Data Protection Impact Assessment

Document Name	DPIA - ICE Infrastructure - Safe and Stable
Author/Owner (name and job title)	Jan Milbourne, Project Manager. Jonathan Wren, Lead Project Coordinators.
Department/Team	Project Management, Office & Digital and IT
Document Status (draft, published or superseded)	Draft
Version Number	V2.1
Release Date	
Approver (if applicable)	
Review Date	
Distribution (internal or external)	Internal

Privacy by design at the ICO

Welcome to the data protection impact assessment process. You should use this every time you want to implement or change a product or process. 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/using, why, where it will be stored and for how long, who will access it and why, how it will be kept secure and whether it's being transferred to any other country.

Your Information Asset Owner (your Director) is ultimately responsible for managing any residual risk once you have completed any mitigations to the risks you identify.

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 to what you are 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 process

You should 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.

Step 1

- Complete DPIA screening assessment. If you conclude that you do not need to complete a DPIA then you must make a record of your decision.
- If you do need to complete a DPIA then start completing the paperwork and notify the IM Service. Depending on what you're doing, the DPIA might need to be reviewed by the DPIA forum. You need to ensure the paperwork is sufficiently detailed, accurate and thorough before the forum is able to review it. This particularly applies to your descriptions of the processing activities you are proposing and how any associated technology works alongside it.
-

Step 2

- The forum is likely to provide advice and recommendations. You should consider this advice. If you decide not to follow it, then you must document your reasons why. If you do follow it, then most actions will need to be completed before go live. For example, updating privacy information or refining access controls.
- The forum is able to escalate risks to our Data Protection Officer and/or Risk and Governance Board if it is not comfortable with the processing activity being suggested or wants sign-off on advice.

When you have completed the DPIA paperwork and any actions, accepting that you might need to revisit it, you should get sign-off from your IAO before your product or service goes live.

If there are residual risks that your IAO would like to discuss, they can contact dpo@ico.org.uk. That discussion can be escalated to our Data Protection Officer and/or Risk and Governance Board if required.

Guidance for completing this template

Complete this Data Protection Impact Assessment (DPIA) template if your 'Screening Assessment - do I need to carry out a DPIA?' indicates a high risk to individuals. If you are 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 will not be able to continue with your plans without changing them, or at all.

Guidance notes are included within the template to help you with its completion- just hover your mouse over any blue text for further information.

The Information Management Service is also available for further advice and support. Please keep in mind our service standards if you require advice.

1. Process/system overview

1.1 Ownership

Project Title:	ICE Infrastructure – Safe and Stable
Project Manager:	Jan Milbourne
Information Asset Owner:	Mike Fitzgerald, Director of Digital, IT and Business Services
Data controller(s)	ICO
Data processor(s)	Microsoft

1.2 Describe your new service or process

In this DPIA, we are assessing the privacy issues around the work undertaken as the first phase of the ICE Implementation project – safe and stable. In this phase we will migrate the ICE registration infrastructure and storage location of data from the ICO's on premise server farm to the cloud in the ICO's Azure tenancy. Additionally, we will be upgrading the software (Dynamics CRM) to the most up to date and supported On Premise version. This will not effect existing ICE Reg functionality.

This work has been sponsored by Digital & IT to move our ICE platforms to stabilise the system in terms of performance and address risks surrounding unsupported and end of life technology. And to also provide a stable environment for future development work. This work will contribute to two Digital and IT objectives, i) to migrate from the on-premise WH data centre to the cloud and ii) to move a step closer to being able to utilise 'Ever green'

supported platforms PaaS and SaaS, removing the need for ICO to be experts on Infrastructure, Servers and maintenance.

Background
In January 2017, a PSIA was approved for the migration of ICO core network services to an externally hosted service, Office 365.

In October 2018, a DPIA was approved for project 0097 "Core Cloud Services – Document Storage". That DPIA covered the implementation of the use of Office 365 for Document Storage and addressed the additional privacy considerations of the use of Office 365 for the storage of ICO documents with the security classification "official" (including official sensitive).

