Good Boost Wellbeing Limited

Data Protection Impact Assessment (DPIA) (#GBP020)

< Good Boost app >

Last updated: 22/12/2022
Next review due: 22/06/2023

Data Protection Officer (DPO): Alex Georgiou

Contents

SECTION 1.0 – Overview

1.0 Overview

This document follows the ICO process for Data Protection Impact Assessment (DPIA) requirements for data protection at Good Boost under the criteria for an acceptable DPIA as set out in European guidelines on DPIAs

Name of controller	**Alex Georgiou**
Subject/title of DPO	Technical Director
Name of controller contact /DPO	Alex Georgiou
Contact details	Alex.Georgiou@goodboost.org / DPO@goodboost.org

1.1 Scope: Health IT System

The Scope of this DPIA is for the Good Boost exercise app as defined in Good Boost registration in the Medicines and Health Regulatory Authorities (MHRA) Class 1 Medical Device, reference number 8728 under 'Biomechanical function analysis/rehabilitation'. This DPIA applies to all uses of Good Boost technology.

The Good Boost app involves the collections and sharing of user data for the purpose of creating an account, tracking performance over time and having the necessary data to make exercise suggestions based on a users preferences, exercise goals, heath details of body part specific information.

The Good Boost app is a native app available as an APK app which is directly installed on tablet computers at venues (such as leisure centres) that have purchased Good Boost. It will be made available as a native android and iOS app in later 2021.

1.2 Top Management Responsibilities

In implementing the DPIA for a given deployment, Top Management must:

- make available sufficient resources
- assign competent personnel from each of the specialist areas that are involved in developing and assuring the IT System and architecture
- nominate a Data Protection Officer (DPO).

Top Management must ensure that appropriate levels of authorisation for the Health IT System and its safety documentation are defined in the DPIA.

1.3 Data Protection Officer

Good Boost's Data Protection Officer (DPO) is a software engineer with sufficient experience and training to conduct and complete the DPIA process and monitoring.

The role of a DPO is to review the data protection processes using their experience to judge the appropriateness and effectiveness of the risk management strategies and mitigating actions. The DPO will monitor the execution of the DPIA and ensure that data protection obligations are being discharged.

1.4 Competencies of Personnel

Personnel have the knowledge, experience and competencies appropriate to undertaking the DPIA tasks assigned to them. Competency and experience records for the personnel involved in performing the data protection risk tasks must be maintained. Alex Georgiou is Good Boost's Technical Director, with a BSc in Computer Technology, 15 years experience in IT system, a certified Microsoft Administrator with extended training as a Data Protection Officer.

1.5 Regular DPIA Process Review

This process review is repeated every 6-months and upon the release of any new feature and/or function that changes the intended use and/or audience of the IT system.

1.6 Technology and Architecture

The Health IT system is the Good Boost app, a mobile app with a cloud based back end and NOSQL database. The mobile app can be used on phone and tablet device.

The system is written using JavaScript, particularly NodeJS and ExpressJS as a framework for a back end and React Native and React for the front end.

The data is stored in a MongoDB (NOSQL) database which has replica set.

All passwords are encrypted in the database. All parameters are encrypted in transit over HTTPS. All data is stored on an encrypted disk at rest. Good Boost follows it's policies and protocols to restrict system access to personnel who require it to minimise unnecessary data access. All personal follow the requirements of the Password Policy and Working from Home policy that directs good practice to minimise system compromise.

All data-entry fields are masked to resist the entry of programming code. All parameter data received by application files is treated to strip out tags and characters likely to be used in programming script, before the data is used internally. All multi step database transactions are contained within a single transaction to ensure that changes are automatic.

