Sensely UK Ask First

Data Protection Impact Assessment

VERSION DATE	NOTES	AUTHOR
2021-12-21		Emma

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. PROJECT CONTEXT

Sensely UK Ltd is a UK-based software and application development company providing healthcare technology solutions for a range of healthcare sector clients and registered as a Data Controller under ZA194147. The organisation is based in London.

Sensely UK Ltd is a subsidiary of Sensely Corporation which has its base in the United States.

Whilst Sensely UK Ltd offers a variety of services, often providing bespoke offerings tocustomers, the intention of this DPIA is to provide an assessment for the core technicalinfrastructure and sharing processes that are common to the Sensely UK Ltd service, namely the AskFirst App. The Sensely UK Ltd Data Protection Officer will then be in a position to identify whether a new or revised DPIA is required for each customer where a deviation from the core product exists.

Information Assets

The Sensely UK Ltd service is built around 3 key information assets;

1. RedCentric Application Server
2. RedCentric Database Server
4. AWS EDM

Processing Activities

- App Registration
- User Spine Matching
- Link to GP System
- Provision of Symptom Checker Service
- Direction to 111 Service
- GP Appointment Booking

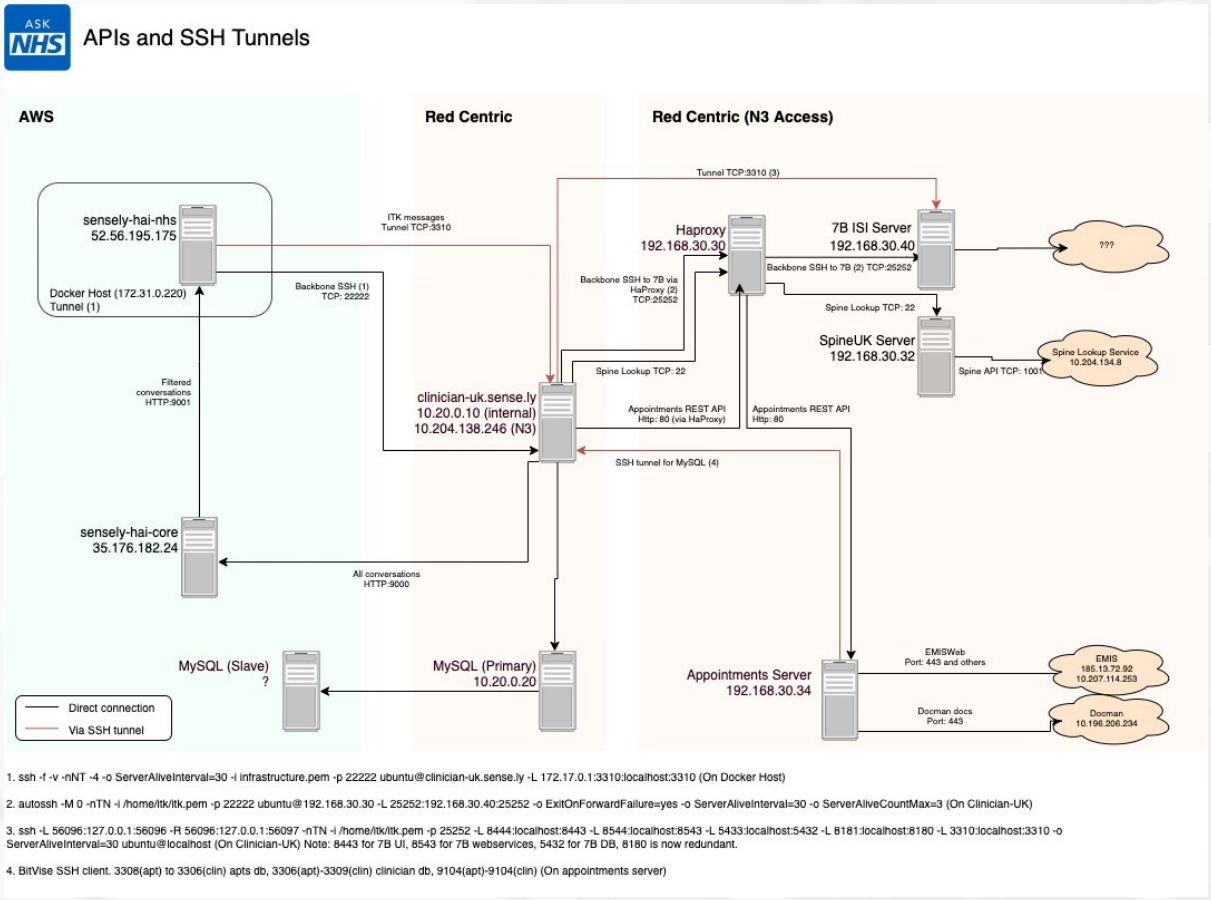
2. STAKEHOLDERS

- Sensely UK
- GP Practices / Commissioning Bodies
- RedCentric
- Amazon Web Services
- Advanced

3. DATA FLOWS

1. User registers with the App by creating an account using name, date of birth, gender and postcode and email address) / alternatively they can use NHS Login
2. Name, date of birth, gender and postcode are sent to Sensely UK secure servers for storage to support account maintenance
3. Name, date of birth, gender and postcode are sent to the Quicksilva spine-matching service who will match the details with the NHS Number and return to Sensely UK secure servers
4. The NHS Number will be sent securely to GP systems to link with the patient record number (the GP will not see this). This returns the EMIS number to be added to the user record.
5. In using the symptom checker, the User will provide the virtual assistant with information about how they are feeling and their symptoms
6. This information is sent securely to Sensely UK secure servers for storage
7. This information is shared with Advanced who return the appropriate question set and the appropriate signposting (outcome) to services
8. Users are directed to appropriate sign posting services which can include 999, GP or self care options
9. If the patient consents and the patient is signposted to the GP, the symptom checker information will be shared with their GP as part of an appointment booking request

10. In using the Administrative Tasks functionality, the user will enter free text information through ‘General Enquiry’ and their information will be sent securely to the GP practice system and a return call or email will be placed
11. De-identified reports are produced for commissioning bodies to demonstrate the performance of the App and how Users have responded



1. ssh -f -v -nNT -4 -o ServerAliveInterval=30 -i infrastructure.pem -p 22222 ubuntu@clinician-uk.sense.ly -L 172.17.0.1:3310:localhost:3310 (On Docker Host)

2. autossh -M 0 -nTN -i /home/itk/itk.pem -p 22222 ubuntu@192.168.30.30 -L 25252:192.168.30.40:25252 -o ExitOnForwardFailure=yes -o ServerAliveInterval=30 -o ServerAliveCountMax=3 (On Clinician-UK)

3. ssh -L 56096:127.0.0.1:56096 -R 56096:127.0.0.1:56097 -nTN -i /home/itk/itk.pem -p 25252 -L 8444:localhost:8443 -L 8544:localhost:8543 -L 5433:localhost:5432 -L 8181:localhost:8180 -L 3310:localhost:3310 -o ServerAliveInterval=30 ubuntu@localhost (On Clinician-UK) Note: 8443 for 7B UI, 8543 for 7B webservices, 5432 for 7B DB, 8180 is now redundant.

