Data Protection Impact Assessment (DPIA) template

You should complete this template where there is a new (or significant change to an existing) service or process that involves the processing of personal data (whether digital or hardcopy). When dealing with an existing process, service or system **only the change should be impact assessed.**

You should start to complete the assessment at the very start of your work and plan to revisit it throughout the lifecycle. Please note that the outcome of the assessment could affect the viability of what you are planning to do. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

The Information Management and Compliance team is available to assist and advise on completing this template. If required this template should be submitted to the DPSIA forum for their consideration and recommendations. For assistance or to submit a DPIA for consideration email informationmanagement@ico.org.uk.

Determining what to complete:

You should complete all aspects of **sections 1 and 2** of this form to determine if a DPIA is required.

If you answer **no** to all screening questions in section 2 a full DPIA isn't required and there is no need to complete the additional sections of this assessment (see Approval).

If you answer **yes** to any of the screening questions in section 2 you **must** complete a full DPIA. You should complete all sections of this form except for 6.3 and 6.4 (see Approval).

Approval:

If a full DPIA isn't required. Inform your IAO and retain a copy of the partially completed form (sections 1 and 2) within your department.

If a full DPIA is required, the completed form **must** be submitted to the DPSIA Forum for their consideration and recommendations.

Once complete you should send this to informationmanagement@ico.org.uk

1. Process/system overview

1.1 Summary

Guidance: For projects please provide the following key details. Non-projects should provide a key contact who is responsible for delivering the system or process.

Project ID:	BDG
Project Title:	Electronic legal bundles
Project Manager:	Raymond Wong

1.2 Synopsis

Guidance: Provide a summary of the process or system including any relevant background information and the key aims/objectives that the system or process must achieve. There is no need for a detailed discussion of data or data flows – these are covered later in the assessment.

The ICO has a well-established process for producing and distributing legal bundles in hard copy format. Discussions took place as far back as 2017 about producing and distributing this information electronically. With new ways of working being developed to cope with the Covid-19 pandemic the Tribunal will require electronic bundles as will other courts. This DPIA covers the risks to the ICO arising from moving to electronic bundles and the risks of using the Bundledocs Ltd Software as a Services solution. It should be noted that the sources of information that make up a bundle, who this is shared with and the basis of our processing remains as it always has; the only change is how we prepare the bundle and the media we distribute.

Bundledocs is required to give both legal teams in the Regulatory Enforcement Directorate the ability to create electronic hearing bundles that are an essential part of the Freedom of Information appeals process, appeals pursuant to the Data Protection Acts 1998 and 2018, the criminal enforcement process and any other ad hoc civil litigation the enforcement legal team is required to respond to.

Both teams were producing paper hearing bundles prior to the onset of Covid-19 and in order to keep operating outside of the office it has been necessary to find different ways of working. This has highlighted the need for electronic bundles and Bundledocs has been identified as a suitable programme that produces bundles that fit the requirements laid down by the Information Rights Tribunal.

The information used to create the bundles is already stored in CMEH and SharePoint and anything additional (in respect of FOI Appeals) is provided by email by the Appellant via the Tribunal. Once created, the bundles will be stored in SharePoint and only provided to the relevant court/tribunal, Appellant/Defendant and any party joined to the proceedings. The bundles will be deleted from Bundledocs.

Upon the conclusion of a case, the bundles will be deleted from Bundledocs and a copy of the bundle will be retained on ICO systems in line with the ICO retention schedule.

We propose using the cloud based Bundledocs service as opposed to the on-premise offering. A cloud service is preferred as it aligns with the ICO IT strategy to reduce on-premise infrastructure with added benefits in service availability for remote working and business continuation scenarios.

Bundledocs primarily rely on Microsoft Azure to deliver its service. Microsoft provide data processing and data storage services that allow it to provide a secure and reliable service to its customers.
Bundledoc rely on Stripe for payment processing, Mailgun for email notifications, and Olark for support chat. Bundledoc suppliers will not have access to ICO data that is uploaded into the digital bundles. ICO data will not be leaving the EU.

Stripe is the payment system for processing their payments.

Stripe does not access any information from the data uploaded to Bundledocs.

Ref link https://stripe.com/gb/privacy

Mailgun

When emailing support@bundledocs.com Bundledoc for service support, they use **Mailgun** to manage email notification. MailGun does not access email content, instead it provides a notification to Bundledocs. MailGun does not access any information from the data uploaded to Bundledocs.

Ref link https://www.mailgun.com/gdpr/

Microsoft Office365 is used to manage our support email account support@bundledocs.com. Microsoft Office365 does not access any information from the data uploaded to Bundledocs.

Olark

When using the Online chat support, Bundledoc uses the Olark service to manage their chats to provide assistance. Olark does not access any information from the data uploaded to Bundledocs.

https://www.olark.com/help/gdpr/

1.3 Definition of processing

Guidance: As a data controller we are required to maintain a "record of processing activities" for which we are responsible (Article 30 refers). The following table is designed to help us define the planned processing operation.

Data controller(s)	ICO
Data processor(s)	Legal IT (Ireland) LTD (Bundledocs)
Joint data controllers	N/A

Purpose of processing	To allow ICO to create and share digital legal bundles.
Categories of data	Names, addresses, contact information, medical records, financial information and criminal convictions and any other personal data contained within correspondence that forms part of the bundle.
Categories of subjects	ICO employees, Appellants/Defendants, Court staff, public authority employees, third party solicitors, prosecution/defence witnesses
Categories of recipients	Bundledocs and third parties relating, court / tribunal, any party joined to the legal proceedings.
Overseas transfers	Bundledocs privacy notice indicates all data is stored in Ireland and Amsterdam. No data is transferred outside of the EEA.

1.4 Purpose for processing

Guidance: State the context and business need being pursued in the processing, including the purposes, aims and the intended benefits for you, data subjects, society or others.

The personal data is being processed to enable ICO staff to use Bundledocs to create electronic legal bundles that are to be used in legal proceedings and that will be shared with courts and parties. The bundles will not be stored on Bundledocs indefinitely and will be downloaded to the ICO network and stored in SharePoint and deleted from Bundledocs at the completion of the legal proceeding.

1.5 Lawful basis

Guidance: State the basis on which the processing is lawful under GDPR Article 6 (consent, performance of contractual obligations to a data subject, compliance with legal obligations, protecting the vital interests of a natural person, public task or legitimate interests). If you are processing based on legitimate interests you must also complete a legitimate interests assessment.

If you are processing data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences, you will also need to state a further basis for that processing –see GDPR Article 9 and 10.

The lawful basis for this processing is article 6(1)(e) – necessary for the performance of a task carried out in the public interest.

The lawful basis for processing special category data is article 9(2)(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

The lawful basis for processing criminal offence data is Schedule 1, Part 3, Para 33 which states -

This condition is met if the processing—

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

1.6 Mandatory requirements

Guidance: Add the following requirements to your project backlog unless they do not apply (e.g. data need not be kept up to date in a system for storing old records). Section 4 can be used to check that these have been completed, particularly if delivery is not being managed as a project.

<u>Data Accuracy</u>

a) Data must be kept up to date
b) There must be means to validate the accuracy of any personal data collected
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject

<u>Retention & Deletion</u>

d) All data collected will have a retention period
e) Data must be deleted at the end of its retention period unless required by the National Archives for permanent preservation
f) Data kept beyond the retention period will be pseudonymised
g) Personal data must be erased upon receipt of a lawful request from the data subject

<u>Information & Transparency</u>

h) The data subjects shall be provided with:
(i) The identity and contact details of the data controller;
(ii) The purposes of the processing, including the legal basis and legitimate interests pursued
(iii) Details of the categories of personal data collected
(iv) Details of the recipients of personal data

<u>Objection & Restriction</u>

i) There must be means to restrict the processing of data on receipt of a lawful request from the data subject
j) There must be means to stop the processing of data on receipt of a lawful request from the data subject

<u>Security</u>

k) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely
l) Identify an Information Asset Owner
m) Update the Information Asset Register
n) Access controls must be in place for both physical and digital records

<u>Is the data being transferred outside the UK and EEA? If so:</u>
o) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries
p) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.

<u>Is the data being transferred to or through another organisation? If so:</u>
q) There must be controls to ensure or monitor compliance by external organisations.

<u>Is consent or pursuit of a contract the lawful basis for an automated processing operation? If so:</u>
r) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject
s) The consent must be recorded in some manner to serve as evidence

<u>Does our Privacy Notice need to be updated? If so:</u>
t) *Update the Privacy Notice*
u) Update the records of processing activities
v) There must be appropriate contracts in place with data processors / sub-contractors

2. Data protection assessment screening

Guidance: The purpose of the screening questions is to determine if a DPIA is required. As a data controller we are required to perform DPIAs where the processing is likely to result in a high risk to the rights and freedoms of individuals (Article 35 refers).

