Data Privacy Impact Assessment

This document records and demonstrates how the Infectious Diseases Data Observatory (IDDO) embeds data protection by design and default into its data processing. It follows the template and Data Privacy Impact Assessment (DPIA) guidance provided by the UK Information Commissioner's Office (ICO), and complies with the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

While not required to complete a DPIA as a processor, IDDO maintains this DPIA as part of its data governance framework to achieve high standards, transparency and confidence in its handling of personal data. The following points should also be taken into consideration when reading this document:

1. While IDDO is based outside the EU, it is bound to comply with the EU GDPR in situations where the controller is established in the EU. As the GDPR provides a high global data protection standard, IDDO has opted to follow GDPR requirements in all its operations to ensure that personal data is processed safely and securely.

2. As IDDO is based in the UK, it must also comply with the UK Data Protection Act 2018 ('UK DPA 2018') and the UK GDPR, including the rules on restricted transfers.

3. IDDO has completed the DPIA process and assessed its outcome in relation to its role as a Processor, and not a Controller (where it is Data Contributors to the IDDO repository who are Controllers). Full details of this relationship, including definitions, can be found in the IDDO Terms of Data Submission.

4. This DPIA process and outcome covers all data processing activity currently undertaken by the IDDO repository, and is therefore applied to every project that makes use of personal data hosted by IDDO. It is kept under review and regularly updated, alongside IDDO's assessment of the Technical and Organisational Measures taken secure information systems.

Finally, this document should be read in conjunction with the following materials, which are further referenced where appropriate in the text:

- IDDO Terms of Data Submission

- IDDO De-identification Procedure
- IDDO Data Access Guidelines
- IDDO Data Use Agreement
- IDDO Technical and Organisational Measures
- IDDO Sub-processors

Organisation details

Name of processor	Infectious Diseases Data Observatory (University of Oxford)
Title of designated individual responsible for data protection	Senior Operations and Development Manager
Name of Processor contact	Jolyon Harris

Table of Contents

1: Identifying the need for a DPIA

Included in this section

This sections broadly explains IDDO's aims, what type of processing is involved to achieve these, and summarises why IDDO has identified the need for a DPIA.

Summary points

- IDDO aims to deliver a repository infrastructure to create standardised datasets that allow researchers to address critical research gaps in a number of infectious diseases.
- IDDO processes data as instructed by Data Contributors through a legally-binding Terms of Submission.
- While not required to complete a DPIA as a processor, IDDO submits this DPIA to achieve high standards, transparency and confidence in its handling of personal data.

1.1 IDDO's aims

The Infectious Diseases Data Observatory (IDDO) aims to build a healthy future for populations most affected by infectious diseases, realised through global scientific partnerships, and achieved by accelerating the effective treatment and control of infectious diseases by strengthening research and generating evidence for policy through equitable secondary data reuse. This mission is based on three fundamental pillars:

1. **Equity:** Delivering collaborative analyses addressing research priorities identified by disease-affected communities.
2. **Science:** Bringing diverse researchers and data sources together, integrating many different types of data for secondary analysis.
3. **Repository:** Hosting data within a robust, secure framework with independent oversight from global experts.

IDDO has 15 years of experience in successfully developing data-sharing solutions that drive the benefits of research through data reuse back to disease-affected countries, founded initially as WWARN (WorldWide Antimalarial Resistance Network) in 2009. During this time, IDDO has developed a research model based on a repository infrastructure that gathers dispersed and disparate individual patient data (IPD) from scattered studies to create standardised datasets that allow researchers to address critical research gaps in a number of infectious diseases, including malaria, neglected diseases and emerging infections.

