Data Protection Impact Assessment (DPIA) – Offsite Archive Storage and Integrated Services (OASIS)

Document Name	Data Protection Impact Assessment – Offsite Archive Storage & Integrated Services (OASIS)
Author/Owner (name and job title)	Steven Johnston, IM&C Team Manager
Department/Team	Information Management and Compliance Team Manager
Document Status	Published
Version Number	V1.1
Release Date	24/07/2023
Approver (if applicable)	Mike Fitzgerald – Director of Digital, IT and Business Services
Review Date	24/07/2024
Distribution	Internal

Guidance for completing this DPIA template

- If you're unsure whether you need to complete a DPIA, use the Screening assessment - do I need to do a DPIA? first to help you decide.
- ***Must*** and ***should*** are used throughout the guidance notes in this template to help you understand which things are a legislative requirement and ***must*** be done versus things that the ICO considers ***should*** be done as best practice to comply effectively with the law.
- You ***must*** complete this DPIA template if your screening assessment indicates a DPIA is required.
- You ***should*** 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.
- We recommend 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. You ***should*** read the guidance notes throughout this template to help you with each section.
- If you are struggling with completing 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. Data processing overview

1.1 Ownership

Guidance notes:

- There ***must*** be a clear owner for any residual risk resulting from your data processing. At the ICO our Information Asset Owners (service directors) are our senior risk owners and ***must*** sign off on your plans.
- We ***must*** understand our role in relation to the personal data being processed. Our obligations will vary depending on whether we are a controller, joint controller or processor.
- If you are procuring a new product or service from a third party, you will typically find information about data protection roles and responsibilities within the service terms and conditions, or any contract being agreed between us and the third party.

Guidance Link: Controllers and processors | ICO

Project Title:	Offsite Archive Storage & Integrated Services (OASIS)
Project Manager:	Steven Johnston / Iman Elmehdawy
Information Asset Owner:	Director of Digital, IT and Business Services
Controller(s):	ICO
Data processor(s):	Offsite Archive Storage & Integrated Services Ltd (OASIS)

1.2 Describe your new service or process

Guidance notes:

- Provide a summary of the service or process you want to implement. Include any relevant background information and your key aims/objectives.

We use off-site storage to manage our physical records and ensure that all aspects of management including environmental control, secure storage and shredding/disposal are standardised and provided professionally. The ICO moved to an off-site storage solution in 2015 and our requirements have remained consistent since then. Our current contract for off-site storage ends on 18 November 23.

We are awarding a new five year contract with the option to extend for a further two, twelve month periods at the discretion of the ICO to OASIS. This has been concluded via competition on the Crown Commercial Services Framework RM6175 Lot 1.

We currently have approximately 2500 boxes containing hard copy records stored with our incumbent off-site storage provider. We will be working with the incumbent supplier Restore and OASIS, to ensure the secure transfer of these boxes.

OASIS will then take responsibility for the secure storage of these boxes and will provide additional services to the ICO including:

- A secure and accessible inventory system to track boxes, accessible only by authorised ICO staff and supplier.
- Ability for ICO to add and edit information about the boxes in the inventory system.
- Ability for ICO to search for boxes and files and filter by metadata.
- Ability to track location of boxes with box locations kept accurate, up to date and auditable.
- Delivery and collection of our boxes to and from ICO premises and the storage facility
- Secure destruction of boxes on request from the ICO.

The purpose of this DPIA is to assess any impact on data subjects as a result of the ICO switching service providers.

1.3 Personal data inventory

Guidance notes:

- We ***must*** have a clear understanding of the personal data being processed. This is **essential** for identifying and managing risks.
- Use the table below to list each category of personal data being processing. Use a new row for each data category. You can add as many rows to the table as you need.
- Categories of data may not be obvious to you from the outset e.g. tracking data (IP or location) or data collated via cookies and you need to take the time to fully understand the extent of the personal data you will process.
- Your data subjects are the individuals the personal data relates to. For example, these could be members of the public, ICO employees, our contractors etc.
- Recipients will be anyone who the data is shared with.
- UK GDPR restricts transfers of personal data outside of the UK so any overseas transfers ***must*** be identified.
- Personal data should be kept for no longer than is necessary. You ***must*** identify a retention period for the personal data you intend to process.