4. BitVise SSH client. 3308(apt) to 3306(clin) apts db, 3306(apt)-3309(clin) clinician db, 9104(apt)-9104(clin) (On appointments server)

Controllers and Processors

SOURCES

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

ICO Guidance - Data Controllers

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. DEFINITIONS / CONTEXT

“It is essential for organisations involved in the processing of personal data to be able to determine whether they are acting as a data controller or as a data processor in respect of the processing. This is particularly important in situations such as a data breach where it will be necessary to determine which organisation has data protection responsibility.

The data controller must exercise overall control over the purpose for which, and the manner in which, personal data are processed. However, in reality a data processor can itself

exercise some control over the manner of processing – e.g. over the technical aspects of how a particular service is delivered.

The fact that one organisation provides a service to another organisation does not necessarily mean that it is acting as a data processor. It could be a data controller in its own right, depending on the degree of control it exercises over the processing operation.”[1]

2. DATA CONTROLLERS

Sensely UK has been assessed to be a Data Controller.

Where the services are provided **outside** of any commissioning arrangement with healthcare partners and data subjects may use the app independently of any relationship with their healthcare provider as a citizen, rather than a patient.

Sensely UK is clearly the Data Controller in this scenario. For these services, Sensely UK have exercised control over the purpose and manner of processing, the lawful basis and have been solely responsible for giving effect to the rights of individuals. Since there are no other parties involved in this part of the Ask NHS product provision, and Sensely UK has an independent relationship with the data subject, prior to any sharing with the healthcare

[1] https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

partners, Sensely UK clearly has autonomy. Sensely UK has determined the information it will require to deliver the service prior to engagement with any third party, such as the EMIS ID and Spine Matching. Its service is designed and operated independently.

In accordance with the Information Commissioner's checklist for establishing whether an organisation is a Controller, it meets the following criterion;

They decide to collect or process the personal data outside of any arrangement with GP practices or CCGs

- ✓ They decide what the purpose or outcome of the processing will be
- ✓ They decide what personal data should be collected
- ✓ They decided which individuals to collect personal data about
- ✓ They are processing the personal data as a result of a contract between themselves and the data subject (Terms and Conditions)
- ✓ They make decisions about the individuals concerned as part of or as a result of the processing
- ✓ They have a direct relationship with the data subject
- ✓ They have complete autonomy as to how the personal data is processed
- ✓ They have appointed processors to process the personal data on their behalf

In some areas, the Ask NHS service has been commissioned by healthcare partners to cover the specific patient population there. Whilst the Ask NHS service has already been designed with a degree of autonomy and an independent relationship with the patient exists, the presence of commissioning bodies who can direct the purpose and manner for processing of the personal data generated lends itself to Sensely UK acting as a Processor. In these circumstances, Sensely UK will be directed by the customer with regards to the shape of the service and the collection and use of the personal data therein

In accordance with the Information Commissioner's checklist for establishing whether an organisation is a Controller, Sensely UK satisfies the following criterion;

- ✓ They decide to collect or process the personal data outside of any arrangement with GP practices or CCGs
- ✓ They decide what the purpose or outcome of the processing will be
- ✓ They decide what personal data should be collected
- ✓ They decided which individuals to collect personal data about

- ✓ They are processing the personal data as a result of a contract between themselves and the data subject (Terms and Conditions)
- ✓ They make decisions about the individuals concerned as part of or as a result of the processing
- ✓ They have a direct relationship with the data subject
- ✓ They have complete autonomy as to how the personal data is processed
- ✓ They exercise professional judgement in the processing of the personal data
- ✓ They have appointed processors to process the personal data on their behalf

2. DATA PROCESSORS

As described above, in commissioned locations, where the GP is established as Controller, Sensely UK has been assessed to be a Data Processor.

In accordance with the Information Commissioner's checklist for establishing whether an organisation is a Processor, Sensely UK satisfies the following criterion;

- ✓ They are following instructions from the commissioning body regarding the processing of personal data
- ✓ They do not decide to collect personal data from individuals, the commissioning body will direct patients towards the app / raise awareness
- ✓ They do not decide what personal data should be collected from individuals.
- ✓ They do not decide the lawful basis for the use of that data
- ✓ They do not decide what purpose or purposes the data will be used for
- ✓ They do not decide how long to retain the data
- ✓ They do not decide whether to disclose the data, or to whom
- ✓ They may make some decisions on how data is processed, but implement these decisions under a contract with the commissioning body
- ✓ They are not interested in the end result of the processing (beyond quality and safety)

There are a number of suppliers that process data on Sensely UK's behalf which would render them Processors or Sub Processors (depending on whether Sensely UK is a Controller or Processor.

- RedCentric
- Amazon Web Services
- Advanced

In accordance with the Information Commissioner's checklist for establishing whether an organisation is a Processor, Sensely UK satisfies the following criterion;

- ✓ They are following instructions from Sensely UK regarding the processing of personal data
- ✓ They are given the data by Sensely UK and instructed on how to process it
- ✓ They do not decide what personal data should be collected from individuals.
- ✓ They do not decide the lawful basis for the use of that data
- ✓ They do not decide what purpose or purposes the data will be used for
- ✓ They do not decide how long to retain the data
- ✓ They do not decide whether to disclose the data, or to whom
- ✓ They may make some decisions on how data is processed, but implement these decisions under a contract with Sensely UK
- ✓ They are not interested in the end result of the processing (beyond quality and safety)

3. APPROPRIATE SHARING DOCUMENTS

"It is good practice for you to have written data sharing agreements when controllers share personal data. This helps everyone to understand the purpose for the sharing, what will happen at each stage and what responsibilities they have. It also helps you to demonstrate compliance in a clear and formal way. Similarly, written contracts help controllers and

processors to demonstrate compliance and understand their obligations, responsibilities and liabilities."2

- For commissioned areas there must be a **Data Processing Contract** between Sensely UK and the GP Practices / commissioning body
- There must be a **Data Processing Contract** between Sensely UK and RedCentric
- There must be a **Data Processing Contract** between Sensely UK and Amazon Web Services
- There must be a **Data Processing Contract** between Sensely and Advanced

4. REVIEW OF PROCESSING CONTRACTS

In accordance with s 59 of the Data Protection Act 2018, there is a need to ensure that the legally required processing clauses are included in any contract between a Controller and Processor or Processor and Sub Processors.