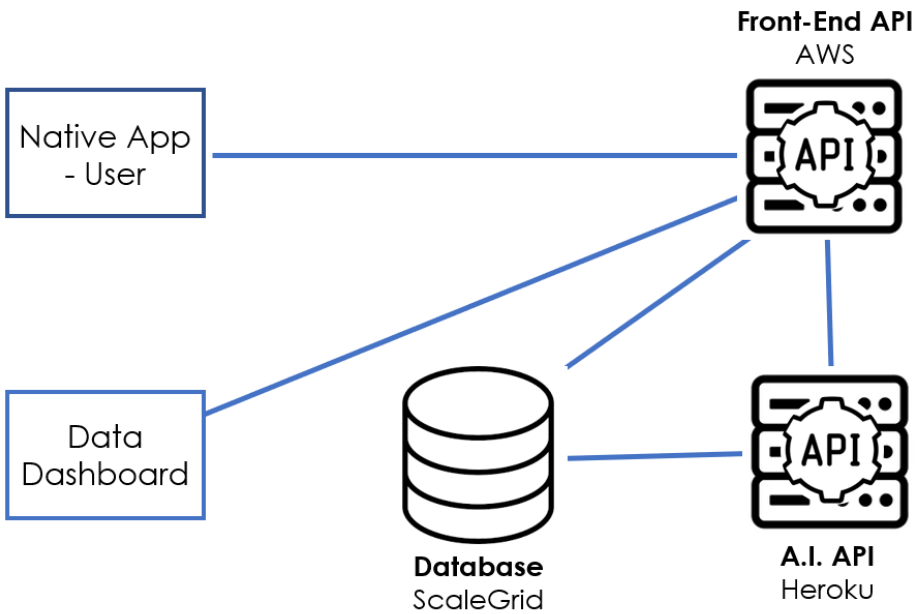
The servers are hosted by AWS, a reputable hosting provider with experience in the healthcare domain. The architecture is designed to provide a high availability service with a minimum uptime percentage of 99.95% at all times during the service provision time in any month.

Maintenance activity that affects the availability of the solution is performed outside of core working hours. The hosting provider keeps scheduled downtime to a minimum and aims to provide 7 days' notice or the maximum period of notice practicable. During service provision time, the hosting provider proactively monitors the operational state of the network to detect faults. As we use cloud servers, we do not have any equipment that requires an Uninterruptible Power Supply (UPS) for the continual operation of our technology and systems.

The performance of the system is monitored by the Company in live service to ensure it remains performant.

Back up procedures are in place to ensure the source code in the Good Boost application server and the data in the database are automatically backed up with replica instances in the cloud system with monthly physical backups. Routine restores are scheduled periodically and performed to confirm the restore capability works appropriately. Backup and restore procedures are documented in the Company's Back Up and Restore Policy (Ref. 3). The Company also has a Business Continuity Plan (Ref. 4) in place which describes how the Company can recover from an incident that threatens to disrupt its normal operations.

Data Flow



1.7 Overview and intended use

The system consists of three components:

1. A native app that is user facing which allow individual to register their details and follow personalised exercises suggested by Good Boost's AI exercise selection system.
2. The Good Boost AI exercise selection system
3. A web-portal for public venues delivering Good Boost that provide a data dashboard overview of the number of users at their venue and aggregate statistic (no individual user data is displayed/accessible)

The service is accessed by users via a native app, either in a community settings (i.e. a leisure centre) on a waterproof tablet computer located in the venue, or with their own personal device (from late 2021). Once registered a user can choose whether to follow a exercise sessions from the exercise library (pre-made exercise sessions that are generic, not personalised) or a personalised session that includes exercises suggested based on the users registered details, preferences and feedback.

Users have the option to register relevant health details and details about a body part(s) with a musculoskeletal condition. Users do not need to have a musculoskeletal diagnosis to register a body part.

The AI exercise suggestion system does not make any diagnosis regarding a users registration details. The system has been designed to filter exercises and suggest exercises based on clinical guidelines, published research and best-clinical practice that are safe and appropriate for the user. The exercise(s) recommended is influenced by multiple factors including physical activity levels, subjective functional movement reporting, equipment and environment preferences and preferences over exercise(s) completed.