2.1 Screening questions

ID	Criteria	Y/N
1	Will the processing involve evaluation or scoring, including profiling or predicting, especially in relation to an individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?	N
2	Will the processing involve automated decision making that will have a legal or similar detrimental effect on individuals? For example, decisions that lead to exclusion or discrimination.	N
3	Will the processing involve the systematic monitoring of individuals in a publicly accessible area? For example, surveillance cameras in a shopping centre or train station.	N
4	Will the processing involve sensitive personal data or data of a highly personal nature? For example, special categories of data (Article 9 refers), personal data relating to criminal convictions or offences (Article 10 refers), and personal data linked to household and private activities.	Y
5	Does the processing involve large scale processing of data at a regional, national or supranational level, and which could affect a large number of data subjects?	N
6	Does the processing involve matching and combining two or more datasets that have been collected for different purposes and/or by different data controllers?	N
7	Does the processing concern vulnerable individuals who may be unable to easily give consent or object to the processing? For example, children, employees, and others who require special protection (mentally ill persons, asylum seekers, patients, the elderly).	Y
8	Does the processing involve the innovative use or application of new technological or organisational solutions? For example, "Internet of Things" applications can have significant impacts on subjects' daily lives and privacy.	N

9	Does the processing prevent individuals from exercising a rights or using a service or contract? For example, where a bank screens its customers again credit reference database in order to decide whether to offer them a loan.	N

*Guidance: If you answer "Yes" to one or more questions you should complete a DPIA. If you answer "No" to all questions a full DPIA is **not** required but you must still keep a record of this document as evidence that you have considered the data processing operation against the screening questions. You can save this locally in your department and it does not need to be submitted for consideration by the DPSIA forum.*

2.2 DPIA approach and consultation

Guidance: Record which parts of the DPIA you will be completing and your rationale (especially if your choices differ from the guidance above).

Explain what practical steps you will take to ensure that you identify and address the data protection risks. Include details of:

- *Who should be consulted, internally and externally? This must include the DPO's team and Cyber Security. You should also consult data subjects or their representatives unless this is not possible or appropriate – e.g. it would be disproportionate, impractical, undermine security or compromise commercial confidentiality.*
- *If data subjects (or their representatives) will not be consulted you must document the reasons for this.*
- *Consider whether consultation with processors or sub-processors is needed.*
- *How you will carry out the consultation. You should link this to the relevant stages of your project management process or delivery plan.*

Data subjects will not be consulted as the information used to create the bundles in Bundledocs is from the ICO's own systems and is already processed by the ICO.

Consultation will take place with the DPO's team to assess the impact of processing on data subjects.

The Cyber Security department undertook a Supplier Assessment of Bundledocs (filed in EDRM/Cybersecurity/Risk Management), which is a standard process for new suppliers. Based on a review of published documentation it gives reasonable confidence that service meets NCSC's SaaS principles. It is ICOs' responsibility to implement and operate to ensure continued security and privacy.

3. Data inventory

3.1 Information flows

Guidance: Provide a systematic description of the processing, including:

- *What personal data is collected*
- *The specific purpose of your processing*
- *The source of the data (including whether the data subjects are vulnerable, the relationship with the data subjects, the manner of collection and the level of control the data subjects have over the data once collected)*
- *The nature and context of the processing (including whether there are new technological developments or any relevant current issues of public concern)*
- *The scope of the processing (including the nature and volume of data, frequency and duration of processing, sensitivity of the data and the extent of the processing)*
- *The storage and transfer of the data (including details of hardware, software, networks, key people and details of any paper records or transmission channels)*
- *Responsibilities for the data (including the information asset owners, how responsibilities for information change through the data flow and the boundaries of responsibilities in any handover)*

You may find it useful to refer to a flow diagram or other way of explaining information flows. You should also say how many individuals are likely to be affected by the processing of personal data.

The bundles created using Bundledocs contain personal data collated from the ICO's current systems such as SharePoint and CMEH. The documents will be uploaded onto Bundledocs in order to create a bundle. The bundle will be stored on Bundledocs throughout the applicable legal proceedings for amendments etc. Once the legal proceedings have been finalised, the bundle will be deleted from Bundledocs and a copy of the bundle will be saved onto the ICO's Sharepoint. The documents will contain personal data including names, addresses, dates of birth, contact information and criminal convictions. The personal information will relate to a range a data subjects including ICO staff, Appellants/Defendants, court staff, public authority staff, third party solicitors and witnesses. The bundles are created in the course of legal proceedings.

All of the documentation used to create the bundle will be from the ICO's own systems and the range of data will vary depending on each case.

The Bundledocs process works as follows:

Documents are extracted from ICO systems (SharePoint/CMEH)

Documents are uploaded onto the Bundledocs system

Bundle created

Bundle shared with supervising solicitor for review

Once approved, the bundle is shared with applicable parties (Court/Appellant/Solicitor etc.)

Once legal proceedings complete, the bundle is deleted from Bundledocs and a copy is stored on Sharepoint

Documents will be redacted within Bundledocs using the redaction feature. We will no longer be redacting documents using e-redact before adding the document to the bundle. The Bundledocs redaction feature allows the individual document to be selected and highlight relevant text for redaction. The redaction is saved to the document and when the bundle is generated, the documents are redacted. The creator of the bundle will check that the redactions have been applied to the final generated document. A second check will be completed on review by the allocated lawyer. The unredacted version of the documents will remain in SharePoint and CMEH.

Once a bundle has been created on Bundledocs, the bundle will be shared with the supervising lawyer to ensure all documents contained within the bundle are correct to avoid accidental disclosure. The bundle being served is a recording of their approval and an email receipt will be generated by Bundledocs to record the serving. This receipt will be stored on SharePoint.

In respect of FOI appeals, elements of the bundle will be provided to the third party (before the bundle is prepared in Bundledocs), who may or may not be joined to the proceedings, to request their authorisation to include their correspondence in the bundle, this correspondence was provided during the Commissioner's investigation and stored in CMEH. They will also be given the opportunity to provide redacted copies for inclusion in the bundle if necessary. This correspondence will be provided to them in a separate PDF and they will not be given a copy of, or access to the full draft bundle. Once authorisation and/or redacted copies have been received, the bundle will be updated accordingly, reviewed and finalised by the lawyer with conduct of the case before being shared with the Appellant and Tribunal.

In respect of all cases, If Counsel has been instructed they will be sent the PDF bundle via an email link that will be password protected as per the functionality provided by bundledocs.

The finalised bundle will be shared with interested parties including the relevant courts, tribunals, counsel, third party solicitors, public authorities and Appellants/Defendants. The bundle will be shared electronically via email in either a PDF version (size permitting) or a Bundledocs password protected link. The link will allow the recipient access to the specific bundle only.

The legal teams were already creating electronic bundles on a day to day basis following the onset of Covid-19 but we were unable to provide them externally to other parties as there were questions around security, the process of creating them was also time consuming. Bundledocs provides a system where the bundle can be created in a faster, more efficient, user friendly way and it meets all the necessary security requirements that will allow the bundles to be shared externally with the parties involved in legal proceedings.

The information will be processed electronically using the Bundledocs software and may be printed if necessary. The team will create approximately 50 bundles per month containing a range of data depending on the particular appeal or prosecution.

The paralegal/legal admin staff will ensure that the bundle is deleted from the Bundledocs system upon completion of the case. The legal team currently have a set procedure for file closures. The file closure procedure has been updated to include the deletion of the bundle from Bundledocs - see Appendix 1.

3.2 Data inventory

Guidance: Identify the personal data to be held, the recipients (those with access to the data), the retention period and the necessity of the data collection, processing and retention.

Data Type	Recipients	Retention Period	Necessity
Defendant/Appellant name, date of birth and contact information (Address, number, email address) and other personal data that might be provided by complainants/Appellants in each case relating to their case.	ICO legal staff, counsel, court/tribunal, third party solicitors	6 Years (on ICO systems) Deleted from Bundledocs as the Appeal/Prosecution is complete.	Necessary to progress and/or defend an appeal or prosecution
Witness details – name, address, job role	ICO legal staff, counsel, court/tribunal, third party solicitors	6 years (on ICO systems) Deleted from Bundledocs as the Appeal/Prosecution is complete.	Necessary to progress a prosecution
Data subject medical information and other sensitive personal data	ICO legal staff ,counsel, court/tribunal, third party solicitors	6 years (on ICO systems) Deleted from Bundledocs as the Appeal/Prosecution is complete.	Sometimes required as part of the prosecution evidence, sensitive data will be redacted

			before disclosing the third parties
Criminal convictions	ICO legal staff, counsel, court/tribunal, third party solicitors	6 years (on ICO systems) Deleted from Bundledocs as the Appeal/Prosecution is complete.	Required to obtain and disclose a defendant's previous criminal convictions in the course of a criminal prosecution

4. Compliance measures

Guidance: Use this section to record your compliance with the requirements in section 1.6. Fill in the details of how the requirements have been met. The requirement source is a reference to GDPR unless otherwise stated.

Requirement	Implementation Details
Data Accuracy	
a) Data must be kept up to date	Information is obtained from the ICO's SharePoint/CMEH systems etc. and is kept up to date in line with current policies. If details change throughout the course of the legal proceedings then the information will be updated in Bundledocs accordingly.
b) There must be means to validate the accuracy of any personal data collected	As above. The information used is from the ICO's own systems. If details change throughout the course of the legal proceedings then the information will be updated in Bundledocs accordingly.
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject	The information will not be stored on BundleDocs for a significant period of time – it is stored on the ICO's systems. However, if data stored on Bundledocs requires updating, we are easily able to do so by amending the bundle.
Retention & Deletion	
d) All data collected will have a retention period	The data will be deleted from Bundledocs once the Appeal/Prosecution is complete. The bundle will be held on the ICO's SharePoint system for 6 years in line with current policy. Once the bundle is deleted from the Bundledocs system it is retained on their backup for 7 days.
e) Data must be deleted at the end of its retention period unless required by the National Archives for permanent preservation	The data is deleted from Bundledocs as soon as it is no longer required for the Appeal/Prosecution.
f) Data kept beyond the retention period will be pseudonymised	N/A – as above. The data will be deleted from Bundledocs as soon as it is no longer required to be on the system.
g) Personal data must be erased upon receipt of a lawful request from the data subject	Upon receipt of a lawful request, the ICO legal team are easily able to amend the bundle on Bundledocs to remove the personal data.
Information & Transparency	
h) The data subjects shall be provided with: ● the identity and contact details of the data controller;	The ICO's privacy notice is to be updated to inform data subjects that Bundledocs are processors for the personal data contained in any bundle.