1.2 Type of processing

IDDO processes personal data only in accordance with the written instructions of the Data Contributor as Controller as contracted through the IDDO Terms of Data Submission. In summary, this includes the following:

- De-identification as documented in the IDDO De-identification Procedure.
- Curation of data through de-identification, verification, cleaning, standardisation and/or mapping to a harmonised format.
- Making a description of the volumes and types of data (called metadata) publicly available - this may include assignment of a digital object identifier (DOI) that can be posted to public inventories.
- Sharing curated data with Data Recipients for research purposes following written approval from the independent Data Access Committee, including international transfers.
- Additional review of applications to access data by Data Contributors where they have elected to do so.
- Where IDDO is involved in these research purposes as a collaborator, secondary analyses of data are in accordance with the IDDO Terms of Submission and the terms of the IDDO Data Use Agreement governing transfer of data, in line with all other Data Recipients.

1.3 DPIA need

IDDO's data protection screening exercise, conducted as a preliminary step to completing a DPIA, identified that the type of data hosted at IDDO and associated research purposes does or might include:

- New technologies (such as machine learning applications).
- Personal data not obtained directly from the individuals and where the right of those individuals to be informed would be impossible to achieve or involve disproportionate effort.
- Special category data on a large scale, including:
    - Patient data, including children and other vulnerable populations, are part of the aggregated dataset.
    - High volume data sets that include multiple data types across varied geographies, retained for long-term repository storage and reuse.

While IDDO is not obliged to complete a DPIA under data protection regulation on account of its status as a Processor, not a Controller, the outcome of this data protection screening process would require a Controller to complete a DPIA. In order to ensure robust standards, and that there is absolute transparency and confidence from IDDO's Data Contributors and other stakeholders in its approach to data protection, IDDO has chosen to document its DPIA process and outcome as a key element of its data governance framework.

2: Description of processing

Included in this section on the **nature** of the processing

- How data are collated, reused, stored and deleted
- The source of the data
- Who data are shared with
- Any processing identified as higher risk

Summary points

- Pseudonymised data are submitted to the IDDO repository under a legally-binding Terms of Data Submission via a secure upload environment.
- Data are licensed through the Terms of Data Submission for curation, secondary analysis, storage and reuse by third parties.
- IDDO's data security measures are detailed in the IDDO Technical and Organisational Measures and IDDO De-identification Procedure.

Further detail on processing activities can be found in the technical and organisational measures implemented by IDDO in accordance with Article 32 GDPR (EU General Data Protection Regulation). They are continuously improved by IDDO to ensure a level of security appropriate to risk, and in line with latest best practice.

2.1 How data are collated

Data Contributors are invited to submit pseudonymised data to the IDDO repository in accordance with the IDDO Terms of Data Submission. Data variables collected for each patient will vary by study. Because data submitted to IDDO originates from scattered clinical studies, there is no standard methodology underlying data collected across studies hosted by IDDO.

Data are submitted via a secure Contributor Data Upload Environment that logs all data contributions. Each dataset is linked to a signed IDDO Terms of Data Submission, where the legal authority is the Data Contributor Institution, and the legal entity for IDDO is the University of Oxford.

2.2 How data are reused

The IDDO Terms of Data Submission grant IDDO (University of Oxford) a limited, non-exclusive licence to use the data for the purposes of:

- Curation
- Collaborative analysis
- Storage of the data
- Sharing of the curated data with Data Recipients, including sharing that entails a transfer to third countries or international organisations.

Only curated data are shared, following a de-identification process that goes further than Pseudonymisation to reduce the risk of re-identification in accordance with best practice. This de-identification process is described in detail in the IDDO De-identification Procedure.