Name of Supplier: Sensely UK (customers may alternatively wish to implement the Processor addendum of the NHS Contract for Services)

Contract reviewed: Sensely UK Standard Processing Contract

Clause	Status	Comments
Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect Personal Data including storage and transmission of data, business continuity, staff	Yes	S 2.2.5

[2] https://ico.org.uk/for-organisations/accountability-framework/contracts-and-data-sharing/

training, auditing, access control and Cyber security?		
Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller?	Yes	S 2.4
Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller?	Yes	Schedule 1
Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law	Yes	s 2.5.1

and in those cases will notify the Controller?		
Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with third party unless required to do so by law?	Yes	s 2.5.4
Does the contract require the Processor to assist the Controller to respond to requests for exercising the data subject's rights i.e. access to information, correction of errors?	Yes	s 2.5.7
Does the contract require the Processor to assist the Controller in reporting information incidents promptly including where it might be required to contact the data subject?	Yes	s 2.5.7
Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction?	Yes	s 2.5.3

Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller?	Yes	s 2.6

Name of Supplier: **RedCentric**

Contract reviewed: RedCentric Master Services Agreement

Clause	Status	Comments
Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect Personal Data including storage and transmission of data, business continuity, staff training, auditing, access control and Cyber security?	Yes	s 20.6 (b)
Does the contract state that the processor shall not engage another processor without prior specific or general	Yes	s 20.6 (f)

written authorisation of the controller?		
Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller?	Yes	Yes – service description documents
Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law and in those cases will notify the Controller?	Yes	s 20.6 (a)
Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with	Yes	s 20.6 (e)

third party unless required to do so by law?		
Does the contract require the Processor to assist the Controller to respond to requests for exercising the data subject's rights i.e. access to information, correction of errors?	Yes	s 20.6 (g)
Does the contract require the Processor to assist the Controller in reporting information incidents promptly including where it might be required to contact the data subject?	Yes	s 20.6 (d)
Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction?	Yes	s 20.6 (j)
Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller?	Yes	s 20.6 (i)

Name of Supplier: Amazon Web Services

Contract reviewed: AWS Processing Contract

Clause	Status	Comments
Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect Personal Data including storage and transmission of data, business continuity, staff training, auditing, access control and Cyber security?	Yes	Section 5
Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller?	Yes	Section 6
Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller?	Yes	Section 1.3
Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law and in those cases will notify the Controller?	Yes	
Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with third party unless required to do so by law?	Yes	Yes
Does the contract require the Processor to assist the Controller to respond to requests for exercising the data subject's rights i.e. access to information, correction of errors?	Yes	Section 7
Does the contract require the Processor to assist the Controller in reporting information incidents promptly	Yes	Section 9

including where it might be required to contact the data subject?		
Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction?	Yes	Section 14
Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller?	Yes	Section 10.3

Risk Assessment

SOURCES

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

Information Commissioner - Data Protection Impact Assessments

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. INTRODUCTION

The UK Information Commissioner determine that Data Protection Impact Assessments are necessary, in certain circumstances, to assess the level of risk to the rights and freedoms of individuals.

Controllers must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The risk assessment serves to identify the level of inherent risk so that the measures being put in place to mitigate the risk are proportionate to the impact that projects or initiatives might have on data subjects.

3. ASSET CRITICALITY SCORING GRID

Typically, critical national services. Absence of system leads to complete failure of dependent systems and services with a high possibility of personal safety issues. Service interruption results in severe reputational damage	5
Predominantly transactional services. Absence leads to operational difficulties that can be coped with for a limited period. May lead to increased risk to stakeholders or organisation.	4
Predominantly data capture, batch processing. Absence leads to operational difficulties, but these are manageable for an extended 2period. Eg. 1 day. Absence of system may lead to a slight increase in risk to stakeholders or organisation.	3
Business Hours Support (8am-6pm) Mon-Fri (not BH). Service Availability 98%. DR optional - dependant on outcome of BIA.	2

4. DATA RISK SCORING GRID

Data is aggregated and anonymised.	2
Low volume of personal data involved or high volumes of anonymised data.	3
High-volume personal data or low volume special category data.	4
High volume and special category data or includes stigmatised information (i.e. mental health data).	5

5. RISK SCORING MATRIX

		Asset Criticality			
		2	3	4	5
Impact of data breach	2	Bronze			
	3		Silver		
	4			Gold	
	5				Platinum

6. ASSESSMENT AND RATIONALE

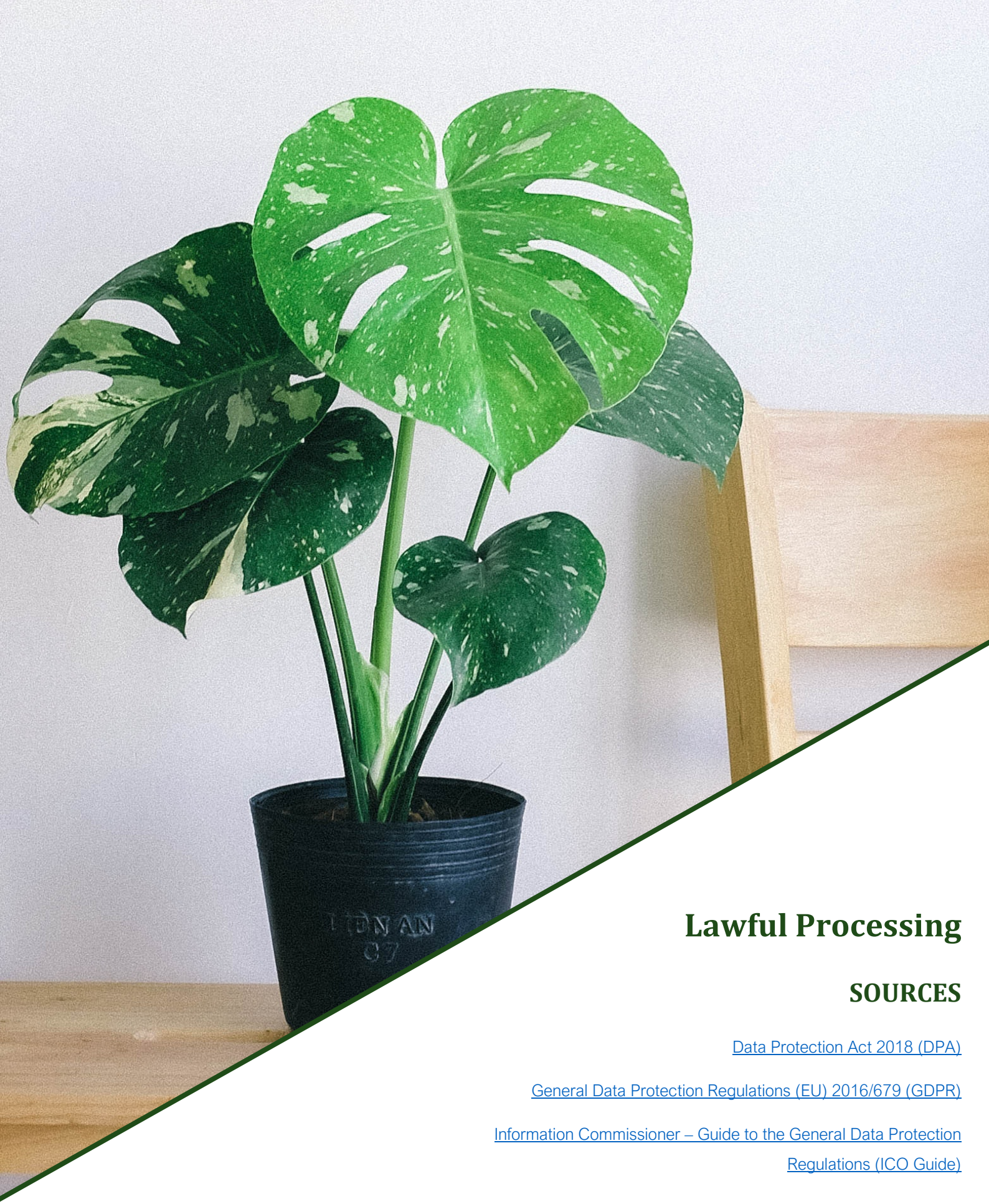
	Predominantly data capture, batch processing. Absence leads to operational