● the contact details of the Data Protection Officer; ● the purposes of the processing, including the legal basis and legitimate interests pursued ● details of the categories of personal data collected ● details of the recipients of personal data	
Objection & Restriction	
i) There must be means to restrict the processing of data on receipt of a lawful request from the data subject	The ICO legal team will each have their own login details to easily access Bundledocs and delete the relevant data upon receipt of a lawful request to restrict processing.
j) There must be means to stop the processing of data on receipt of a lawful request from the data subject	N/A The ICO legal team are able to access Bundledocs and delete the data upon receipt of a lawful request to stop processing.
Security	
k) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely	Training will be provided to staff once Bundledocs is rolled out to the team. The training will include (but not limited to): • How to upload documents onto Bundledocs • How to add and remove documents • How to review the documents contained in the bundle and make amendments • How to redact documents within the bundle • How to securely share the bundle
l) Identify an Information Asset Owner	Director of Legal Services (Regulatory Enforcement)
m) Update the Information Asset Register	All FOIA/Enforcement appeals are recorded on each team's asset register.
n) Access controls must be in place for both physical and digital records	The ICO legal team will have an account with Bundledocs. The staff member will be provided with a log in and set up a secure password. The administration staff will create the bundles and will then add the allocated Lawyer/Paralegal as a collaborator to the bundle. Each staff member will only have access to bundles they have created or bundles that have been shared with them by another staff member. If a bundle is printed, the bundle will be placed into legal's lockable rolling store.
Conditional Requirements	

o) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries	N/A - ICO data will not be leaving the EU
p) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.	DPO team to be consulted as part of the completion of this DPIA
q) There must be controls to ensure or monitor compliance by external organisations.	External organisations will not be given access to Bundledocs and will only be provided with access to finalised copies of the relevant bundles if they are party to a legal proceeding. Bundledocs will be subject to Gcloud 11 Call-Off Contract technical standards required are that the supplier maintain its ISO/IEC 270001:2013 certification and compliant with CSA CCM v1.2 for the term of the Call off contract..
r) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject	N/A
s) Any consent must be recorded in some manner to serve as evidence	N/A
t) Update the Privacy Notice	We will work with the Information Management Service to get the privacy notice updated.
u) Update the Article 30 Records of Processing Activities	We will work with the Information Management Service to get the ROPA updated.
v) There must be appropriate contracts in place with data processors / sub-contractors	We will work with the relevant ICO legal/procurements teams to put a contract in place with Bundledocs for the bundling service.

5. Data protection summary risk assessment

Guidance: Record a summary of identified and assessed risks to data subjects' rights, the actions you have taken (existing) and could take (expected) to reduce the risks. Detail any future steps that will be necessary (eg the production of new guidance or security testing for new systems). Some example risk sources have been listed to aid you below and in Appendix 2. The examples are not exhaustive. Equally not all will be relevant to your specific processing activities. See Appendix 1 for guidance on assessing impact and probability.

Risks should be considered from the data subject's perspective not the ICO's (eg a reputational risk to the ICO should not be recorded here). Some example threats to consider include:

- *Discrimination*
- *Identity theft and fraud*
- *Financial loss*
- *Damage to data subjects' reputation*
- *Loss of confidentiality of professional secrets*
- *Unauthorised reversal of pseudonymisation*
- *Social or economic disadvantage*
- *Deprivation of legal rights or freedoms*
- *Data subjects losing control over their data*
- *Loss of privacy or intrusion into private life*
- *Prevention from accessing services*

Risk Description	Response to Risk	Risk Mitigation	Expected Risk Score		
			I	P	Total
[Guidance: Describe the cause and likelihood of; and the threat to the data subjects rights, and the impact on the data subject should the risk be realised- 3 elements]	*[Guidance: Describe risk treatment (e.g. reduce, avoid, accept or transfer)]*	*[Guidance: Describe existing activity and controls to reduce risk and any further activity or controls to be taken that are expected to reduce the risk- 2 elements]*	*[Guidance: I is impact score and P is probability score and IxP is the Total Score. Probability is the likelihood of the risk being realised after Risk Mitigations have been achieved.*		
Weakness in the build configuration and maintenance of the Bundledocs software and SaaS, leave ICO information at risk of theft or hacking	Accept	Current mitigation: Bundledocs operates on the MS Azure platform which provides sufficient tools to secure the information. Bundle docs publishes the techniques and tools used to secure our information. The ICO Cyber Security department has undertaken a Supplier Assessment based on a review of published documentation and concluded that it gives reasonable confidence that the service meets NCSC's SaaS principles and is therefore suitable for our information which classified as Official Sensitive.	3	1	3 Low

Failures in setting up and operating the Information Management policies for Bundle docs lead to; Data being retained beyond the retention period, or information being visible to people who do not have a business need, or poor naming and version control resulting in incorrect documents being included in a bundle.	Reduce	Current mitigation: To reduce this risk, the legal team's file closure procedure has been updated to ensure that on completion of a case, the bundle will be deleted from Bundledocs and a copy will instead be stored on the ICO's Sharepoint system. Expected Mitigation: The implementation phase will define roles and responsibilities, including a System Admin role and Audit, Access rights and access protocols, (use of 2FA and password complexity). Training and departmental policies will be developed for the Legal Bundle process from creation, modification, distribution and deletion.	2	2	4 - Low

Accidental disclosure of confidential information to a third party due to human error when preparing the bundle.	Reduce	Expected mitigation: Training will be provided to staff. The training will include (but not be limited to): • How to upload documents onto Bundledocs • How to add and remove documents • How to review the documents contained in the bundle and make amendments • How to redact documents within the bundle • How to securely share the bundle Also a peer review of prepared bundles will take place before disclosure. Bundles will be shared with the supervising solicitor to ensure all documents contained within the bundle are correct. The bundle being served is a recording of their approval and an email receipt will be generated by Bundledocs to record the serving. This receipt will be stored on SharePoint.	3	2	6 - Medium

Bundles are shared without password protection and are accessed by an unauthorised third party.	Reduce	Expected mitigation: Bundledocs allows completed bundles to be shared with a third party via a invite link. Assigning additional password protection to the bundle document is optional, and relies on the user remembering to do it. Consequently there is a risk the user may forget to do this. We will make assigning a password a mandatory part of our bundle preparation process. This will be set out clearly in the written procedure we are developing. We will also provide training to end users to show them how to assign password protection to their bundle before sharing.	3	2	6 - Medium
Non-essential cookies are dropped on ICO user devices without appropriate consent	Reduce	Expected mitigation: IT will approach BundleDocs and seek assurances from them that they will address the lack of a consent mechanism on their website to improve their PECR compliance.	1	1	1

The UK's departure from the EU means we don't have the same data protection assurances for personal data being stored on servers outside the UK.	Accept	Current assurance flows from the fact that both the ICO and BundleDocs operate within the EEA and are subject to GDPR. It is not possible at this time to predict the data protection legal framework post Brexit. However BundleDocs will likely still be operating within the EEA and the same or similar GDPR protections will remain. We will also have an existing contract with BundleDocs based on G-cloud 11 framework which provides further assurances which will last post Brexit.	1	1	1

6. Expected residual risk and sign off

6.1 High and medium level expected residual risk

Guidance: Record details of the remaining risk. It is never possible to remove all risk so this section should not be omitted or blank. If the residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO by following the process used by external organisations.

All residual risk is assessed as either low or medium and can be accepted. The most significant risk is a human error when creating the bundle which results in us making an inappropriate disclosure of personal data. It is not possible to completely eliminate this risk but we are confident we are putting sufficient measures in place to mitigate this risk as far as is reasonably possible.

6.2 Necessity and proportionality

Guidance: If you answered "Yes" to one or more of the screening questions in Section 2.1 you should discuss the necessity and proportionality of the collection, processing and retention of this data here, weighing the impact on data subjects rights and freedoms against the benefits of the processing activity. You should also consider whether there are other reasonable ways to achieve the same result with less impact on data subjects.

The information stored on Bundledocs will come from our own ICO systems such as SharePoint and CMEH. Bundledocs is a means of collating the documents containing data and is necessary to conduct a prosecution and process an appeal. The data will be retained on Bundledocs whilst required during legal proceedings. On completion of the legal proceedings, the data will be deleted from Bundledocs and a copy will be stored on ICO systems.

6.3 DPO recommendations

Guidance: Record any recommendations from the DPO or their delegates and responses here. This serves as useful tool when reconsidering a rejected DPIA or in recording the justification if the organisation rejects the DPO's advice.

No	Recommendation	Project Team Response
1	Legal team should clarify if redaction feature in Bundledocs will be used. If yes update section 3.1 'Information flows' to include this part of the processing and consider if there are any additional risks.	Accept
2	A written procedure that establishes governance standards needs to be created. This should document the: - Process of peer review - Establish naming / labelling conventions for documents and bundles	Accept

	- Access controls and method for sharing bundles with third parties - Information management responsibilities	
3	IT to contact BundleDocs and request they implement compliant cookie control.	Accept

6.4 Sign Off

Guidance: Send this to the DPSIA forum to consider the privacy and security risks involved in the processing, the solutions to be implemented and the residual risk.