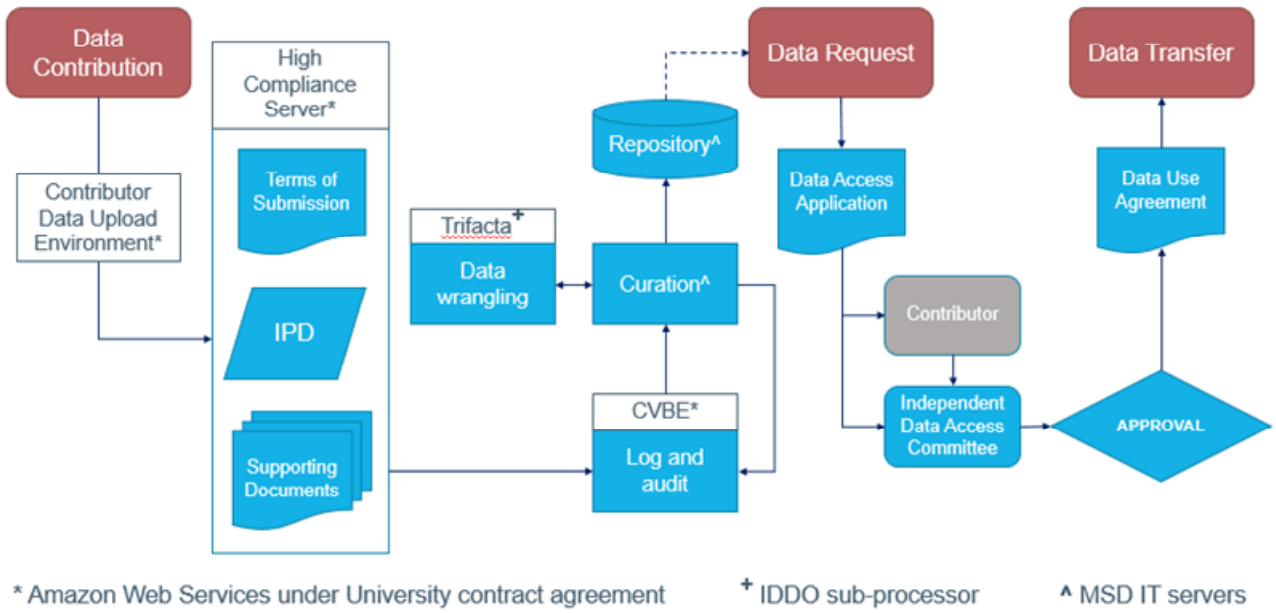
2.3 How data are stored

A complete overview of the data flow through the IDDO repository is shown at **Figure 1** below. The IDDO Technical and Organisational Measures provide detail on the security infrastructure implemented by IDDO to ensure that personal data cannot be read, copied, altered or removed by unauthorised persons during any transfer or while being stored. On initial submission, data are stored on a High Compliance Server (HCS) that is only available to a very select group of users on the Oxford network or via VPN managed by University of Oxford IT Services. Access is limited to users using a virtual desktop, thus restricting movements of files on and off the HCS.

2.4 How data are deleted

Deletion uses a command line programme that overwrites, truncates and renames file contents before unlinking from a directory, and uses 35 passes to overwrite data. Deletion is traceable to individual authorised users.

Figure 1 High-level overview of data contribution, processing and transfer at IDDO.



2.5 Source of data

Data relate to patients who have received treatment for the following infectious diseases during the course of a clinical trial or hospital admission:

- Chagas disease
- COVID-19
- Ebola virus
- Malaria
- Visceral leishmaniasis
- Schistosomiasis
- Soil-transmitted helminthiases

- Trachoma
- Anti-microbial resistance (AMR)

Data relating to other infectious diseases may be captured in time, but are not expected to impact the overall assessment of risk. With the exception of COVID-19 and AMR, the majority of data are from LMICs where these diseases are endemic, in some cases including children. Consequently, the overall data hosted by IDDO was hitherto been geographically dispersed, and IDDO's value has been derived from combining scattered small clinical studies to provide greater analytical power.

2.6 Who data are shared with

The IDDO Data Access Guidelines describe in detail the criteria by which data are able to be accessed, and by whom. Access to data is limited to Data Requestors working in a relevant field and with a formal affiliation to a health, research, humanitarian, government, inter-government or academic institution with legal status. Decisions on access are made a by an independent Data Access Committee (DAC) in response to a correctly completed Data Access Application Form and according to certain principles, where the applicant should propose to address the following aims:

- Address knowledge gaps of importance to those affected by or at risk of infectious diseases of poverty and emerging infections.
- Protect the rights and privacy of individuals and communities from whom the data originate.
- Operate in a transparent manner and promote equitable collaboration that recognises and protects the interests of those who generate the data.
- Conduct research which contributes towards improving research capacity, health and policy in regions affected by or at risk of infectious diseases.

