ImproveWell.

Data Protection Impact Assessment

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. VERSION CONTROL

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 LTD with connectivity and cloud-hosted servers, and Zendesk to support ImproveWell LTD'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.
January 2020	Added Appendix for Brexit Assessment, removed UKFast Servers as a processor
June 2020	Added Appendix D – Proportionality of Automatically Collected Data
March 2021	Full DPIA refresh (Completed by Kafico Ltd – ImproveWell Ltd's Data Protection Officer)
May 22	Added Sentry as a Processor

2. PROJECT CONTEXT

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

The App User could be a professional from a different organisation, or a service user / patient, customer employee or other stakeholder. The data subject enters minimal Personal Data (largely by virtue of an email address and general role description) 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 LTD.

2. DATA FLOWS

REGISTRATION

1. App User downloads the ImproveWell App and selects ‘Register for an Account”
2. Full name, email address, password are provided and authentication email is issued
3. Clicked link in authentication email completes creation of new account
4. Account data are sent by encrypted transmission to AWS (Amazon Web Storage)

LOGIN

1. On accessing the App, User is presented with Login page
2. User enters email and password
3. Reads and clicks to accept Privacy Policy
4. Sets user profile
5. Login complete

AMENDMENT OF PERSONAL DATA

1. Employee clicks profile icon
2. User is presented with Profile page
3. User clicks 'edit profile'
4. Changed data are sent by encrypted HTTPS transmission to secure storage (AWS)
5. Amendment complete

IMPROVEWELL.COM DEMO REQUEST

1. Potential Customer visits www.improvewell.com
2. Clicks ‘book a demo’
3. Enters full name, contact email, telephone number, organisation and job title.
4. Sent by encrypted HTTPS transmission to secure storage (Zendesk)
6. Submission complete

SALES ENQUIRY

1. Potential Customer visits website
2. Clicks ‘sales enquiry’
3. Enters full name, contact email, telephone number, organisation and job title
4. Sent by encrypted HTTPS transmission to secure storage (Zendesk)
5. Submission complete

CUSTOMER SUPPORT ENQUIRY

1. Customer visits www.improvewell.com
2. Clicks 'customer support'
3. Enters full name, contact email
4. Sent by encrypted HTTPS transmission to secure storage (Zendesk)
5. Submission complete

FEEDBACK SYSTEM 1: IMPROVEMENT IDEA SUBMISSION

1. User clicks 'Share idea for improvement'
2. Enters ideas for improvement
3. Sent by encrypted transmission to secure storage (AWS)
4. Liaises with managers or group leads for idea development and follow up
5. Idea submission complete

MESSAGE SUBMISSION

1. User clicks 'My messages'
2. Enters message related to the improvement idea (some modules)
3. Sent by encrypted transmission to secure storage (Google Firebase)
4. Sent by encrypted transmission to secure storage (AWS)
5. Message submission complete

FEEDBACK SYSTEM 2: SENTIMENT SUBMISSION

1. User opens ImproveWell App home page
2. Selects appropriate icon to share how their day is going (some modules)
3. Enters up to five words for reasons why (some modules)
4. Sent by encrypted transmission to secure storage (AWS)
5. Sentiment submission completed

FEEDBACK SYSTEM 3: SURVEY SUBMISSION

1. User opens ImproveWell App
2. Selects survey to complete
3. Sent by encrypted transmission to secure storage (AWS)
4. Survey submission completed

IMPROVEWELL INSIGHTS MODULE

1. Data subjects are provided access to a unique web-link, by the customer or participating organisation, to IW Insights
2. Users then have the option to share improvement ideas, share how their day is going (some modules), or complete a survey via a web form
3. User completes web form submission
4. Sent by encrypted transmission to secure storage (AWS)
5. ImproveWell Insights submission completed
6. Customer is able to access submissions through the data dashboard website
7. Submissions appear in anonymised form

ImproveWell use a provider called Sentry for logging application errors as well as tracking the time of events that their users experience in their app.

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 and the European Data Protection Board provide 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.