Guidance Link: What is personal data? | ICO

Category of data	Data subjects	Recipients	Overseas transfers	Retention period
Personal data will be contained in the paper records we send off-site for storage. This could be all categories of personal data processed by the ICO including special category and criminal offence data. But will typically be personal data associated with	Typically ICO employees / former employees, members of the public, controller and public authority representatives, elected officials and any other data subjects the ICO interacts with as part of its business operations.	OASIS	No If yes, list the countries the data will be transferred to:	Anything up to: 6 years Then reviewed. Some records may be retained

ICO financial records, its casework and investigations, legal files and controller fee payments.				longer if they meet TNA preservation criteria.
Name & contact details.	ICO staff requiring access to the OASIS Bridge inventory system or otherwise involved in managing the service contract.	OASIS	No If yes, list the countries the data will be transferred to:	Other (please specify time period below) If selecting other, please specify the length of time personal data will be retained: Duration of contract and then likely deleted as part of the contract exit process.

1.4 Lawful basis for processing

Guidance notes:

- To process personal data, you ***must*** have a lawful basis. Select a lawful basis for processing the personal data in your inventory from the drop-down lists below.

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

First, select a lawful basis from Article 6 of the UK GDPR.

Article 6(1)(e) - public task

If more than one lawful basis applies to your processing, please list any additional basis here:

Guidance notes:

- If your personal data inventory includes any ***special category data,*** you ***must*** identify an additional condition for processing from Article 9 of the UK GDPR.

Guidance link: Special category data

Next, if applicable, select an additional condition for processing from Article 9 of the UK GDPR:

Article 9(2)(g) - reasons of substantial public interest

If you have selected conditions (b), (h), (i) or (j) above, you also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018. Please select from the following:

Choose an item.

If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of the conditions set out in Part 2 of Schedule 1 of the DPA 2018. Please select from the following:

6. Statutory and government purposes

Guidance notes:

- If you are processing **criminal offence data,** you ***must*** meet one of the 28 conditions for processing criminal offence data set out in paragraphs 1 to 37 Schedule 1 of the DPA 2018.

Guidance Link: Criminal offence data

Finally, if applicable select an additional condition for processing any criminal offence data:

6. Statutory and government purposes

1.5 Necessity and proportionality

Guidance note:

- You ***must*** assess whether your plans to process personal data are both necessary and proportionate to you achieving your purpose. You should explain why this is the case below.
- You ***must*** take steps to minimise the personal data you process; processing only what is adequate, relevant and necessary.
- You ***should*** think about any personal data you can remove without affecting your objective.
- You ***should*** consider if there's any opportunity to anonymise or pseudonymise the data you're using.

The ICO has maintained an off-site storage contract for a number of years. Whilst the number of paper records we hold is steadily decreasing we still require storage for approximately 2500 boxes of records which will continue to decrease throughout the duration of this contract. Procuring a professional supplier for these services is both a necessary and proportionate way for us to meet our storage needs.

The personal data involved is already processed by the ICO and there's no additional personal data being collected as a result of the change of supplier. Through our established annual destruction process we'll steadily decrease the personal data processed year on year. However, some records may need to be preserved for a lengthy period for transfer to the National Archives, and ensuring these are being stored in a suitable, secure environment like that offered by OASIS is the best way to maintain their integrity.

1.6 Consulting with stakeholders

Guidance notes:

- You ***should*** consult with relevant stakeholders both internally (for example Cyber Security, Legal Services, IT etc.) and externally to help you identify any risks to your data subjects.
- Briefly outline who you will be consulting with to inform your DPIA.
- Where appropriate you ***should*** seek the views of your data subjects, or their representatives, on your intended processing. Where this isn't possible, you should explain why below.

We've worked closely with colleagues in Procurement and Legal Services during the tender process to ensure prospective suppliers, including OASIS, can meet our minimum security standards and provide assurance about their UK GDPR compliance.

The Cyber Security Service has been approached for advice and we've submitted a Supplier Risk Assessment for their consideration.