Data will be released to those approved by the DAC after the execution of the IDDO Data Use Agreement which outlines the contractual terms of data use.

IDDO utilises risk-assessed sub-processors to support processing for the achievement of its aims, as described in the IDDO Sub-processors document.

2.7 Higher-risk processing

As outlined in the section above on DPIA need, the data protection screening process identified that the type of data hosted at IDDO and associated research purposes included some higher-risk categories according to GDPR.

The processing described in this DPIA has been determined to be exempt from ethical review by the Oxford Tropical Research Ethics Committee (OxTREC), which operates under the policies of the Central University Research Ethics Committee (CUREC) at the University of Oxford.

Included in this section on the **scope** of the processing

- The nature of the data (e.g. special category)
- How much data is collected and used
- How often data is collected
- How long data is kept
- How many individuals are included

Summary points

- Data hosted by the IDDO repository are special category health data from individual patients treated for infectious diseases.
- Data originate from a range of geographic sources representing endemic regions for these infectious diseases.
- The IDDO repository currently hosts data from around one million individual patients, retained in accordance with EU regulations.

2.8 The nature of the data (e.g. special category)

Data collated by IDDO falls into the special category pertaining to health. As identified in the Transfer Risk Assessment in the Appendix, this special category data includes the following categories of people: adults, children and vulnerable adults. The categories of personal information includes: Age, Gender, Medical records, Medication records and Location data.

2.9 How much data is collected and used

IDDO collates data from clinical studies of differing size and design, as well as observational data from hospitals and treatment centres. IDDO therefore has no control over the volume or means of data collection. As a broad principle, observational data volumes are higher due to the nature in which data were collected. Clinical studies tend to be smaller as they are based on patient recruitment for treatment concerning neglected diseases, though through the process of collation form a larger aggregate dataset. All of these factors are taken into account during the de-identification process to minimise the risk to re-identification, as detailed in the IDDO De-identification Procedure document.

2.10 How often data are collected

Data collection methodology, including timing and frequency, is under the purview of Data Contributors to IDDO as the Controllers of that data. Once data is uploaded to IDDO, it is maintained on the IDDO repository as per the IDDO Terms of Data Submission. Data Contributors are able to access their contributions via their IDDO secure account to provide updated files or supplemental documentation as required.

2.11 How long data are kept

In accordance with EU regulations on clinical trials, curated data within IDDO's secure storage environment have been authorised by the IDDO Terms of Data Submission for processing as part of a Collaborative Analysis and for storage for a

period of 25 years from the date of submission of data to the IDDO repository by the Data Contributor (subject to earlier termination). IDDO and Data Contributors may agree to extend this 25-year period if they jointly determine that there is a scientific need for such an extension.

2.12 How many individuals are included

The IDDO repository currently hosts around one million IPD. The majority of data are patients who have been treated for COVID-19, with the remainder consisting of patients treated for malaria, Ebola virus disease, visceral leishmaniasis, soil-transmitted helminthiases, schistosomiasis, Chagas disease and AMR. The repository continues to grow as new datasets are submitted, both for existing and new diseases of focus

2.13 What geography is covered

For all diseases, the data have been collected in locations where the disease is endemic. Aside from the COVID-19 global pandemic, the rest of the infectious diseases for which IDDO hosts data have mostly been produced within lower-resource settings, often through clinical trials. Endemic regions for these diseases cover Latin America, Sub-Saharan Africa, South and Southeast Asia. Driving the benefits of reuse of this data back to disease-endemic countries is a guiding principle for IDDO, and over half (52%) of researchers who have been granted access to data through IDDO are based at research institutions in these lower-resource settings.