Considered by	**Date**	**Project Stage**
DPIA Forum	11/05/2020	Planning
Louise Bogle Acting Director of Legal Services (Regulatory Enforcement)	21/05/2020	Planning

7. Integrate the outcomes back into the plan

Guidance: Identify who is responsible for integrating the DPIA outcomes back into any project plan and updating any project management paperwork. Who is responsible for implementing the solutions that have been approved? Who is the contact for any data protection concerns which may arise in the future?

Action to be taken	Date for completion	Responsibility for Action	Completed Date
Clarify use of redaction and update section 3.1	ASAP	RH/RW	14/05/2020
Draft written procedure that establishes governance standards	Before deployment	RH	14/05/2020
Contact BundleDocs and request they implement compliant cookie control.	ASAP	RW	14/05/2020

Contact point(s) for future data protection concerns	Director of Legal Services (Regulatory Enforcement)

8. Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description
V0.1	24/04/20	Rachel Harrison	Draft DPIA
V0.2	11/05/2020	Steven Johnston	DPIA Forum recommendations
v.1.0	15/05/2020	Steven Johnston	Final release

9. Template Document control

Title	Data Protection Impact Assessment Template
Version	2.0
Status	Final release
Owner	DPSIA Forum
Release date	17/07/19
Review date	17/07/20

Appendix 1

CASE CLOSURE AND ARCHIVING ADMIN – APRIL 2020 ONWARDS

CASE CLOSURE	
Task	**Completed**
Receive template email filled out by solicitor with an attached decision – query with them if any information is missing – open the email and keep it minimized to access easily.	
• Open the **'Closure Tracker (Current)'** in **'FOI Appeal Log – Admin'** within SharePoint and fill in the relevant fields with info from the closure email • **Date Received (date on email from solicitor)** • **EA Ref** • **Appellant** • **Solicitor (initials)** • **Decision Date** • **Name of Admin (initials)** As each task below is completed, colour the relevant cell in the tracker to green.	
• Open **'Closure Summary to CO and Signatory Template'** document from the **'Templates'** library in SharePoint and copy the body onto a new email. Fill in all necessary fields using information from the solicitor's email, then send to the following recipients: • **Case Officer** • **Signatory** • **CAD FOI Appeals** • **CAD Managers** ***Make sure to attach the decision PDF included in the solicitor's email before circulating.**	
Save a copy of the sent email to the SharePoint folder for the case. Use the following naming convention: [Date][Time] Internal Email Att Re Case Closure Summary [EA Ref] Example: *"20200225 1324 Internal Email Att Re Case Closure Summary EA20202020"*	
• Save another copy of the email into the relevant tribunals library in the **'Judicial Decisions'** subsite in SharePoint –	

you'll need to edit properties and enter a title and change the year to correspond with the EA reference. ***Make sure to check-in the email so other users can see it.**	
Open the **'Case Closure form'** within the appeal SharePoint folder, and use the email and attached decision from the solicitor to fill in the remaining details. If you are ever unsure about certain information, check with the solicitor before completing. Print a double-sided copy of this form and keep the electronic form open to refer to in the next steps.	
Open the '**New FTT Appeals Log 03032020'** located in the **'Legal Admin'** library within SharePoint and copy/paste the entry on the **'Open'** sheet over to the **'Closed'** sheet in ascending order of the EA reference. Fill the remaining columns using the information from the case closure form. ***Make sure to remove the entry on the open sheet and delete any blank rows.**	
Double check that the data entered into the '**New FTT Appeals Log 03032020'** is correct before saving and closing.	
Finally make sure to delete the digital version of the bundle/s from the **BundleDocs** website – select the button on the far right of the bundle list to bring up the **'Update Bundle'** menu. Now click the red dustbin icon in the lower left corner of this menu and confirm that you want to delete this bundle.	
ARCHIVING	
Open the **'Restore Archiving Form'** within the **'Legal Admin'** library, copy the top right column from the closure form and paste over the same column on the restore form. This will push the original column to the side – highlight this column, right click and the select **'Delete Cells'** to remove it. Under the drop down containing **'Open/Closed/Open & Closed/ Electronic Only'** enter the number of folders for each category where applicable: Example: 1 x Open Folder 2 x Closed Folders • Print a copy of this form and place on top of the case closure form printed earlier.	

An email is circulated every month by Information Management containing information about deadlines and also links to the relevant spreadsheets and forms needed for archiving. Click **'FOI and Enforcement Archive List'** to open spreadsheet and scroll to the bottom where the latest entries are. Each row represents a physical box containing the archived files – you can put as many different cases into one box that will fit, although it's best to keep multiple files for the same appeal together in one box if possible.	
Get a new archiving box from the Sandfield Ground Floor East print hub (more can be ordered from facilities if necessary) and use a marker to write the box number on both sides. The boxes are in sequential order so for example, if the last box in the spreadsheet is titled '2020-017' then the next box should be '2020-018'.	
Fill in the following columns with the relevant information on the next available row in the spreadsheet: • **Box No** – '2020-170' • **Retention Expiry Date** – '11/03/2026' – *this is always 6 years after the 'Date Issued'* • **Date Issued** – '11/03/2020' – this is the date of creating the box • **Location** – ICO-164 (always this) • **Department –** FOI Legal (always this) • **Owner –** Your name	
Now every appeal within the box needs to be added along the row of the spreadsheet. The columns start from 'File Title (A)' up to 'Notes' which represents one entry and then a new entry begins with each 'File Title' column (B,C,D etc.). ***An entry should be made for each bundle for an appeal, so if an appeal contains an open and a closed bundle, then two separate entries are required.** Fill in the following columns for each entry by using the **'Restore Archiving Form'** we filled in previously: • **File Title –** 'Apples v IC (1 x Open Bundle) • **Opened –** 'DD/MM/YYYY' • **Closed –** 'DD/MM/YYYY' • **Court/Tribunal Number –** 'EA/1111/1111' • **Case reference –** 'FS50111111' ***If you have been told the bundle needs to be preserved for the national archives, make sure to write 'Preserve' in the Status column and write 'For TNA' in the 'Retain Reason' column.**	

Finally if you have one large appeal across two or more boxes then in the final column in the entry entitled 'Notes', write the following with the box number/s that contain the rest of the appeal. • See box '2020-999' for folders 3 and 4 of the Closed Bundle Then do this vice versa in the 'Notes' column for the other box/s • See box '2020-998' for folders 1 and 2 of the Closed Bundle	
The final step is to fill in the **'Collection and Delivery Sheet'** which is another spreadsheet that is provided in the email from Information Management. This flags which boxes we want to send to Restore and also any that we want to retrieve from Restore. The first part of the spreadsheet is for **'Sending to Restore' –** there are four columns to fill in for each box: • **Box Number** – '2020-999' • **Collect From** – 'Your Name' • **Number of Boxes** – This should always be '**1'** as each row represents one box • **New Box or a Return** – if this a box that had previously been retrieved from Restore and is being returned, enter 'Return' – otherwise enter 'New Box' The second and final part is for **'Retrieving from Restore' –** this only has two columns to fill in: • **Box Number** –'2020-000' • **Deliver to** – 'Your Name' *A solicitor will let you know if they need an appeal retrieving from Restore so you'll need to check the **'FOI and Enforcement Archive List'** to get the number for the box/s that contain the appeal – the retrieval is free if brought with the Restore collection or there is a charge for quick retrieval if the appeal is needed before then.	

Appendix 2: 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 3: Common risks to data subjects

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 any other specific risks that may apply in relation to your intended processing.

- 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

Data Protection Impact Assessment – Microsoft 365

Document Name	Data Protection Impact Assessment – Microsoft 365
Author/Owner (name and job title)	Will McLoughlin – Senior Product Owner, Productivity and Collaboration
Department/Team	Digital Data & Technology, Product and Infrastructure
Document Status (draft, published or superseded)	Published
Version Number	V1.0
Release Date	22/09/2023
Approver (if applicable)	Mike Fitzgerald, Director of Digital, IT and Business Services
Review Date	22/09/2024
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 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 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? and this indicates a high risk to data subjects. 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 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.

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:	Product Ownership of Microsoft 365 (M365)
Project Manager:	Will McLoughlin
Information Asset Owner:	Mike Fitzgerald
Controller(s)	ICO & Microsoft
Data processor(s)	Microsoft

ICO as controller and Microsoft as our processor

The ICO is controller and determines the purpose(s) of processing data using M365. ICO has control over what we use M365 for as well as its implementation and configuration in our business.

Our use of the services is governed by Microsoft's Product Terms[1] and Data Protection Addendum[2], and Microsoft, as a data processor, processes our "Customer Data" (defined below in 1.3) to provide us with their Online Services.

Microsoft as controller for their specific legitimate business operations

In addition Microsoft uses personal data to support a limited set of their own legitimate business operations described by them as:

[1] Microsoft Product Terms
[2] MicrosoftProductandServicesDPA(WW)(English)(Jan2023)(CR).docx (live.com)

(1) billing and account management;
(2) compensation (for example, calculating employee commissions and partner incentives);
(3) internal reporting and modelling (for example, forecasting, revenue, capacity planning, product strategy);
(4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products;
(5) improving the core functionality of accessibility, privacy, or energy efficiency; and
(6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Customer Data outlined in the Online Service Terms). [3]

Microsoft is controller of this processing of personal data in order to support these operations and, by using their services we must accept that this processing takes place.

Microsoft states it aggregates personal data before using it, removing Microsoft's ability to identify specific individuals, and uses personal data in the least identifiable form that will support their processing. Microsoft further states it will not use Customer Data or information derived from it for profiling or for advertising or similar commercial purposes.[4]

1.2 Describe your new service or process

This DPIA covers the ICO's use of the Microsoft 365 suite of applications as provided under our E5 licencing arrangement. This document substantially builds on the PSIA that was produced in December 2016 when Office 365 was being procured by the ICO. Foundational risks, mitigations, security provisions, and rights considerations that were covered in that PSIA are intentionally not duplicated here.

However, this DPIA does build on and support numerous DPIAs that were produced for individual Office 365 applications, addressing all current Office 365 applications available to colleagues through our MMD and Office on the Web offers, as per the following list (current as of September 2023):

Bookings
Calendar
Excel
Exchange
Forms
Kaizala
Lists
OneDrive
OneNote

[3] Guidance for Data Controllers Using M365 Section 2
[4] MicrosoftProductandServicesDPA(WW)(English)(Jan2023)(CR).docx (live.com)

Outlook
People
Planner
Power Apps
Power Automate
Power BI
PowerPoint
Power Virtual Agents
Project
SharePoint
Stream
Sway
Teams
To Do
Visio
Viva Connections
Viva Engage
Viva Insights
Whiteboard
Word

Whilst all applications listed above are available to ICO staff as part of our E5 licence, not all are actively used by the ICO. Further detail about applications currently in use and their current deployment can be found in Appendix 3. This appendix will be updated if and when our application use changes.

It is recognised that it may still be necessary to create exceptional additional DPIAs for some M365 applications, for example if and where the ICO's intended specific use of that application is significantly at variance with the contents of this DPIA, or simply where a more in-depth assessment of an application will assist with managing risks. In such cases, this master document will be updated to provide reference to the additional documentation, along with the rationale for its creation.

Some M365 products include extensibility options that enable, at the controller's choosing, sharing of data with independent third parties. For example, Exchange Online is an extensible platform that allows third-party add-ins or connectors to integrate with Outlook and extend Outlook's feature sets; the same is true for Teams. These third-party providers of add-ins or connectors act independently of Microsoft, and their add-ins or connectors must be enabled by the users or enterprise administrators, who authenticate with their add-in or connector account.

Such third-party add-ins or connectors are disallowed by default at the ICO, and not automatically covered by this DPIA. Each one required or requested would need to be the subject of its own DPIA Screening Assessment (as a minimum), on a case-by-case basis.

1.3 Personal data inventory - explain what personal data is involved

Category of data	Data subjects	Recipients	Overseas transfers	Retention period
Customer Data: This is all data, including text, sound, video, or image files and software, that ICO provides to Microsoft through use of Microsoft online services. It includes data uploaded for storage or any processing activity, as well as customisations. Examples of Customer Data processed in M365 by the ICO will include, but are not limited to: • Email content in Exchange Online • Documents or files stored in SharePoint Online or OneDrive for Business. • Meetings and conversations • Community and channel posts	ICO Staff and all other data subjects whose data the ICO processes as part of its day to day operations.	Primarily Microsoft but Microsoft also shares data with third parties acting as their sub processors to support functions such as customer and technical support, service maintenance, and other operations. Microsoft states any subcontractors to which Microsoft transfers Customer Data, Support Data, or Personal Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the Product Terms agreed	As described in their Guidance for Data Controllers using Office 365 - Microsoft GDPR | Microsoft Learn[8] and the Product Terms[9], for instances of M365 provisioned in the United Kingdom, Microsoft will store the following Customer Data at rest only within the UK: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site, (3) files uploaded to OneDrive for	Data is retained by Microsoft for the duration of our use of the service. As a customer ICO at all times during the term of our subscription will have the ability to access, extract, and delete Customer Data stored in the service, subject in some cases to specific product functionality intended to mitigate the risk of inadvertent deletion (for example, Exchange recovered items folder), as further described in product documentation. Except for free trials and

[8] Guidance for Data Controllers using Office 365 - Microsoft GDPR | Microsoft Learn
[9] Microsoft Product Terms

• Chats • Voicemail • Shared files • Recordings and transcriptions. • Profile data such as email address, profile picture and phone number • Call history		between ICO and Microsoft. All third-party sub-processors with which Customer Data from Microsoft's Core Online Services is shared are included in the Online Services Subcontractor list.[5] All third-party sub processors that may access Support Data (including only Customer Data that the ICO chooses to share during support interactions) are included in the Microsoft Commercial Support Contractors list.[6] Microsoft commit that they will not transfer to any third party (not even for storage purposes) data that we provide to them through our use of	Business, and (4) project content uploaded to Project Online. For personal data from the United Kingdom, Microsoft will ensure that transfers of personal data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of UK GDPR. Microsoft continues to abide by the terms of the Privacy Shield framework. "Microsoft practices privacy by design and privacy by default in its engineering and business functions. As part of these efforts, Microsoft performs comprehensive privacy reviews on data processing operations that have the potential to cause impacts to the rights and freedoms of data subjects. Privacy	LinkedIn services, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of the our subscription so that we may extract the data. After the 90-day retention period ends, Microsoft will disable a customer's account and delete the Customer Data. ICO retention periods for our data will vary but information within the M365 environment should be managed by Information Asset Owners as per the ICOs Retention and Disposal Policy.

[5] Service Trust Portal (microsoft.com)

[6] Download Services Supplier List from Official Microsoft Download Center

		the business cloud services that are covered under the Microsoft Product Terms.[7]	teams embedded in the service groups review the design and implementation of services to ensure that personal data is processed in a respectful manner that accords with international law, user expectations, and our express commitments. These privacy reviews tend to be very granular—a particular service may receive dozens or hundreds of reviews. Microsoft rolls up these granular privacy reviews into Data Protection Impact Assessments (DPIAs) that cover major groupings of processing, which the Microsoft EU Data Protection Officer (DPO) then reviews. The DPO assesses the risks related to the data processing to ensure that sufficient mitigations are in place. If the DPO finds unmitigated risks, he or she recommends changes back to the engineering group. DPIAs will be reviewed and	

[7] https://www.microsoft.com/en-us/trust-center/privacy/data-location

			updated as data protection risks change."[10] In the UK, as of September 2022, the provisions made for restricted international transfer of data under the Privacy Shield framework are covered under International Data Transfer Agreements (IDTA): International data transfer agreement and guidance | ICO[11] Update Sept 2023: On 8 June 2023, the UK and US governments announced their commitment in principle to establish a UK-US data bridge. This marks the UK's intention to establish a data bridge for the UK extension to the EU-US Data Privacy Framework, subject to finalising the UK's assessment of US data protection laws and	

[10] GDPR Data Protection Impact Assessments, DPIA support & FAQs (microsoft.com)
[11] International data transfer agreement and guidance | ICO

			practices. This would allow for the free flow of personal data between the UK and certified organisations in the US. UK-US data bridge: joint statement - GOV.UK (www.gov.uk)	
Service-generated Data: This is data that is generated or derived by Microsoft through operation of the service, such as use or performance data. Most of these data contain pseudonymous identifiers generated by Microsoft.	ICO staff	As above	Structural transfer of Diagnostic Data to the USA.	This data is retained for a default period of up to 180 days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.
Diagnostic Data: This data is collected or obtained by Microsoft from software that is locally installed by Customer in connection with the Online Service and may also be referred to as telemetry. This data is commonly identified by attributes of the locally installed software or the machine that runs that software.	ICO staff	As above	Structural transfer of Diagnostic Data to the USA. We only allow Microsoft to collect Required diagnostic data, which does not include personal, sensitive or identifiable data.[12]	This data is retained for a default period of up to 180 days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.
Support Data/Feedback data	ICO Staff	As above	Structural transfer of Diagnostic Data to the USA.	This data is retained for a default period of up to 180 days from collection,

[12] Required diagnostic data for Office - Deploy Office | Microsoft Learn

Information related to troubleshooting tickets or feedback submission to Microsoft. This is data provided to Microsoft by ICO through an engagement with Microsoft to obtain technical support for Online Services			We have enabled Customer Lockbox in our Admin Portal. Customer Lockbox ensures that Microsoft can't access our content to do any service or support operations without our explicit approval.	subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.

1.4 Identify a lawful basis for your processing

M365 is core business technology at the ICO essential for delivering our statutory functions and ICO has invested in Enterprise (E5) licencing for all colleagues.

Our lawful basis for using M365 to process personal data for general processing purposes is Article 6(e): public task. For the processing of special category data the further basis for processing are Article 9(2)(g) – substantial public interest and DPA 2018 schedule 1 part 1 paragraph 6 – statutory etc and government purposes.

For personal data processed under Part 3 DPA 18 the processing is based on law and is strictly necessary for the performance of a task carried out for that purpose. Our Safeguards Policy[13] outlines our sensitive processing for law enforcement purposes and explains:

i) Our procedures for securing compliance with the law enforcement data protection principles;

ii) Our policies as regards the retention and erasure of personal data, giving an indication of how long the personal data is likely to be retained.

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

The data processing listed in 1.3 is effectively a set of conditions that enable Microsoft to provide the ICO with the M365 service we have chosen. It's necessary for the ICO to use M365 in order to deliver our statutory functions effectively or pursue our legitimate business interests.

As detailed in the standard Online Services Terms and Data Protection Addendum, Microsoft also uses Personal Data to support a limited set of their own legitimate business operations as outlined in 1.1 above. They are the controller for this processing and are also required to consider necessity and proportionality themselves, as well as comply more widely with relevant data protection legislation in the jurisdictions in which they operate.

1.6 Outline your approach to completing this DPIA

[13] Safeguards Policy | ICO

Throughout the inception and drafting of this DPIA, I have consulted with Steven Johnston, Team Manager, Information Management. I have also been guided and closely advised by Mike Fitzgerald as Information Asset Owner. Since this DPIA is designed to supplement multiple previous DPIAs, and not to cover any specific new usage of data, it is not anticipated that additional consultation of data subjects is required. If such a requirement emerges, that consultation will accordingly be reflected in later updates.

Update September 2023: in updating this document I have consulted with our commercial legal team on aspects relating to the transfer of data overseas.

In assessing the potential for a subsequent restricted transfer of personal data that is processed by the ICO for law enforcement purposes, the ICO has obtained, and relies upon, Microsoft's assurances that no restricted transfer will undermine the level of protection of individuals provided for in the UK, and that all personal data that is subject to a restricted transfer will, at all times, receive the same level of protection that is provided for within the UK, regardless of whether it is at rest or in transit.

2.0 Personal Data Lifecycle

Guidance: 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 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 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:

Customer data will be collected in a variety of ways by the ICO for processing within M365 applications. Most of the personal data we process is provided directly to us by data subjects. But we also receive personal data indirectly.

Further information about how we typically obtain personal data is contained in our customer privacy notice[14] and staff privacy notice[15].

Some additional categories of personal data are processed as a direct result of our staff using M365 applications. Microsoft systematically collects Telemetry Data about the use of its software. There are three levels at which this data can be set to be collected: Required (Lowest), Enhanced, and Optional (Highest). ICO devices are set to provide **Enhanced** diagnostic data to Microsoft under a known commercial identifier. As part of Microsoft Managed Desktop, IT admins cannot change these settings. As outlined in this DPIA for MMD, the Enhanced setting enables Advanced Threat Protection through use of the diagnostic data collected.

In Office for the Web, the default level is set to the (lowest) level of required data. Microsoft states it has limited the amount of telemetry events to a minimum, and has contractually agreed to never include any Content Data in these events.

In addition, Microsoft collects detailed personal information about the usage of Teams, OneDrive, SharePoint and the Azure Active Directory. Microsoft makes some of these Diagnostic Data available through audit logs and reports for admins.

Personal data related to troubleshooting tickets or feedback submissions to Microsoft is data actively and intentionally provided to Microsoft by ICO through an engagement with Microsoft in order to obtain technical support.

Technology used for the processing:

M365 suite of applications as provided under our E5 licencing arrangement (see 1.2 above).

M365 Telemetry Data is collected via a built-in telemetry client built into installed apps on desktops/laptops, on mobile devices and in the browser version of the apps.

M365 Usage Data is collected in log files of Microsoft's cloud servers, in so-called system-generated event logs.

Storage location:

Customer data is typically stored at rest only within the UK (See 1.3 above).

Telemetry Data is currently sent regularly, in batches, to Microsoft's servers in the United States. The Diagnostic Data are sent in an undocumented binary format. Provisions under IDTA for restricted transfer of data apply to EEA and third countries.

Usage Data is hosted[16] in Microsoft's UK and/or EMEA data centres.

[14] How do we get information? | ICO
[15] Policies - Staff Privacy Notice.pdf - All Documents (sharepoint.com)
[16] Location of data in Microsoft Teams - Microsoft Teams | Microsoft Learn

Access controls and data sharing:

Access is controlled through Azure Active Directory Single Sign On. This is made available to all ICO colleagues from the moment a New Starter request sent by People Services is processed by IT Help – their Azure Identity is set up and they are allocated to various security groups, which automatically provisions an M365 E5 licence to the user.

Data may be shared with recipients as detailed in 1.3.

Microsoft states it will not disclose Customer Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as Customer directs, (2) as described in the OST, or (3) as required by law.[17]

Disposal:

Customer Data: Throughout the duration of our contract we are able to dispose of customer data as we see fit by implementing retention and disposal rules via Purview within the M365 product set. For M365 subscriptions, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the Customer Data.

Service-generated (Diagnostic/Telemetry) Data: This data is retained for a default period of up to 180 days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.

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?

Microsoft already included in the Staff Privacy Notice.

As with a number of other processors there is no clear place in our Global PN to list Microsoft. Where specific applications are used for clearly defined processing activities Microsoft is listed as a processor. For example our use of Microsoft services is referenced in relation to our chatbot, Forms use is referenced for responding to ICO consultations and surveys, website hosting in Azure and use of Teams for delivering webinars and broadcast events.

[17] Privacy & data management overview - Microsoft Service Assurance | Microsoft Learn

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?

Customer data can typically be edited by ICO staff if it becomes inaccurate within M365 applications such as Word, Forms, Excel etc. This won't be the case for data such as chats, voicemail and call history which will be an accurate record of events. Similarly service generated data, diagnostic data and support data will be accurate reflections of events and there should be no issues with accuracy.

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

ICO privacy information explains how we get personal data: How do we get information? | ICO

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?

Automated retention and disposal is enabled through the M365 Compliance Center, now known as Purview. Currently configured for Outlook (12 months), Teams chats (7 days), and inactive 365 Groups (12 months). A proposal has been approved and is being finalised (as of September 2023) to introduce 12 months retention for Teams channel messages. Work is ongoing to define and apply retention schedules throughout SharePoint Online.

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

Yes ☐ No ☒

Integrity and confidentiality

11. Where will the personal data be stored?

M365, within our Microsoft Azure Tenant, on UK located servers.

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.

Usage policies and how to guides created and maintained for M365; in-house and external training provided for all colleagues.

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 ☐

Online Services Terms govern ICO use of the Microsoft Office 365 suite.

Individual Rights

Guidance: 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. However you need to be sure your new service or process can facilitate the exercise of these rights by the data subject i.e. it should be technically feasible for us to action a request if required.

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.	Excessive personal data shared with Microsoft and third parties as controllers.	Reduce	Existing mitigations: Additional Optional Connected Experiences Disabled. Third Party Apps in Teams Disabled. Usage policies created to guide. Customer Lockbox enabled.	3	1	3 - Low
2.	Colleagues overshare personal data on open forums such as Teams, Yammer, SharePoint.	Reduce	Existing mitigations: Training, usage policies, and How-to/etiquette guides produced to remind staff about appropriate use. Expected mitigation: further guides to be produced as and when required.	1	1	1 - Low
3.	Personal information is disclosed to unauthorized third-party organization	Reduce	Existing mitigation: Usage data is only accessible via M365 administrators, it is not shared with 3rd party organisations.	2	1	2 - Low

	during diagnostic/fault resolution activities.		M365 user feature Customer Lockbox is active. Microsoft support engineers requiring access to user data must first submit a lockbox data request. This can only be approved by M365 administrators.			
4.	Personal information is disclosed to unauthorized third-party applications (in e.g. Teams, Outlook, Power BI).	Reduce	Existing Mitigation: Apps policy restricts access to only approved Microsoft applications with known functionality. Expected Mitigation: All new third-party apps will be individually assessed before becoming available to ICO staff.	3	1	3 - Low
5.	Unauthorised disclosure of customer data by Microsoft to a third party	Accept	Existing Mitigations: Agreed Product Terms provide that Microsoft will not disclose Customer Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as Customer directs, (2) as described in the OST, or (3) as required by law. Microsoft will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing	4	1	4 - low

			so. Upon receipt of any other third-party request for Customer Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer. Microsoft will not provide any third party: (a) direct, indirect, blanket or unfettered access to Customer Data; (b) platform encryption keys used to secure Customer Data or the ability to break such encryption; or (c) access to Customer Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request. In support of the above, Microsoft may provide Customer's basic contact information to the third party.[18]			
6.	Microsoft security controls are not adequate resulting in a loss of confidentiality, integrity or availability of data.	Accept	Existing Mitigation: Agreed Online service terms provide that Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data and Personal Data. These measures are set forth in a Microsoft Security Policy. Microsoft make that policy available to ICO as Customer, along with descriptions of the	4	1	4- low

[18] Guidance for Data Controllers using Office 365 - Microsoft GDPR | Microsoft Learn

			security controls in place for the Online Service and other information reasonably requested by Customer regarding Microsoft security practices and policies. In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. Further detail about Security measures is available in the online service terms.			
7.	ICO unable to communicate details of any personal data breach resulting from our use of M365 to data subjects.	Accept	<u>Existing Mitigation:</u> Agreed Product Terms provide that if Microsoft becomes aware of a breach of security Microsoft will promptly and without undue delay (1) notify ICO of the Security Incident; (2) investigate the Security Incident and provide ICO with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. Notification(s) of Security Incidents will be delivered to one or more of ICO's administrators Microsoft will make reasonable efforts to assist ICO in fulfilling our obligations under UK GDPR Article 33 and 34 to notify the relevant supervisory authority and data subjects about such Security Incident.	4	1	4 - low
8.	Data transferred overseas to a non-adequate country.	Accept	<u>Existing Mitigation:</u>	3	1	3 - low

			All transfers of Customer Data out of the European Union, European Economic Area, and Switzerland by the Core Online Services shall be governed by the Standard Contractual Clauses/IDTA, and underpinned by a transfer risk assessment. We have enabled Customer Lockbox in our Admin Portal. Customer Lockbox ensures that Microsoft can't access our content to do any service or support operations without our explicit approval.			
9.	Personal data retained for longer than necessary	Accept	<u>Existing Mitigation</u> At all times during the term of ICO subscription we will have the ability to access, extract and delete Customer Data stored in each Online Service. Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of our subscription so that we may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data within an additional 90 days. Microsoft retains service generated and diagnostic data for a default period of up to 180 days from collection, subject to longer retention periods	2	3	6 - medium

			where required for security of the services or to meet legal or regulatory obligations. ICO retention periods for our data will vary but information within the M365 environment should be managed by Information Asset Owners as per the ICOs Retention and Disposal Policy.[19]			

[19] Guidance for Data Controllers using Office 365 - Microsoft GDPR | Microsoft Learn

5.0 Consult the DPO

Guidance: Once you have completed all of the sections above you should submit your DPIA for consideration by the DPIA Forum who will provide recommendations on behalf of our DPO. The process to follow is here.

Any recommendations from the DPOs team will be documented 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.	There is reference to usage guides, how to policies and etiquette guides for staff to mitigate some risks yet it was noted that these aren't particularly accessible to staff and therefore their impact is limited. Consideration should be given to the creation of a guidance gateway, perhaps on IRIS, for all existing M365 guidance so staff understand where to go for information on M365 applications. Staff need to be clear about what expected use is, what is prohibited and also know when / where to raise queries if they intend new or novel uses of a particular application.	07/12/2022	We recognise the need for continuous review and refresh, and additions to policies, guides, and other resources that help colleagues get the most out of Microsoft 365. We are working with ITHelp and Business Partners to ensure the Digital Support Hub on Iris signposts to all such resources. We have also started to make use of Yammer to grow a community of Microsoft champions and ordinary users sharing best practice for usability and information security. This can also act as an open forum for queries about new or novel uses of the applications, with the answers given displayed for the benefit of everyone.
2.	The content of the DPIA completed by the Dutch Ministry of Justice and Securities was discussed which flags a	07/12/2022	This document was used for reference in the production of this DPIA, and the various risks and mitigations

	number of risks relating to M365 applications. Project team are advised to consider the measures suggested to mitigate risks identified as part of that DPIA to see if any can be implemented by ICO to further reduce risks.		considered against our own position. To briefly address those which we consider applicable here: 1. E2EE for Teams 1-2-1 calls. This has to be user enabled at both ends, so is not practically applicable at tenant level. Its use also disables transcription and recording, which are occasionally useful functions, so we do not see it proportionately necessary to recommend users enable E2EE for 1-2-1 calls at this time. 2. Structural transfer of telemetry to the USA. We only allow required diagnostic data to be collected by Microsoft, which does not include personal, sensitive or identifiable data.[20] 3. (N/A) 4. (N/A – Data Viewer Tool not enabled) 5. Difficulty to exercise data subject access rights to Required Service Data. We will monitor any developments by Microsoft of the DSAR tool. 6. Lack of control: personal data shared with Microsoft and third parties as controllers. Additional Optional Connected Experiences and Teams Third Party Apps both disabled. 7. Employee monitoring system: chilling effect. We have enabled anonymisations to data in Teams Analytics & reports, Viva Insights partially disabled. Further uses of Analytics subject to new DPIAs.

[20] Required diagnostic data for Office - Deploy Office | Microsoft Learn

3	Appendix 3 should be completed in full with text in each row so it's clearer as to whether there are / aren't any specific privacy friendly features deployed for applications that are currently blank.	07/12/2022	Accept – appendix 3 updated

6.0 Integrate the DPIA outcomes back into your plans

Guidance: Completing sections 1 to 5 of your DPIA should have helped you identify a number of key actions 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 suitable 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 from the DPO.

Use the table below to list the actions you now need to take and to 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

Training, usage policies, and How-to/etiquette guides to be reviewed regularly and made available to staff. Further support documents to be produced if M365 usage expands.	Ongoing – no fixed completion date	Will McLoughlin – M365 product owner	N/A
Continue to monitor developments regarding implementation of the EU Data Boundary by Microsoft.	Ongoing – no fixed completion date	Will McLoughlin – M365 product owner	N/A
Request a Transfer Risk Assessment for Microsoft 365 Products	31 October 2023	Will McLoughlin – M365 Product Owner	

7.0 Expected residual risk and sign off by IAO

Guidance: 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.

Note: 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.

The expected risk score for most risks is low and these can be accepted.
There is one medium risk associated with the ICO retaining personal data for longer than is necessary.

7.1 IAO sign off

Guidance: 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
Mike Fitzgerald – Director of Digital, IT and Business Services	22 September 2023	Review of DPIA

8.0 DPIA 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	30/09/2022	Will McLoughlin / Steven Johnston	First Draft
V0.1	07/12/2022	Steven Johnston	DPIA forum
V0.1	13/12/2022	Will McLoughlin / Steven Johnston	Project team responses added to 5.0, Sections 6.0 and 7.0 completed, Appendix 3 updated.
V0.2	19/09/2023	Will McLoughlin / Kate Range / Steven Johnston	Reviewed and updated to incorporate renewed Microsoft Terms and additional legal advice agreed by Kate Range – Head of Legal Services.
V1.0	22/09/2023	Mike Fitzgerald	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: 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

Appendix 3

Whilst all M365 applications are technically available to ICO staff as part of our E5 licence some aren't actively being used. The table below summarises our current use of the M365 applications suite along with any specific steps taken to implement each application in a privacy friendly way.

When considering the deployment of a particular application consideration will always be given to deploying in the most privacy friendly way that still allows us to achieve our purpose and the table below will be updated.

Where the ICO's intended use of an application is significantly at odds with the contents of this DPIA or simply where a more in depth assessment of an application will assist with managing risks this will be completed.

Applications	**Currently actively used by ICO staff Y/N**	**Any additional DPIA or similar risk assessments**	**Notes on deployment of any specific privacy friendly features**
Bookings	N	N	N/A
Calendar	Y	N	Calendars and individual appointments can be set to Private by all users.
Excel	Y	N	N/A
Exchange*	Y	N	*Hybrid configuration: On Cloud side various Mail flow rules, alerts, cloud message recall configured.
Forms	Y	N	N/A
Kaizala	N	N	N/A

Lists	Y	N	N/A
OneDrive	Y	0097 - Core cloud - One Drive - DPIA.docx	N/A
OneNote	Y	N	N/A
Outlook	Y	N	N/A
People	Y	N	N/A
Planner	Y	N	N/A
Power Apps	Y	N	Individual apps should be subject to DPIA Screening as a minimum.
Power Automate	Y	N	Only Standard 365 Connectors enabled for all users. Third Party connectors would need to be fully assessed on their individual merits.
Power BI	Y	N	Governance and request process around access to: Desktop version; Workspaces; Datasets; ability to Publish to Web. Tight restrictions on external sharing, direct queries, export of data to csv/xls. No third party apps or use of APIs by default.
Power Virtual Agents	N	N	N/A
PowerPoint	Y	N	N/A
Project	Y	N	N/A

SharePoint	Y	Intranet Upgrade Data Protection Impact Assessment v0.2.docx	Group based permissions management, retention labelling.
Stream	Y	Teams Live Events and Stream - DPIA.DOCX	Ability to use recording functionality, live events and Stream controlled by IT and limited to preapproved members of staff on request.
Sway	Y	N	N/A
Teams	Y	Team main DPIA 30-09-2020.docx	Teams apps policy restricts access to only approved Microsoft applications with known functionality. All new apps in Teams are first fully assessed before becoming available to ICO staff.
To Do	Y	N	N/A
Visio	Y	N	N/A
Viva Connections	N	N	N/A
Viva Engage	Y	N	Disabled upload of non-image file formats
Viva Insights	Y	N	Only individuals can view personal data and insights based on work patterns in their emails, meetings, calls, and chats. Individual employees choose the insights and experiences they want to receive.

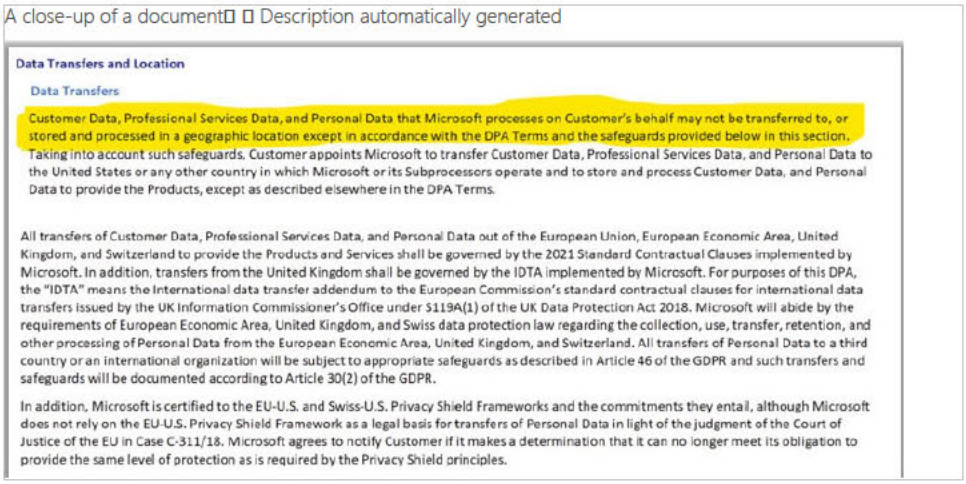
			Item insights and people insights disabled at tenant level via Powershell.
Whiteboard	Y	N	N/A
Word	Y	N	N/A

From: [redacted]
To: Will McLoughlin
Cc: Rob Tomlinson; [redacted]; Mike Fitzgerald
Subject: RE: Data Transfers in Microsoft Support
Date: 22 August 2023 10:01:47
Attachments: image001.jpg
image004.jpg
image005.jpg
image006.gif

External: This email originated outside the ICO.
Morning Will,

Thanks for following up. We have had a response from the GetHelp team this morning which I can share with you below:

" As stated in our DPA all Customer data is processed in accordance with the DPA Terms and the necessary safeguards:



The DPA contains multiple references to data processing that can be used to assure customers that we are processing their data in a compliant way. For example:

To the extent Microsoft uses or otherwise processes Personal Data subject to the GDPR for business operations incident to providing the Products and Services to Customer, Microsoft will comply with the obligations of an independent data controller under GDPR for such use.

Further relevant information regarding data processing can be found under the following DPA sections:

- Nature of Data Processing; Ownership
  - **Processing to Provide Customer the Products and Services**
  - **Processing for Business Operations Incident to Providing the Products and Services to Customer**
- Disclosure of Processed Data
- Processing of Personal Data; GDPR
  - **Processor and Controller Roles and Responsibilities**
  - **Processing Details**
  - **Records of Processing Activities**

Customers can also be assured that when contractual agreements are in place that explicitly describe the processing, Microsoft must meet those obligations.

As a data processor, Microsoft sometimes partners with subcontractors, also known as subprocessors, to perform work on Microsoft's behalf. Microsoft ensures that subprocessors adhere to Microsoft's privacy and security commitments.

Microsoft permits identified authorized subprocessors to process customer data or personal data to deliver only the services Microsoft has retained them to provide. Microsoft prohibits subprocessors from using the data for any other purpose. This is also explained in the ***Notice and Controls on Use of Subprocessors*** section of the DPA

Customers can find the authorized subprocessors on the *Microsoft Online Services Subprocessors List.*

More explanations about subprocessors is also available in the FAQ list at the end of the following page : Microsoft Data Access Management

Should ICO require any additional information or questions, don't hesitate to reach out to us. "

Thanks,

[redacted]

From: Will McLoughlin <Will.McLoughlin@ico.org.uk>
Sent: Tuesday, August 22, 2023 9:17 AM
To: [redacted]
Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>; [redacted]

[redacted] Mike Fitzgerald <Mike.Fitzgerald@ico.org.uk>
Subject: [EXTERNAL] RE: Data Transfers in Microsoft Support
Importance: High

> You don't often get email from will.mcloughlin@ico.org.uk. Learn why this is important

Good morning [redacted]

I hope you had a great weekend and a good start to the new week.

Just wondering if you have anything to share yet, or an update on the projected GetHelp response time?

Any further information you can share will be greatly appreciated.

Thanks again,
Will

Logo

Will McLoughlin

Senior Product Owner – Productivity and Collaboration
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 03304146156
ico.org.uk twitter.com/iconews

For information about what we do with personal data see our privacy notice

---

From [redacted]
Sent: Friday, August 18, 2023 4:12 PM
To: Will McLoughlin <Will.McLoughlin@ico.org.uk>
Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>; [redacted]
Subject: RE: Data Transfers in Microsoft Support

External: This email originated outside the ICO.

Hi Will,

A further update. A GetHelp support agent has been aligned to the ticket I raised this afternoon.

They will be drafting a response of which I will share as appropriate with you early next week.

Have a great weekend in the meantime.

Thanks,

[redacted]

From: Will McLoughlin <Will.McLoughlin@ico.org.uk>
Sent: Friday, August 18, 2023 2:42 PM
To: [redacted] >
Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>; [redacted]
Subject: [EXTERNAL] RE: Data Transfers in Microsoft Support

Thanks for the updates, [redacted] and we really appreciate your efforts to expedite this as swiftly as possible.

Will

From [redacted]
Sent: Friday, August 18, 2023 2:40 PM
To: Will McLoughlin <Will.McLoughlin@ico.org.uk>
Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>; [redacted]
Subject: RE: Data Transfers in Microsoft Support

External: This email originated outside the ICO.

Hi Will,

A further update. I have raised an internal case to engage our Privacy and Compliance team this afternoon.

This is called a "GetHelp" and usually takes 48 hours for an agent to be assigned to help answer a query.

Please expect further updates to follow.

Thanks,

[redacted]

From: [redacted]
Sent: Friday, August 18, 2023 2:14 PM
To: Will McLoughlin <Will.McLoughlin@ico.org.uk>

Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>; [redacted]
Subject: RE: Data Transfers in Microsoft Support

Hi Will,

A quick update. I have raised this with CELA and will come back to you as soon as I hear back from them.

Currently no ETA I can advise on, but will ensure to be proactive in order to obtain a prompt reply.

Thanks,

[redacted]

From: Will McLoughlin <Will.McLoughlin@ico.org.uk>
Sent: Friday, August 18, 2023 10:01 AM
To: [redacted]
Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>; [redacted]
Subject: [EXTERNAL] RE: Data Transfers in Microsoft Support
Importance: High

Hi [redacted]

Please could you put to CELA the following question:

Please provide a list of all countries in which ICO Customer Data (i.e. excluding telemetry and other Microsoft generated data, and Professional Services data) is processed by Microsoft. Please include locations of any sub-processors used by Microsoft in the processing of such ICO Customer Data.

Could you also give us a timeframe for when we can expect a response – this is now a high priority matter for us.

Thanks
Will

From: [redacted]
Sent: Tuesday, August 15, 2023 4:31 PM
To: Will McLoughlin <Will.McLoughlin@ico.org.uk>
Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>; [redacted]
Subject: RE: Data Transfers in Microsoft Support

External: This email originated outside the ICO.

Hi Will,

Thanks for flagging and I suspect this is exactly as you say, the CPMC resources are only available to those who are Compliance Program members.

I've been doing some research into the handling of support cases from an information privacy perspective and in short, there are no straightforward answers or guidance I am able to share.

Instead the best route to obtain definitive confirmation to the questions you have is for me to raise a Privacy Request with CELA, our Corporate External and Legal Affairs division.

So that I can ensure absolute accuracy, please can I ask you to provide clear verbatim to outline each of your queries in relation to this?

I will then copy and paste this verbatim and raise the Privacy request this afternoon. Please feel free to also ask the question around what is involved in joining the Compliance Program.

Feel free to come back to me with any queries.

Thanks,

[redacted]

From: Will McLoughlin <Will.McLoughlin@ico.org.uk>
Sent: Tuesday, August 15, 2023 3:45 PM
To: [redacted]
Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>; [redacted]
Subject: [EXTERNAL] RE: Data Transfers in Microsoft Support

Hi [redacted]

Thanks again for your time today and the helpful discussion.

I'm having a look through some of the Trust Portal resources now, and just wondering why we don't have access to the Compliance Program for Microsoft Cloud (CPMC) resources, located here:

Resources for your Organization - CPMC (microsoft.com)

How might these resources be made available to us? Do we need to join the Compliance Program, and if so what is involved in doing so?

Regards,
Will

From: [redacted]
Sent: Monday, August 14, 2023 2:45 PM
To: Will McLoughlin <Will.McLoughlin@ico.org.uk>
Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>; [redacted]
Subject: RE: Data Transfers in Microsoft Support

External: This email originated outside the ICO.

Hi Will,

I have sent a place holder across for tomorrow at 3pm.

Hope this slot works otherwise happy to reschedule to an alternative.

Thanks,

[redacted]

From: Will McLoughlin <Will.McLoughlin@ico.org.uk>
Sent: Monday, August 14, 2023 12:16 PM
To [redacted]
Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>; [redacted]
Subject: [EXTERNAL] RE: Data Transfers in Microsoft Support

Hi [redacted]

Thanks for getting in touch (and thanks to [redacted] for the link-up).

Do you have any availability for a call this week – I think it will be easier for us to explain that way.

Thanks,
Will

From: [redacted]
Sent: Monday, August 14, 2023 10:58 AM
To: Will McLoughlin <Will.McLoughlin@ico.org.uk>
Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>; [redacted]
Subject: RE: Data Transfers in Microsoft Support

External: This email originated outside the ICO.

Hi Will,

Would it be possible to elaborate a little more on the queries you have?

With some additional context and clarification I may be able to help or at the very least advise who and how to get the answers.

Thanks,

[redacted]

From: [redacted]
Sent: Monday, August 14, 2023 10:51 AM
To: Will McLoughlin <Will.McLoughlin@ico.org.uk>; [redacted]
Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>; [redacted]
Subject: RE: Data Transfers in Microsoft Support

Adding [redacted]

Hi Will,

Sorry for the delay.

I have added [redacted] to the email.

[redacted] – Please could you provide guidance on how Microsoft's support model works.

Thanks.

Regards,

[redacted] | Microsoft 365 Engineering [redacted]

Email & IM [redacted]

Accelerating your journey to Microsoft 365 - Getstarted HERE

From: Will McLoughlin <Will.McLoughlin@ico.org.uk>
Sent: Tuesday, August 8, 2023 11:58 AM
To: [redacted]
Cc: Rob Tomlinson <rob.tomlinson@ico.org.uk>
Subject: [EXTERNAL] Data Transfers in Microsoft Support

Hi [redacted]

Hope you are both well.

Bit of a random one, we would like to discuss with somebody how Microsoft's support model works in practice with regard to the following: https://learn.microsoft.com/en-us/compliance/regulatory/offering-eu-model-clauses#microsoft-and-european-union-model-clauses

Is there somebody well versed in this stuff who would be happy to have a conversation with us?

Thanks,
Will

Will McLoughlin

Senior Product Owner – Productivity and Collaboration
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 03304146156
ico.org.uk twitter.com/iconews

For information about what we do with personal data see our privacy notice