The user can use the app to follow an exercise programme with instructions (both written and animation videos). The user can provide feedback after their exercise session. This includes how satisfied they were with the exercise or any difficulties performing the movement. This information is used to adapt the users exercise suggestion for their next session. This is an on-going feedback loop system.

2.0 – Data Collected

2.0 Data Collected (Data Scope)

The Good Boost technology requests data from users. Some data is mandatory, some data is optional. For some mandatory fields, users have the option for 'prefer not to disclose'

Personal Details
Email address*
Phone number
Name*
Gender
Year of Birth* (not date of birth)
Post code/zip code*
Country*
Employment status

Sensitive Data
Ethnicity

Physical Health and Physical Function Details (Special Category Data)
Exercise safety screening details*
Long-term health conditions
Body part specific information (i.e. musculoskeletal details, knee pain)
Outcome measure data (i.e. self-reported pain, function, wellbeing)

All data fields marked with an * is a mandatory field. Other fields are optional and/or have the option 'prefer not to disclose'. If a user does not provide physical health and Physical function details, they will have limited access to the features on the Good Boost app, i.e, there will be no personalised exercise programmes, as there is insufficient data to suggest exercises.

All users to make use of the Good Boost app enter into a contract with Good Boost upon registration and the legal grounds for processing (GDPR Article 6, 1(b). Users are provided with the details (terms & conditions and privacy policy) of how their data will be processed in order to use the Good Boost app service and must opt-in and accept the terms & conditions and privacy policy to complete registration and form a contract. In the event a user does not agree and consent, no data will be stored and the user will be unable to enter any further data as part of Good Boost exercise recommendation app. Good Boost also use the data collected and processed data to analyse user updates and improve the product, completed under GDPR Article 6, 1(f).

2.1 Conditions for processing sensitive / special category data

Good Boost collect and process sensitive and special category data under GDPR Article 9, 2(h). Users are made aware of the sensitive and special category data being collected and how it will be processed.

Ethnicity is gathered for the purposes of analysing user uptake demographics. Users are provided with the options of 'prefer not to disclose'

The physical health data is collected and processed for the safety of the user through screening processes to ensure the users is suitable to engage in physical activity without needing to seek further consultation with a GP or health care professional.

Health details regarding long-term health conditions and body part specific information (musculoskeletal details) is used to inform further safety screening, sign-posting to resources and to collect the data to be processed through Good Boost A.I. knowledge map to suggest an appropriate exercise programme to follow.

Ongoing post-exercise feedback data is collected to create a continuous feedback loop to inform future exercise suggestions based on user preferences. Outcome measure data is collected before every personalised exercise session on the app and at time-based interval (e.g. 4-weekly). Time-based interval outcome measures are optional.

2.2 Data Details

For all of the data collection fields, only the minimum required data collection takes place. This includes data such as date of birth, which isn't collected, year of birth is the only data collected.

For many personal data and sensitive personal data such as gender and ethnicity, users have the option to select 'prefer not to disclose'.

For health data, the minimum amount required is collected. This is to ensure adequate screening processes for physical activity safety. The joint specific information (musculoskeletal details) is gathered specific to the individuals answers, rather than a generic 'capture all' form. As a result, the physical health data collection process is designed to minimise data collection for the data only required for processing.

A user does not need to provide any health data (with the exception of safety screening data) to use Good Boost pre-made exercise programmes that involve no personalisation.

2.2.1 How often is data being collected

Data is collected at user initial registration to the Good Boost app. On-going data is collected if a user updates their details within the Good Boost app.

The only on-going data collection is the outcome measure data. For the time-based outcomes for self-reported pain, function and wellbeing, these are optional data collection points.

2.2.2 How long will data be kept

Data will be kept up to 10 years.
All users are provided with the details to review and request to remove data.

2.2.3 How many people are affected

The number of people affected is dependant on the number of people who voluntarily sign up and register with Good Boost.