Included in this section on the **context** of the processing

- The nature of IDDO's relationship with the data subjects
- Control of data by data subjects and their expectations
- Inclusion of children and other vulnerable groups
- Any prior concerns over this type of processing or security flaws
- The novelty of the processing and current technology in this area
- Current issues of public concern that should be considered
- IDDO association with approved codes of conduct or certification schemes

Summary points

- IDDO processes data as instructed by the Controller who holds the direct relationship with the original data subjects.
- A number of submitted clinical study data include children, accounted for in the appended Transfer Risk Assessment.
- IDDO's processes are designed to promote the benefits of data reuse for researchers in disease-endemic settings.

2.14 The nature of IDDO's relationship with the data subjects

IDDO processes data as instructed by the Controller who holds the direct relationship with the original data subjects. IDDO's priority is therefore the ethical and secure processing of this data, providing mechanisms whereby the Data Contributor as Controller is able to act in the best interests of the data subjects, including the ability to be directly involved with decisions on how the data are accessed and used. This follows representation that the Data Contributor has confirmed the following by signing the IDDO Terms of Data Submission:

- That it has obtained all necessary licences, permits and/or consents or waivers for the processing of its data by IDDO, including for the sharing of the curated data by IDDO with Data Recipients.
- The submission falls under pre-existing regulatory or ethics approvals or it has obtained any regulatory and/or ethics committee approvals, if required, to submit data to IDDO.
- The Data were collected in compliance with all Applicable Regulations and Data Protection Laws that apply to the Contributor.
- It has the right to enter into the IDDO Terms of Data Submission agreement.

2.15 Control of data by data subjects and their expectations

Control of data and expectations in relation to data subjects have been determined by the Controller who collected the data. IDDO acknowledges that it shall have no rights in or to the data other than the right to use it in accordance with the express terms of the IDDO Terms of Data Submission. Each Party may give notice to terminate that agreement at any time without cause and without liability, whereupon personal data are deleted or returned to the Data Contributor. The agreement also allows that specific IPD records be deleted on request and under the instruction of the Data Contributor.

2.16 Inclusion of children and other vulnerable groups

Due to the diseases of focus, a number of submitted clinical study data include children, accounted for in the Transfer Risk Assessment below. Relevant data variables representing more vulnerable groups include comorbidities (for example, HIV) and pregnancy status. The majority of IPD hosted by IDDO are associated with poverty in lower-resource settings and certain diseases can carry stigma in some cultural settings. Surveillance data hosted by IDDO was collected during treatment in hospitals and treatment centres, which would include adults who lacked the opportunity, or in severe cases, the capacity to provide ethical consent for themselves to share their data. This observational data has therefore been subject to an additional statistical disclosure protocol to determine and mitigate the risk of re-identification, alongside additional local ethical approvals.

2.17 Any prior concerns over this type of processing or security flaws

The responsible sharing and reuse of IPD from clinical trials is now considered a research norm in principle, if not in practice. The majority of funders supporting clinical studies, as well as the journals publishing them, and multilateral agencies such as the WHO, have published data sharing policies which seek to maximise the volume and impact of data sharing by ensuring that data are findable, accessible, interoperable and reusable: the FAIR principles. All data processing services that IDDO provides for Data Contributors through its repository contribute to these principles.

Concerns remain amongst potential data contributors, however, regarding the manner in which these principles are implemented, including:

- Ensuring that risks to data subjects are managed in compliance with relevant legal and ethical regulations.
- Equitable access to data is maintained for researchers in lower-income settings and from where data have originated.
- Mechanisms ensure that research results are impactful in disease-endemic countries and serve to improve the health of those affected populations.

2.18 The novelty of the processing and current technology in this area

The processing is not novel within the clinical research sector. Alongside data protection, IDDO prioritises investment of its resources in the curation of data, allowing for data across different studies to be combined for secondary analysis. This processing is fundamental to maximising the reuse of data for research.