In November 2020 a DPIA was approved for SP online for casework documents, the hosting and storage of documents will not change as a result of this work, therefore this DPIA does not need to be updated and can be referenced for this work.

In June 2022 a DPIA was approved for the ICE Infrastructure – Safe & Stable migration of the ICE Registration system.

The CRM server farm has been developed to support the maintenance of the public register and associated collection of fees as well as DP and FOI complaints, advice, information requests and personal data breaches.

Since ICE registrations was delivered in 2013 the register has grown considerably, as has the ICO, and the number of staff using ICE. Though updates have been made along the way, ICE is unrecognisable from what was delivered eight years ago, and a replacement of the infrastructure that ICE sits on is required.

Projections show us that this pressure will continue to increase over the coming months and we will be dealing with unprecedented volumes of email and transactions as the current rate of growth continues for both registration and casework. We have also seen a notable decrease in performance over time, with performance issues being logged regularly, as well as evidence of the system working under pressure, with system jobs not completing in allocated times and servers logging warnings and errors.

To assist with this programme of work, we undertook a short discovery to explore and agree the approach for the future of the ICE infrastructure. This is a large programme of work and we recognise that this will need to be completed in phases, with the most urgent need of a resilient and scalable systems being prioritised and delivered in phase 1 and 2.

Phase 1 will migrate ICE registration to its own server farm within the ICO tenancy. Until this phase is completed and signed off, ICE 360 will remain on premise.

Phase 2 will replicate the server farm built in phase 1, but as a separate server farm within the ICO tenancy for ICE 360.

This allows us to meet the objectives for resilient and performant systems, by separating at application layer.

In these phases other connections into these applications, functionality and business processes will remain the same.

V.2 Update – Phase 2 update – Casework migration

Following the successful deployment of the ICE registration infrastructure upgrade in August 2022, we will now replicate those steps for ICE360 Casework. ICE360 infrastructure and storage location of data will be migrated from the ICO's on premise server farm to the cloud in the ICO's Azure tenancy and upgrade the software (Dynamics CRM) to the most up to date and supported on-premise version. This will not effect existing ICE 360 functionality but development work will focus on enabling existing functionality to work on upgraded version of CRM.

1.3 Personal data inventory - explain what personal data is involved

Categories of data	Data subjects	Recipients	Overseas transfers	Retention period
All information within our care relating to registration processed through ICE registration:- Organisation details – name, address, any trading names Main Contact details including name, phone number, email and postal address Registerable particulars - sector, subsector and nature of work Information about the fee tier they are paying – i.e. number of staff and turnover Data Protection Officer (DPO) – name, phone number, email and postal address, preferences about publication of details. Payment details for the processing of fees – for direct debit payments this will include account number	ICO Staff Enquirers Main contact for registered organisations including sole traders. DPO contact for register organisation	ICO: Access to registration system through CRM using role based privilege	UK only	Retention will be as described in the ICO Retention Schedule.

and sort code; for card payments these details will not be included				
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	Retention will be as described in the ICO Retention Schedule. Further details of retention on post go-live are in the recommendations below.

1.4 Identify a lawful basis for your processing

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 necessary to process this personal data

We are collecting the minimal personal data required and relevant to the completion of the regulatory activity of the ICO including the following tasks:

- Collection and management of information about organisations (including contact details of DPO & contact points and financial information) required to pay a fee under the DP regulations 2018;
- 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.

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 (phase 1). SOR Ref: 000067 – ICE Stablisation 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.

As there is no change to the data being collected or the purposes for which it is being processed as part of our registration or casework functions, we do not intend to consult more widely.

We will review this DPIA again in full before we make the correlating changes to upgrade ICE Casework to a safe and stable platform (phase 2); although we do not intend to make any changes to the data being collected or the purposes for which it is being processed.
Nov 2022 - DPIA reviewed and updated in preparation for Casework migration.

We will complete a further full DPIA for any phases of the ICE transformation beyond this.

2.0 Data flows

2.1 Provide a systematic description of your processing, from the point that the data is first collected through to its destruction.