2. ACCOUNTABILITY

ImproveWell LTD is a Data Processor and is therefore required to provide assurance that its is technical and organisational measures are comparable to those implemented by the Controller and are proportionate to the risk. Unlike the Controller, ImproveWell LTD is not in a position to assess the risk to the rights and freedoms of particular data subjects since the Company is not in control of establishing the lawful basis or a direct route for giving effect to data subject rights. However, due to the nature and scope of processing, it seems reasonable to assume that implementing the described project represents a low to moderate risk to the rights and freedoms of data subjects in the event that appropriate technical and organisational measures are not put in place at all. This assessment will therefore explore each of the elements drawn out within data protection legislation for mitigation of those risks.

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 period, e.g. one 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%. Disaster Recovery optional - dependant on outcome of Business Impact Assessment.	2

4. DATA RISK SCORING GRID

Data are 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 special category data that includes stigmatised information (i.e. mental health data).	5

5. RISK SCORING MATRIX

	Asset Criticality				
Impact of data breach		2	3	4	5
	2	Bronze			

	3		Silver		
	4			Gold	
	5				Platinum

6. ASSESSMENT AND RATIONALE

What score has the project been given in terms of criticality of resulting asset or service?	Business Hours Support (8am-6pm) Mon-Fri (not BH). Service Availability 98%. DR optional - dependant on outcome of BIA. (Score of 2)
Rationale	The system would not be considered to be 'business critical' for our ImproveWell LTD's customer organisations, in the sense that the App is supplementary to critical or core services. These factors combined leads this assessment to determine that the processing is inherently low risk. However, ImproveWell LTD has still worked hard to ensure that protection measures are in place to prevent any impact on the rights and freedoms of individuals using the App.
What consideration has the project been given in terms of the nature and volume of data being processed?	Low volume of personal data involved / high volumes of anonymised data.
Rationale	

	It is anticipated that the App will be used for predominantly low risk activities in the form of anonymised expert patient / service user / stakeholder feedback or identified but low sensitivity employee feedback.
Overall risk score given to the processing activity / project in question.	BRONZE.
Does the project involve introduction of a cloud service to be assessed?	Introduces cloud services that will need to be assessed.
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)?	No 'high' authentication activities undertaken.
Does the project involve access by data subjects to their own personal data requiring a 'low' level of authentication (i.e. access to training records)?	User access to own feedback records.

7. RISK ASSESSMENT CONCLUSION

The project has been assessed to have an overall risk score of BRONZE 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 Controller.

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

ImproveWell LTD’s Customer has been assessed to be a Data Controller.

This is because:

- ✓ They decided to collect or process the personal data.
- ✓ They decided what the purpose or outcome of the processing was to be.
- ✓ They decided what personal data should be collected.
- ✓ They decided which individuals to collect personal data about.
- ✓ They obtain a commercial gain or other benefit from the processing, except for any payment for services from another controller.
- ✓ The data subjects are their employees, expert patients/service users/stakeholders.

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

- ✓ They exercise professional judgement in the processing of the personal data.
- ✓ They have a direct relationship with the data subjects.
- ✓ They have complete autonomy as to how the personal data are processed.
- ✓ They have appointed the processors to process the personal data on their behalf.

2. DATA PROCESSORS

ImproveWell LTD has been assessed to be a Data Processor.

This is because:

- ✓ The company is following instructions from someone else regarding the processing of personal data.
- ✓ It was given the personal data by a customer or similar third party or told what data to collect.
- ✓ It does not decide to collect personal data from individuals.
- ✓ It does not decide what personal data should be collected from individuals.
- ✓ It does not decide the lawful basis for the use of that data.
- ✓ It does not decide what purpose or purposes the data will be used for.
- ✓ It does not decide whether to disclose the data, or to whom.
- ✓ It does not decide how long to retain the data.
- ✓ The company makes some decisions on how data is processed but implement these decisions under a contract with someone else.
- ✓ The company is not interested in the end result of the processing.

Amazon Web Services (AWS) has been assessed to be a Sub Processor.

This is because:

- ✓ It is following instructions from someone else regarding the processing of personal data.
- ✓ It was given the personal data by a customer or similar third party or told what data to collect.
- ✓ It does not decide to collect personal data from individuals.

- ✓ It does not decide what personal data should be collected from individuals.
- ✓ It does not decide the lawful basis for the use of that data.
- ✓ It does not decide what purpose or purposes the data will be used for.
- ✓ It does not decide whether to disclose the data, or to whom.
- ✓ It does not decide how long to retain the data.
- ✓ It might make some decisions on how data is processed but implement these decisions under a contract with someone else.
- ✓ It is not interested in the end result of the processing.

