DATA PROTECTION IMPACT ASSESSMENT - Off-site Document Storage Re-tender V1.0

Reference number: DPIA-490

Author: Eileen Hudson
Email: eileen.hudson@nottinghamcity.gov.uk

DATA PROTECTION IMPACT ASSESSMENT

When to complete this template:

Start to fill out the template at the beginning of any major project involving the use of personal data, or, where you are making a significant change to an existing process that affects personal data. Please ensure you update your project plan with the outcomes of the DPIA.

Table of Contents

1. Document Control

1. Control Details

Author of DPIA:	Eileen Hudson, Principal Records Officer
Owner of project:	Eileen Hudson, Principal Records Officer Alison Liversidge, Information Compliance Specialist
Contact details of Author:	Eileen.Hudson@nottinghamcity.gov.uk Alison.Liversidge@nottinghamcity.gov.uk 0115 876 3855

2. Document Amendment Record

Issue	Amendment Detail	Author	Date	Approved
V0.1	First draft	Eileen Hudson	14/06/2023	

3. Contributors/Reviewers

Name	Position	Date
Eileen Hudson	Principal Records Officer	14/06/2023
Alison Liversidge	Information Compliance Specialist	

1. Glossary of Terms

Term	Description
NCC	Nottingham City Council
IC	Information Compliance
Box-it	Current document storage provider

Author: Eileen Hudson
Email: Eileen.Hudson@nottinghamcity.gov.uk

2. Screening Questions

1. Does the project involve personal data? **Yes**	**If 'Yes', answer the questions below. If 'No', you do not need to complete a DPIA but make sure you record the decision in the project documentation.**
2. Does the processing involve any of the following data: medical data, ethnicity, criminal data, biometric data, genetic data and any other special/ sensitive data?	**Yes**
2. Does the processing involve any systematic or extensive profiling?	**No**
3. Does the project involve processing children's data or other vulnerable citizen's data?	**Yes**
4. Does the processing involve decisions about an individual's access to a product, service, opportunity or benefit that is based on any evaluation, scoring, or automated decision-making process?	**No**
5. Does the processing involve the use of innovative or new technology or the novel application of existing technologies?	**Yes**
6. Does this project involve processing personal data that could result in a risk of physical harm in the event of a security breach?	**Yes**
7. Does the processing combine, compare or match data from multiple sources?	**No**
8. Does the project involve processing personal data without providing a privacy notice?	**No**
9. Does this project process data in a way that tracks on line or off line location or behaviour?	**No**
10. Will the project involve using data in a way it has not been used before?	**Yes**
11. Does the project involve processing personal data on a larger scale?	**Yes**
12. Will the project involve processing data that might prevent the Data Subject from exercising a right or using a service or entering into a contract?	**No**
If you answered 'Yes' to any <u>two</u> of the questions above, proceed to Question 3 below. If not seek advice from the DPO as you may not need to carry out a DPIA.	**Proceed**

Project Title: **Off-site Document Storage Re-tender**

Team: **Information Compliance, Legal and Governance**

Directorate: **Finance and Resources**

DPIA Reference number: ***DPIA-490***

Has Consultation been carried out? At the present time, consultation has not been carried out. However, the team are planning to consult with internal stakeholders to see what their priorities are for an off-site storage provider, as well as the possibility of digitisation of paper records. The team are also planning on undertaking some soft market research with providers through Procurement.

1. DDM attached?	**No – we are in the process of drafting various documents for the tendering process and for the various NCC Boards. These can be made available once drafted.**
2. Written evidence of consultation carried out attached?	**No – see above**
3. Project specification/ summary attached?	**No – we are in the process of drafting the specification for procurement and can be made available on request.**
4. Any existing or previous contract / SLA / processing agreement attached?	**Yes**
5. Any relevant tendering documents attached?	**No – we are in the process of drafting various documents for the tendering process and for the various NCC Boards. These can be made available once drafted**
6. Any other relevant documentation attached?	**No**