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

As stated in 1.2, the initial phase of this work is to remove risk and secure the safe and stable platforming of the CRM Dynamics infrastructure supporting our ICE (Registration and 360) applications by upgrading to the latest supported technology. Under phase 1 and 2 the aim is to reach a safe and stable infrastructure for our Registration and Casework ICE applications and their associated ecosystems.

The plan, as proposed in the technical roadmap, is to achieve this by upgrading the CRM dynamics for each app to their current versions, from 8.2.5.4 to 9.1 and to have these hosted on a IaaS server farm. This will be achieved via a "leapfrog" approach where we use staging servers to upgrade our CRM databases to version 9.1 ("hopping" through two staging environments as version 8.2.28.11 and 9.0.3 on the way). Taking this approach will mean that the upgrades are applied one at a time. Additionally through this course of work, the SSIS servers and Integration Services web services will be moved from SQLP server and to an IaaS virtual machine.

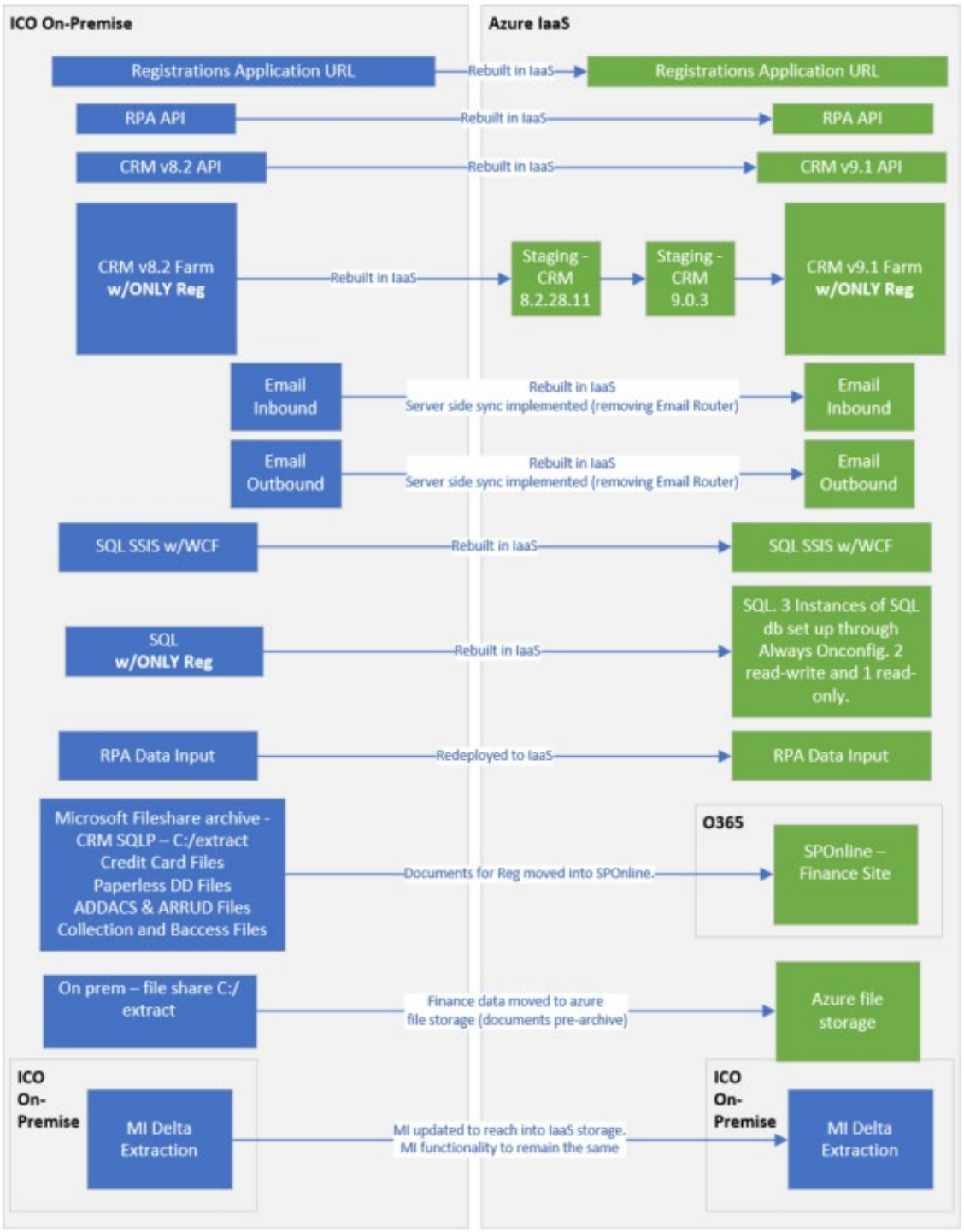
Once we've imported our organisation into upgraded version, data left behind on servers will be retained for a period until we are satisfied that we have no unexpected issues in the Live environment and will then be deleted. The exact length of this period is yet to be defined. The deletion will involve the following steps:

- Disable and delete old Registration organisation,
- Database for old Registration only,
- Confirm that old file storage locations for Reg don't contain any remaining information e.g. letters, paperless DDs.
- Disable and delete old Casework organisation,
- Deletion of the database for old Casework

Through the course of these phases of work, the type of personal data collected, the purpose of our processing, the source of the data, the nature and scope of processing are unchanged by the migration of the servers to infrastructure as a service within the ICO Azure tenancy.

As well as hosting the ICO ICE production platforms, the changes made to our pre-production, test and development environments will also be based on the same CRM server farm design, to make the development, testing and deployment of new functionality easier, safer and faster in the future.

The diagram below provides detail on information flow for the replacement of on-premise servers with infrastructure as a service.



V.2 Update – Phase 2 update – Casework upgrade
Migration for casework will have the same impact on data flows as described in the diagram above for Reg with the exception of RPA steps which are not relevant for casework.

Casework documents will continue to be stored in SharePoint Online (crmdocuments) and will not be impacted by this migration.

3.0 Key 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?

As there is no change to the data being collected or the purposes for which it is being processed as part of our casework or registration functions, we do not to communicate any changes. In the stages outlined in this DPIA, although we will be moving towards IaaS, the data will still remain within the ICO Azure tenancy, therefore there is no change in the relationship with Microsoft. Before a full move up to the cloud is undertaken, a further DPIA will be submitted for this change.

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

Data can easily/quickly be updated as required and reflected immediately within the ICE applications. Where this relates to published information on the pubic register, this is updated each morning.

Additionally, we will retain the provisions already in place to remove information as appropriate.

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

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?

Data held in line with existing retention schedule.

Data is destroyed in line with disposal procedure and automated where possible.

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: ICE Registration, ICE 360, SharePoint online.

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, training or instructions required for staff to operate within ICE as functionality remains as- is during phase 1 and 2. It is purely a change to where the servers are hosted and upgrades to the application software to most supported versions.

Accountability

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

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

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*	*2*	*6 - medium*
1. System not secure Leading to unauthorised access, misuse of data or data being stolen by a third party from the cloud infrastructure	~~Avoid~~ Amended to: Reduce. (See recommendation 8)	Existing mitigation: Careful assessment of the cloud service provider's security measures has taken place. Expected mitigation: Regular updates regarding the provider's appropriate security measures should be available. Also regular security patching of systems applied.	4	1	4 - low

2. Data transferred overseas to a jurisdiction that does not adequately protect data subject rights	~~Reduce~~ Amended to: Avoid (see recommendation 9)	Existing mitigation: A contractual agreement has been set up with the cloud service provider to agree how the service will be managed. As documented in technical plans, we are entrusting the provider to host our data via data centres in the UK. Data will not be transferred, shared or held elsewhere unless otherwise agreed.	4	1	4 - low
3. Data subjects unable to exercise their rights, such as access their data held in the cloud infrastructure	Reduce	Existing mitigation: Internal processes for retention/removal/correction of data will remain the same. Contract in place and guarantees of the cloud service provider's availability, confidentiality and integrity have been reviewed.	3	1	3 – low
4. Data processor fails to process data in accordance with our instructions	Reduce	Existing mitigation: Contract in place Expected mitigation: Frequent liaison with provider and monitoring of	3	1	3 - low