What description has the project been given in terms of criticality of resulting asset or service?	difficulties, but these are manageable for an extended period. E.g. 1 day. Absence of system may lead to a slight increase in clinical risk
Rationale	AskFirst is not an emergency care service nor does it have significant dependencies. The impact of its loss or interruption would be largely reputational in nature since being able to log in and access the services is fundamental to the delivery of other Sensely UK products and services. Whilst disruption to the functionality is likely to cause patient and customer frustration, some interruption can be tolerated as no loss to life or significant patient outcome affects are anticipated. Patients are able to move towards more traditional routes for symptom checking and appointment booking.
What score has the project been given in terms of the nature and volume of data being processed?	High volume and special category data and includes stigmatised information.
Rationale	The app can be used to describe and submit a wide range of symptoms and book appointments or be follow signposting to local services. Cumulatively, this can result in a high volume of special category data being collected by the service.
Overall risk score given to the processing activity / project in question.	Criticality 3 Impact of data breach 5 GOLD

Does the project involve access by data subjects to their own personal data that requires a 'high' level of authentication (i.e. access to their own health or finance records)?	The following activities warrant a 'high' level of authentication according to NHS Digital guidelines. 1. Manage / view appointments 2. Register for online account where treatment requires high level identity assurance or access to / adding to existing medical record

6. RISK ASSESSMENT CONCLUSION

The project has been assessed to have an overall risk grading of GOLD and so the measures to be applied will be proportionate to reduce the inherent risk levels to a suitable level such that they can be accepted by the stakeholders.



Lawful Processing

SOURCES

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. DEFINITIONS / CONTEXT

Controllers must have a valid lawful basis in order to process personal data.

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

Most lawful bases require that processing is 'necessary'. If Controllers can reasonably achieve the same purpose without the processing, they won't have a lawful basis.

Controllers must determine the lawful basis before they begin processing, and should document it.

Controller's privacy notices should include your lawful basis for processing as well as the purposes of the processing.

If the purposes change, Controllers may be able to continue processing under the original lawful basis if the new purpose is compatible with the initial purpose (unless the original lawful basis was consent).

If Controllers are processing special category data they will need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

Where such processing could result in a decision that affects an individual, must offer a right to object before such decisions are taken, in accordance with Article 22.

2. DATA CATEGORIES

The UK GDPR / DPA 18 and EU GDPR governs the processing of data that identifies living individuals and provides that Special Categories of Data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,

and the processing of genetic data, data concerning health or data concerning a natural person's sex life or sexual orientation.

The initiative involves processing of Personal Data and Special Category Data and therefore requires both a lawful basis under Art 6 UK GDPR and an condition for processing of Special Category Data

3. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

UK GDPR Article 6 (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

Once transferred to GP practice or 111, it is assumed that the lawful basis becomes Art 6 (1) (e) Public Task.

4. CONDITION FOR PROCESSING SPECIAL CATEGORY DATA

Article 9 2 (a) Explicit consent

Once transferred to GP practice or 111, it is assumed that the lawful basis becomes Art 9 (2) (h) Medical Purposes.

7. EXPECTATIONS / COMMON LAW CONFIDENTIALITY

The test for a breach of confidence has developed (in correlation with the application of the Human Rights Act 1998 and Article 8 (1) of ECHR) and now concerns whether individuals have a ***reasonable expectation*** of privacy such that sharing information may constitute misuse of private information.

The duty towards confidentiality can therefore be overridden where it is deemed that the individual reasonably expects such a disclosure.

The importance of managing patient / service user expectation is further demonstrated by the introduction of the 8th Caldicott Principle which aims to ensure 'no surprises' for patients and service users by making sure providers are fully transparent.

Since consent is the identified lawful basis for processing, there is a requirement to ensure that data subjects are informed about the processing and have the opportunity to ask questions or to object to processing. Through this process, there can be some confidence that the common law duty of confidentiality is also satisfied.

Additionally, users are provided with examples of sharing that may occur without their consent such as court or police disclosures.