3. Project - impact on individual's privacy

Issue	Questions	Examples	Yes/No	Initial comments on issue & privacy impacts
Purpose and means		Profiling, data analytics, Marketing. Note: The GDPR requires a DPIA to be carried out where there is systematic and extensive evaluation of personal aspects relating to individuals based on automated processing, including profiling, and on which decisions about individuals are based.		
	Please give a summary of what your project is about (*you can also attach or embed documents for example a project proposal*).			NCC has been using Box-it as the off-site document storage provider since 2010. The contract for the service has expired since 2015, and since then has been on a rolling yearly contract. However, in April 2023, Information Compliance were made aware that this was unable to continue and the service had to go out to tender. Information Compliance have been trying to undertake this re-tender process since 2019 but this has stalled due to the Covid-19 pandemic.
	Aims of project Explain broadly what the project aims to achieve and what types of processing it involves.			The aims of the project is to ensure that an offsite storage provider is awarded the contract to provide physical storage of all manner of documents in an offsite storage facility and to help NCC to digitise selected records and to provide these in a PDF or alternative suitable format. We will also be asking them to confidentially destroying records on the request of NCC. IC will be also looking into the prospect of obtaining a new case management system for internal users to record their box contents and to retrieve their documents as the current database/s are not currently fit for purpose, and the IT support Information Compliance have is restricted to one team member leading to a single point of failure in this area.
	Describe the nature of the processing How will you collect store and delete data? Will you be sharing with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are			The various aspects of processing IC would be asking the document storage provider to undertake will be: the storage of paper records (equating to around 23,000 boxes), adaptation or alteration when preparing files for digitisation, the retrieval and delivery of information to various NCC sites, disclosure of information when digitising records, erasure or destruction of data through confidentially destroying paper records that have reached their retention, or when they are no longer required. All types of processing are deemed of high risk as the offsite provider will be responsible for the protection of all types of data – personal, sensitive and

	involved? Who will have access to the project personal data, how is access controlled and monitored and reliability of staff assessed? Will data be separated from other data with in the system?		commercially sensitive data that requires to be kept by NCC. The majority of long retention dates are for boxes owned by People and Legal and these are deemed of particularly high risk due to the nature of the data (ASC, CIS, Mitigation, Deeds, Legal cases involving Children and Adults). Staff at the offsite provider will have access to these records (to securely store and deliver to NCC sites) possibly with an external scanning provider if it deemed best value to separate the two functions Information Compliance feels would be necessary to future proof these documents. The current system of allowing only relevant NCC staff access to particular records will continue to be implemented if a new system is created, and this will remain in the same way as it is now (managed by Records Management, ensuring that Records Management e-learning has been completed and team manager authorisation provided)	
	Privacy Implications Can you think of any privacy implications in relation to this project? How will you ensure that use of personal data in the project is limited to these (or "compatible") purposes?		Yes	If a new provider is awarded the contract, there will need to be measures in place in order to ensure that NCC's data is protected from any unauthorised access or breach. There will be a processing agreement in place with the new provider to ensure all Data Protection and Records Management aspects are covered, unless this is within the contract which will be reviewed by the DPO and other Legal colleagues (such as contracts).
	New Purpose Does your project involve a new purpose for which personal data are used?		No	The main processing elements and purposes will remain the same as they are now with Box-it. However, there will be a focus on digitisation of records which have a longer retention period (35+ years) in order to remove these from physical storage and to be more accessible as part of the move towards hybrid working. This new development will also form a large part of the specification as part of the tendering process.
	Consultation Consider how to consult with relevant stakeholders: Describe when and how you will seek individuals' views- or justify why it's not appropriate to do so. Who else do you need to involve in NCC? Do		Yes	This is a back office function which will not directly affect the way that NCC delivers services to citizens. IC has already met with NCC IT around the provision for the documents which will be digitised and have some help from that area. IC has put requested IT support with the project.

	you plan to consult Information security experts, or any other experts?			IC aim to also ask for department subject matter experts to assist us with the thoughts around digitising documents and where they could be stored (SharePoint, specific case management system etc.).
Individuals (data subjects)	Will the project:	Expanding customer base; Technology which must be used by individuals; Hidden or complex uses of data; Children's data		
	Affect an increased number, or a new group, or demographic of individuals (to existing activities)?		No	The storage of paper records will remain the same as it is now, but with the external storage provider that will be awarded the contract.
	Involve a change to the way in which individuals may be contacted, or are given access to services or data? Are there any areas of public concern that you should factor in?		No	The storage of paper records will remain the same as it is now, but with the external storage provider that will be awarded the contract.
	Affect particularly vulnerable individuals, including children?		Yes	There are many boxes in storage that hold children's data and those of adults, and vulnerable individuals. There will be no change in how these are managed, just who will be the provider of the storage.
	Give rise to a risk that individuals may not know or understand how their data are being used?		No	The storage of paper records will remain the same as it is now, but with the external storage provider that will be awarded the contract.
Parties	Does the project involve:	Outsources service providers; Business partners; Joint ventures		
	The disclosure of personal data to new parties?		Possibly	If a new external storage provider is awarded the contract then citizens, colleagues and commercially sensitive data will be disclosed to this new provider due to the movement and storage of c23, 000 boxes will commence.