		performance will take place to ensure compliance with our instructions.			
5. Unauthorised destruction or loss of data	Reduce	Existing mitigation: A contractual agreement has been set up with the cloud service provider to agree how the service will be managed and the appropriate security measures in place to ensure the availability, confidentiality and integrity of data. Expected mitigation: Data will be backed up in the event of destruction or loss of data.	3	1	3 - low
6. Data is kept for longer than is necessary (by us and processor)	Reduce	Existing mitigation: Application of ICO's relevant retention policies will be programmatically applied to data held in ICE. Alerts are configured to notify when deletion jobs fail. Expected mitigation: On premise data will be decommissioned as part of this stages covered by this project, as post go-live of both applications will be in the ICO's Azure tenancy. The deletion will involve the following steps: • Disable and delete old Registration organisation,	2	2	4 - low

		• Database for old Registration only, • Confirm that old file storage locations for Reg don't contain any remaining information e.g. letters, paperless DDs. • Disable and delete old Casework organisation, • Delete database for old Casework Further information of these steps is outlined in 2.0.			
7. ICO / Kainos not configuring new servers correctly	Reduce	Existing mitigation: contract in place with data processor to ensure that ICO security standards are maintained. Comprehensive design documentation produced for the configuration of all servers and components, held in LLD, HLD and design document, all submitted to ICO cyber team for SOR. We have captured lower level detail in wiki's for playbook and roll-out plans. Testing carried out throughout the process of deployment, including in test environment before decision taken to deploy to Live. Further testing around integrity of data before import to live is finalised. Expected mitigation: Back-ups of existing database retained. Further testing of the sql server failover completed successfully for both ICE	3	1	3 (low)

		Registration and Casework. Seamless failover between servers provides resiliency and stability.			

5.0 Consult the DPO

Guidance: Submit your DPIA for consideration by the DPIA Forum. The process to follow is here.
Any recommendations from the DPOs team will be documented below and your DPIA will be returned to you. You should then record your response to each recommendation.

	Recommendation	Date and project stage	Project Team Response
1.	**Sections 1.1 and 1.3 -** it was flagged that Kainos will have a role to play in this project and are likely a data processor and recipient. Microsoft will also be a recipient so please also include them in your data inventory. You should consider the role of Kainos within this DPIA, update it accordingly and consider any risks associated with their involvement.	Planning 21/03/2022	Project team happy to add Kainos as a data processor in 1.1 and recipient into the data inventory section in 1.3. Although no data will be sent to Kainos, as part of the work they will have limited access to our live systems in order to aid the roll-out. Also happy to include Microsoft on the basis of the ongoing IT support they provide. Risks have already been covered, as these were written with the consideration that Kainos would be contracted to assist with work and that Microsoft are an ICO IT partner.
2.	**Section 1.3 –** specific retention periods should be identified and documented in this DPIA to ensure these are understood and implemented correctly by the project team. Relevant retention periods can be found in Part 8 of the Retention and Disposal Policy.	Planning 21/03/2022	The specific retention periods relating to ICE Reg /Casework are as follows: 8.18 – Data Protection Fee Information – Electronic Records – 2 years. 8.19 – Data Protection Fee Information – Paper Records – 2 years. 8.20 – Data Protection Fee Information – Digital Mailroom Scan (copy of paper records) – 9 months.