8. CONSENT CONDITIONS

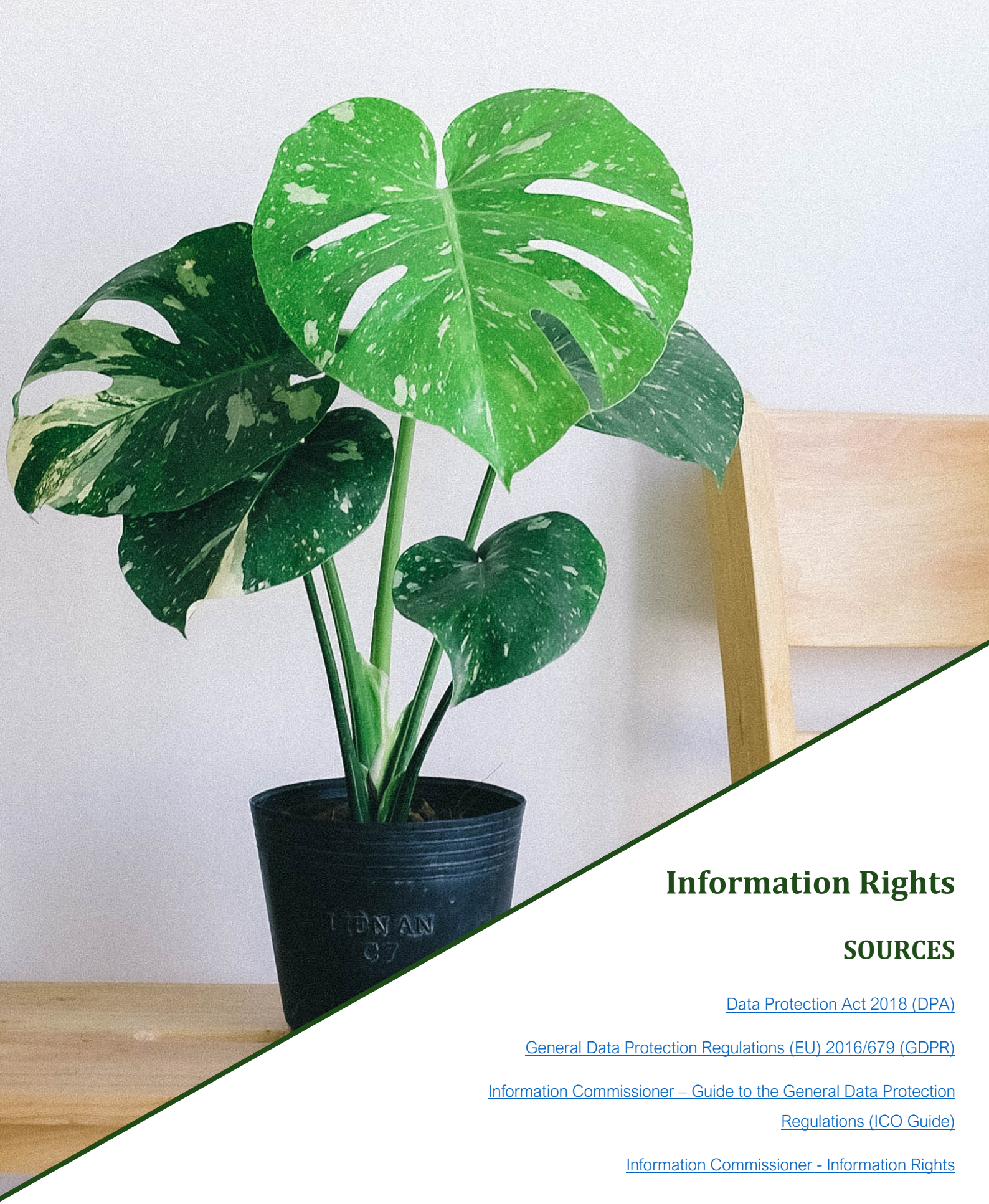
In accordance with the Information Commissioner's guidelines on consent, the Sensely UK model has been assessed to be lawful.

- ✓ The request for consent is prominent and separate from terms and conditions
- ✓ Individuals are required to positively consent
- ✓ Does not use pre-ticked boxes or any other type of default consent
- ✓ Uses clear, plain language that is easy to understand
- ✓ Specifies why data is collected and what will be done with it
- ✓ Gives separate distinct ('granular') options to consent separately to different purposes and types of processing
- ✓ Names the organisation and any third-party controllers who will be relying on the consent

- ✓ Tells individuals that they can withdraw their consent
- ✓ Ensures that individuals can refuse to consent without detriment
- ✓ Consent is not a precondition of a service – users may still use the App without consenting to share with GP

9. REPORTING / ANALYTICS

De-identified reports are produced and shared with commissioning bodies on required. In his instance, they are the Controller and will define the nature and scope of the reports in accordance with data protection legislation.



Information Rights

SOURCES

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

Information Commissioner - Information Rights

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. DEFINITIONS / CONTEXT

The UK and EU GDPR provides the following rights for individuals: The right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, rights in relation to automated decision making and profiling.

2. FACILITATION OF INFORMATION RIGHTS

Information Right	Applies?	How Supported
Right to Access	Yes	Individuals have the right to access their personal data and this right helps individuals to understand how and why you are using their data, and check you are doing it lawfully. Individuals are able to contact Sensely to request access to their information although, there is little information that they do not already have access to by virtue of the App itself. Users can access their profile information as well as having the symptom checker emailed to themselves. Data subjects are made aware of this right in the Sensely UK privacy policy. Requests that relate to GP data will be escalated to the GP Controller to action.
Rectification and Restriction	Yes	At present, the data subject is not able to make amendments directly through their profile, but this has been raised as a development ticket. This is due to the potential complexities of breaking the match with NHS spine data and the individual losing functionality with the App because they have not updated their details with their NHS providers.

		Data subjects can, however, email a request for their information to be corrected through our Data Protection Officer and there are SOPs in place to ensure a prompt and consistent response in line with Article 16.
Portability	Yes, data subjects do have a right to portability of their personal data under this lawful basis.	As with the right to access, Sensely is able to obtain machine readable copies of the personal data held within the App and send to an alternative provider of their choice. Data subjects are made aware of this right in the Sensely UK privacy policy.
Erasure / Objection / Consent wthdrawal	Yes	It was considered that Sensely may have a requirement to retain information beyond the period of consent in order to establish a defence to legal claims but essentially, as the App is not determined to be a medical device, and the action of the App is merely signposting, it was ultimately decided that, claims of medical negligence for example would not be possible. Ultimately it was determined that, where an individual requests erasure of their personal data, through withdrawal of consent, Sensely UK will give effect to that right unless Controllers provide other instructions during the onboarding process. These three rights are grouped together as the process is largely the same. Individuals are provided with the details of the Data Protection Officer within the Privacy Policy to make information rights requests. The Product Team maintains a log of information rights requests to ensure that the organisation is able to monitor compliance with legal timeframes and that Sensely are appropriately giving effect to data subjects' rights.
Profiling and Automated Decision Making	There is no profiling or automated decision-making taking place and	NA

	so these rights would not apply to processing under this DPIA.	

Sensley UK has an Information Rights Protocol in place and has appointed a Data Protection Officer to oversee compliance with the legislation.

3. RETENTION AND WITHDRAWAL OF CONSENT

Sensely has documented the consideration of how long records should be retained in certain circumstances. In summary, the App record will be remain active regardless of whether the use appears “active” this is because the App is for use when the individual is experiencing symptoms and requires signposting or information. This is not a daily activity and, in the same way as one may not visit their GP for months or years, it follows that the user may not access the App for long periods of time but still wish for it to be available to them when needed.

Instead, the user is made aware of their right to close their account at any time, thus withdrawing consent. Following a systematic review of each processing activity, it was determined that there is no compelling (or legal) reason for Sensely to retain the user personal data beyond their direct engagement with the App. However, should Controller customers seek a variation on this process, they may request it.

Therefore, below describes the agreed process for anonymising the user’s data in the event that consent is withdrawn.

Record	Owner	Description	Retention Period Trigger	Action	Anonymisation / De-identification Process	Method of Review and Destruction

User App Account	Director	Personal data collected and retained as a single unit pertaining to the App usage of a specific individual.	User requests account closure / erasure of personal data.	De-activate, anonymise and inform data subject.	Following data categories are removed; 1. Surname 2. First name 3. Email address 1 4. Email address 2 5. Home address 6. Phone number 7. EMIS ID 8. User's device ID 9. NHS No following data categories are amended; 10. Date of Birth – converted to age 11. Home Post Code – converted to outerpostcode The following datacategories remain; 12. Gender It is determined that an individual cannot be identified through; • Gender • Outer postcode • Age And therefore, the information is no	See Information Rights and Access Protocol.

					longerpersonal data.	