	The involvement of sharing of personal data between multiple parties?		Possibly	There could be the sharing of personal and sensitive information between different parties if it is deemed by NCC's leadership that it would be more beneficial to have one provider providing an archive service, and one provider undertaking the digitisation of paper records.
Data categories	Does the project involve:	Special personal data; Biometrics or genetic data; Criminal offences; Financial data; Health or social data; Data analytics: Note: the GDPR requires a DPIA to be carried out where there is processing on a large scale of special categories of data or of data relating to criminal convictions and offences		
	The collection, creation or use of new types of data?		Yes	At the present time, Information Compliance have stemmed the amount of new boxes entering storage per year (1500 from 2019 to 100 in 2022). However new boxes are entering storage and will contain various personal data. The new use of data will potentially be the digitisation of data that have longer retention period (35+ years). There will be more work undertaken in the future around the use of SharePoint/Case Management systems to store digitised files for easy retrieval and use by NCC colleagues as part of the hybrid working model.
	Use of any special or privacy-intrusive data involved? • Political opinions • Religious beliefs or philosophical beliefs • Trade union membership • Genetic data • Biometric data • Sexual life • Prosecutions • Medical data		Yes	Special data contained within the boxes held at off-site storage will contain the following: • Political opinions • Religious beliefs or philosophical beliefs • Trade union membership • Sexual life • Prosecutions • Medical data • Criminal data There may be biometric/genetic data but IC are yet to come across this in exercises to remove data from off-site storage.

	• Criminal data (Criminal data processing, i.e. criminal convictions, etc. also has special safeguards under Article 10)			
	New identifiers, or consolidation or matching of data from multiple sources? (For example a unique reference number allocated by a new management system)		Possibly	Currently, Box-it use a barcode system in order to automatically update their systems when boxes are in, out, or destroyed. This has an M number attached which is their unique code. The internal off-site database uses a box code consisting of two letters and four numbers. If a new provider comes in, there may be a new way of them identifying the boxes, and this may be the case if a new internal database is also procured as part of this process.
Technology	New solutions:	Locator or surveillance technologies; Facial recognition; Note: the GDPR requires a DPIA to be carried out in particular where new technologies are involved (and if a high risk is likely)		
	Does the project involve new technology that may be privacy-intrusive?		No	

Data quality, scale and storage	Data:	New data		
	Does the project involve changes to data quality, format, security or retention? What are the benefits of the processing? i.e. will the new system have automatic retention features? Will the system keep the information in a safer format etc.?		Yes	The main change will be to the storage of physical paperwork in boxes held off site. Information Compliance will set out in the specification how we expect data to be stored, and to what high standards especially for those documents in the 'strong room' (registers, deeds). If a new provider is awarded, then this will change the way documents are stored securely as well as how the provider may undertake destruction of boxes. A change to the format of the data will take place if we decide that historical scanning of paperwork (and the destruction of the physical paperwork) will take place as the data will only be held electronically and work will be required to ascertain how we can futureproof these electronic documents up to 100 years in the future without them digitally degrading.
	Does the project involve processing data on an unusually large scale?		Yes	
Monitoring, personal intrusion	Monitoring:	Surveillance; GPS tracking; Bodily testing; Searching; Note: the GDPR requires a DPIA to be carried out where the project involves systematic monitoring of a publicly accessible area on a large scale		
	Does the project involve monitoring or tracking of individuals or activities in which individuals are involved?		No	
	Does the project involve any intrusion of the person?		No	
Data transfers	Transfers	Transfers outside the EEA		
	Does the project involve the transfer of data to or activities within a country that has inadequate or significantly different data protection and privacy laws?		No	This should not change even if the digitised documents are to be stored on Microsoft SharePoint. Microsoft's DPA states that "*Taking into account such* safeguards, *Customer appoints Microsoft to transfer Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Sub processors operate and to store and process Customer Data, and Personal Data to provide the Products, except as*

				described elsewhere in the DPA Terms." However, NCC IT confirms that Microsoft processes all NCC data in the UK South region of the EEA and NCC IT is not planning to allow any change in this position. NCC will ensure that the contract with any service provider who processes NCC personal data outside the UK/EEA will ensure NCC continues to comply with data protection legislation.

