# Data Protection Impact Assessment Summary Report

# Sensely UK Ask NHS App

| | |
|---|---|
| Title | Data Protection Impact Assessment |
| Project | Sensely UK Ask NHS App |
| Author | Data Protection Officer |
| Date | December 2017 – May 2018 |
| Version | V0.1 |
| Status | Live Document |

Contents

## Contents

## 1. Introduction and 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 and has 9 employees.

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

## 2. Necessity of Privacy Impact Assessment

*'Regulation 2016/6791 (GDPR) applies from 25 May 2018. Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA), as well as Directive 2016/680.*

*A DPIA is a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them).'*

Whilst Sensely UK Ltd offers a variety of services, often providing bespoke offerings to customers, the intention of this DPIA is to provide an assessment for the core technical infrastructure and sharing processes that are common to the Sensely UK Ltd service, namely the Ask NHS provision. 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.

This approach is in line with GDPR article 35(1);

*'a single assessment may address a set of similar processing operations that present similar high risks'*

GDPR article 35(4) and recitals 71, 75 and 91 provide some examples of processing that pose a high risk to the rights and freedoms of data subjects and therefore warrant a DPIA.

Summarily these are;

1. Evaluation such as profiling and prediction, in particular health, behaviour, location or movements
2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing and has an effect on the data subject such as exclusion or discrimination.
3. Systematic monitoring: processing used to observe, monitor or control data.

4. Sensitive data: this includes special categories of data as defined in Article 9 (such as health).
5. Data processed on a large scale: the GDPR does not define what constitutes large-scale but the Working Party 29 guidance puts forward the following for consideration; a. the number of data subjects, the volume of data; the duration, or permanence, of the data processing activity; the geographical extent of the processing activity.
6. Datasets that have been matched or combined, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that the data subject might not expect.
7. Data concerning vulnerable data subjects: the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data.
8. Innovative use or applying technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology can trigger the need to carry out a DPIA.
9. Data transfer across borders outside the European Union.

For the purposes of this assessment, it would appear that examples 1, 2, 3,4,5,6,7 and 8 are relevant and so a DPIA is determined to be necessary.

## 3. Information Assets

The Sensely UK Ltd service is built around 5 key information assets;

1. RedCentric Application Server
2. RedCentric Database Server
3. Clinician UK
4. AWS EDM

## 4. Processing Activities

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

Sensely UK has developed a Processing Activities Log, in line with GDPR Article 30, that identifies all processing activities that involve personal data across the business. The log identifies the lawful basis, information rights, sharing partners and security measures.

## 5. Overseas Information Flows

The Sensely servers are located in the UK and the vast majority of processing occurs here.

There is an exception; where samples of the symptom checker are sent to the Sensely Corporation office in the United States. These are small audio recordings that are de-identified and allow scrutiny where the technology has been unable to match audio content.

For example, it allows the system to identify that, when a user says “tummy ache” this should be linked to “stomach ache” within the technology.

The recipients of the data within the US have no direct way to identify the individual other than through recognising their voice which is been deemed to be extremely unlikely.

The technical and organisational measures in place for this flow are;

- Standard Operating Procedure has been provided to those involved to ensure consistent approach to management of the data
- Data minimisation exercise has been completed
- Access is restricted to two members of staff only
- Audio files are not retained for longer than 6 months. After which they are permanently and securely destroyed.
- During the review, audio files are held separately to any other Sensely Corporation data and in a repository where the key to encryption is not available i.e. Sensely identifier

The legal basis for this transfer of personal data is assessed to be GDPR Article 49 1 (a), having obtained explicit consent from users by virtue of a compliance transparency notice and positive affirmation of consent via the App. There is a recognition, following the introduction of GDPR that more emphasis on this transfer should be placed on the inherent risks and this is currently being developed for further assurance.

Sensely UK are also in the process of putting in place EU Model Clauses to satisfy Article 46 and provide additional assurances for this isolated transfer between its US and EU entities.

## 6. Lawfulness

For a documented determination of the Data Controller / Processor relationship, see Appendix B. GDPR Art.6(1) provides that in order for the processing of personal data to be lawful, the controller requires either the consent of the data subject or another lawful basis. This section will therefore explore the lawful basis for processing and identify how that lawful basis is satisfied.

The lawful basis for the processing of Personal and Special Categories of data collected from the App user (data subject) through the App interface (whether mobile or web), has been identified as;

Art.6(1)(a) - *the data subject has consented to the processing*

And

Art.9(2)(a) *The data subject has given explicit consent.*

GDPR provides that consent must be freely given affirmative action, unambiguous, specific, informed, accessible and distinguishable from other matters, evidenced and provide the ability to withdraw consent.