As part of the onboarding with OASIS we'll engage with them on the migration of existing information assets and the set up and management of our records in their inventory system – OASIS Bridge. Any additional risks identified will be added to this assessment.

As the records to be sent off-site for archiving are typically non-current, historical records, it's not practical to consult with the relevant data subjects. The sharing of data about ICO staff is minimal and is of a nature typically expected by ICO employees. As such there will be no consultation with ICO staff.

2. 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.
- This ***must*** include the source of the data, how it is obtained, what technology is used to process it, 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, for example a new piece of software, you ***must*** explain how this technology works and outline any 'privacy friendly' features that are available.
- If helpful you can use the headings provided below to help you construct your lifecycle. You can include a flow diagram if this helps your explanation.

Data source and collection:

Historically paper records containing personal data have been created as part of the ICO's routine business operations, with data source and the means of collection being determined by the relevant ICO department. For example data could be gathered as a result of a controller paying a data protection fee or our investigations and legal teams pursuing regulatory action. When routine access to these paper records is no longer required, they can be archived off-site until they reach their retention period and a decision about disposal is made.

The volume of paper records requiring off-site storage has been steadily decreasing in recent years due to digitisation and we're not expecting the ICO to generate a significant volume of new records during the course of this contract. We do currently have approximately 2500 boxes containing records stored with our incumbent provider, and these will be moved as part of the onboarding process to be stored with OASIS.

The processing involved as part of this change of suppliers will be twofold. Firstly there will be a initial transfer of existing records from the incumbent supplier to OASIS. Secondly there will be the routine data processing as part of the supply of services for the duration of the contract. In summary:

[redacted]

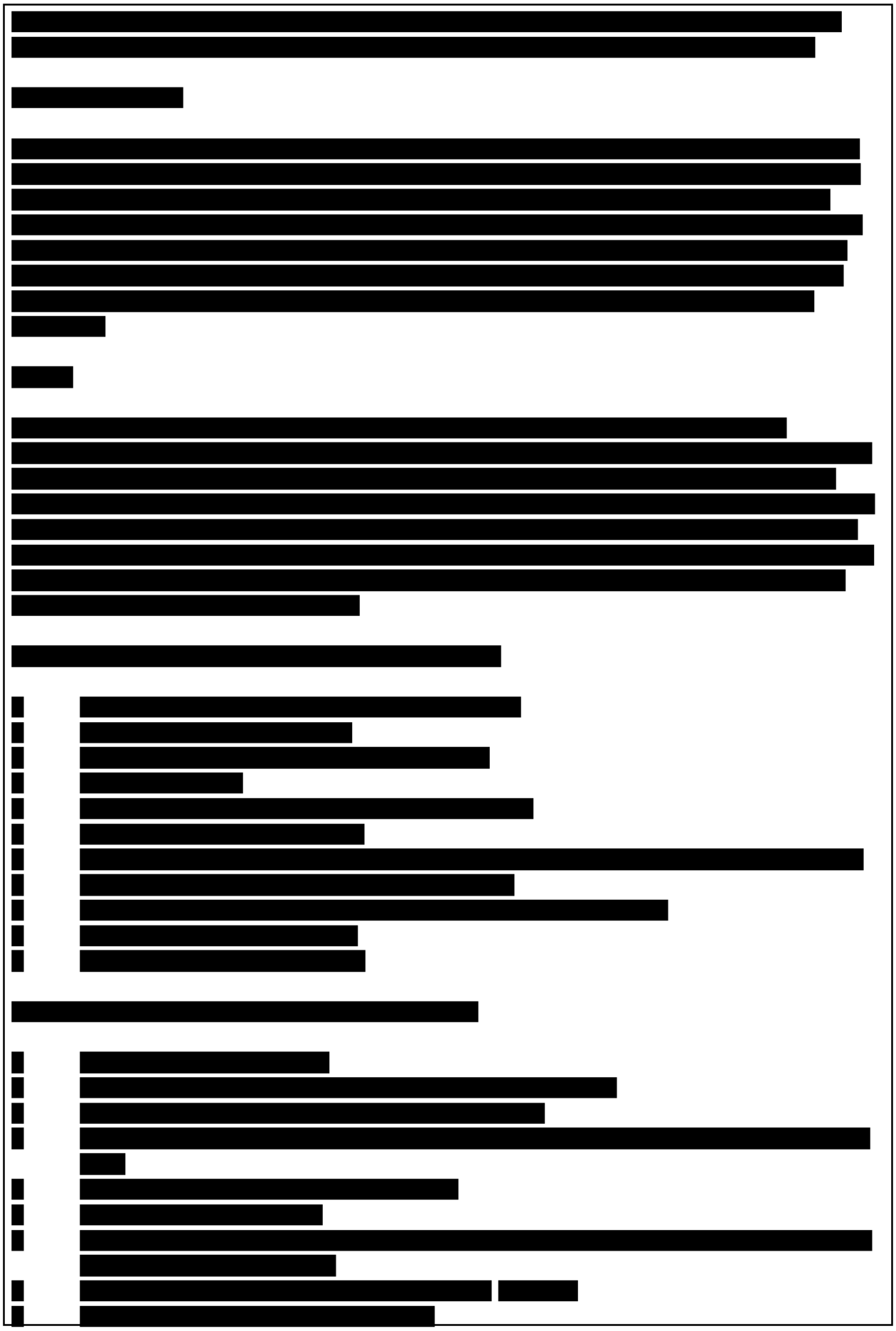
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]