			8.21 – Digital Scans of Direct Debit Mandates – 6 years. 12.1 Completed Advice cases – 2 years 3.7 Completed Information Rights cases – 2 years 8.8 PDB No action/Informal action – 2 years 8.9 PDB Reg Action Taken/Investigation – 6 years 8.15 & 10.6 PDB NIS/eIDAS – 6 years 8.2 Completed Complaints Cases - 2 years 9.1, 9.2 & 9.3 All Civil & Criminal Enforcement Cases (partial cases – 2 years. Retention managed via Crimson case) 14.3 Complaints CCA – 6 years
3.	**Section 2.0 – data flows** A firmer commitment on the deletion of data on the old servers is required to ensure this information isn't retained longer than necessary. Can you be more specific on the time you'll be keeping the old servers for and who is responsible for reviewing, making the decision to destroy and then actioning this? We'd recommend you commit to reviewing whether old servers are still needed every 3 months and assign ownership for this task until destruction actually takes place. Additionally this is unclear and could do with rewriting: *"data left behind on servers will be retained for a period until we are satisfied that we have no unexpected issues"* – is this just the backup copy or is some data not being migrated? Also there is mention of two staging servers and it's unclear if data is	Planning 21/03/2022	There is a difference between the retention details for information left on the Old Servers and the Hopping Servers. See details below: **Old servers** • A full copy of the live Reg /Casework data, all back-up history (for 2 days) as of the point of go-live. • The current finance archive files are on the file share. Archive files from the last 6 years will be moved manually from the file share into the new infrastructure. New archive process will move files to SP online using PowerShell script. The retention on this site will be for 6 years based on original creation date. • Due to the relationship between the Old Reg and Casework versions of CRM, the Old Reg will be deactivated and made inaccessible to users after go-live (once the data migration back-up has completed). 1 copy of the back-ups will be kept in the meantime, before the deletion post

	being migrated twice so there may be two copies that will need to be deleted. Lastly the diagram included adds little and isn't a data flow of personal data so could be removed.		casework go live. Old Reg mailboxes and will also been be shut down during the period including Old Reg router queues. • Servers and SQL database to be decommissioned post casework go-live. • 1 month after full sign off (including casework go-live) we submit a change request for the deletion of the data from the legacy servers and databases. **Hopping servers** • Dry runs of the migration process using the hopping servers have already begun. Full copy of the live data will remain on each of the 3 hopping servers, during go-live weekend. Post-go live these will be deleted. This is anticipated to be a quick process so will be actioned once the new live system has been signed off and handed over to users. Comprehensive post go-live documentation has been produced including checklist of what needs to be deleted including: o Crm logs (from org import) o App data on each of 3 crm severs o Organisation from deployment manager for each server o Database on each server. o Back-ups o Empty recycle bin • The same hopping severs can be reused for Reg and Casework. In order to save time and

			expense, we can delete the data from the hop servers after Reg go-live and then power them down until they are ready for the casework deployment.
4.	**Section 3.0 Q5-7 Accuracy –** This section needs to focus on the accuracy of the migrated data rather than how ICE is kept up to date. For example how will you ensure the data that ends up on the new server is the same as the old? What steps can be taken to confirm the migration has been successful and data hasn't been corrupted? Will there be restrictions placed on using the systems (i.e. taking them offline) whilst the migration occurs so there is no conflict between the two servers?	Planning 21/03/2022	There a couple of different points to address here which relate to data integrity: 1. The process being followed for the ICE infra upgrade involves a back-up and restore as opposed to a more traditional migration. This means that same database is being upgraded (and moved between servers via the "hop" process) rather than being migrated into a new database. This approach was selected specifically because it would achieve a safe and stable platform for ICE whilst still being a less risky process for a technical perspective. 2. There are also measures in place to alert the team during the process if there are issues during the back-up and restore. If this process fails, then an alert has been set in SQL. The import into the new version is done via the CRM deployment manager, and an alert is given here if this process fails (with an attached log file). 3. Additionally, the Go-live plan will include measures for ensuring and testing data integrity. This will include: a. Technical process for migration and upgrade of database has been successfully tested in the Dev and Test environments. And a dry-turn migration

			into new the live subscription has been completed. b. Cross checks will also be performed during the dry-run of the upgrade in order to minimise risk to data integrity on go-live weekend. c. Upon go-live, SQL queries to compare counts in old and new environments, including: i. High level record counts.sql - gives a count of records for the main ICE entities; ii. Entity breakdown counts.sql - gives a breakdown count for major entities; and iii. Time and date stamp of last item added to the database in Old and New Reg/Casework. d. Checks on email servers pre and post go-live; e. User testing will also be conducted on go-live weekend.
5.	**Section 3.0 Q9 –** again retention periods need to be clearly defined so the project is clear as to when information should be deleted and when. Please also clarify to what extent deletion isn't automated and outline your approach to any manual deletions as this hasn't been covered.	Planning 21/03/2022	See details in recommendation 3. Old Reg server data will be deactivated until it can be safely deleted with the Old Casework following casework go-live. Manual deletion of data applies to data we are hopping because we want to control when this happens. i.e. it will be reviewed every 3 months.