*Freely Given Affirmative Action*

In order to consent to be freely given, data subjects must have a genuine choice. For Sensely UK Ltd, data subjects that do not use the service will not experience any reduction or alteration to the service delivered by healthcare providers as a result. There is no element

of their healthcare that is 'conditional' on the use of the service, thereby creating the 'power imbalance' cited by the Information Commissioner in her Guidance (currently under consultation)[1] and GDPR Rec.32, 43; Art.7(4). Sensely UK Ltd provides the data subject with the genuine choice to make use of Ask NHS App as a tool for signposting and information but, if not used, information can still be made available to them, or to those involved in their care through the current, albeit, less integrated methods.

*Unambiguous*

GDPR provides that consent can be obtained by any appropriate method but that consent must be given by a statement or a clear affirmative action and that opt out, silence inactivity, failure to opt-out, or 'passive acquiescence' would not constitute valid consent[2].

Users of the Sensely UK Ltd App, having read both the Privacy Policy and the Terms of Service must confirm that they have read the privacy policy and wish to proceed by clicking the 'I Agree' button. They may not continue with their registration until these actions are completed.

*Specific*

The WP29 has clarified (in Opinion 15/2011) that, in order to be specific, consent must be intelligible and that the controller must be clear and precise in its explanation of the scope and consequences of data processing.

In addition, consent must not apply to a set of open-ended processing activities, rather it should be limited to specific context.[3] Sensely UK Ltd provides a comprehensive and specific privacy policy that describes the information flows and uses for the information provided by or about the user. The policy describes the primary uses for the information as well as technical / quality processes and marketing activities.

*Informed*

Consent must be 'informed' and so Sensely has ensured that all processing activities identified in the Article 30 Processing Activities Log are included in the privacy policy and

[1] https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf
[2] Rec.32 and Art.7(2)
[3] https://www.whitecase.com/publications/article/chapter-8-consent-unlocking-eu-general-data-protection-regulation

therefore the data subject is aware of all the activities they are consenting to. This includes sharing partners such as Data Processors.

*Accessible and Distinguishable from Other Matters*

This means that the nature of the processing should be described in an intelligible and accessible form, using clear and plain language[4]. The explanation should include the identity of the controller and the purposes for which the personal data will be processed.

At present, the privacy policy is available in the form of the written policy on the website as well an Easy Read document and a video which provides information about who the Controller is and who the key sharing partners are.

The Terms of Service are separate from the Privacy Policy thus rendering them distinguishable. This provides the user with an opportunity to consider their agreement to both the use of the App and the information sharing associated with the App usage separately.

In line with the recommendations of the WP29 Opinion, the policy avoids the use of the word "may" to remove ambiguity. The policy is broken down into headed sections to allow the user to find the information they seek. The use of icons is incorporated to provide a visual guide and technical language is avoided. The document is written with intention to reduce "information fatigue".

Videos provide another option for users where text might prevent them accessing the information and the Easy Read versions support individuals with learning difficulties as well as children and young people.

*Evidenced*

Since the user is not able to proceed with accessing the App without having provided consent, the existence of an account is deemed to be evidence of consent.

*Provide the ability to withdraw*

Article 7 (3) provides that

[4] Rec.32, 42; Art.4(11), 7(1)

"The data subject shall have the right to withdraw his or her consent at any time. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent"

The Sensely UK Privacy Policy makes it clear that the individual may withdraw their consent at any point and provides a mechanism to achieve this, whereby the data subject emails Sensely to request withdrawal. Sensely has a protocol in place to respond to such requests There are plans to automate this further, such that withdrawal would be as easy as provision of consent.

## 7. Legitimacy

Rec.50; Art.5(1)(b) provides that;

*'Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes'.*

Whilst there may be a lawful basis for processing information about the data subject, there is still a need to ensure that each use of the data is legitimately required for the purposes of delivering the service to which the data subject has consented.

The Processing Activities Log is scrutinised at each Sensely UK Information Governance Steering Group to ensure that there is no "mission creep" where growth and development of the business might result in unexpected uses of the data that the data subject has not consented to. Additionally, for any reports or data extracts required by customers, a Data Report Review Form is required to be completed. This form is reviewed by the Data Protection Officer who will provide advice in relation to whether the disclosure aligns with the lawful basis for processing.

The core processing activities are explored below;

## 8. Records Retention

Article 5 provides that personal data be

"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed…"

Sensely has documented the consideration of how long records should be retained in certain circumstances. In summary, the App record will 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.

In response to such a request, the data items set out in identified as creating any risk of identification, whether direct or indirect will be removed, thus rendering the information anonymous (such that data subject is not or no longer identifiable pursuant to Recital 26).

## 9. Data Subject Rights

Where consent is the lawful basis for processing personal data, data subjects have the following rights;

- Right to be Informed
- Right to Object
- Right to Portability
- Right to Rectification
- Right to Withdrawal of Consent
- Right to Erasure
- Right to Access

## Right to be Informed

Article 12 provides that the individual has a right to transparent communication that in concise, easily accessible and clear. As discussed under section 6, there are various measures in place to ensure that the individual is providing informed consent and that the transparency requirements of GDPR are satisfied.

Additionally, Article 12 provides that there should me measures in place to give effect to data subjects' rights. This is discussed in more detail below.

Recital 60 talks about the use of visualisation tools such as Icons and these have been incorporated into the Sensely UK Privacy Policy located here. This policy was moved from the bottom of the page to the top to ensure greater accessibility.

Recital 60 also provides that the notice should discuss profiling and automated decision making which has been incorporated into the Sensely policy within its own section. The checklist at Appendix E indicates where the elements of the Sensely UK Policy comply with the requirements of the ICO checklist.

## Right to Object, Withdrawal of Consent and Erasure

Article 21 provides that

"The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her … including profiling …. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims"

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 decided that, where an individual requests erasure of their personal data, through withdrawal of consent, Sensely UK will give effect to that right.

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.

### Right to Rectification

At present, the data subject is not able to make amendments 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.

### Right to Access

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.

### Right to Portability

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.

## 10. Profiling and Automated Decision Making

Data Protection Law has provisions on automated individual decision-making (making decisions solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual).

GDPR Article 22 protects individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them

A legal effect is something that adversely affects someone's legal rights. Similarly, significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

The ICO advises that, if your processing does not match this definition then you can continue to carry out profiling and automated decision-making.

For the Ask NHS App, there appears to be no automated decision making involved since the decision around following any signposting or engaging with healthcare providers via the App is made by the individual.

There is clearly profiling taking place since the algorithm used will identify choices that are appropriate for the individual based on their responses, however the resulting decisions are made by the individual and the profiling itself does not result in an impact on the legal rights of the individual nor any significant negative effect for those having decisions made about them. Where a clinician has identified risk and feel an intervention or care option is appropriate, the individual being profiled is likely to benefit from any decisions made. Additionally, the data subject retains choice and control about whether to take options provided to them such as referral to a third-party healthcare provider.

Since the processing does not fully match the definition, it is concluded that the processing can proceed without the additional restrictions under Article 22 whilst ensuring that information rights and transparency requirements are observed.

## 11. Direct Marketing

Recital 70 provides that,

"Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information"

Sensely UK has a separate section within the privacy policy related to direct marketing and makes it clear about the two types of activity that take place. These are;

1. Using App User contact details to email them about new features and updates in relation to the App itself. Request feedback or send surveys to find out if the App is working well for them and how they used it.
2. Users are provided with an opportunity to object to this usage by virtue of an unsubscribe link in each communication. A suppression list is maintained to ensure that individuals are not contacted again once they have opted out of such messages.
3. Sharing App User personal data with third party analytics or marketing organisations such as Cookies, Google Analytics and Facebook.

There are currently no direct marketing activities taking place.

## 12. Privacy by Design

This DPIA is retrospective although a privacy impact assessment has been in place for two years prior which allowed the risks to be monitored and mitigated. This document represents a more comprehensive consideration of privacy and how that is built into the App, in particular with reference to the changes brought by GDPR.

Moving forward, Sensely UK has a Change Management Policy which ensures that changes made by any area of the business are considered against a threshold of impact (this includes privacy). It provides a consistent approach to triggering Data Protection Impact Assessment. A DPIA protocol is also in place, allowing employees to determine whether the change warrants a DPIA and therefore should be referred to the Sensely UK Data Protection Officer (DPO).

## 13. Cyber Security

- **SECTION REDACTED TO PREVENT EXPLOTATION**

**Inappropriate Access**

Access controls in place to ensure only the correct individuals have access to the data, such as administrator accounts and profiles applied to the system

- Role based access controls ensure that only qualified, authorized individuals have access to systems and data.

Authentication methods (password, text challenge, PIN, smartcard) in place to protect access to the data

- Authentication to the Sensely products and services is through username and password. Employee access to high risk back-end systems also requires multi-factor authentication.

See Appendix C for Authentication rationale.

## 14. Obligations of Secrecy

Sensely UK uses a third-party provider to host and provide access to the personal data it processes and uses a third-party provider for spine matching services.

Both providers are engaged by virtue of a Data Processing Contract that complies with GDPR Article 28 and creates an obligation of secrecy such that the processing is restricted to the narrow instructions provided by Sensely UK. These have been reviewed in year and compliance monitoring has been initiated.

Sensely UK employees and contractors are equally obliged to maintain confidentially through their employee and service contracts.

All employees are provided with annual Information Governance training by an experienced Data Protection Officer.

## 15. Governance

Sensely has appointed a Data Protection Officer who holds ISEB Data Protection, ISEB Freedom of Information, CISP Information Security and Post Graduate Diploma Information Rights Law and Practice. Contact details have been provided to both the ICO and the public through the privacy notices.

Sensely UK has established an Information Governance Steering Group which is attended by key team members including the DPO. See Appendix D for the IGSG Standard Agenda and TOR.