[redacted]

[redacted]

3. Key UK GDPR principles and requirements

Guidance notes:

- Answering the questions in this section will help you comply with essential data protection requirements.
- You may identify specific actions that are needed and you should add these to your list of DPIA outcomes in section 6.0.

3.1 Purpose & Transparency

Guidance notes:

- In most cases you will need to communicate essential information about your data processing to your data subjects. A privacy notice is the most common way of doing this.
- You ***must*** review the existing privacy notice on the ICO website. If your data processing involves the personal data of ICO staff, review our Staff Privacy Notice on IRIS.

- You need to decide if our existing privacy notices sufficiently cover your plans. If not, you ***must*** get them updated or you ***must*** provide your data subjects with a separate, bespoke privacy notice.

Q1. How will you provide your data subjects with information about your data processing?

An update is required to our existing privacy notice/s. This required action has been added to the DPIA outcomes (see section 6.0).

Guidance notes:

- If you identified consent as your lawful basis for processing in section 1.4 you ***must*** maintain appropriate records of the data subjects consent.

Guidance Link: Consent

Q2. Are you satisfied you're maintaining appropriate records of data subjects' consent?

N/A - no processing based on data subjects consent

Guidance notes:

- If you identified legitimate interests as your lawful basis for processing in section 1.4 you ***should*** complete a Legitimate Interests Assessment (LIA). A template LIA is available here.

Guidance Link: How do we apply legitimate interests in practice?

Q3. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

N/A - no processing based on legitimate interests lawful basis

If applicable, please provide a link to your completed assessment.

3.2 Accuracy

Guidance notes:

- All reasonable steps should be taken to ensure personal data is kept accurate and up to date. Steps ***must*** be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

Q4. Are you satisfied the personal data you're processing is accurate?

Yes

Q5. How will you ensure the personal data remains accurate for the duration of your processing?

Hard copy records will reflect historical events and shouldn't require any updates. An addendum can always be added to a record if required following a data subject request.

ICO staff names and email addresses for access to OASIS Bridge can be updated by contacting the supplier as and when required.

3.3 Minimisation, Retention & Deletion

Guidance notes:

- You should only collect and hold the minimum amount of personal data you need to fulfil your purpose. Data should be retained for no longer than is needed for that purpose and then deleted without delay.

Q6. Have you done everything you can to minimise the personal data you're processing?

Yes

Q7. How will you ensure the personal data are deleted at the end of the retention period?

On an annual basis the Information Management and Compliance Service (IM&C) will use the OASIS Bridge inventory system to identify a list of files / boxes past their retention period.

The ICO department that owns the records will be provided with the relevant list of records, and are required to review and confirm whether records can be disposed of or need to be further retained. The IM&C Service will liaise with OASIS to ensure records requiring disposal are disposed of by following the OASIS destruction procedure outlined above (page 16).

Q8. Will you need to update the ICO retention and disposal schedule?

No

3.4 Security: Confidentiality, integrity and availability

Guidance notes:

- Personal data ***must*** be processed in a way that ensures it is appropriately secure and protected from unauthorised access, accidental loss, destruction or damage.
- You ***must*** make sure access to the personal data is limited to the appropriate people and ensure you're confident the processing system being used is secure.

Guidance link: Security

Q9. Where will the personal data be stored and what measures will you put in place to maintain confidentiality, integrity and availability?

[redacted]

Q10. Have you confirmed there are appropriate access controls to keep the personal data secure?

Yes

Q11. Has the cyber security team completed a security assessment of your plans?

In progress

Q12. If yes what was the outcome of their assessment?

Q13. 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.

Training will be provided by OASIS on how to utilise OASIS Bridge after commencement of the contract.

At a later date, once the contract is established, and training has been received by the IM&C service, we'll review our Off-site Storage Guidance to reflect the change of supplier and any change of process.

3.5 Accountability and governance

Guidance notes:

- The accountability principle makes us responsible for demonstrating our compliance with the UK GDPR. We do this by clearly assigning responsibilities for compliance tasks, and by maintaining relevant records relating to our processing activities and decision making.
- Your Information Asset Owner is the risk owner for any residual risk associated with your data processing and ***must*** sign off this DPIA.

Q14. Is your Information Asset Owner aware of your plans?

Yes

Q15. Will you need to update our article 30 record of processing activities?

Yes

Q16. If you are using a data processor, have you agreed, or will you be agreeing, a written contract with them?

Yes

3.6 Individual Rights

Guidance Note:

- UK GDPR provides a number of rights to data subjects when 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 ***must*** 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

Q17. Is there a means of providing the data subjects with access to the personal data being processed?

Yes

Q18. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes

Q19. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes

Q20. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes

Q21. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

N/A

Q22. Can we erase the personal data on receipt of a request from the data subject?

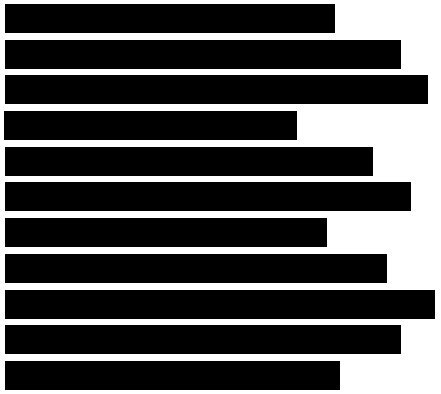
Yes

4. Risk assessment

Guidance Note:

- You ***must*** use the table below to identify and assess risks to individuals. You can add as many rows to the table as you need.
- **Remember:** we have an **Averse** risk appetite towards compliance risks (see our Risk Management Policy and Appetite Statement for more information).
- You ***must*** identify measures to reduce the level of risk where possible.
- In the risk description column, you can select from common risks to individuals in the drop-down list provided. Alternatively, you can enter your own risk descriptions if preferred.
- **The drop-down list is not exhaustive**, and you must identify and assess risks within the context of your planned processing.
- Mitigation measures can be existing, i.e. they're already in place and reduce the risk without any further action being needed. Or they're expected i.e. these are additional measures you intend to take before the data processing begins in order to further reduce risk.
- Use the risk scoring criteria in Appendix 1 to score your risks. You ***must*** score both the impact (I) and probability (P). The expected risk score total is the result of I multiplied by P.
- When considering probability, you should score based on all your mitigation measures having been implemented in order to get an *expected* risk score.

Risk description	Response to Risk	Risk Mitigation	Expected Risk Score		
			Impact	Probability	Total
Example: *Access controls are not implemented correctly, and personal*	Choose an item.	*Existing mitigation: We have checked that the system we intend to procure allows us to*	3	1	3 - low

data is accessible to an unauthorised party.			*set access permissions for different users.* *<u>Expected mitigation</u>: 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.*			
1.	**Access controls are not implemented correctly and personal data is accessible to an unauthorised third party**	Treat: this risk is being reduced by management action such as implementing controls or tackling the cause	Existing mitigation:  Expected mitigation: We will discuss specific access needs for OASIS Bridge as part of the contract on-boarding and ensure	**3**	**1**	**3 - low**

			principle of least privilege is implemented.			
2.	**Personal data is retained for longer than is necessary by us**	Tolerate: this risk is being accepted	Existing mitigation: IM&C service provide oversight of the destruction process for hard copy records in off-site storage, with annual reviews taking place and action taken to progress destructions. Retention reviews are diarised in the IM calendar for the end of each financial year. [redacted] Expected mitigation:	**2**	**2**	**4- low**
3.	**Security controls are inadequate for protecting personal data resulting in a loss of confidentiality, integrity or availability.**	Tolerate: this risk is being accepted	Existing mitigation: [redacted]	**3**	**1**	**3 - low**

			Expected mitigation: Cyber Security supplier assessment is pending and any required actions will be followed up.			
4.	**Individuals are unable to exercise their rights in relation to our processing**	Tolerate: this risk is being accepted	Existing mitigation: Agreed SLAs with OASIS should ensure timely recall of hard copy records from storage. [redacted] Expected mitigation:	**3**	**1**	**1 - low**

5. Consult the DPO

Guidance Note:

- Once you have completed all of the sections above you ***must*** 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 then proceed with completing the rest of this template.

	Recommendation	Date and project stage	Project Team Response
1.	In section 2. Personal data lifecycle, under Technology used for the processing (on page 13) it says: [redacted]		**Accept** Any comments: [redacted] If rejecting DPO recommendations explain why:

2.	[redacted]	Planning	**Accept** Any comments: [redacted] If rejecting DPO recommendations explain why:
3.	Clarify that retention reviews are diarised in IM&C Service team calendar for the end of each financial year.		**Accept** Any comments: Expected mitigation for Risk 2 updated. If rejecting DPO recommendations explain why:
4.	Categies of data in 1.3 could do with some more examples, financial records, legal files, special category data, conviction and health data (we have enforcement cases where there is information about s 55).		**Accept** Any comments: "including special category and criminal offence data." Added to description of data categories in 1.3. If rejecting DPO recommendations explain why:

5.	Section 1.5 - for necessity recommended to stay away from limited space and focus on the rest, more suitable security, shredding and environment control.		**Accept** Any comments: This sentence opening has been removed from 1.5: "Due to limited physical space in ICO premises" If rejecting DPO recommendations explain why:

6. Integrate the DPIA outcomes

Guidance Note:

- Completing sections 1 to 5 of your DPIA will have helped you identify a number of key actions that you now ***must*** 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 DPOs team.
- 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
Update Privacy Notice	Contract commencement – 18/11/2023.	SJ/IM	
Review Cyber Security Service assessment when received for any risks or actions required.	ASAP when received.	SJ/IM	11/09/2023 – Cyber Security Service advised *"Security opinion is "**met**". This reflects our view that the Supplier has met all our minimum requirements".* No change to risk assessment as a result of this outcome.
Review our Off-site Storage Guidance	Within 3 months of contract commencement.	SJ/IM	
Update ROPA	Contract Commencement – 18/11/2023	SJ/IM	

Agree and implement appropriate access controls for OASIS Bridge	During on boarding.	SJ/IM	

7. Expected residual risk and sign off by the 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 ***must*** consult the ICO as the regulator by following the process used by external organisations.

The expected residual risk to data subjects from this processing operation is assessed as being low and can be accepted.

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.
- Once your DPIA has been signed off it is complete. You should review it periodically or when there are any changes to your data processing.

IAO (name and role)	**Date of sign off**
Mike Fitzgerald – Director of Digital, IT and Business Services	24/7/23

8. DPIA change history

Guidance note:

- You should track all significant changes to your DPIA by updating the table below.

Version	Date	Author	Change description

V0.1	19/7/2023	Steven Johnston	First Draft
V0.1	24/07/2023	Steven Johnston	DPIA Forum recommendations added to 5.0. Response added to recommendations and summary of residual risk completed.
V1.0	24/7/2023	Mike Fitzgerald	IAO sign off
V1.1	11/09/2023	Steven Johnston	Cyber Security Service opinion received and action marked as complete in 6.0.

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 (e.g. 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.