2.2.4 What geographic areas are covered

The United Kingdom is covered. Good Boost intends to operate a publicly downloadable exercise app in other territories that is intended for personalised exercise only, and not any specific therapeutic purpose.

2.2 Data Details

For all of the data collection fields, only the minimum required data collection takes place. This includes data such as date of birth, which isn't collected, year of birth is the only data collected.

For many personal data and sensitive personal data such as gender and ethnicity, users have the option to select 'prefer not to disclose'.

For health data, the minimum amount required is collected. This is to ensure adequate screening processes for physical activity safety. The joint specific information (musculoskeletal details) is gathered specific to the individuals answers, rather than a generic 'capture all' form. As a result, the physical health data collection process is designed to minimise data collection for the data only required for processing.

A user does not need to provide any health data (with the exception of safety screening data) to use Good Boost pre-made exercise programmes that involve no personalisation.

2.2.1 How often is data being collected

Data is collected at user initial registration to the Good Boost app. On-going data is collected if a user updates their details within the Good Boost app.

The only on-going data collection is the outcome measure data. For the time-based outcomes for self-reported pain, function and wellbeing, these are optional data collection points.

2.2.2 How long will data be kept

Data will be kept up to 10 years from the most recent log in date of the user. Data is kept for 10 years to support the ongoing clinical evaluation, learning and product development of the Good Boost system. All users are provided with the details to review and request to remove data.

2.2.3 How many people are affected

The number of people affected is dependant on the number of people who voluntarily sign up and register with Good Boost.

2.2.4 What geographic areas are covered

The United Kingdom is covered. Good Boost intends to operate a publicly downloadable exercise app in other territories that is intended for personalised exercise only, and not any specific therapeutic purpose.

2.3 Nature of the Data Processing

2.3.1 Data Collection Method

Data is collected via the Good Boost app via an end-to-end encrypted data transfer process to Good Boost secure, cloud storage database.

2.3.2 Data Storage

Data is stored on Mongo DB via Scale Grid. (additional details)

2.3.3 Data Use

Data is used for:

- Registering unique users
- Enabling account log-in credentials
- Safety screening
- Personalised exercise calculation and exercise suggestion

2.3.4 Deletion of Data
All users are provided with the details on their data ownership and ability to request, review and delete their data at anytime in the Privacy Policy.

Data will be kept to up to 10 years by Good Boost for the purpose of ongoing clinical reviews, evaluation and product development.

2.3.5 Data Sharing
Good Boost may share non-personally identifiable data with academic and evaluation partners for the purposes of clinical audits and service evaluation. No personal data to identify any user is ever shared with a third party without additional and explicit consent which is collected as an opt-in consent agreement when registering with the Good Boost app.
Where data sharing with academic partners takes place, a data sharing agreement is created with the academic/evaluation partner.

Aggregate data is shared with Good Boost venues, such a leisure centres, so they can review the collective activity in their venues. No data is ever shared that can be attributed to a single user (through low number suppression) and no personal details are shared. Users are informed of their data being included in aggregate data dashboard in the Privacy Policy. The aggregate data includes:

- Number of users
- Exercise sessions completed
- Average demographic details (age, gender)
- Outcome measure change (i.e. change in self-reported pain, function and satisfaction)

2.4 Contexts of the Data Processing
2.4.1 Good Boost Relationship with Users
Good Boost users voluntarily register and use Good Boost digital services. Our relationship with users is to provide them with exercise libraries and personalised exercises.

2.4.2 How much control do users have
Good Boost users have full control and rights over their data to request, review, edits and request for data removal at any time.

2.4.3 Good Boost users expectation of data use
Good Boost provides full details in our terms and conditions and privacy policy on the Good Boost app and how their data is used and processed. This is ensure users are fully informed and enter into an opt-in contract for Good Boost digital services.

2.4.4 Children and vulnerable adults
Good Boost only accepts users who are aged 18 or over to register. Good Boost is not designed to support vulnerable adults.

2.4.5 Approved code of conduct and certification
Good Boost is certified by Cyber Essentials and adheres to the Caldicot Principles .
Principle 1 — justify the purpose(s) for using confidential information.
Principle 2 — only use confidential information when absolutely necessary.
Principle 3 — use the minimum information that is required.
Principle 4 — access to confidential information should be on a strict need-to-know basis.
Principle 5 — everyone must understand their responsibilities.
Principle 6 — understand and comply with the law.
Principle 7 — the duty to share personal information can be as important as the duty to have regard for patient confidentiality.

2.5 Purpose of Processing

2.5.1 What is intended to be achieved through processing?

Process the data Good Boost collects is for 6 core purposes.

1. Ensure user validation and ability for account creation and unique log-in credential
2. Evaluate user safety and suitability in taking part in physical activity and exercise
3. Create personalised exercise programs based on a combination of health data, user personal preferences and post-exercise feedback data
4. Gather output and outcome data so users can review their activity and observe measured changes over time
5. Gather output and outcome data so Good Boost can review the effectiveness of the digital service and make ongoing service improvements
6. Gather output and outcome data to report aggregate data to customer, funders and stakeholders

2.5.2 What is the intended effect on users?

The intended effect of data processing on users is:

1. Ensure user validation and ability for account creation and unique log-in credential
2. Evaluate user safety and suitability in taking part in physical activity and exercise
3. Create personalised exercise programs based on a combination of health data, user personal preferences and post-exercise feedback data
4. Gather output and outcome data so users can review their activity and observe measured changes over time

2.5.3 What is the benefit of processing for users?

Overall, that users have a valuable digital exercise service that promotes accessible and achievable physical activity and that community venues can deliver exercise programs that are suitable for a wide ranges of individual users needs.

2.5.4 What is the benefit of processing for Good Boost

That Good Boost can deliver a personalised exercise service and gather the data to evaluate performance and for ongoing service improvement.

2.6 Consultation Process

2.6.1 External consultation process and co-design

Good Boost has completed focus groups with service users and with older adults living with musculoskeletal conditions (core user group) to understand preference for app design, development and data collection for current and future technology and data collection. This process has highlighted that users and potential users want to be informed of their data rights and ability to request, review, edit and delete their data.

Good Boost has had external consultation with Oxford Clinical Allied Technology and Trial Services Unit (OxCATTS) as part of our external review on data collection and design for outcome measurement.

2.6.2 Internal consultation process

Goods Boost internal consultation process for data collection and data processing is led by:
Ben Wilkins, CEO & Clinical Safety Officer
Dr. Ben Waller, Clinical Director
Alex Georgiou, Technical Director and Data Protection Officer

The design of the data collection, database architecture, data processing, data security, data governance, and data management has been collectively designed, reviewed and implemented by the senior team with the support of the wider Good Boost team.

2.7 Necessity and Proportionality

2.7.1 Lawful Basis for Processing

Reviewing the purposes of processing activities and select the most appropriate lawful bases.
The lawful basis under the Data Protection Act 2018 is:

- **Article 6(1)(b)** processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"
- **Article 6(1)(f)** processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- Article 9 (2)(h) provides for exceptions to processing data related to medical and social care, which must be necessary

The processing of data is necessary for the relevant purpose and there is no other reasonable and least intrusive way to achieve that purpose.

2.7.2 Processing for intended purposes

The processing of user data fulfils the intended purposes as listed in 2.5.1. The only other way to achieve the same outcome would be a 1-2-1 consultation with a suitably qualified exercise instructor or health care professional to create a personalised exercise programme. This would undermine the mission of Good Boost to offer an affordable and accessible service and be impractical to scale to support more people to be physically active.

2.7.3 Function Creep

To prevent the user of information and data for a purposes that is not the original specific purpose Good Boost will annually review the collection and processing of user data and that it fulfils the intended purposes.

2.7.4 Data Quality & Data Minimisation

To ensure data quality Good Boost completes data accuracy audits to ensure that data is being accurately collected and stored in databases to ensure data quality. This is part of Good Boost Clinical Risk Management Plan.

As part of data collection minimisation, Good Boost annually reviews the data being collected to achieve it's intended purposes. This review is intended to reduce data collection where possible.

2.7.5 Information provided to individuals

Good Boost provided information to users during the registration and sign-up process and provides it's terms and conditions, privacy policy and key data and clinical policies on the Good Boost website for public access.

2.7.6 Ensuring user rights to their data

Every user has the right to request, review, edit and remove their data. Fully details are provided in Good Boost Privacy Policy.

3.0 – Data Risk Analysis

In accordance with the data risk management process a data risk analysis has been undertaken to understands the risks associated with use of Good Boost's digital exercise app. Section 3.0 described the process and methodology in identifying and analysing risks alongside the estimation of the relative risk to users data.

3.1 – Datal Risk Analysis Process

The data risk analysis process involves three key steps.

1. Identification of potential risks to users data
2. Analysis and scoring of risks
3. Estimation of the risk to users data

This process involves a multi-disciplinary group of clinical, engineering and operational staff members that is led by the DPO and supported by the CSO. The multi-disciplinary process for risk identification, analysis and estimation is to ensure maximum likelihood of identifying risk and collective analysis and evaluation.

The extent of each data risk analysis must be proportional to the scale, complexity and level of data risk association with the exercise technology and user of the technology.

3.2 – Identification of Risk to Users Data

The known and foreseeable hazard to users with respect to the intended use of the digital exercise system in both normal and fault conditions will be identified for analysis and risk estimation.

The process of risk identification follows best practice as recommended by the Health and Safety Executive and following guidance from the Information Commissions Office.

The potential hazards to users data are listed and described in *Table 3.1*

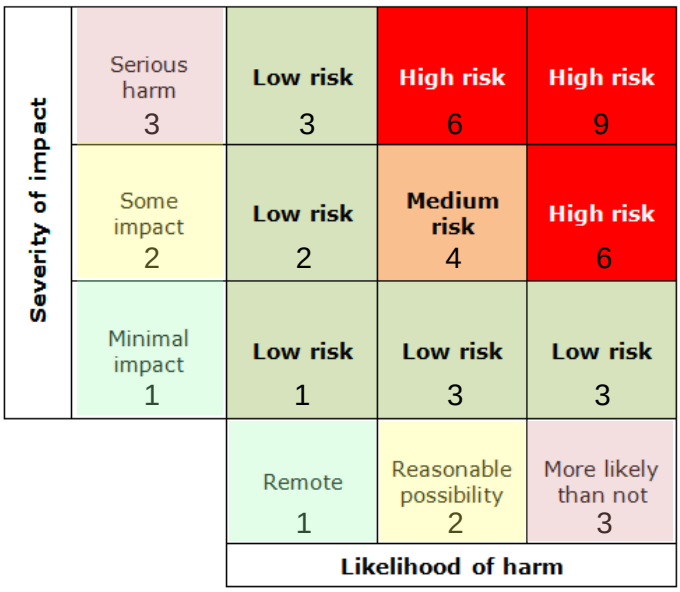
3.3 – Estimation of Data Risk

Estimation of data risk uses criteria specified below that includes:

- Severity of the impact
- Likelihood of the harm
- The resulting overall data risk

To estimate the clinical risk a Clinical Risk Matrix has been applied to quantity the total risk and the risk acceptability definitions suitably evaluate and respond to each risk.

The Data Risk Matrix and scoring criteria are displayed below.



Matrix from the Information Commissions Office (ICO) – Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/

The matrix has been adapted to illustrate the quantitative values places for the severity and likelihood ratings (1-3). Each score is multiple to create the overall data risk score (1-9).

3.4 – Risk Identification and Risk Assessment

Each identified data risk has been scored in the Table 3.1 below. The data risk score is calculated and presented. The proposed risk mitigation is described and the newly assessed data risk score is calculated. The evaluation on the impact of individuals in listed in the final column.

Table 3.1 – Data Risk Table

Risk Description	Severity	Likelihood	Score (SxL)	Proposed Risk Mitigation	Severity	Likelihood	Score (SxL)	Evaluation – impact on individuals after applying solution
Privacy Policy and use of data is not easy to access prevent informed data consent.	3	1	3	Privacy policy alliable on the app during registration, option to email privacy policy to users registered email for further review, privacy policy available on website.	2	1	2	Users have sufficient information on data use and able to provide informed data consent for lawful processing of data.
Data controllers do not have sufficient governance controls to ensure personal data will be handled safely or securely	3	2	6	Protocols and policies on data handling and data use for controllers. Controllers have training on data protection. Support from DPO.	2	1	2	Data controllers have sufficient governance and support to handle data safely and securely.
Data processors do not have sufficient governance controls to ensure personal data will be handled safely or securely	3	2	6	Protocols and policies on data handling and data use for processors. Processors have training on data protection. Support from DPO.	2	1	2	Data processors have sufficient governance and support to handle data safely and securely.
Information access unlawfully or inappropriately by staff	3	3	9	Protocols and policies on data handling and data use for processors and controllers. All user accounts have unique I.D to separate personal data from other data. Personal data is restricted to authorised personnel only, to minimise unlawful and inappropriate data access.	1	1	1	Mitigation of risk for unlawful or inappropriate data access through controls and access measures.
Information used for purposes that intended purposes	3	1	3	Clear data purpose and intended use in privacy policy.	2	1	2	Information to be used for intended purposes.

3.4 – Risk Identification and Risk Assessment

Risk Description	Severity	Likelihood	Score (SxL)	Proposed Risk Mitigation	Severity	Likelihood	Score (SxL)	Evaluation – impact on individuals after applying solution
Information not kept securely on systems leading to a cyber security incident	3	3	9	Data is stored on credible cloud database with mutli-factor authorisation and limited personnel with access to personal data to prevent any cyber attack. Regular penetration testing	2	2	4	Policies, protocols and activities in place to minimise risk of data loss/theft due to cyber security incident,
Data loss due to total system failure	3	2	6	Automatic back ups on Scale grid and Heroku systems with multiple synchronised instances of DB for back-up. Monthly manual back up by DPO on encrypted external drive.	2	1	2	Limited risk of data loss. If data loss occurred, impact would be limited to regular back-ups
Data breach due to intentional or unintentional staff member action	3	2	6	Policies and protocols to ensure staff laptops are encrypted, password protected, anti-virus, VPN and only use private networks with firewalls. All staff have training and provided with ongoing support by top management and DPO. Limited access for personal data by authorised persons only with multi-factor authentication.	3	1	3	Risk of data breach minimised to ensure user data security
Data loss due to unsecure transfer of data between app and database	3	2	6	The data transfer between app to database is end-to-end encrypted to minimise risk. Regular load testing and penetration testing to identify and resolve any architecture weaknesses.	3	1	3	Risk of data breach minimised to ensure user data security
Users not being able to request data removal due to technical issues	2	2	4	User are provided with multiple options to contact Good Boost / DPO to request information on their data in the event they have technical issues by requesting through the app or email.	2	1	2	Multiple channels to contact Good Boost are made available to users
User not logging out and leaving account logged in and accessible to others	2	2	4	Auto log-out after 60 minutes of inactivity	2	1	2	Limited risk and exposure of non-user accessing account

4.0 – Measures to Reduce Data Risk

Following risk identification, analysis and evaluation, control measures to mitigate risk have been identified. These are listed below with key details.

Privacy Policy

The Good Boost Privacy Policy is available during registration and sign up, so the individual is able to review the full policy ahead of agreeing to register and submit their initial personal detail for Good Boost user account creation. The privacy policy is also available on the Good Boost website. The privacy policy provides the individual with details of what data is to be collected, how it will be processed and their data rights. It also includes the details to contact Good Boost / DPO for any data requests. The new user must tick box and agree they accept the privacy policy, otherwise the individual is unable to complete the registration process.

Data Handling and Data Processing Policy

Good Boost Data Handling and Data Processing Policy outlines the key measures, protocols and actions required anyone handing data.

Access and Authorised Persons Policies

Good Boost's access and authorised person policy stipulates the requirements for access to specific systems at Good Boost and the process for system access and privileges. Only authorised persons at Good Boost, who sign an additional agreement acknowledging their position and responsibility and completed additional data protection training have access to user personal data.

Database Design

The Good Boost database design partitions user personal data from other data that is required for processing and review (i.e. to evaluate service performance and conduct audits). Each users is provided with a unique ID number. The partitioning of the personal data ensure that other data cannot be associated with any individual, as there is insufficient identifiable data.

In addition to the database design, the database can only be accessed by authorised persons who must follow the Good Boost password policy and multi-factor authentication.

Data Authorisation Agreement between Controller and Processor

Good Boost (data controller) work with an app development agency, Dev2Grow (data processor). Good Boost and Dev2Grow have a development contract for the development, coding and deployment of Good Boost that includes the requirements of data protection. In addition to the contract, Good Boost and Dev2Grow have a Data Authorisation agreement, further outlining the requirements for data protection that adheres to the General Data Protection Regulation (GDPR) and ensure cyber security and defences to mitigate the risk of systems breach and data compromise. The data authorisation agreements also stipulates the authorised persons at Dev2Grow who also have access to the user database for the purpose of maintenance.

Data Sharing Agreements between academic / evaluation partners

For each evaluation and/or research project, an evaluation or research ethic application will be created. This include a data sharing agreement with relevant parties.

4.0 – Measures to Reduce Data Risk

Database and code back-ups and retore plan

Automatic back-ups of the Good Boost database take place in Scale Grid. There are three instances of the server (all synchronised) for back up safety. A physical back up is created monthly by the DPO on an encrypted device which is stored in a locked security drawer.

Technology Risk Management Plan

Good Boost's Technology Risk Management Plan identified, analyses and evaluates are risks to Good Boost technology stack. Where risks are intolerable, control measures have been identified and applied to mitigate risk. These include:

- Policies and procedures
- Training for all staff
- Cyber security features: anti-virus, laptop encryption, virtual private networks
- Penetration and load testing – acunetix penetration testing system

Cyber Essentials certificate

Good Boost is certified by Cyber Security essentials to identify and mitigate risks to Good Boost technology stack.

ICO registration

Good Boost is registered with the Information's Commission Office (ICO) with Alex Georgiou registered at the Good Boost Data Protection Officer.

Ref Number: ZA501212

5.0 – Delivery

5.1 Delivery

The delivery of the measures to reduce data risks are led by the DPO who has full ownership.

5.2 Monitoring

The delivery of the measures are monitored by the DPO, with a 6-monthly review. Certain measures such as data backups and penetration testing occur on regular cycle (daily, monthly)

5.3 Review process

The Data Protection Impact Assessment is reviewed every 6-months to ensure all risks are being controlled and any new potential risks are identified, analyses and appropriate measures are adopted.

6.0 – Sign off and record outcomes

Following risk identification and analysis and evaluation will take place to determine whether the clinical risk is acceptable as defined in the criteria defined in the Clinical Risk Management Plan.

Item	Name/position/date	Notes
Measures approved by:	Alex Georgiou – DPO	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Ben Wilkins – CSO	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	All control measures in place and confirmed	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:	All accepted	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	Ben Wilkins	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Alex Georgiou - DPO	The DPO should also review ongoing compliance with DPIA

Signed: Alex Georgiou

Alex Georgiou – DPO
22nd December 2022

END OF DOCUMENT