 7.**

There is a residual risk that a lack of ongoing communication and business process around changes to the schedule could result in updates that are not feasible or made in a timely way in ICE.

In addition to the product owner's routine annual review of the DPIA which could potentially identify changes, there needs to be ongoing dialogue between the business, LIMO's, IAO's, IM and the product owner, if updates to the ICO retention schedule are made that are likely to affect ICE Casework systems. The project team recommends that this may be the best way to facilitate further changes to the technical implementation of the ICO retention schedule to casework system's going forwards.

This is that the product owner can gain an understanding of the requirements, and provide technical advice on solutions to best achieve the changes necessary, and to communicate to business timescales and recourses that will be needed.

7.1 IAO sign off

Guidance Note:

- Your IAO owns the risks associated with your processing and they have final sign off on your plans. You **must** get your IAO to review the expected residual risk and confirm their acceptance of this risk before you proceed.

IAO (name and role)	Date of sign off	Project Stage
Michael Fitzgerald – Director of Digital, IT and Business Services	24 February 2024	ICE Retention and Deletion work

8.0 DPIA Change history

Version	Date	Author	Change description
V0.1	24/02/23	Jan Milbourne & Jonathan Wren	Completed draft, IM recommendations and IAO sign off.

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: example risks to data subjects

Guidance Note:

- The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

9.0 DPIA Template Change History (for Information Management Service only)

Version	Date	Author	Change description
v0.1	01/06/2020	Steven Johnston	First draft
v1.0	07/10/2020	Steven Johnston	First release
v1.1	07/01/2021	Iman Elmehdawy	Amendment to guidance note page 2.

v1.2	18/03/2021	Helen Ward	Addition of Privacy by design at the ICO (pages 2 and 3)
v1.3	24/06/2021	Steven Johnston	Section 3.0 Q13 amended. Removed request for link to security assessment.
v2.0	07/03/2022	Steven Johnston	Full document review. Simplified privacy by design explanation on page 3 and made minor format changes throughout. Guidance note for 2.0 was updated and flow headings inserted to the text box. Next review date set to 31/1/2023.
V2.1	11/05/2022	Ben Cudbertson	Amended title of section 2 from 'data flows' to 'personal data lifecycle'
V2.2	26/10/2022	Steven Johnston	Guidance notes updated throughout following feedback from Project Management Office.