4. Legal Framework and Governance – Compliance

Ref.	Question	Response	**Further action required** (and ref. to risk register as appropriate)
1. Applicable laws and regulation			
1.1	Which data protection laws, or laws which impact data protection and privacy, will be applicable to the project?	• UK General Data Protection Regulation • Data Protection Act 2018 • Human Rights Act 1998	
1.2	Are there any sector-specific or other regulatory requirements or codes of practice, which should be followed?	ISO 15489-1:2016 - Records Management ISO 9000 and ISO 9001 – Quality Management Principles	
2. Organisation's policies			
2.1	Is the project in compliance with the organisation`s information management policies and procedures (including data protection, information security, electronic communications)?	Yes.	

2.2	Which policy requirements will need to be followed throughout design and implementation of the project?	Data Protection Policy Information Security Policy Records Management Policy	
2.3	Are any changes/updates required to the organisation`s policies and procedures to take into account the project? **Note: new requirements for *"Accountability"* under the GDPR, including record-keeping, DPOs and policies**	If a new organisation is awarded the contract, there will need to be some updates to the training information provided by Information Compliance about how colleagues can access their boxes, and if a new system is procured as part of this process, documents and intranet pages will need to be updated along with communications to all staff. There may need to be some updates to record-keeping if any identifiers of the boxes are needing to be changed.	
3. Training and roles			
3.1	Will any additional training be needed for staff in relation to privacy and data protection matters arising from the project?	A refresh of training will be produced for all users of the off-site storage provision in order for them to understand how the change in provider may affect how boxes are retrieved and sent back to storage. This may also lead to a refresh of the Record Management e-learning.	

5. Personal Data Processing Compliance

Ref.	Question	Response	**Further action required (**and ref. to risk register as appropriate)
1.	**Personal Data Processing**		
1.1	Which aspects of the project will involve the processing of personal data relating to living individuals?	The storage of paper records (equating to around 23,000 boxes), adaptation or alteration when preparing files for digitisation, the retrieval and delivery of information to various NCC sites, disclosure of information when digitising records, erasure or destruction of data through confidentially destroying paper records that have reached their retention, or when they are no longer required.	
1.2	Who is/are the data controller(s) in relation to such processing activities?	Nottingham City Council.	
1.3	Who is/are the data processor in relations to such processing activities?	Chosen Offsite storage provider. Chosen scanning provider (if separate to the storage provider)	
2.	**Fair and Lawful processing - GDPR Articles 5(1)(a), 6, 9, 12, 13**		
2.1	Which fair processing conditions are you relying on? GDPR: Article 6(1) (legal basis for processing) and, for sensitive personal data, Article 9(2).	6(1). **Choose at least one of the following for personal data**, **usually (e)**-(Cross out the rest) ~~a) Consent~~ ~~b) Performance of contract~~ ~~c) Legal obligation~~ d) ~~Vital interests~~ **e) Public interest / exercise of Authority** 9(2) Choose at least 1 for special data-usually g (cross the rest out) ~~a)Explicit consent~~	The lawful basis under Article 6 and special conditions under Article 9 would be completely dependent on the information that is stored off-site. The lawful basis for processing the data will be dependent on the purposes for which the data is processed or the business area using it. Commonly, NCC processes personal data in pursuit of its public functions as a local authority. Therefore, Public Task is usually the lawful basis.

		~~b) Employment / social security / social protection obligations~~ ~~c) Vital interests~~ ~~d) Non-profit bodies~~ ~~e) Processing made public by data subject~~ ~~f) Legal claims~~ **g) Substantial public interest** ~~h) Health, social care, medicine~~ ~~I) Public interest for public health~~ **j) Archiving, statistics, historical research** **For any criminal Data** Comply with Article 10 **if it meets a condition in Part 1, 2 or 3 of Schedule 1.** • ~~Employment, social security and social protection~~ • ~~Health and social care purposes~~ • ~~Public health~~ • ~~Research~~ Substantial public interest: • **Statutory and government purposes** • ~~Equality of opportunity and treatment~~ • ~~Racial and ethnic diversity at senior levels of organisations~~ • ~~Preventing or detecting Unlawful Acts~~ • ~~Protecting the public against dishonesty etc~~ • ~~Regulatory requirements relating to unlawful acts and dishonesty etc~~ • ~~Journalism etc in connection with unlawful acts and dishonesty etc~~ • ~~Preventing fraud~~	However, this data may relate to several other functions, even informal ones. There will be some data or processing which will not be appropriate.

