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

Commented [SJ1]:

Commented [SJ2]:

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