			Finance records (referenced in section 6 below) will be held in CRM for 14 day and the automatically transferred to SharePoint, where they will be retain for 6 years from created on date before automatic deletion.
6.	**Section 3.0 Q11 –** SharePoint online is mentioned here but the significance of this isn't explained in the DPIA. Why is this relevant to this project? Please add more detail.	Planning 21/03/2022	As detailed in the data flow diagram, 4 categories of DP Fee finance information will be moved from the MS fileshare archive on CRM SQLP to a finance SharePoint online site. These include: Credit Card Files Paperless DD Files ADDACS & ARRUD Files Collection and Baccess Files
7.	**Section 3.0 Q14 –** similar to recommendation 4 the focus here needs to be on the migration which is the scope of this DPIA not how ICE is used. Please consider whether any training, policies etc. are required for the build and transfer to the new servers.	Planning 21/03/2022	Familiarisation session ran with DP Fees group and team managers concerning a few minor visual differences with the screens. This session was recorded and has been shared with Reg GM and Team managers. Familiarisation sessions run for ICE360 Ambassadors, recording of demo and release note also shared though differences are few and all are superficial, 'look and feel' changes.
8.	**Section 4.0 risk assessment –** Risk 1 isn't being avoided as you've detailed mitigation steps you're planning to take. Please amend risk response to Reduce.	Planning 21/03/2022	Agreed by project team. Section has been amended.
9.	**Section 4.0 risk assessment** Risk 2, overseas transfer.	Planning 21/03/2022	Agreed with comment in last paragraph, the risk has been changed from reduce to avoid, as we would think it is best if the DPIA reflects the fact that we have

	No overseas transfer has been detailed in the DPIA (see your data flow at 1.3) so it's unclear why this risk has been included. If there is an overseas transfer you need to provide more detail about where data is being transferred to and consider appropriate mitigation and any safeguards to make the transfer lawful. If there is no transfer either remove the risk or change your risk response to avoid; you've avoided the described risk by selecting a supplier with UK only data storage.		avoided this risk by ensuring that our supplier will only hold data in UK based data centres.
10.	**Section 4.0 risk assessment** Risk 5 destruction or loss of data: More detail is needed regarding the planned backup process to achieve the low probability score. For example what would be the process for backups, has this been tested so you're confident recovery works?	Planning 21/03/2022	Post-go live, backups will be stored in Azure VMs and no longer on the same sever as the database. SQL backups are completed using Azure Backup for SQL VMs, with the backup data being held in an Azure storage account (which supports up to 30 days worth of backups). According to non-functional requirements("restore data up to 5 calendar days prior to current day") set as 6 days. They will be stored in UK south or west data centre (tbc). Log back-ups of SQL are taken every hour (MS functionality supports up to 30 days worth of backups).
11.	**Section 4.0 risk assessment**	Planning 21/03/2022	See further details added in comments on recommendation 3. Due to the Old Reg and casework

	Risk 6 – revisit mitigation as deletion steps aren't clear. Additionally as per recommendation 3 if there's no clear plan or commitment in place to review when on premise data will be deleted then your probability score for this risk is currently likely higher.		existing on the same server, then after Reg go-live, Old Reg will be deactivated and inaccessible to users. The deletion of the data will be 1 month after the sign off post casework go-live when the servers and SQL database can be decommissioned. Change requests will be submitted in order to delete the data from Old Reg and then the underlying database the following week.
12.	**Section 4.0 risk assessment** An additional risk is recommended for ICO / Kainos not configuring new servers correctly.	Planning 21/03/2022	Project team agree with recommendation to add in further risk for "severs configured incorrectly". Please see the further details below, risk now added to table above (risk no. 7): "Existing mitigation: contract in place with data processor to ensure that ICO security standards are maintained. Comprehensive design documentation produced for the configuration of all servers and components, held in LLD, HLD and design document, all submitted to ICO cyber team for SOR. We have captured lower level detail in wiki's for playbook and roll-out plans. Testing carried out throughout the process of deployment, including in test environment before decision taken to deploy to Live. Further testing around integrity of data before import to live is finalised. Expected mitigation: Back-ups of existing database retained. Impact: 3 Probability: 1 Total: 3 (low)"