		~~• Suspicion of terrorist financing or money laundering~~ ~~• Counselling~~ ~~• Safeguarding of children and of individuals at risk~~ ~~• Safeguarding of economic well-being of certain individuals~~ ~~• Insurance~~ ~~• Occupational pensions~~ ~~• Political parties processing~~ ~~• Disclosure to elected representatives~~ ~~• Informing elected representatives about prisoners~~ ~~Additional Conditions~~ ~~• Consent~~ ~~• Vital interests~~ ~~• Personal data in the public domain~~ ~~• Legal claims~~ ~~• Judicial Acts~~	
Note: different conditions may be relied upon for different elements of the project and different processing activities. Also, the scope of special category data is wider under the GDPR, and in particular includes genetics & biometric data, and sexual orientation.			
2.2	How will any consents be evidenced and how will requests to withdraw consent be managed?	NCC will not rely on consent as a legal basis for processing data.	
Note: new requirements for obtaining and managing consents within the GDPR.			
2.3	Is the data processing under the project covered by fair processing information already provided to individuals or is a new communication needed (see also data subject rights below)?	Not necessary – service team's own privacy notices highlight to data subjects how long NCC retains their information.	
Note: more extensive information required under the GDPR than under current law, and new requirements on how such information is provided. Also a general principle of "*transparency*". It is important to assess necessity and Proportionality			

2.4	If data is collected from a third party, are any data protection arrangements made with such third party?	No.	
2.5	Is there a risk of anyone being misled or deceived?	No.	
2.6	Is the processing "fair" and proportionate to the need's and aims of the projects?	Yes – we will require the offsite storage provider to provide NCC with all those processing activities to help us manage our physical data on citizens, staff and commercial aspects.	
2.7	Are these purposes clear in privacy notices to individuals? (see above)	N/a – see above	
3. Adequate, relevant and not excessive, data minimisation - GDPR Article 5(1)(c)			
3.1	Is each category relevant and necessary for the project? Is there any data you could not use and still achieve the same goals?	Yes – the information that is held by the offsite storage provider (currently Box-it) and data held on the internal database is necessary as an audit trail and to help find and retrieve information easily and accurately.	
Note: GDPR requires data to be "limited to what is necessary" for the purposes (as well as adequate and relevant).			
3.2	Is/can data be anonymised (or pseudonymised) for the project?	No.	
4. Accurate and up to date - GDPR Article 5(1)(d)			
4.1	What steps will be taken to ensure accurate data is recorded and used?	It is the responsibility of the individual box owner or service area to ensure that the box information recorded is accurate and reflects the contents of the boxes. IC is trying to improve this going forwards, but it is difficult to get staff to undertake this retrospectively. Information Compliance will undertake some data analysis exercises if the boxes need to	

		be moved over to a new provider ensure both their records and those held on the internal database match.	
For example: checks when receiving/sending information from/to third parties, or transcribing information from oral conversations or handwritten documents, any automatic checks on information not meeting certain criteria.			
4.2	Will regular checks be made to ensure project data is up to date?	Please see above.	
5. Data retention - GDPR Article 5(1)(e)			
5.1	How long will personal data included within the project be retained?	Each box has its own defined retention date as set by the box creator. Retention dates range from 1 year to 100 years (maximum that can be recorded, but these are usually needing to be kept in perpetuity).	
5.2	How will redundant data be identified and deleted in practice? Consider paper records, electronic records, equipment?	Information Compliance are undertaking a project to remove boxes at their retention date automatically, and to tackle the historic backlog of retained boxes. This will continue to take place if a new provider is awarded the contract. Information Compliance will attempt to remove all non-compliant boxes before their movement over to a new provider, or if this is not possible, to have a plan on how to remove these as soon as possible once they are moved over.	
5.3	Can redundant data be easily separated from data which still need to be retained?	This should be identified by box owners and their service areas from the information held on the internal database. The offsite provider cannot do this as they will remove a whole box rather than individual documents.	
6. Data subject rights - GDPR Articles 12 to 22			
6.1	Who are the relevant data subjects?	Citizens, staff, external stakeholders, members of the public.	

