ImproveWell.

Privacy Impact Report – March 2019

Date	Review Outcome
July 2017	Initial draft.
January 2018	Removed reference to the use of video as this functionality has been removed. Added flow for sentiment diary functionality.
May 2018	Completed in line with GDPR implementation.
November 2018	Reviewed following draft of Processing Activities Log.
March 2019	Reviewed following the appointment of Amazon Web Services (AWS) to assist ImproveWell with connectivity and cloud-hosted servers, and Zendesk to support ImproveWell's 24/7 customer support ticketing system. Updated data flow maps following launch of new corporate website and three core feedback systems. Added appendix B: system diagram.

Party	Role	Processing Categories	Data Categories	Processors	Sub-Processors
App User	Data Subject	Information related to quality improvement, including basic information about the App User	Personal Data (low risk, very minimal)	N/A	N/A
ImproveWell	Data Controller	Information related to quality improvement, including basic information about the App User	Personal Data (low risk, very minimal)	UKFast Servers AWS Servers	UKFast & AWS Privacy Policies confirm no third parties are supplied with information without consent of ImproveWell
Customer	Data Controller	Information related to quality improvement, including basic information about the App User	Personal Data (low risk, very minimal)	Out of scope for ImproveWell	Out of scope for ImproveWell

ImproveWell.

Initiative Description and Scope

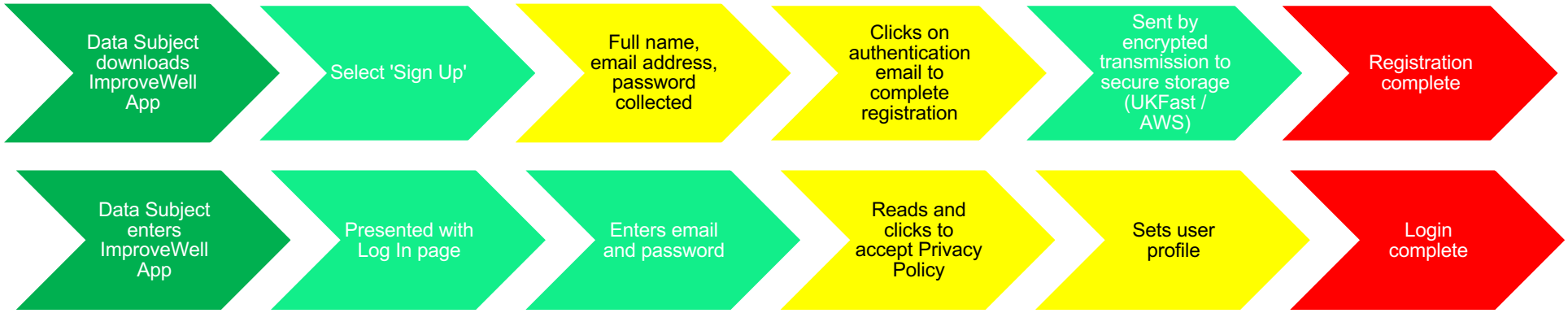
The ImproveWell platform has a smartphone app and data dashboard with three core feedback systems.

The App User is an employee who enters minimal Personal Data (largely by virtue of an email address and job title) into the App and submits (i) theme-based ideas for improvement; (ii) whether they have had a good day, sometimes with reasons why; and (iii) answers to surveys.

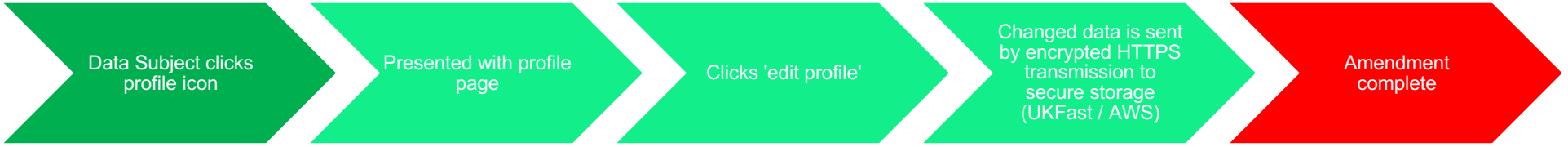
These data are then used to manage quality improvement by the customer and for aggregated purposes by ImproveWell.