6.0 Integrate the outcomes back into your plans

Guidance: Identify who is responsible for integrating the DPIA outcomes. The outcomes include any expected mitigation you need to take as identified in your risk assessment and any further actions resulting from the DPOs recommendations.

Action	Date for completion	Responsibility for Action	Completed Date
Deletion (decommissioning) of backed up data of information on old servers.	3 month rolling review period post-go live.	Head Digital & IT Architecture	
Testing of deployed systems (and post patching testing)	On-going	Project team	Phase 1 post go-live: 02/09/22.
Regular security updates/patching – strategy to be documented in collaboration with ICO Infra.	On-going	Project team & ICO infra team	
Performance monitoring	On-going	Project team (ICO and Kainos)	

7.0 Expected residual risk and sign off

Guidance: Summarise the expected residual risk below. 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 (e.g. 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.

This is a new way of upgrading ICO live systems, so there are still some residual risks that we may encounter unexpected issues during the process, in the most extreme of scenarios this would result in a loss of service for the business as core ICO systems would be down.

However, there multiple layers of mitigation in place to prevent such a scenario from occurring:

Firstly, we have produced comprehensive documentation on configurations of the components required in order to host the upgraded version of ICE Reg.

Secondly, throughout the process of creating and configuring the new server farms project team (including ICO and Kainos) have worked collaborative with internal ICO networking and infrastructure teams, as well as the specialist Kainos DBA and security teams.

Thirdly, technical testing of environments and process is being carried out throughout the project cycle including the technical testing of environment configurations, testing the processes for upgrading CRM and dry-runs of upgrading the live environment using the hopping servers. Each of these stages allows us to identify issues and either fix or adjust the design accordingly if necessary. Extensive documentation is being produced from these sessions including the Playbook and wiki docs for all processes in addition to go-live plans.

Additionally, manual testing (including smoke and regression testing) is being conducted in multiple environments (Dev & Test). Reported bugs are being fixed and re-released for further testing on weekly schedule.

Finally, during the process of deploying the upgraded ICE Reg system, we will for a period of time keep a back-up of the data on the old servers (and review this every 3 months) before a decision is taken to decommission the old servers.

Though there may still be unknown residual risks to the project due to the approach we are taken to upgrade our ICE Reg to a safe and stable platform, we believe that the layered approached outlined above prioritises the security of ICO assets throughout the process.

7.1 IAO sign off

IAO (name and role)	Date	Project Stage
Michael Fitzgerald – Director of Digital, IT and Business Services	17/5/2022	Evolutionary development/Delivery – ICE Registration
Michael Fitzgerald – Director of Digital, IT and Business Services	8/12/2022	Evolutionary development/Delivery – ICE 360 Casework

8.0 Change history

Guidance: To be completed by the person responsible for completing the DPIA and delivering the system, service or process)

Version	Date	Author	Change description
V0.1	01/03/22	Jan Milbourne	First Draft
V0.1	22/03/2022	S Johnston	DPIA forum recommendations added to 5.0.
V1.0	05/05/2022	Jan Milbourne & Jonathan Wren	Responses to DPIA forum added to 5.0. Also 7.0 and 7.1 completed.
V2.0	30/11/2022	Jan Milbourne & Jonathan Wren	Reviewed and updated in preparation for ICE360 Casework migration.
V2.1	07/12/2022	Jan Milbourne	Updated following DPIA Forum recommendations: a) Risk 7 addition of mitigation detail re sql server failover (from Reg upgrade lessons learned) b) Clarification of 2.0 "Database for old Casework" should read "Deletion of database for old Casework"

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: 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 data 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