In response to such a request, the data items set out above are removed, thus rendering the information anonymous (such that data subject is not or no longer identifiable pursuant to Recital 26).

Data Minimisation

SOURCES

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. DEFINITIONS / CONTEXT

Processing of personal data must be adequate – sufficient to properly fulfil your stated purpose

Processing of personal data must be relevant – has a rational link to that purpose

Processing of personal data must be limited to what is necessary – you do not hold more than you need for that purpose

You should periodically review your processing to check that the personal data you hold is still relevant and adequate for your purposes

You must not collect personal data on the off-chance that it might be useful in the future. However, you may be able to hold information for a foreseeable event that may never occur if you can justify it

Article 6(4)(e) permits the processing of pseudonymized data for uses beyond the purpose for which the data was originally collected.

Recital 78 and Article 25 list pseudonymization as a method to show GDPR compliance with requirements such as Privacy by Design

Recital 26, the GDPR limits the ability of a data handler to benefit from pseudonymized data if re-identification techniques are “reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.”

GDPR identifies four types of data;

(1) Identified (subject is immediately identified)

(2) Identifiable (subject could be identified through indirect identifiers such as NHS No)

(3) Article 11 De-Identified (identity is not apparent from the data; data is not directly linked with data that identifies the person. Could potentially be re-identified if matched to additional identifying data. No known, systematic way for the controller to reliably create or re-create a link with identifying data)

(4) Anonymous / Aggregated. Identification is not possible.

2. ASSESSMENT OF COLLECTED DATA FIELDS

The Symptom Checker provides the users with a dynamic questionnaire, the questions of which have been authored and governed by Sensely UK clinical steering group in association with the Advanced Clinical Knowledge Unit. The questions are periodically reviewed for accuracy through end to end audits, patient and clinician testing this serves to ensure that all questions are necessary for the intended purpose and that superfluous information is not being collected.

Regarding other data fields collected, a rationale has been provided below to demonstrate that the minimum necessary data has been collected to deliver the intended and consented purposes.

Title	Collection Source	Use / rationale
Full Name	Data Subject Account Creation	Necessary for the user to have a unique accountNecessary for identity validation Necessary to link with health record
Gender	Data Subject Account Creation	Necessary for dynamic questions (i.e. could you be pregnant?)
DOB	Data Subject Account Creation	Necessary for identity validation Necessary for dynamic questions (i.e. could you be pregnant?)
Postcode	Data Subject Account Creation	Necessary for identity validation Necessary to establish locality for advice (i.e. nearby pharmacy)
Email address	Data Subject Account Creation	Necessary to validate identity Necessary to provide individual with outcome of questionnaire
Password	Data Subject Account Creation	Necessary to secure account
Full Address	Returned from Spine Matching	Necessary for the user to have local services signposted to them Necessary for identity validation

EMIS No	Linkage with GP System	Necessary to support integrated functionality
Health Information Symptoms	Data Subject Entry	Core element of the service
NHS Number	Spine Matching	Mandatory identifier in health and care
Audio File	Data Subject Entry	Necessary to support verbal option within the App (where selected by user)
Weight	Data Subject Connected Device Use or Data Entry (Long Term Conditions)	Necessary to support additional elements of the service; to provide symptom checking, signposting or triage services
Blood Pressure	Data Subject Connected Device Use or Data Entry (Long Term Conditions)	Necessary to support additional elements of the service; to provide symptom checking, signposting or triage services
Smoking Status / E-cigarette use	Data Subject Entry (Long Term Conditions)	Necessary to support additional elements of the service; to provide symptom checking, signposting or triage services
Alcohol Consumption	Data Subject Entry (Long Term Conditions)	Necessary to support additional elements of the service; to provide symptom checking, signposting or triage services
Physical Activity	Data Subject Entry (Long Term Conditions)	Necessary to support additional elements of the service; to provide symptom checking, signposting or triage services
Carer status	Data Subject Entry (Long Term Conditions)	Necessary to support additional elements of the service; to provide symptom checking, signposting or triage services
Free text goal setting	Data Subject Entry (Long Term Conditions)	Necessary to support additional elements of the service; to provide symptom checking, signposting or triage services
Free text request	Data Subject Entry (Admin Requests)	Necessary to support additional elements of the service; to provide symptom checking, signposting or triage services
Confirmation of relation to child and confirm that they hold parental	Entry by parent or guardian where account opened for under 16s	Necessary to identify where account relates to a third party below 16 such that information will not be attached to the parent record in error – but rather to the child's record

responsibility		
Communications usage information: time	During use of video functionality	Determined by video software provider in their capacity as Controller in their own right (for this data collection)
Communications usage: duration of usage	During use of video functionality	Determined by video software provider in their capacity as Controller in their own right (for this data collection)
Communications usage: source and destination identifiers	During use of video functionality	Determined by video software provider in their capacity as Controller in their own right (for this data collection)
Communications usage: completion status	During use of video functionality	Determined by video software provider in their capacity as Controller in their own right (for this data collection)
Communications usage: IP address	During use of video functionality	Determined by video software provider in their capacity as Controller in their own right (for this data collection)
Communications usage: amount of usage.	During use of video functionality	Determined by video software provider in their capacity as Controller in their own right (for this data collection)

TRANSPARENCY

In accordance with ICO guidelines and established best practice, the Sensely UK Privacy Policy at https://www.sensely.com/privacy-centre/ has been reviewed for conformance;

- The privacy policy explicitly mentions transfers to third countries (“Sensely and Your Information”)
- In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon is specified (“Sensely and Your Information”)
- The privacy policy includes the sources from which personal data originates (“How Does Sensely UK Collect my Information?”)
- Identifies whether there is profiling or automated decision making involved (“Does Sensely UK Use profiling or Automated Decision Making?”)
- The notice includes storage periods for records (“How Long Does Sensely Store my Information?”)
- The notice includes the contact details for the DPO (Contact)
- The privacy policy names all recipients of the personal data (“Who Does Sensely UK Share My Information With?”)
- The notice includes descriptions of the information rights and how to engage them (“What Are My Information Rights?”)
- The notice describes any intended or potential further access (“Does Sensely UK Use My Information?”)
- The privacy policy includes information about how to raise complaints and contact the ICO (“Complaints”)
- The privacy policy is visible from every landing page of the website (always in a link at the bottom but also embedded into App)
- The privacy policy avoids the use of qualifiers such as "may" or "might

- The notice is multi layered, allowing the user to jump to the section that most interests them (Privacy dashboard includes detailed, icon level and narrated video notices such that those with different needs can consume the information).
- The right to object or withdraw consent are made particularly clear to the data subject (“Right to Object or Withdraw Consent”)

TECHNICAL AND ORGANISATIONAL MEASURES

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. DEFINITIONS / CONTEXT

- Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- While information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures
- Measures taken should consider available technology, costs, nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons
- The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk
- The impact of non-secure data processing can be as serious as becoming a victim or fraud or being put at risk of physical harm or intimidation
- Additionally, individuals are entitled to be protected from less serious kinds of harm like embarrassment or inconvenience
- The data should be accessed, altered, disclosed or deleted only by those authorised to do so (and that those people only act within the scope of the authority given to them);
- The data held must be accurate and complete in relation to why it is being processed; and
- The data should remain accessible and usable, i.e., if personal data is accidentally lost, altered or destroyed, Controllers should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

2. PROPORTIONALITY

In accordance with the above risk assessment, the project has been defined as having a GOLD degree of risk to the rights and freedoms of data subjects in the event that appropriate technical and organisational measures are not put in place – based on the nature and volume of the data being processed.