Sentry has been assessed to be a Sub Processor.

This is because:

- ✓ It is following instructions from someone else regarding the processing of personal data.
- ✓ It was given the personal data by a customer or similar third party or told what data to collect.
- ✓ It does not decide to collect personal data from individuals.
- ✓ It does not decide what personal data should be collected from individuals.
- ✓ It does not decide the lawful basis for the use of that data.
- ✓ It does not decide what purpose or purposes the data will be used for.
- ✓ It does not decide whether to disclose the data, or to whom.
- ✓ It does not decide how long to retain the data.
- ✓ It might make some decisions on how data is processed but implement these decisions under a contract with someone else.
- ✓ It is not interested in the end result of the processing.

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]

In accordance with data protection legislation, there is a Processing Contract in place between ImproveWell LTD and the customer as Controller.

There is also Processing Contract in place between ImproveWell LTD and AWS as Sub Processor that mirrors the obligations imposed on ImproveWell LTD by the Controller customer.

PROCESSING CONTRACT REVIEW

In accordance with s 56 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 Data Processor: Amazon Web Services (AWS).

Contract reviewed: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

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	Yes	Section 1.3

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

the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller?		
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 including where it might be required to contact the data subject?	Yes	Section 9
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

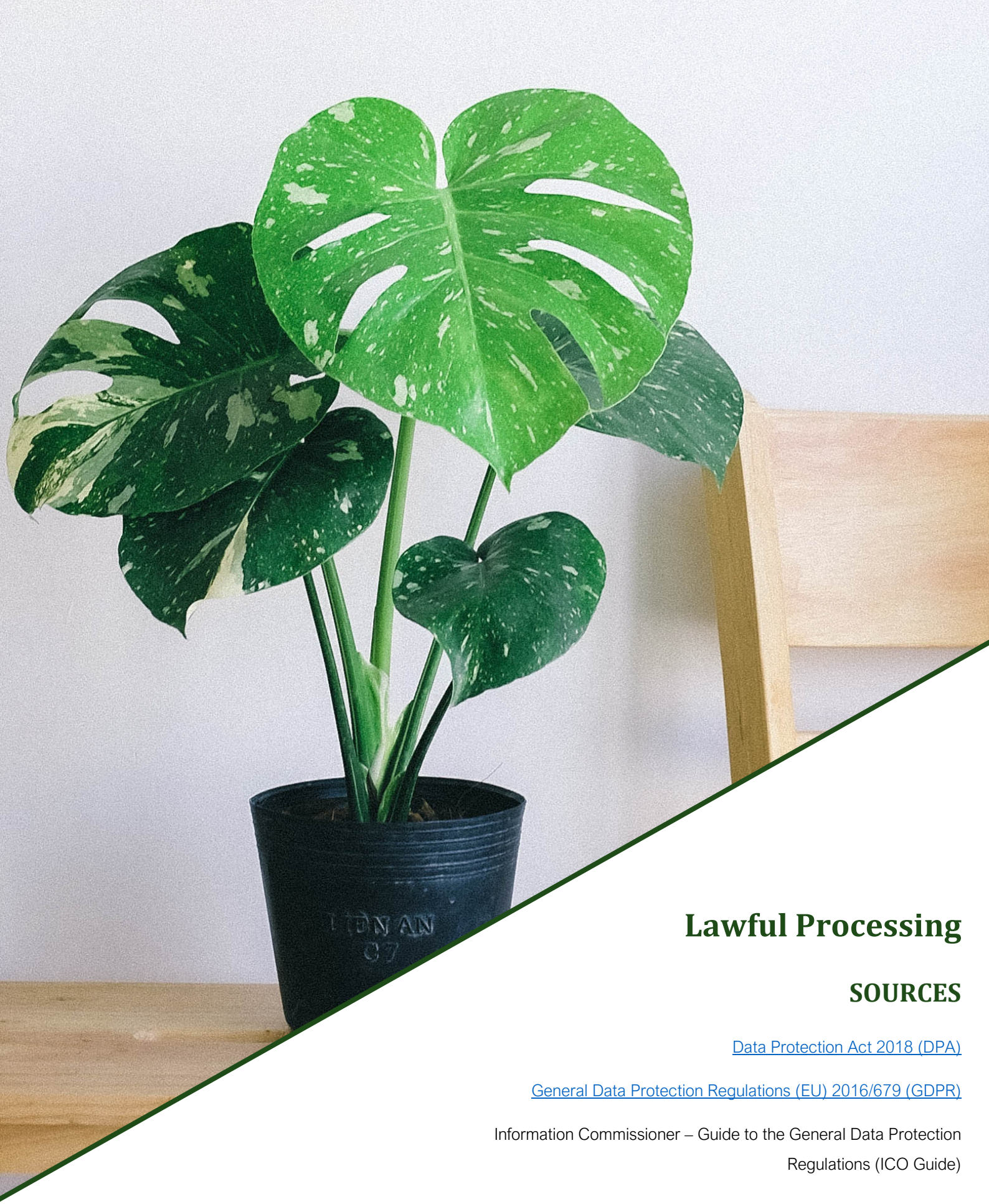
Name of Data Processor: ImproveWell LTD

Contract reviewed: Data Processing Contract ImproveWell LTD Sep 21 v1

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	Data Processor Obligations - 2.5.5
Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller?	Yes	Sub-Processing - 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	Data Processor Obligations Section & Purpose for Processing
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	Data Processor Obligations - 2.5.1 /
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	
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	Requests from Data Subjects and Regulators - 8. Enforcement by Third Parties / 2.5.7 - provide reasonable

		assistance to the Controller in 2.5.7. / Requests from Data Subjects and Regulators 3 3.11
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?		Data Processor Obligations - 2.5.5 / 2.5.6 / 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	1 Introduction - 1.4 / 6 / 7