6.2	Will data within the project be within the scope of the organisation`s subject access request procedure?	Yes.	
6.3	Are there any limitations on access by data subjects?	Yes – Any rights requests will be handled under the Council's existing policies and procedures.	
6.4	Is any data processing under the project likely to cause damage or distress to data subjects? How are notifications from individuals in relation to damage and distress managed?	All rights requests will be handled under the Council's existing policies and procedures. Nottingham City Council can restrict the above rights in certain circumstances for example to avoid obstructing an investigation, avoid prejudicing the prevention, detection, investigation, or prosecution of criminal offences or to protect the rights and freedoms of others. This is not unique to this processing activity.	
6.5	Does the project involve any direct marketing to individuals? How are requests from data subjects not to receive direct marketing managed?	No.	
6.6	Does the project involve any automated decision making? How are notifications from data subjects in relation to such decisions managed?	No.	
6.7	How will other rights of data subjects be addressed? How will security breaches be managed?	These rights will be processed by the Information Compliance Team at Nottingham City Council. All breached will be dealt with by the Information Compliance team and the Data Protection Officer.	

7. Data Security - GDPR Articles 5(1)(f), 32

For example:

- **Technology**: encryption, anti-virus, network controls, backups, DR, intrusion detection;
- **Physical**: building security, clear desks, lock-leads, locked cabinets, confidential waste;

Organisational: protocols on use of technology, asset registers, training for staff, pseudonymisation, regular testing of security measures.			
Describe the source of risk and nature of potential impact on the individuals. Include associated compliance and corporate risks as necessary -What security measures and controls will be incorporated into or applied to the project to protect personal data? Consider those that apply throughout the organisation and those which will be specific to the project. N.B Measures that are appropriate to the nature of the data and the harm which may result from a security breach	**Likelihood of harm** Remote, Possible or Probable	**Severity of harm** Minimal, Significant or Severe	**Overall Risk** Low, Medium or High
1. Loss of paperwork during the move from Box-it to the new provider. This would be a breach of the Article 5 Principle (f) 'security' of the UK GDPR.	Possible	Severe	High
2. Data that has been processed previously has been retained for longer than necessary when the data is no longer needed. This would be a breach of the Article 5 Principle (e) 'storage limitation' of the UK GDPR.	Probable	Significant	Medium
3. Destruction of records that have not been authorised by the off-site provider. This would be a breach of the Article 5 Principle (f) 'security' of the UK GDPR.	Possible	Significant	Medium
4. Intentional unauthorised access to data by the staff at the offsite storage provider. This would be a breach of the Article 5 Principle (f) 'security' of the UK GDPR.	Possible	Severe	Medium
5. Data that is digitised is not future proofed and the data is no longer recoverable in the future. This would be a breach of the Article 5 Principle (f) 'security' of the UK GDPR.	Probable	Significant	High
6. Risk that the awarded offsite storage provider does not have the relevant standards and data protection aspects in place. This would breach all standards under the UK GDPR.	Remote	Minimal	Low

7. Lack of knowledge between colleagues if the process needed to change if a new provider is awarded the contract. This could breach the Article 5 Principle (d) 'accuracy' of the UK GDPR.		Probable	Significant	Medium
Identify measures to Reduce Risk- Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk that you have identified				
Risk	Options to reduce or eliminate risk	**Effect on risk** Eliminated/ Reduced or Accepted	**Residual risk** Low/Medium/High	**Measures approved** Yes/No
1. Loss of paperwork during the move from Box-it to the new provider. This would be a breach of the Article 5 Principle (f) 'security' of the UK GDPR.	The new awarded offsite provider will, as part of the contract, have to ensure that there is a robust process in place to ensure no documentation goes missing at any time of the contract. This will be ensured through Procurement, Legal and Data Protection. Information Compliance may also assist with this process to ensure the process is as robust as possible.	Reduced	Medium	Yes
2. Data that has been processed previously has been retained for longer than necessary when the data is no longer needed. This would be a breach of the Article 5 Principle (e) 'storage limitation' of the UK GDPR.	Information Compliance are taking a proactive approach to this by contacting box owners at the time their boxes are due to expire and this process will continue for all paper documents. Historical paperwork will be removed from storage prior to the move by Information Compliance.	Reduced	Low	Yes
3. Destruction of records that have not been	An audit trail will be undertaken at all times and we will expect the offsite	Reduced	Low	Yes