This assessment will therefore explore each of the elements drawn out within data protection legislation for mitigation of those risks such that the residual risk is low enough to support implementation.

CLOUD HOSTING AMAZON WEB SERVICES

These assurance items are based on the NHS Digital Health and Social Care Cloud Security – Good Practice Guide.

- Sensely UK have used the functionality within AWS to offer (TLS Version 1.2) to encrypt communication between cloud components, data centres and internal communications between cloud admin portal and the cloud itself.
- AWS holds and maintains certification to ISO 27001 to include the physical security of the data centres.
- Sensely UK undertake regular penetration testing of the network architecture ensuring that the Penetration test is well scoped
- Sensely UK have selected UK jurisdictions for its AWS hosting locations including backups
- Sensely UK uses a SOC Certified password control provider to ensure that keys are secure https://1password.com/soc/. They are externally audited and provide audits on activities therein https://support.1password.com/events-reporting/
- Sensely UK have deployed the application across multiple AWS Availability Zones in the same region for fault tolerance and low latency
- AWS customers are protected by Amazon's firewall service called Shield as standard.
- AWS supports enforced encryption to AES256 at rest https://docs.aws.amazon.com/whitepapers/latest/efs-encrypted-file-systems/enforcing-encryption.html
- AWS has given assertions regarding their data sanitisation approach for cloud storage. If the customer needs a specific standard/method of sanitisation such as DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88 (“Guidelines for Media Sanitization”) the customer can use a secure delete tool which behaves on the AWS storage in the same way it would on a local physical disk.. The provider has confirmed they will delete data on request of the controller

and that the appropriate deletion tool will be used in accordance with the risk posed by the data therein.

- Regarding equipment disposal, AWS is certified with ISO/IEC 27001:2013, and CSA STAR CCM v3.0.1.
- AWS security protections and control processes (including sanitisation) are independently validated by multiple third-party independent assessments: https://aws.amazon.com/compliance/programs/
- "AWS operates our data centers in alignment with the Tier III+ guidelines, but we have chosen not to have a certified Uptime Institute based tiering level so that we have more flexibility to expand and improve performance. AWS' approach to infrastructure performance acknowledges the Uptime Institute's Tiering guidelines and applies them to our global data center infrastructure design to ensure the highest level of performance and availability for our customers."
- AWS has submitted an NHS Data Protection and Security Toolkit at AWS Toolkit Submission.

CLOUD HOSTING AMAZON WEB SERVICES

These assurance items are based on the NHS Digital Health and Social Care Cloud Security – Good Practice Guide.

- Sensely UK have used the functionality within RedCentric to offer (TLS Version 1.2) to encrypt communication between cloud components, data centres and internal communications between cloud admin portal and the cloud itself.
- RedCentric holds and maintains certification to ISO 27001 to include the physical security of the data centres.
- Sensely UK undertake regular penetration testing of the network architecture ensuring that the Penetration test is well scoped
- Sensely UK have selected UK jurisdictions for its RedCentric hosting locations including backups
- Sensely UK uses a SOC Certified password control provider to ensure that keys are secure https://1password.com/soc/. They are externally audited and provide audits on activities therein https://support.1password.com/events-reporting/
- Sensely UK have deployed the application across multiple Availability Zones in the same region for fault tolerance and low latency
- RedCentric uses AES 256 which is industry standard (active) https://www.digitalmarketplace.service.gov.uk/g-cloud/services/507232349999721
- RedCentric have provided such assurances via the Digital Marketplace https://www.digitalmarketplace.service.gov.uk/g-cloud/services/507232349999721 that include assertions around effective data sanitisation
- RedCentric operate in line with Uptime Institute level III https://www.datacenterhawk.com/colo/redcentric/80-clifton-st/london

REDCENTRIC DUE DILIGENCE

RedCentric do not transfer data outside of the UK.

The processor has achieved the following accreditations that assist to reduce the risk to the rights and freedoms of data subjects;

- The processor has completed a compliant NHS Data Protection and Security Toolkit for the current year https://www.dsptoolkit.nhs.uk/OrganisationSearch/YGMAP
- the processor has achieved ISO27001 status

As part of the impact assessment, a review of media coverage was undertaken to determine whether there have been reports of breaches or complaints relating to suppliers or partners involve in the project.

- At the time of writing, RedCentric had no media presence with regards to data breaches

Checks have been undertaken with regards to the UK Information Commissioner; RedCentric are not currently registered with the ICO. However, since they act only as a Processor for this project, it is not deemed to be a concern.

The stakeholders have identified the following leads for data protection matters;

- data.protectionofficer@redcentricpc.com

AWS DUE DILIGENCE

Sensely UK have selected UK jurisdictions for AWS data hosting.

The processor has achieved the following accreditations that assist to reduce the risk to the rights and freedoms of data subjects;

- The processor has completed a compliant NHS Data Protection and Security Toolkit for the current year https://www.dsptoolkit.nhs.uk/OrganisationSearch?searchValue=8JX11
- the processor has achieved ISO27001 status

As part of the impact assessment, a review of media coverage was undertaken to determine whether there have been reports of breaches or complaints relating to suppliers or partners involve in the project.
AWS have been subject to media reporting in relation to data breaches and also subject to some litigation related to data protection compliance. However, they are a widely used and trusted provider and no ICO advice suggests that they should not be used.

Checks have been undertaken with regards to the UK Information Commissioner;

- AWS are registered with the Information Commissioner https://ico.org.uk/ESDWebPages/Entry/ZA481902

AWS have identified the following leads for data protection matters;

- https://aws.amazon.com/contact-us/compliance-support/

ADVANCED (ODYSSEY) DUE DILIGENCE

Advanced indicate that they may access UK data from overseas branches however, written assurance has been obtained to confirm that no Sensely UK data is accessed from or transferred outside the UK.

The processor has achieved the following accreditations that assist to reduce the risk to the rights and freedoms of data subjects;

- NHS Data Protection and Security Toolkit https://www.dsptoolkit.nhs.uk/OrganisationSearch/8HN06

As part of the impact assessment, a review of media coverage was undertaken to determine whether there have been reports of breaches or complaints relating to suppliers or partners involve in the project.

- At the time of writing, the stakeholders had no media presence with regards to data breaches

Checks have been undertaken with regards to the UK Information Commissioner;

- Advanced are registered with the Information Commissioner https://ico.org.uk/ESDWebPages/Entry/ZA770802
- Advanced have not been subject to ICO fines or undertakings in the last 3 years

The stakeholders have identified the following leads for data protection matters;

- dataprotection@oneadvanced.com

SENSELY UK DUE DILIGENCE

Sensely UK has selected UK jurisdictions for all its UK personal data. Any supply chain overseas transfers are covered by Standard Contractual Clauses in accordance with Data Protection Act 2018 and current ICO guidelines.

Sensely UK has achieved the following accreditations that assist to reduce the risk to the rights and freedoms of data subjects;

- A compliant NHS Data Protection and Security Toolkit for the current year at https://www.dsptoolkit.nhs.uk/OrganisationSearch/8JG57
- Cyber Essentials accreditation

As part of the impact assessment, a review of media coverage was undertaken to determine whether there have been reports of breaches or complaints relating to suppliers or partners involve in the project.

- At the time of writing, Sensely UK had no media presence with regards to data breaches

Sensely UK are registered with Information Commissioner at https://ico.org.uk/ESDWebPages/Entry/ZA194147

- The stakeholders have identified the following leads for data protection matters;
    - ig@sensely.com

- The stakeholders have policies that cover the following subjects;
    - Information Governance
    - Data Protection Impact Assessments
    - Data Subject Rights
    - Information Incidents
    - Information Security

    - Privacy / Confidentiality
    - Risk and Audit

- All employees of the relevant stakeholders have clauses within their contracts that include confidentiality and compliance with company Information Governance Policies.

- All employees that access personal data as part of their role have Data Protection and Security Training each year.

PROFESSIONAL USERS - AUTHENTICATION

To ensure that the authentication of professional users of the system is in line with Gov.UK and NIST standards, the following assurances have been sought in relation to access to the system by Sensely UK team members;

- For the purposes of two factor authentication, the individual is required to provide ‘something they know’ – username and password and ‘something they have’ – digital token code.
- Sensely UK also have the VPN (username and password) individual level and additional username password to access individual components.
- Sensely UK uses a SOC Certified password control provider to ensure that keys are secure https://1password.com/soc/. They are externally audited and provide audits on activities therein https://support.1password.com/events-reporting/
- The software allows different privileges for different job roles

It has been confirmed that Sensely UK would access personal data in the following scenarios;

- Monitoring activity and quality
- Administering user accounts
- Responding to incidents
- Responding to Information Rights Requests
- Technical support and development
- Analytics

DATA SUBJECT – IDENTITY VERIFICATION

Initial access to the service or system involves only provision of personal data and not access to existing information. According to https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity this does not require verification of identity but rather subsequent authentication only.

SYSTEM AUDIT

- The AskFirst system / software enables and supports investigations for any reason (e.g. inappropriate access or cyber security incident)
- The system / software allows identification of any changes which have been made to clinical or administrative data, Patient/Service User data. This includes identifying what changes were made, by what user and at what time.
- The system / software allows monitoring of whether access controls are working as intended. Administrators may audit the movements of all staff, so it is possible to check that they are not accessing areas which they shouldn’t be, or seeing things or doing things they shouldn’t be.
- The system / software satisfies the data subject's legal right to see who has accessed or modified their record, because the audit trail includes who, when and why that user accessed the information
- Audit trail includes updates, backups, any maintenance activities or reference data changes (e.g. an update to the clinical coding scheme data or adding in a drug data base)

No	Describe source of risk and nature of potential impact on individuals.	Inherent Likelihood of harm	Inherent Severity of harm	Inherent Overall risk	Options to reduce or eliminate risk	Effect on risk	Residual risk
1	There is a risk that the Controller and Processor relationship has not been sufficiently defined and documented. This may result in ineffective management of risk and could result in improper management of data subjects' personal data.	Moderate	Low	Moderate	The above assessment has identified and rationalised the Controller and Processor relationships. For ad hoc projects where relationships may differ, additional assessments shall be made as part of the specification process.	Eliminated	Low
2	There is a risk that the Processors are not engaged by virtue of an Art 28 / s59 compliant processing contract. This could result in the Processor managing data subjects' personal data improperly.	Moderate	Low	Moderate	Processors have been identified and the contracts have been reviewed in accordance with Art 28 / s 59 of UK GDPR / DPA 18.	Eliminated	Low

3	There is a risk that the lawfulness of processing personal data processed is not determined and documented including appropriate UK and EU GDPR articles and common law of confidentiality / Misuse of Private Information. This could undermine data subject rights to transparency around data processing and result in data being processed unlawfully.	Moderate	Low	Moderate	A lawful basis has been established by virtue of the assessment above.	Reduced	Low
4	There is a risk that the data subjects are not made aware of processors or recipients of their data or the wider activity of research is not known to them. This undermines their Right to be Informed and their ability to raise objections.	Moderate	Low	Moderate	The above assessment concludes that the transparency materials conform to best practice.	Reduced	Low
5	There is a risk that personal data is retained for longer than the intended purposes contrary to data protection law and results in a greater risk to the rights and freedoms of individuals in the event of system compromise or personal data breach.	Moderate	Low	Moderate	The above assessment includes a rationale for records retention as well as a process for removing personal data in the event that consent is withdrawn.	Reduced	Low

6	There is a risk that the project introduces changes that compromise the Controller's ability to give effect to the information rights of data subjects.	Moderate	Moderate	Moderate	Each of the information rights have been assessed as part of the DPIA. The rights are communicated to the data subjects through the privacy notice.	Eliminated	Low
7	There is a risk that data at rest is not protected with sufficient technical and organisational measures such that this may result in incidents or personal data breaches that pose a risk to the rights and freedoms of data subjects.	Moderate	Moderate	Moderate	Data is held within accredited data centres offering encryption at rest and appropriate safeguards for the international transfer of personal data.	Eliminated	Low
8	There is a risk that data in transit is not protected with sufficient technical and organisational measures such that this may result in incidents or personal data breaches that pose a risk to the rights and freedoms of data subjects.	Moderate	Moderate	Moderate	Data in transit mechanisms have been reviewed against NIST and Gov.UK best practice standards and confirmed to be appropriate.	Reduced	Low

- This Impact Assessment demonstrates that the risk to the rights and freedoms of individuals appear to have been effectively mitigated such that the residual risk is acceptable – particularly in light of the nature and volume of information involved.
- The assertions above are based on assurances and evidence provided by the stakeholders at the time of drafting and the impact assessment should be reviewed regularly to ensure its reliability as a compliance tool.

Role: Emma Cooper, Kafico Ltd, External Data Protection Consultant

Date: November 2021