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	Information Provision 2.6



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 the Controller's 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 its 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 are 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 Article 6 of UK GDPR and a condition for processing of Special Category Data.

Data Processors are not in a position to determine the purpose and means of processing. However, for the purposes of supporting customers and ensuring that they are acting to support customers with their assessments, the following assumptions have been made.

3. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

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

4. CONDITION FOR PROCESSING SPECIAL CATEGORY DATA

Article 9 2 (a) Explicit consent.

7. EXPECTATIONS / COMMON LAW CONFIDENTIALITY

Whilst consent is the identified lawful basis for processing, there is a still a legal requirement to ensure that data subjects are informed about the processing and have the opportunity to ask questions or to object to processing. Additionally, there is a need to ensure that the common law duty of confidentiality is also satisfied.

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.

For the ImproveWell App, it is determined that individuals reasonably expect any disclosures of their personal data to the customer or participating organisation since these types of disclosures are made clear in the transparency notices.

8. CONSENT CONDITIONS

In accordance with ICO Guidelines on obtaining lawful consent, the following assurances have been sought and obtained:

- ✓ The request for consent is prominent and separate from terms and conditions.
- ✓ Individuals are required to positively opt in.
- ✓ 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 are collected and what will be done with them.
- ✓ 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 their employment.
- ✓ Keeps a record of when and how consent was obtained from the individual.
- ✓ Keep a record of exactly what they were told at the time.
- ✓ Regularly reviews consents to check that the relationship, the processing and the purposes have not changed.

- ✓ Has processes in place to refresh consent at appropriate intervals, including any parental consents.
- ✓ Uses privacy dashboards or other preference-management tools as a matter of good practice.
- ✓ Make it easy for individuals to withdraw their consent at any time and publicise how to do so.
- ✓ Act on withdrawals of consent as soon as possible.
- ✓ Doesn't penalise individuals who wish to withdraw consent.

9. REPORTING / ANALYTICS

In the event that The Controller ceases their instructions to process Personal Data, ImproveWell shall render the data anonymous using the approach described below;

Following data fields are removed:

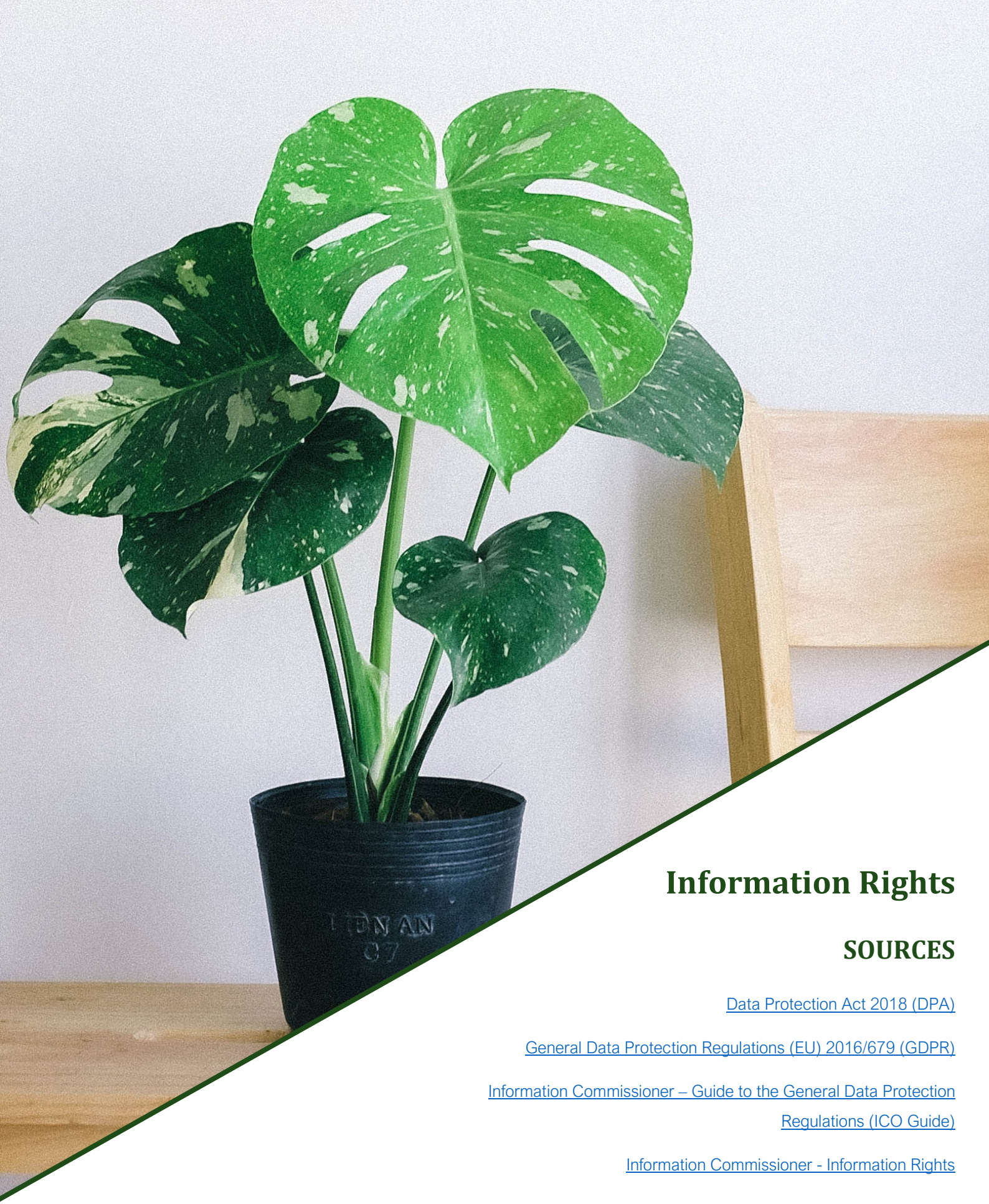
- Full name
- Email address
- Password

Leaving the following data fields:

- Organisation
- Date Stamp
- Profile level 1 (e.g. Directorate / Division) [amalgamated if <5 similar profiles]
- Profile level 2 (e.g. Ward / Team) [amalgamated if <5 similar profiles]
- Profile Level 3 (Role) [amalgamated if <5 similar profiles]
- Innovations
- Sentiment (5 Emojis “how was work today?”)

- Good Day Measure (Have you had a good day – Yes / No and then free text)
- Reference No
- Chat Data (redacted where personal data is present)

Anonymous data shall be used beyond the term of the contract for analytics and product development such as machine learning. The data shall not be published or actively linked with other data sets that could render it Personal Data at a later date.



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.

Processors are contractually bound to supporting Customer Controllers with their information rights requests by virtue of a Data Processing Contract. This means that they will work to support the Controller towards a timely and complete response to any request made by data subjects.