authorised by the off-site provider. This would be a breach of the Article 5 Principle (f) 'security' of the UK GDPR.	provider to only accept requests for deletion that come from Information Compliance to ensure that this does not happen.			
4. Intentional unauthorised access to data by the staff at the offsite storage provider. This would be a breach of the Article 5 Principle (f) 'security' of the UK GDPR.	The contract and processing agreement will set out the security requirements for staff who work as part of the provider. We would expect that if there is any unauthorised access detected that this would be dealt through the data breach protocol.	Reduced	Low	Yes
5. Data that is digitised is not future proofed and the data is no longer recoverable in the future. This would be a breach of the Article 5 Principle (f) 'security' of the UK GDPR.	Information Compliance will want to build this into the specification as the contract will run for 10 years however there will be a lot of work undertaken to ensure that this risk is mitigated as much as possible – there is no way to know how technology will look in 100 years as IT has not been around that long at present.	Accepted	Medium	Yes
6. Risk that the awarded offsite storage provider does not have the relevant standards and data protection aspects in place. This would breach all standards under the UK GDPR.	Procurement selection documents for publication must have rigorous data protection and IT security questions in order to ensure that due diligence can be carried out on providers prior to award	Reduced	Low	Yes
7. Lack of knowledge between colleagues if the process needed to change if a new provider is awarded the contract.	If the processes need to change, Information Compliance will conduct training and produce guidance to inform colleagues, and will send out comms	Reduced	Low	Yes

This could breach the Article 5 Principle (d) 'accuracy' of the UK GDPR.	across the organisation to inform colleagues of the change.			
8. Data processors - GDPR Article 28 & direct obligations in other articles				
8.1	Are any data processors involved in the project?	Off-site storage provider – not currently awarded. Processing Agreement has been created for Box-it for this financial year.		
8.2	What security guarantees do you have?	Unable to comment until procurement award is granted.		
For example: specific security standards or measures, reputation and reviews				
8.3	Please attach the processing agreement	Current Processing Agreement for Box-it for 2022/2023		
For example: security terms, requirements to act on your instructions, regular audits or other ongoing guarantees Note: new requirements for the terms of contracts under the GDPR (much more detailed than current law).				
8.4	How will the contract and actions of the data processor be monitored and enforced?	Power to audit under the processing agreement.		
8.5	How will direct obligations of data processors be managed?	Under the processing agreement		
Note: New direct obligations for processors under the GDPR, including security, data protection officer, record-keeping, international data transfers.				
For example: fair & lawful, lawful purpose, data subject aware, security, relevance.				
9. International data transfers - GDPR Articles 44 to 50				
9.1	Does the project involve any transfers of personal data outside the European Union or European Economic Area?	No	See 'Data Transfers' above on page 13.	

9.2	What steps are taken to overcome the restrictions?	N/A	
For example: Safe Country, contractual measures, binding corporate rules, internal assessments of adequacy Note: GDPR has similar methods to overcome restrictions as under current law, but there are differences to the detail and less scope for an "own assessment" of adequacy.			
10. Exemptions			
10.1	Will any exemptions for specific types of processing and/or specific DP requirements be relied upon for the project?	No	
For example: crime prevention, national security, regulatory purposes Note: Exemptions under the GDPR to be assessed separately, and may be defined within additional EU or UK laws.			

6. Sign off and record outcomes

Item	**Name**	**Date**
Measures approved by: (project owner) This must be signed before the DP can sign off on the DPIA.	Eileen Hudson (E.S.Hudson)	15/06/2023
Residual risks approved by: (If accepting any residual high risk, consult the ICO before going ahead)	Eileen Hudson (E.S.Hudson)	15/06/2023
DPO advice provided: (DPO should advise on compliance, measures and whether processing can proceed)	*T.Pollard*	15/08/2023
Summary of DPO advice: *Procurement process must ensure that data protection and IT security questions draw out correct information from bidders so that necessary scoring can ensure that a provider with sufficient guarantees is awarded the contract.* *Processing terms in contract must be reviewed by Information Compliance team before publication*		
DPO advice accepted or overruled by		If overruled, you must explain your reasons
Comments:		
IT Security Officer: Where there are IT security issues		
IT Officer comments:		
SIRO Sign off: (For major projects)		
Consultation responses reviewed by:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA