Addressing Psychosocial and Lifestyle Risk Factors to Promote Primary Cancer Prevention: an integrated platform to promote behavioural change (iBeCHANGE)

Project Number: 101136840

D7.2 – iBeChange Platform Design Regulatory Requirements

Related Work Package	**WP7 – Ethical, Privacy, and Data Protection**
Related Task	**Task 7.1 – Ethical and Legal Inventory**
Lead Beneficiary	i~HD
Contributing Beneficiaries	ICO, IEO, SPORDATA, EUT, POLIMI
Document version	V1.0
Deliverable type	R
Dissemination level	PU
Due date	30/11/2024
Delivery date	17/12/2024
Authors	Nathan Lea (i~HD), Muna Khogali (i~HD), Dipak Kalra (i~HD)
Contributors	Maria Serra Blasco, Anna García Serra (ICO), Emilia Ambrosini (POLIMI), Carolina Falcone, David Sũnol (EUT), Massimo Monturano, Marianna Masiero, Elisa Tomezzoli, Giorgia Miale (IEO), Virginia Sanchini (UNIMI), Chloe Laurent (SPORDATA), Laura Genga (TU/e)
Reviewers	iBeChange Consortium

iBeCHANGE - 101136840 – D7.2 “iBeChange Platform Design Regulatory Requirements”

Funded by the European Union

This project has received funding from the European Union’s Horizon Europe research and innovation programme under the Grant Agreement Number 101136840.

Disclaimer

Version history

Version	Description	Date completed
V0.5	Initial draft for DPO and Research Team Comments, and wider Consortium Review drafted by Nathan Lea and Muna Khogali	15/11/2024
V1.0	Updates post research team and DPO reviews and comments	06/12/2024
V1.1	Final Version post Consortium Review	16/12/2024

Table of Contents

List of Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
DMP	Data Management Plan
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EEA	European Economic Area
EHDS	European Health Data Space
FAIR	Findable, Accessible, Interoperable and Reusable Principles
FRIA	Fundamental Rights Impact Assessment
GDPR	General Data Protection Regulation
HTA	Health Technology Assessment
ICF	Informed Consent Form
IG	Information Governance
IRB	Independent Review Board
JCA	Joint Controller Agreement
MDR	Medical Device Regulation
PIL	Participant Information Leaflet
PROMS	Patient Reported Outcome Measures
RCT	Randomised Control Trial
REC	Research Ethics Committee
ROPA	Record of Processing Activity
UKICO	UK Information Commissioner’s Office

1 Introduction

This Deliverable provides a basis for the broad regulatory requirements for the iBeChange Platform. It is underpinned by an Information Governance checklist that incorporates a Data Protection Impact Assessment (DPIA) for the project which is guiding the recommended regulatory conformance needs. The DPIA has been conducted since the commencement of the project to understand the proposed architectures and the data flows for the project so that regulatory conformance can start to be considered and broad requirements can be established early in the development lifecycle.

The use of a DPIA is steeped in compliance with the General Data Protection Regulation (GDPR), which requires that Data Controllers run a DPIA for high-risk processing. Whilst not in and of itself a legal entity or Data Controller, the iBeChange Consortium is composed of multiple legal entities that hold a Data Controller responsibility for any data that they are bringing to the project. "They will also likely hold Joint Controller responsibility for their involvement in the project and any data processing that occurs, as they share a common interest in the results of the processing.

To that end, they will each need to conduct their own DPIAs to cover their activities for iBeChange. Partners may, therefore, wish to reuse this project-wide DPIA to meet their obligations or use it as reference material to conduct their own activities, where they may go into more detail about their specific activities. This DPIA should, therefore, be seen as reference materials that establish a common view and understanding of the data flow and regulatory requirements for the project as a whole to ensure that partners have a common view of those requirements and risk management strategies.

The DPIA has enabled iBeChange to identify and align with regulatory requirements imposed by the following EU-wide existing and forthcoming Regulations in addition to GDPR: the Artificial Intelligence (AI) Act, the Medical Device Regulation (MDR) and the European Health Data Space (EHDS). In addition to this, the regulatory requirements need to be addressed within the requirements of local Research Ethics Committee approvals and compliance with local regulations around the conduct of research studies that the DPIA has helped to map and identify.

In its current state, the DPIA represents how the Project and development work is meeting the requirements to date and indicates what requirements will need to be met. In addition to this, iBeChange needs to be prepared to meet these regulatory requirements that are forthcoming. The Deliverable, therefore, distils specific requirements around adherence to the AI Act and wider trustworthiness expectations as outlined in the Assessment List for Trustworthy AI with additional analysis of the AI Act itself. These also provide a basis for adhering to the requirements related to the EHDS and MDR.

With this in mind, it is important to emphasise that any DPIA is a living document that needs to be routinely updated. As the project proceeds and the Platform is developed, the DPIA and any partner-specific DPIAs will be routinely updated every six months or in the event of any major change in processing. This Deliverable commences with an overview of the approach to understand the requirements sources and achieve overall regulatory compliance under Section 2, which provides an Information Governance Assessment for the project, incorporating the DPIA. Section 3 articulates the additional Platform Requirements, and Section 4 offers conclusions.

2 Information Governance Assessment Checklist: iBeChange

2.1 Introduction to IG Assessment process

Under the General Data Protection Regulation (GDPR), a Data Protection Impact Assessment (DPIA) is only required where proposed data processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)). However, Article 35(3) explicitly requires one where there is 'large-scale' processing of 'special category' (e.g. healthcare) data, and then a DPIA is required.

Another possibility is that the data being processed is already anonymised (see Recital 26), so it falls outside GDPR altogether, so no DPIA is required.

However, good project management and information governance suggest that there should be a general approach to risk assessment for any project or business enterprise – if only to determine whether a DPIA might be required.

Ideally, one should work from a simple initial Checklist (this document), which identifies possible areas of information risk and compliance requirements, to a 'discussion note' which explores any issues in more depth and may help identify the necessary mitigation methods and mechanisms to offset most if not all risks. Only if risks are unmitigated or remain 'high' would you move to a formal DPIA report.

2.2 The IG Assessment approach

There should be an overview of the proposed project or business change to explain what processing is envisaged as well as the purpose and intended outcome. The 'purpose' is important to establish the legal basis for the processing as well as ensure that any possible mitigations or countermeasures do not undermine the main rationale for the processing.

The next step is to establish what compliance requirements may apply: GDPR, contractual or other regulatory restrictions, consent requirements, or obligations to preserve the data for legal or other reasons (including the benefit of posterity, perhaps).

Once the precise range of obligations has been established, then appropriate checks can be made and recorded within the document.

The most obvious of these being GDPR compliance. There must be a 'High Risk' assessment (Appendix A) to determine whether the supervisory authority needs to be informed – generally, it is expected that it will not be necessary; if so, then a formal DPIA report will be needed. Appendix B has a broader Privacy Impact Assessment that may reveal broader issues.

Initial conclusions as to the next steps or particular countermeasures to be considered should be detailed below. These results should be seen as a basis to start addressing the requirements for meeting trustworthy AI expectations and wider regulatory requirements, as described in Section 3. These will be addressed throughout the coming 18 months of the project and serve as a basis for conducting a compliance review as part of D7.5, the iBeChange Platform Implementation Compliance Review.

2.3 Project Background/Overview

iBeChange is a multisite, multinational initiative across Europe to develop a behavioural change platform designed to improve risk management for preventing cancer and other disease through the use of multiple engagement techniques across two studies and sub-studies. This will involve the collection of multiple types of data including health, wellness, voice and geolocation data, amongst others as described in this DPIA. There will be use of mobile devices and in a sub-study consumer-grade wearable devices to monitor psychosocial and behavioural risk factors.

Two sub-studies will be conducted for the Project with wearables: the first is a feasibility and suitability study to explore the use of wearables for collecting data around key determinants for behaviour change and healthy lifestyle promotion, leveraging data being collected through smartphones. This will also include geolocation data and voice recordings to measure emotional responses. The second study will aim to test the added value of including wearables to have a more fine-graded detection of psychosocial and behavioural risk factors.

The studies will involve the recruitment of participants and will be conducted at each of the participating sites. This will include the handling of personal special category data for recruitment, data capture and, thereafter, analysis of the project to implement its goals. Each clinical partner will approach patients attending for care and invite them to participate in iBeChange as a research study over the two studies. The studies will be conducted across all clinical centres ICO, IEO and UMFCD, and will also be performed at UNIPA and POLIMI by involving a small sample of healthy people to evaluate users' acceptability, usability, and satisfaction with the overall iBeChange system.

The studies need to be approved by each recruitment site's local independent review board and/or research ethics committee approvals. The study details, including recruitment approaches, will be outlined in a protocol for each site, including inclusion and exclusion criteria. Each site will have its own requirements for the translation of the protocol, informed consent forms, and information leaflets to the local language according to local requirements. This may include the need to request explicit consent for the capture and use of geolocation data and voice recordings to assess emotional state in addition to consent to participate in the study.

It remains the responsibility of the Clinical Recruitment sites to determine whether additional, explicit consent needs to be sought for the Geolocation and Sound recordings data, or if this is not explicitly required, the studies offer the option for participants to decline consent for these data items to be collected and used. Once approved, each site will oversee the conduct of the study according to the requirements of each of the local jurisdictions. Categories of personal data will be listed according to the Protocol, ICFs and PILs.

This DPIA is being conducted to assess the risks to data protection and research ethics for the conduct of the studies and the development of the solutions. It should, therefore, be read alongside any ethically approved protocols, informed consent form templates and participant information leaflets. Please also refer to the attached Data Management Plan Deliverable 7.1, which should be used as the background material for this DPIA. Further details will be added as the project proceeds.

The outputs of this DPIA are to inform the conduct of the Project more generally and the development of materials around data processing for the ICFs and PILs. Additionally, they will inform the drafting of data-sharing agreements (likely Joint Controller Agreements) for the

Project, including any Studies and development work. The specific activities are outlined in the Record of Processing Activity provided below.

2.4 Comparison of process steps (simplified):

This allows identification of what processing is new or changed through the project:

Step	Current	Proposed
Research Participant Recruitment	None currently	Each clinical partner will approach patients attending for care and invite them to participate in iBeChange as a research study. These partners include IEO, ICO, and UMFCD. UNIPA and POLIMI will approach a small sample of healthy participants.
Research Study Conduct	None currently	Each of the sites will capture data as specified in the ROPA and, in time, the research protocol. This data will be shared with POLIMI, TU/e and EUT to conduct the analyses as defined in the technical specifications and protocol.
Analyses	None Currently	The collected data will be co-assessed with data gathered from publicly available datasets that have been identified and listed in D3.2 by SPOREDATA to help with developing training with machine learning algorithms that can help guide recommendations as provided by the platform.
Development of the iBeChange Platform	The project aims to develop the behavioural change platform and assess its impact and acceptance. There is no platform currently, and the development work is underway	The platform is developed and will be informed by the interventional studies as described. The data processed by the platform has been added to the DMP and the data gathered during the evaluations is also included.

2.5 Initial Conclusions

Concerning further countermeasures or business viability

1. iBeChange is leveraging new technologies to help understand the key determinants of behaviour change for healthier lifestyles and richer recommendations to that effect.
2. Whilst the nature of the Project and work around behaviour change is personal and sensitive, the approach to conducting this work within the bounds of traditional, ethically

approved and well-documented approaches means that the potential risk for causing distress to participants as well as their rights and freedoms is well addressed.

3. The Project does not appear to represent a high risk therefore to the participants and researchers, so it should not require any specific additional measures or report to Supervisory Authorities.
4. This determination, however, is subject to the views of each of the individual partners, and this DPIA may be used by them to conduct their own risk management and/or reports to Supervisory Authorities declaring any perceived high-risk concerns should they deem it appropriate.

2.6 Compliance Checks required:

Requirement	**Notes** [replace guide text with response]
Does the project involve processing 'personal data' of any sort?	Yes – trial participants will have their personal data recorded along with clinical data from their medical records as well as wearables and mobile devices. Additionally, psychosocial data, social demographics, activity data, and other experiential data will be collected, as outlined in the DMP. Note that data will also be collected as part of the studies using smartphones and wearables as described in the ROPA.
Does the project involve processing 'confidential data' of any sort?	Yes – aside from trial and medical record data, the other personal data from the evaluations will be held in confidence. It is not yet clear whether the data can be considered commercial in confidence, but IP is protected under the consortium agreement. Furthermore, any wearables and mobile data will be handled pursuant to the service and API licenses that impose confidentiality requirements for data subjects/
Does data need to be held for GCP compliance?	Yes – this is a trial, and Good Clinical Practice compliance is a key requirement
Does data need to be held to meet 'Open Data' requirements?	No – the utility of the data outside the project is limited, and as per the DMP, there are no plans to reshare the data for reuse. If this were to change, then the DPIA will be rerun and the DMP updated
Does data need to be held to meet the International Committee for Medical Journal Editors requirements or commitments?	Yes, as best practice for high publication standards

2.7 GDPR Compliance Checklist – where 'personal data' is processed:

Requirement	**Notes** [replace guide text with response]
a) Is processing lawful, fair, and transparent?	Yes – processing will be pursuant to an ethically approved research protocol informed consent of the participants in line with Participant Information Leaflets (PIL) and any opinions of Research Ethics Committees as part of local jurisdiction research governance regulations. Any publicly available data sets will be used in line with their agreements and stipulations, which ensure that data sharing and reuse are determined to be lawful.
b) Is the purpose (or purposes) of the processing clearly defined	Yes – this will be made clear in the PILs and Informed Consent Forms (ICF) as well as the governing protocol.
c) adequate, relevant and limited to what is necessary	Yes – this forms part of the justification for the protocols and original project proposals.
d) accurate and, where necessary, kept up-to-date	Yes – data quality checks will be in place (including a readiness plan) for each aspect of the data processing. This will be added to the DPIA in the first quarter of 2025.
e) kept and permitted identification of data subjects for no longer than is necessary	Yes – for retention as part of research governance regulations, legal obligation for research studies and for any subsequent certifications for Medical Device Regulations and AI Act compliance (where needed).
f) processed securely	Yes – the security design is underway and will form part of the contractual obligations for a Joint Controller Agreement (JCA) when it is drafted. Please see the responses from EUT around the security of the solution provided as part of the risk management assessments available on request.
2) can you demonstrate this compliance?	Yes – iBeChange will be subject to internal audits and quality assessments for compliance, which will be mandated in the JCA.
[See detailed Transparency Checklist below]	
Did the data come from publicly accessible sources?	Please refer to Deliverable 3.2, which describes the potential publicly available datasets that will assist the Project This does not apply to other data collected in the project.
Are data subjects informed before processing starts for any new purpose if incompatible with the original purpose where the controller wants to use data for a different purpose to the purpose for which they currently hold data	Yes – they will be by virtue of the ICFs and PILs and data will only be processed on their explicit consent to participate.

Requirement	**Notes** [replace guide text with response]
Does the Privacy Notice and/or PIL cover this processing?	Yes – they will when they are drafted. This is currently underway.
What patient choices are available? Are these explained?	Yes – they will be as part of the informed consent process and in the PILs and ICFs. This will include the right to withdraw from the study at any time without giving any reason and without the risk of their care being compromised. Any data collected will not be used for further analyses but archived for regulatory compliance purposes under local jurisdiction requirements.
What are legal bases under Article 6	This will depend on the jurisdiction and the local Supervisory Authority guidelines. It will either be Consent, Public Task for Public Authorities (hospitals and universities) or legitimate interest for any Private Sector partners.
What are legal bases under Article 9 (if ‘special category’ data)	Under Article 9.2(j) – Scientific Research for public interest.
Are Article 6 legitimate interests explained where relevant?	This is unlikely but any partner wishing to use LI will need to do this as part of their own DPIA.
Are details of statutory obligations for Article 6 explained where relevant.	Yes – they will be in the PIL and ICF.
Is this proposed processing compatible with the declared purposes?	Yes – as per Research Ethics Approvals and assessments for internal and any external audit.
If for research, do we meet Art 89(1) data minimisation	Yes – this will be tested by Research Ethics Committees
[See detailed table below]	
Do we support data subject rights?	Yes – this will be in line with GDPR rights as specified in the PILs as well as additional rights for participating in a research study.
There is no use of automated decision making (e.g. profiling)	No – AI will be used to make recommendations only and not make any closed-loop decisions
A28 & 29: What measures are there to ensure processors comply?	Standard terms for iBeChange Partners appointing Processors will be added to the JCA including consent from other Partners to appoint as well as a template Data Processing Agreement if Partners wish to use it.
A30: Is there an entry for this processing/data held in the register?	Each Partner will maintain a Record of Processing Activity and the Project has also developed one overall for reference. It is available on request.

Requirement	**Notes** [replace guide text with response]
A32-34: Do we ensure appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures?	The JCA will stipulate all of these, including baseline security requirements, liabilities and responsibilities that will be explicitly stated. EUT have provided core security provision details as at the risk assessment review available on request.
A37-39: Is there a DPO and have they been or will they be consulted?	All DPOs across partners have been informed of the project and will have access to this DPIA as well as be part of the JCA Negotiations.
What form of data will be transferred to a third country or international organisation	No extra EEA transfers are expected.
Are there safeguards for international transfers?	N/A
Do we meet medical confidentiality requirements?	This will be tested as part of the DPIA process and internal audits in line with the protocol specification and Research Ethics Approvals.

2.8 Data Subject Rights:

Note if supported and what process/procedure applies; if not, then describe the legal justification for not supporting this right.

To be informed: about processing, about choices, about rights, about controller	This will form part of the PILs and ICFs. These will be translated to the local language for the site and its regulatory requirements locally.
the right of access to see or receive a printed copy	This will form part of the PILs and ICFs as per site-specific procedures and regulations.
the right to rectification – to correct any material errors in the personal data	This will form part of the PILs and ICFs as per site-specific procedures and regulations.
the right to erasure – where appropriate, to ask that all personal data is erased	This will be limited to the archiving of data where erasure would breach local research governance regulations and GDPR. If a Participant withdraws from the Trial, their data will no longer be analysed but archived for research governance regulatory needs. Participants will be informed about this in the PILs and ICFs.
the right to restrict processing – to ask that some or all processing cease [see opt-out]	By withdrawal from the study – this will be made clear in PILs and ICFs.
the right to data portability – this only applies to data provided directly by individual	In line with local regulatory processes, the process will be made clear upon request, and the right will be described.

the right to object to and not to be subject to automated decision-making, including profiling	This is not part of the studies and is not applicable.
Right to object to a Data Processing Authority (typically the relevant supervisory authority of each Member State)	Supervisory Authority details will be provided for each site on the PILs.
Where consent is the legal basis, the right to withdraw consent	As specified in the PILs and ICFs where applicable.

2.9 Detailed Transparency Checklist[1]

Does privacy information provided to data subjects include:

The name and contact details of our organisation	Will be placed for each partner in the PILs
The name and contact details of our representative (if applicable)	As above.
The contact details of our data protection officer (if applicable)	As above.
The purposes of the processing	Specified in the PILs.
The lawful bases for the processing	Specified in the PILs.
The legitimate interests for the processing (if applicable)	Where applicable, specified in the PILs.
The categories of personal data obtained (if the personal data is not obtained from the individual it relates to)	Specified in the PILs.
The recipients or categories of recipients of the personal data	Specified in the PILs.
The details of transfers of the personal data to any third countries or international organisations (if applicable)	Not currently applicable.
The retention periods for the personal data.	Specified in the PILs in line with the local site regulatory specifications.
The rights available to individuals in respect of the processing	Specified in the PILs.
The right to withdraw consent (if applicable)	Specified in the PILs – including how Participants can do this.
The right to lodge a complaint with a supervisory authority	Specified in the PILs with the contact details of the local Supervisory Authority for each site.
The source of the personal data (if the personal data is not obtained from the individual it relates to)	Specified in the PILs.
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	Where required, specified in the PILs.

[1] Taken from UK Information Commissioner's Office template as an example

(if applicable, and if the personal data is collected from the individual it relates to)	
The details of the existence of automated decision-making, including profiling (if applicable)	Recommendations will be made in line with the AI Act requirements. The recommendations are based on the user profiling (done in VUM, T3.4), where his/her preferences and limitations are taken into account.
We provide individuals with privacy information at the time we collect their personal data from them – or where we obtain personal data from a source other than the individual it relates to; we provide them with privacy information within a reasonable period of obtaining the personal data and no later than one month	As part of the informed consent procedure where potential Participants will have the time to review the PILs.
if we plan to communicate with the individual, at the latest, when the first communication takes place	As part of the research participation, this will be specified on the protocol.
if we plan to disclose the data to someone else, at the latest, when the data is disclosed	A part of the PILs.
We provide the information in a way that is: ☐ concise; ☐ transparent; ☐ intelligible; ☐ easily accessible; and ☐ uses clear and plain language.	This will be checked by each site according to their own standards and regulatory specifications.
When drafting the information, we: ☐ undertake an information audit to find out what personal data we hold and what we do with it. ☐ put ourselves in the position of the people we’re collecting information about. ☐ carry out user testing to evaluate how effective our privacy information is	As above
When providing our privacy information to individuals, we use a combination of appropriate techniques, such as: ☐ a layered approach; ☐ dashboards; ☐ just-in-time notices; ☐ icons; and ☐ mobile and smart device functionalities.	This will be handled by having the PILs, potentially the templates on the iBeChange Website and websites of all the sites and partners. The platform will incorporate these aspects as well.

2.10 Security & Access Control Checklist

Controls need to be appropriate to the level of risk: identified special category data needs more protection against potential misuse than non-personal data.

Data Security classification (above Official)	o - Official-Sensitive x - Secret o - Top Secret o - Public Domain
Personal Data involved [GDPR]	Yes
Special Category of personal data involved [GDPR]	Yes
Electronic Communications (inc. cookies) [PECR]	Yes – including website
Credit Card data	No
Legal enforcement [LED2018]	No
Financial data	No – only social-economic
Intellectual Property (detail owner)	As per CA
Commercial in confidence (detail owner)	N/A
Data Location (storage or processing) (include any back-up site(s))	o - UK x - EU/EEA o - EU White-list o - USA o - Other:
Is data held in a secure data centre?	TBC – it will be dependent on supplier and technical requirements
Is this a new supplier, location, or system?	TBC by contracting parties
Is all user access subject to 2-factor authentication?	o - no control o - single factor (e.g. just password) x - 2-factor (e.g. password & fob) o - biometric [note: GDPR reqs] o - Other control:
Are there established JML procedures?	As per each partner. This will be a requirement under the JCA
Are there checks that passwords are robust and secure enough?	As per each partner. This will be a requirement under the JCA
Are all administrator & user accounts routinely monitored?	As per each partner. This will be a requirement under the JCA
Are systems protected against malware and other attacks?	This will be a requirement under the JCA

[Need some aspect of CIA/impact-likelihood assessment]

2.11 Information Asset Register Checklist

o	Are there new IAs being created?	Yes – platform and analytics as per DMP and ROPA
o	Are old IAs being retired?	No
o	Have IAOs & IACs been consulted?	Yes
o	Has IAR been updated/amended?	In progress for each site
o	Data Retention classification & period	Defined per site and partner according to local jurisdiction

o	Data retention procedure/functionality in place	As above

2.12 Appendix A – Supervisory Authority 'High Risk' Check

If the DPIA shows 'high risk' processing, which cannot be mitigated, then the DPIA should be sent to the relevant authority for review before any processing starts. Note that their review may take several weeks to process. A 'High Risk' assessment represents a 'risk to the rights and freedoms of individuals' – so it may extend beyond GDPR consideration, including Human Rights.

GDPR Article 35(3) provides three examples:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 1013; or
c) a systematic monitoring of a publicly accessible area on a large scale

As a case in point, the UK Office of the Information Commissioner (UKICO) cites the following, but a different Supervisory Authority definition can be provided if needed:

1. Systematic and extensive profiling with significant effects
2. Large-scale use of sensitive data [viz. 'special category' in GDPR terms]
3. Public monitoring

These being the same as (a)-(c) above. They further identify:

1. **New technologies**: processing involving the use of new technologies or the novel application of existing technologies (including AI).
2. **Denial of service**: Decisions about an individual's access to a product, service, opportunity or benefit that are based to any extent on automated decision-making (including profiling) or involve the processing of special category data.
3. **Large-scale profiling**: any profiling of individuals on a large scale.
4. **Biometrics**: any processing of biometric data.
5. **Genetic data**: any processing of genetic data other than that processed by an individual GP or health professional for the provision of health care directly to the data subject.
6. **Data matching**: combining, comparing or matching personal data obtained from multiple sources.
7. **Invisible processing**: processing of personal data that has not been obtained directly from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort.
8. **Tracking**: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.
9. **Targeting of children or other vulnerable individuals**: The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.

10. **Risk of physical harm**: Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

2.13 ‘High Risk’ assessment using UKICO criteria:

Criterion:	Assessment	Comments
New technologies	Low	These are being deployed within a secure, highly governed research initiative where the risks are mitigated by ensuring there is negligible life or well-being-threatening impact of the algorithms and their recommendations.
Denial of service	Negligible	
Large-scale profiling	N/A	
Biometrics	N/A	
Genetic data	N/A	
Data matching	Low	Some matching across data collected with consent.
Invisible processing	N/A	
Tracking	Low	With consent to participate and note the potential need for explicit consent to the processing of geolocation and voice recording data, where participants may need to be given the option of refusing that these data items are collected data processed as part of the study.
Targeting of children or other vulnerable individuals	N/A	

Criterion:	Assessment	Comments
Risk of physical harm	Low	Only insofar as participants may injure themselves as part of any physical activity that is recommended (for research ethics committees to consider).

[The assessment can be one of N/A (not applicable), Low, Medium, or High. The comments should explain how the assessment is justified.]

2.14 Appendix B – Broad Privacy Risk Assessment:

#	Risk Description/detail	Discussion
1.	Data accuracy and timeliness	Yes – as discussed above
2.	Differential treatment of patients/data subjects	N/A
3.	Data Accuracy and identification	Yes – as discussed above
4.	Holding/sharing/use of excessive data within iBeChange systems	No – as per protocols
5.	Data held too long within iBeChange systems	No – as per protocols
6.	Excessive range of access in terms of users to personal data (consider new users/change of access privileges)	No – privilege management will be a requirement of the JCA
7.	Potential for misuse of data, unauthorised access to systems	No – as above.
8.	New sharing of data with other organisations, including new or change of suppliers	Yes – in line with the JCA and Grant Agreement as well as Research Ethics Committee approvals.
9.	Variable and inconsistent adoption/implementation	N/A
10.	Legal compliance, particularly DP transparency requirements and support for data subject rights	As per this DPIA and internal and external audits
11.	Medical confidentiality	As above.

3 Wider Platform Regulatory Requirements

In addition to the research governance and data protection requirements assessments for regulatory compliance that have been reviewed as part of the DPIA, there is a very recent regulation that needs to be considered as part of the requirements moving forward. One example is the AI Act, which imposes specific requirements on any AI solution that is to be developed as a product. This is the case for any medical device or tool that is likely to be brought to market.

The AI Act aligns with the Medical Device Regulation and imposes similar requirements for notification to notifiable authorities and certification by competent authorities for any “High-Risk” AI system that is being developed and brought to market. Medical devices and interventional tools fall into the High-Risk category.

iBeChange is not likely to achieve any certification or reach market penetration within the project's lifetime. However, it will likely wish to take forward any developments as a product after the project as part of a wider sustainability effort. Whilst it is not a foregone conclusion that the Platform would be considered a medical device or an interventional tool, it is very likely to fall into that category.

In any event, iBeChange is handling novel approaches to behaviour change using AI to help power its interventions and interactions with participants and users. It must certainly demonstrate trustworthiness in terms of its development and platform operation. With this in mind, iBeChange has ensured that existing approaches for demonstrating trustworthiness have formed part of developing the requirements. The Project has adapted the Assessment List for Trustworthy AI (ALTAI)[2] to enhance the DPIA specifications and to develop additional requirements for Platform development.

3.1 Scoping Compliance and AI Act Roles

We have adapted the list above to articulate the specific requirements for the Platform design that need to be honoured to comply with the regulatory frameworks applicable to iBeChange. We provide explanatory notes for each case. It must also be noted that the assessment of iBeChange must consider not just the context of the Project as a series of research studies around developing an integrated, interventional behaviour change platform but also the different layers of governance that need to be applied. Specifically, some of the requirements relate to AI-driven components of the platform, some relate to the wider infrastructure design of the platform, and some relate to the processing of personal data therein (as articulated in the DPIA).

In addition to the different technical layers that need to be addressed, assessment requirements will relate back to the parties involved in the development, management and use of the system, and, notably, the impacts on the clinical teams that may use it and the affected individuals (i.e. patients and the wider public). Where needed, in our discussion of the requirements below, we specify where the requirements relate specifically to the development of and future management of the platform.

The AI Act provides a series of specific roles for those involved in the development of AI. When considering the regulatory requirements for the iBeChange Platform, we have been keen to ensure that compliance is holistic. This means that regulatory requirements around not just AI but also GDPR, research governance and other regulations are all addressed. In any event, we have framed

[2] https://altai.insight-centre.org

the following compliance requirements to try to identify the likely responsibilities of iBeChange Partners. Two key roles are directly relevant:

Providers under the AI Act are developers of AI systems or general-purpose AI Models. Providers will put AI Systems on the market and share the greatest compliance requirements and regulations under the AI Act. iBeChange developer partners would likely be Providers under the AI Act.

Deployers are institutions that use AI under their authority to commission and deploy such tools for professional and fiduciary duties (i.e. not for personal and non-professional use). There would likely be clinical sites and public service providers who would commission and deploy the iBeChange Platform.

In articulating the requirements these roles are important to how the Project will need to address their compliance processes. As a reminder, AI assessments cannot be performed in isolation from the wider requirements as outlined in the DPIA and in the forthcoming text. Understanding the AI Act does nevertheless allow for further contextualisation of responsibility and oversight. This will also help to define the ongoing DPIA updates and assessments as the project develops and the Platform is implemented. The ALTAI self-assessment questions serve as a solid basis for enhancing the requirements management for regulatory compliance, and the following section introduces the ALTAI.

3.2 The ALTAI and its role

The ALTAI provides a clear and readily useable set of requirements sources that help achieve compliance with expectations around trustworthiness in AI use and development. Developed after the European Commission-sponsored review on AI implications for Europe, the ALTAI covers the expected requirements for AI Act compliance well while also serving as a basis for handling data quality and integration requirements in line with the EHDS expectations.

The ALTAI categorises seven broad requirements for trustworthy AI. Whilst several of these are not Platform or development-specific, we include requirements that affect more the context of the proposed Platform operation if not the Platform itself. The seven requirements are:

1. Human agency and oversight
2. Technical robustness and safety
3. Privacy and data governance
4. Transparency
5. Diversity, non-discrimination and fairness
6. Environmental and societal well-being and
7. Accountability

The self-assessment questions under each of these categories have been used to articulate and define the enhanced regulatory requirements. These are aligned with the appropriate scope discussions and AI Act roles, as described in the previous section.

3.3 Requirements Focus: Human Agency and Oversight

Human Agency and Oversight reminds us to ensure we have fully understood and risk-managed the deployment of the Platform in use and that users (either clinical or patient) remain in control of the system and its recommendations. To achieve this properly, the Platform itself will need to

enact specific requirements. Still, it will remain the responsibility of the Providers and Deployers of the system to ensure that technical and organisational measures are also in place (including training, education and policy).

The Platform must, therefore, be clearly categorised and its activity determined as to whether it:

- Is a self-learning or autonomous system;
- Is overseen by a Human-in-the-Loop;
- Is overseen by a Human-on-the-Loop and/or
- Is overseen by a Human-in-Command.

All users must be reminded of the need for training and awareness on how to exercise oversight of the Platform use and its recommendations., which is currently under development as part of the studies that are being developed.

The Platform itself must provide a basis to detect and respond to address undesirable adverse effects it may have on the end-user, be they clinical or patient. The Platform must also honour the need for a 'stop button' or procedure to safely abort an operation when needed. This would likely be the ability to remove any AI processes in making recommendations should the need arise.

In addition to this, there must be a process by which the Platform allows for oversight and control measures to reflect the self-learning or autonomous nature of its AI components and any recommendations that are made, whether AI has been used to make them or not. This will allow users to fully assert control of how the Platform behaves, though this may be balanced against interference with the Platform recommendations if users simply do not agree with what is recommended.

3.4 The Fundamental Rights Impact Assessment (FRIA)

Alongside the DPIA, FRIA is a newer risk management tool provided for by the AI Act. It is designed to assess the fundamental impacts of AI tooling on rights. As with many of the requirements listed below, regardless of the AI involvement, the FRIA provides the opportunity to provide further assurance to users and the public that a particular intervention is robust in terms of its likely impacts on individuals and their outcomes.

A FRIA will reinforce the risk management processes for the Platform, and we will conduct an assessment as part of D5.4 on Regulatory Framework compliance.

Broadly, as per the AI Act, an FRIA includes a description of the Deployer's processes in which the high-risk AI system will be used in line with its intended purpose. It provides a description of the period within which each high-risk AI system is intended to be used and the frequency with which each high-risk AI system is intended to be used.

As with a DPIA and ROPA, it defines the categories of natural persons and groups likely to be affected by the Platform use in the specific context of iBeChange studies and any further deployment areas. It explores the specific risks of harm likely to have an impact on the categories of natural persons as defined and a description of the implementation of human oversight measures according to the instructions for use.

A FRIA articulates the measures to be taken in the case of the materialisation of identified risks, including the arrangements for internal governance and complaint mechanisms for Platform operation. This will be in line with the measures outlined in the research protocols.

3.5 Requirements Focus: Technical Robustness and Safety

The robustness and safe operation of the platform are spread across both its development and deployment. Part of the requirements as provided by the ALTAI and AI Act focus on the need to guard against adversarial, critical or damaging effects (e.g. to human or societal safety) in case of risks or threats such as design or technical faults, defects, outages, attacks, misuse, inappropriate or malicious use. To a degree, the DPIA and security analyses of the platforms meet these requirements, but as an additional set of requirements, the following should also be continually addressed:

- Infrastructure should be certified for cybersecurity (e.g. the certification scheme created by the Cybersecurity Act in Europe) or demonstrate compliance with specific security standards.
- Cyber Attacks exposure should be assessed, including when using AI, assessing potential forms of attack to which the Platform could be vulnerable and different types of vulnerabilities and potential entry points for attacks such as:
    - Data poisoning (i.e. manipulation of training data);
    - Model evasion (i.e. classifying the data according to the attacker's will);
    - Model inversion (i.e. infer the model parameters).
- The Platform must be protected by measures to protect the integrity, robustness and its overall security against potential attacks over its lifecycle – which is part of the ongoing DPIA assessments.
- The Platform must be penetration tested at least annually.
- The Platform Providers and Deployers must use of security measures in place and system updates to maintain the security resilience and operation of the system.

3.6 Requirements Focus: Privacy and Data Governance

Note that much of these have already been addressed by the DPIA and operation of the Platform, though they are listed here for completeness and as an indication of the evolving nature of the risk assessments under these newer regulations.

The Platform Providers and Deployers must continue to support the following measures and introduce any that have not been implemented.

Conduct a Data Protection Impact Assessment (DPIA) – underway as part of the Project oversight and as presented in section 2, but this and local DPIAs must also be initiated and adapted to the newer regulatory oversight;

Identify partner Data Protection Officers (DPO) and include them at an early stage in the development, procurement or use phase of the Platform – which is also underway, though more involvement will occur once the JCA is shared for signature;

Oversight mechanisms for data processing (including limiting access to qualified personnel, mechanisms for logging data access and making modifications) need to be provided and enhanced. This is very clear from the assessment and oversight of using audio recordings and free text narratives in terms of the data protection requirements and security, given that these are by

their nature identifiable and, therefore, should have access limited only to the research teams that need them for stress analyses.

Measures to achieve privacy by design and default (e.g. encryption, pseudonymisation, aggregation, anonymisation) are being achieved by incremental security reviews and are part of this DPIA process. This is included in the ROPA where possible, but technical =measures will need to be introduced based on the forthcoming developments.

Data minimisation, in particular, personal data (including special categories of data) - this is in part already addressed by identifying line-by-line each data item and why it is needed for the research as per the ROPA ahead of ethics committee applications, but the Platform itself should minimise what data is stored and made available during use to strictly what is necessary.

Implement services to honour the right to withdraw consent, the right to object and the right to be forgotten in the development of the Platform where appropriate. Much of this is established via the IRB / REC approvals process. The Platform itself must still be able to implement these points in line with the specifications within the DPIA on data archiving and retention and under the limitations of the right to be forgotten as defined.

Address privacy and data protection implications of its non-personal training data or other processed non-personal data – this is where data capture mechanisms and data providers need to ensure that the data they capture and provide also meets this standard and relates to the data quality and bias items that are defined below.

Align the Platform and associated services with relevant standards (e.g. ISO25000, IEEE26000) or widely adopted protocols for (daily) data management and governance, including ISO 27000 series and ISO 9000 Series.

Assess the impact on the right to privacy, the right to physical, mental and/or moral integrity and the right to data protection – these form part of the ongoing risk management as defined in the DPIA. However, the Platform must establish mechanisms that allow flagging issues related to privacy concerning the Platform and its operation. This could be a report from within the Platform or be provided as part of the current study materials as a bare (if undesirable) minimum pending further development work.

3.7 Requirements Focus: Transparency

Transparency in not only data handling but also system operation is more critical with the advent of AI and its regulation. Note that these requirements are in addition to data use transparency as addressed by the DPIA but should not be viewed as an AI-only requirement as they have implications for the overall Platform operation.

The Platform must communicate to users that they are interacting with an AI system instead of a human when this may be the case. Further, it must provide mechanisms to inform users about the purpose, criteria and limitations of the decision generated by the AI components of the Platform.

Though an overall project requirement and one aspect that must be made clear in PILs and REC approvals, the Platform must be able to communicate the benefits of the AI components to users, expected or actual.

The Platform's technical limitations and potential risks of its AI components revealed to users, such as their level of accuracy and/or error rates where applicable.

In line with Human Oversight, the Platform must provide users with appropriate training material and disclaimers on how to use the Platform adequately.

The Platform must also provide an explanation of the recommendation(s) to the users, particularly if they were AI-influenced.

The Platform should also prompt the users to articulate if they understand the recommendation(s) of the recommendations and why they were made, regardless of whether AI was involved in their presentation.

3.8 Requirements Focus: Diversity, non-discrimination and fairness

Arguably, this set of requirements is the most novel in terms of requirements under regulation. Between the ALTAI and the AI Act, Data Quality, Bias and Representation have very much some far more regulated insofar as some level of quality and bias needs to be measured and expected in training data and anything that is generated by the AI. Whilst these matters have always held importance and some degree of understanding, the extent of bias in source data is only now starting to be more fully realised.

Data quality and bias likely impose more requirements on data providers and capture mechanisms, as well as on the management of participant recruitment. The Platform design must nevertheless take these into consideration as it is developed.

In addressing bias and quality, the AI Act requires that the Platform must document and assess (Note this is a direct quote from Article 10 of the AI Act) where Article 2 states:

Training, validation, and testing of data sets shall be subject to data governance and management practices appropriate to the intended purpose of the high-risk AI system. Those practices shall concern in particular:

a) the relevant design choices;
b) data collection processes and the origin of data, and in the case of personal data, the original purpose of the data collection;
c) relevant data-preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation;
d) the formulation of assumptions, in particular with respect to the information that the data are supposed to measure and represent;
e) an assessment of the availability, quantity and suitability of the data sets that are needed;
f) examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations;
g) appropriate measures to detect, prevent and mitigate possible biases identified according to point (f);
h) the identification of relevant data gaps or shortcomings that prevent compliance with the AI Act Regulation and how those gaps and shortcomings can be addressed.

Whilst these frame AI component regulatory requirements, none of these criteria is excluded from best practices in any data handling programme. In recognising this and the design and development choices, the Platform and Data Providers:

- Must establish a strategy or a set of procedures to avoid creating or reinforcing unfair bias in the AI system, both regarding the use of input data and the algorithm design.
- Must assess the diversity and representativeness of end-users and/or subjects in the data.
- Should test for specific target groups or problematic use cases.
- Should research and use publicly available technical tools that are state-of-the-art to improve your understanding of the data, model and performance.
- Should assess and put in place processes to test and monitor for potential biases during the entire lifecycle of the Platform and its performance (e.g. biases due to possible limitations stemming from the composition of the used data sets (lack of diversity, non-representativeness).
- Must, where relevant, consider diversity and representativeness of end-users and or subjects in the data.
- Should, where possible, put in place educational and awareness initiatives to help designers and developers be more aware of the possible bias they can inject in designing and developing the Platform, especially the AI Components.
- Should provide a mechanism that allows for the flagging of issues related to bias, discrimination or poor performance of the system and its recommendations.
- Should establish clear steps and ways of communicating any identified issues on how and to whom such issues can be raised.
- Should identify the subjects that could potentially be (in)directly affected by the Platform in addition to the (end-)users and/or subjects.
- Should articulate and operate in accordance with a definition of fairness commonly used and implemented in any phase of the process of setting up the AI system.
- Should consult with the impacted communities about the correct definition of fairness, i.e. representatives of elderly persons or persons with disabilities.
- Should establish mechanisms to ensure fairness in the Platform.

3.9 Requirements Focus: Environmental and societal well-being

With regard to the considerations of environmental impact, the key factor here for Platform design is to ensure that processing needs and the use of high-performance computing are limited to what is only necessary for its operation. In developing the Platform, developers should be mindful that their design choices limit the requirement for energy expenditure and resource use.

With regard to Societal Impact, the following should be borne in mind. When interacting directly with users, the Platform and its Providers and Developers must assess whether the AI system encourages users to develop attachment and empathy towards it. This forms part of the research oversight for participants in addition to design choices.

As a reminder of Transparency, the Platform must ensure that it clearly signals, where appropriate, that its social interaction is simulated and that it has no capacities of "understanding" and "feeling" whatsoever.

As a wider issue for all Project Partners, the social impacts of the Platform need to be well understood. This may include assessments as to whether there is a risk of job loss or de-skilling of the affected workforce. The same is true for any potentially affected stakeholders outside of the Platform users, including carers and relatives. These points do not have any particular design decision implications but do have a wider assessment need in the context of the research.

3.10 Requirements Focus: Accountability

Accountability is currently being addressed as part of the GDPR and research governance regulatory requirements. These will nevertheless need to be revisited as part of design decisions and ongoing risk management approaches for the Project to address the following requirements heralded by the need for trustworthy AI.

The Platform will need to put in place measures that address the traceability of the AI system during its entire lifecycle. This will include measures to continuously assess the quality of the input data to the Platform and its overall operation.

The Platform will also need to trace back to which data and model was used for a certain recommendation(s). This relates to the need to establish measures to continuously assess the quality of the output(s) of the AI system. All of this will rely on being able to effectively and adequately log Platform operations when making recommendation(s). This requires the design of logging facilities and recording recommendations as part of the system’s operation.

4 Conclusions

This deliverable reports how iBeChange is managing existing regulatory requirements through its adherence to research governance and GDPR. It presents a project-wide DPIA that articulates compliance requirements and wider regulatory elements that will be published under Deliverable D7.4 within six months of this Deliverable. This Deliverable has also provided the requirements imposed on the Platform by newer regulations and trustworthiness expectations primarily introduced by the AI Act and consideration of the ALTAI as developed at the behest of the European Commission.

The requirements in and of themselves do not land solely on the Developer teams for the Platform as they relate to wider decisions and interactions with data providers, research participants and the goals of the research studies. It should be noted that the requirements around data quality and assessing bias, representation and fairness add significantly to the existing requirements as outlined by the DPIA. That is not to suggest that any of the other six newer requirements headings are any less critical.

By listing the key requirements, iBeChange has a basis to start implementing design choices for its platform that aim to achieve a high standard of regulatory compliance across different requirements sources. Whilst the Project is not looking to certify a product for introduction to the market within its lifetime, adherence to these requirements offers the best opportunity to allow the research to proceed and its outputs to be fully provided to the highest standard possible. It will also allow alignment with the MDR and AI Act certifications should the Project result in a potential product to bring to market as a medical device or interventional tool.

The Next steps will be to engage with the developers and data providers to ensure these requirements are fully met to the best of our ability. It will pave the way for the introduction of the JCA and additional governance requirements within six months, as well as the overall platform development by M30. The Deliverable recommends that the DPIA be continually updated with an additional Fundamental Rights Impact Assessment by M18.