2. FACILITATION OF INFORMATION RIGHTS

Information Right	Applies?	How Supported.
Right to Access	Yes, data subjects do have a right to request access to their information under this lawful basis.	The system being introduced allows personal data to be extracted / printed and provided to data subject on request.
Rectification and Restriction	Yes, data subjects do have a right to request the rectification and restriction of their personal data under this lawful basis.	The system being introduced allows personal data to be amended / access restricted and provides an audit trail of such amendments.
Portability	Yes, data subjects do have a right to portability of their personal data under this lawful basis.	The system being introduced allows personal data to extracted in digital form and sent to another provider on request.

Erasure	Yes, data subjects do have a right to erasure of their personal data under this lawful basis.	The system being introduced allows personal data to be completely removed or anonymised at the request of the data subject.
Profiling and Automated Decision Making	There is no profiling or automated decision-making taking place (that meets the threshold of Art 22) and so these rights would not apply to processing under this DPIA.	Not Applicable.
Object	Yes, the data subject does have a right to object to processing of their personal data under this lawful basis.	The system being introduced allows personal data to be completely removed or anonymised at the request of the data subject.

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 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
- 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 BRONZE level 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. The system is not determined to be a critical asset since it is supplementary to core organisational services. Absence of the service would have very little operational impact on both the provider and their customer. The nature of volume of the personal data is determined by the customer in how they choose to use the service – some may prefer surveys to be anonymous for example.

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.

3. SECURITY OF DATA IN TRANSIT AND AT REST

CLOUD HOSTING AMAZON WEB SERVICES

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

- IW has ensured that any steps necessary to ensure that the cryptography offered by AWS (TLS Version 1.2) are active and are appropriate for their products and services.
    - Communications between cloud components are encrypted to TLS Version 1.2.
    - Communications between cloud data centres are encrypted to TLS Version 1.2.
    - Communications between cloud admin portal and the cloud are encrypted to TLS Version 1.2.

- AWS architecture utilise strong cryptography as defined by NIST SP800-57 to encrypt communications between the Cloud and the End-user. Confirmed by AWS https://aws.amazon.com/blogs/security/tls-1-2-to-become-the-minimum-for-all-aws-fips-endpoints/
- Data is stored in UK and backed up in the EU. Standard Contractual Clauses are in place as an appropriate safeguard.
- IW applies the AWS secure key management services, providing strong cryptography as defined by the current version of NIST and FIPS standards. e.g. NIST SP800-57 Part 1'.
- IW confirms that the project utilises the AWS strong cryptography for data at rest as defined by the current version of NIST SP800-57?
- Data at rest encryption is tested annually against a recognised standard (ISO) by AWS to test the encryption
- AWS customers are protected by Amazon's firewall service called Shield as standard to protect the application from DDOS.
- 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 Uptime

- ImproveWell LTD has deployed across multiple AWS Availability Zones in the *same* region for fault tolerance and low latency.
- If one of the availability zones become available, ImproveWell LTD are able to rebuild in another location, generally within 30 minutes.
- AWS holds and maintains certification to ISO 27001 to include the physical security of the data centres.
- AWS has submitted an NHS Data Protection and Security Toolkit at AWS Toolkit Submission.

4. PROFESSIONAL USERS - AUTHENTICATION

To ensure that the authentication of professional users of the system is in line with UK GOV and NIST standards, the following assurances have been sought and confirmed:

- The password is at least 8 characters long but does NOT set a maximum length.
- The system prevents commonly used passwords for professional users
- The system explains the password constraints to professional users
- The system does not have a limit on the number of password attempts. However, the system will block multiple attempts to send data to the App from the same IP address. While this has a different intention (to prevent DDOS attacks) it will have the same result.
- The system hides passwords by default
- The system allows users to paste their password
- Passwords are stored salted and hashed, using algorithms and strengths recommended in NIST Cryptography Standards
- When the professional user logs in, they are able to see when the credentials were last used

- If a professional user enters their account details incorrectly, the system conceals whether they got the username or password wrong
- If locked out or changing password, the professional user is sent a time-limited password-reset code to the phone number or email that they registered with that does not use password reset questions and does not use password reminders
- When the professional user password is changed, the professional user receives an alert making them aware that their password has recently been changed
- The software allows different privileges for different job roles
- The role that the professional user is logged in under presents itself on screen throughout their use of the system
- The organisation that they are logged in under presents itself on screen throughout their use of the system
- The system is able to provide a view of access levels for all staff members at any one time and suports the ability to immediately ‘block’ a user

5. DATA SUBJECT USER AUTHENTICATION

The system does not permit direct system access for data subjects. Those completing surveys are directed to a link on a web portal.

The surveys, when transmitted to the professional user, are anonymous.

IP addresses are collected by ImproveWell LTD but will only ever be linked to a data subject for information security purposes.

6. SYSTEM AUDIT

The audit functionality has been explored to ensure it is meets with best practice and provides sufficient transparency for data subjects and investigative ability for Administrators.

- The 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 user or administrative data, 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)
- There is a way of viewing or restoring an individual User record as it was on any previous date.
- Successful login audit data includes User id, date and time (to the second).
- Password changes audit data includes User ID, User whose password was changed, Date and time, end-user device (or Solution) identification information.
- Front Line Users are not able to see any submitted, bespoke surveys. Management users are able to see submitted surveys that they have created. Administrators can see all surveys submitted.

7. PHYSICAL SECURITY

ImproveWell LTD deliver its services through a number of remote working consultants and so there has been work undertaken to obtain assurances around secure remote working practices.

In particular, ImproveWell LTD employees or consultants are required to complete a Remote Working and Use of Personal Device questionnaire, requiring them to make the following assertions and confirmations:

- Default passwords (factory settings) on personal laptops and other devices have been amended.
- Default passwords (factory settings) on home routers have been amended.
- Use of personal devices for work are via Standard User accounts and not Administrator login.
- Passwords for personal laptop have a reasonable password threshold in place.
- Personal laptop or mobile device is not used by any other person. Or, if used by other person(s), a separate user profile and password is used.
- Firewalls are activated on your personal devices and that the default settings have been changed.
- Personal device is set to report quarterly to identify performance and activity of firewalls and other malware countermeasures that protect the confidentiality, availability and integrity of the organisation's information assets. Any anomalies must be reported to the Directors.
- Any software applications that are not used, are removed from all personal computers and devices
- Programmes are not able to run automatically and require administrator permissions.
- There are malware programmes running.
- Anti-virus software is updated as updates become available.
- All versions of software are the latest version and supported by the manufacturer.
- Access to physical buildings are appropriately restricted and that laptops and devices are appropriately secured when not in use.
- Care is taken to avoid downloading material or accessing sites that may pose a risk to laptops and devices and that those devices include programmes that highlight high risk websites.

Additionally, with regards to the hosted servers being used for customer data;

- All ImproveWell LTD servers are hosted within industry standard data centres that conform to industry best practices and standards for security as defined in the relevant contract terms and conditions.

8. INTERNATIONAL TRANSFERS

The ImproveWell App involves the transfer of personal data outside of the United Kingdom (Ireland) which means that safeguards must be identified to legitimise such transfers.

Hosted storage for the ImproveWell App involves transfers to countries outside of the UK to EU member states (Ireland) and flows back to the UK are covered by Standard Contractual Clauses as confirmed by Amazon Web Services.

9. DUE DILIGENCE

ImproveWell LTD has achieved the following accreditations that provide assurance that there is a reduction in the risk to the rights and freedoms of data subjects:

- ImproveWell LTD has completed a compliant NHS Data Protection and Security Toolkit for the current year (Toolkit Submission)
- ImproveWell LTD has achieved Cyber Essentials accreditation

Media Coverage of Breaches

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 ImproveWell LTD. At the time of writing, ImproveWell LTD had no media presence with regards to data breaches.

Checks with Information Commissioner

Checks have been undertaken with regards to the UK Information Commissioner. ImproveWell LTD is registered with the Information Commissioner and their registration number is ZA275449. There have been no fines or undertakings issued to ImproveWell LTD by the ICO.

Data Protection Lead

ImproveWell LTD has identified the following leads for data protection matters:

Data Protection Officer: emma.cooper@kafico.co.uk

Director: lara.mott@improvewell.com

Director: john.masterson@improvewell.com

Training and Awareness

The company has 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.

Obligations of Secrecy

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

10. CONCLUSION

Data Protection Impact Assessments will routinely conclude with a risk scoring grid and final sign off by appropriate parties. ImproveWell LTD is a Processor and so is not in a position to identify nor sign off risks as having been appropriately mitigated since the risk appetite for each customer will differ.

Rather, this document serves more as a demonstration of Privacy by Design such that customers, as Controllers may use its contents to make their own assessments in accordance with their obligations under data protection legislation.