Data Flow Maps

Registration and login

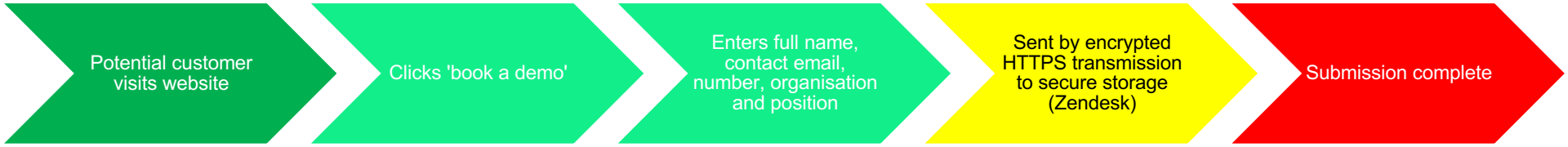


Amendment of Personal Data

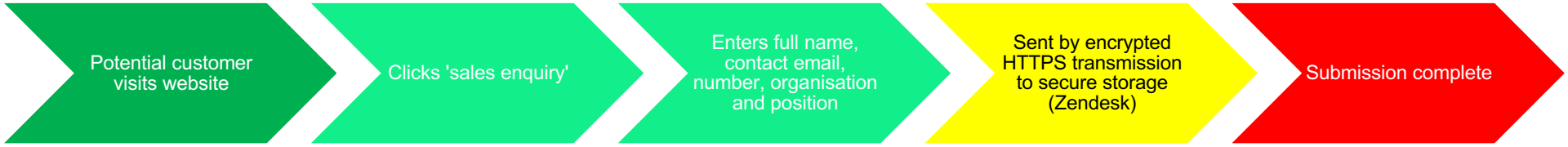


ImproveWell.

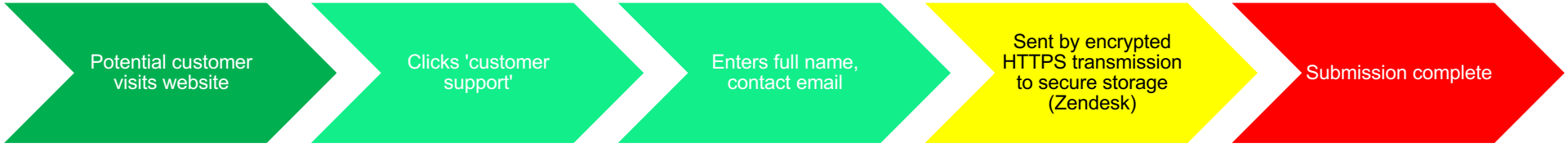
Customer demo request



Sales enquiry



Customer support enquiry

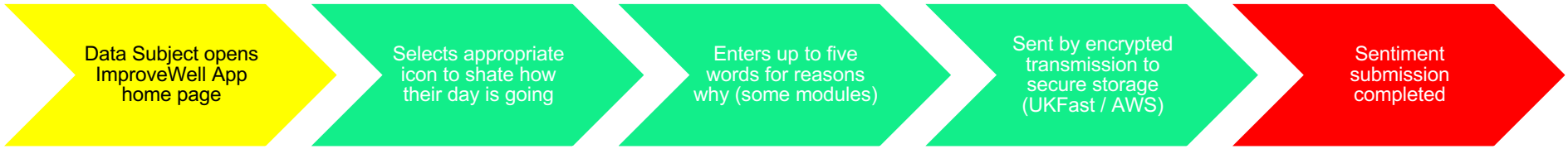


ImproveWell.

Feedback system 1: improvement idea submission

Message submission

Feedback system 2: sentiment submission



Feedback system 3: survey submission

ImproveWell.

Contractual / Sharing Chain

Party	Processing Activity	Contract / Agreement	Lawful Basis
App User (Data Subject)	Providing data within the App for various compatible purposes	Privacy Policy in place providing information about the various uses for the data and how the user may exercise their rights.	**DPA 2018** Schedule 9, Condition 1: The data subject has given his consent to the processing. **GDPR** 6(1)(a) – Consent of the data subject **CLDC** Duty of confidence does arise due to presence of personal information. Set aside lawfully by virtue of informed consent which is deemed to be legitimate and proportionate. See Data minimisation (Appendix A.). **ECHR Art 8** Does represent a (minimal) interference. Lawfully interfered with by virtue of informed consent which is deemed to be legitimate and proportionate. See Data Minimisation (Appendix A.)
(ImproveWell) Data Controller	Processing information entered by Data Subject in respect to identity, sentiment and improvement suggestions	Privacy Policy in place providing information about the various uses for the data and how the user may exercise their rights.	Processing is limited to that detailed in the privacy policy and in line with consent provided (GDPR Art 29.)
UKFast / AWS (Data Processor)	UKFast provide Cloud storage for data generated by App users.	Data Processing Contract limiting further use of Personal Data to that which is specified by the Data Controller	Processing is limited to that detailed in the privacy policy and in line with limitations placed by provided by virtue of Data Processing Contract. (GDPR Art 28 / DPA s 86 (1) (b))

Party	Processing Activity	Contract / Agreement	Lawful Basis
Various clients i.e. hospital trusts (Data Controller)	Reports of improvement information and sentiments entered by Data Subject. Includes identity and improvement suggestions	App Usage Agreement (DSA)	Processing is limited to that detailed in the privacy policy and in line with best practice agreed by virtue of Data Sharing Agreement (GDPR Art 29.).

Data Protection Principles

Fair, lawful and transparent processing	• ImproveWell App has a Privacy Policy in place that underpins the consent model for the user. • Privacy Policy informs users that transfer of data across the internet cannot be entirely secure (as per IGA Guidance). • Privacy Policy identifies the categories of personal information including technical information. • Privacy Policy identifies that it will share information with its partners such as the relevant organisation. • Privacy Policy confirms that ImproveWell does not intend to collect health data via the "How I'm Feeling" sentiment function • Privacy Policy identifies both the primary function of the App as well as technical administration and improvement of the App itself. • Privacy Policy identifies how data subjects might exercise their rights to access of their data including possible charges. • Privacy Policy identifies how data subjects might exercise their rights to correction of inaccurate data. In addition, there is a facility within the App for the user to amend their profile.
Purpose limitation	• Privacy Policy describes standard and potential uses for the data. • Clauses for the third-party storage provider include limitation of data use and the requirement to obtain permission from the data controller prior to any deviation. • Any changes to the project shall be subject to PIA development to ensure there is no 'mission creep' that could undermine lawful basis.

ImproveWell.

Data Minimisation	• A data minimisation exercise has been completed at Appendix A and the data collected appears to be the minimum required for the purpose.
Accuracy	• Data subjects can exercise their right to ensure personal data is accurate through the edit profile functionality. • Contact details are available within the privacy policy to request changes to Personal Data.
Not held for longer than necessary	• A retention schedule has been developed in 2018 as well as a method to put data 'out of use' on the request of the user.
Rights and freedoms of data subjects	• The Privacy Policy indicates that data could be used for direct marketing in the future and that data subjects will be notified. • The Privacy Policy provides contact details for a user to exercise their rights under privacy legislation. • ImproveWell has developed a method for making data 'portable' under GDPR.
Organisational and Technical security measures	• A Privacy Impact Assessment has been completed. • Data Sharing Agreements / Contracts have been reviewed. • ImproveWell has submitted an IG Toolkit for the 2018/19 year. • Initial registration / log in is two-factor and does not require specific validation of identity (name and password) due to low risk data set. • Passwords and data are encrypted at rest in the mySQL database. • Passwords and data are encrypted in transit. • App is not classified as a medical device via MHRA. • ImproveWell has Information Governance resource available to support staff and technical development. • Contract with UKFast / AWS for third party database includes: ✓ Identification of Data Controller and Data Processor roles ✓ Purpose and Use limitation ✓ Confidentiality clauses ✓ Staff training ✓ Data Protection Policy ✓ Business Continuity

	✓ UK and Ireland only Processing
Not transferred outside the EU	• No data is transferred outside of the UK and Ireland.

ImproveWell.

Appendix A: Data Minimisation

Box no (data flow mapping exercise)	Name of Field	What is the source of the data? Which system is it from?	Justification for use (explain why this field is required and how the project would be affected if not available)
1	Full name	Data subject enters into App	Required in order to identify the individual to allow follow up within their organisation – such as engagement with roll out of related improvements.
2	Email address	Data subject enters into App	Required in order to authenticate the individual as an employee of the customer organisation and to send alerts related to the user profile.
3	Password	Data subject enters into App	Required in order to authenticate the individual as the appropriate user of the profile. Without it, Personal Data would be vulnerable to unauthorised access.
4	Job title	Data subject enters into App	Required in order to identify the individual to allow follow up within their organisation – such as engagement with roll out of related improvements.
5	Sentiment	Data subject enters into App	Required in order to allow the user to communicate job satisfaction / morale and for organisations to assess workforce sentiment. This is not a mandatory route for App engagement.

ImproveWell.

Appendix B: System Diagram