IDDO curation is based on established global standards developed by CDISC (Clinical Data Interchange Standards Consortium) for drug regulators. IDDO also draws on expertise from sub-processors to improve the efficiency of curation processes and visualization of the metadata associated with the IPD (as listed in the IDDO Sub-processors document). IDDO is supported by University of Oxford IT infrastructure. IDDO is not currently operating a Secure Research Environment model for data access (a highly secure computing environment that provides remote access to health data for approved users) due to sustainability of costs,

ease of access to data from lower-income settings and adequate risk management around personal data from a combination of legal, ethical and regulatory mechanisms.

2.19 Current issues of public concern that should be considered

As researchers in low-resource settings may have limited access to the resources needed to make use of shared data for secondary analysis, there is concern that data sharing could provide greater academic benefit to higher-resourced research institutions. IDDO's activities are explicitly designed to address this inequity through training and capacity development to address resource gaps and provide direct benefit to the research communities who generate the data (outlined in Figure 2 below). Research is encouraged through collaborative Study Groups, which engage the primary data contributors and support any resource gaps, such as statistics or manuscript writing. Furthermore, a publication policy, which recognises those who generate the data, is in place to ensure appropriate recognition and increase the visibility of research undertaken in endemic countries.

As noted later, this focus on maximising reuse of data in low resource settings militates against consideration of some data security measures. Specifically, the use of Secure Research Environment model, whereby data is accessed remotely is deemed unviable owing to the costs of set up, and the challenges of making such a solution work in low resource settings where power or internet connectivity may be compromised.

2.20 IDDO association with approved codes of conduct or certification schemes

IDDO is associated with the following codes of conduct, certifications and standards:

- **Data protection:** IDDO's data governance complies with the General Data Protection Regulation (EU) 2016/679, as well as local national data protection legislation including the UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018.
- **Data curation standards:** Study Data Tabulation Model (SDTM) developed and maintained by the Clinical Data Interchange Standards Consortium (CDISC).
- **De-identification and statistical disclosure:** With reference to standards established by the European Medicines Agency (EMA Policy 0070) and the U.S. Health Insurance Portability and Accountability Act (HIPAA).
- **Repository certification:** CoreTrustSeal (pending).

Included in this section on the **purposes** of the processing

- What IDDO is seeking to achieve
- The intended effect on individuals
- The benefits of the processing

Summary points

- IDDO aims to increase reuse of quality data able to deliver meaningful research impact to guide health policies.
- IDDO has prioritised the leadership role of disease-affected communities in planning and executing research to address their own health priorities.
- Study methods and data collection have lacked standardisation, which IDDO is addressing to improve analysis of health interventions.

2.21 What IDDO is seeking to achieve

In recent years, COVID-19 has accelerated the trend of proliferation of health data repositories, while policy leaders in open science, including funders, journals and multilateral agencies, have continued to push for more data sharing and open access to research results. However, significant barriers to sharing data still persist, and simply sharing data is not an end in itself, with only increased reuse of quality data able to deliver meaningful research impact to guide policies. As outlined in Figure 2 below, IDDO addresses these challenges by collating and standardising available data, maximising the utility of existing resources to address priority questions in treatment. In doing so, it builds on a global collaborative framework to prospectively assemble future studies, guide optimal data collection and make research methods more efficient. This ensures the utility of scarce research resources, maximises the benefit received from the contributions of clinical study participants, and accelerates science to tackle the major challenge of optimising clinical treatment of poverty-related infectious diseases.

2.22 The intended effect on individuals

No direct effect is intended through processing the collated data. However, analysis of this data could lead to a better understanding of the disease and subsequent treatment. IDDO has prioritised the leadership role of disease-affected communities in planning and executing research to address their own health priorities using methodologies most appropriate for their context. Aiming to drive the benefits of data reuse back to countries of data origin, IDDO has embedded local leadership, collaboration, and credit mechanisms throughout its processes, providing end-to-end solutions for the clinical research data lifecycle. IDDO now plays a leading role in the broader movement of global and regional repositories pursuing a data sharing paradigm that prioritises equitable data reuse in partnership with disease-endemic regions for better global health.

2.23 The benefits of the processing

Currently, large volumes of data from clinical trials and public health interventions concerning poverty-related infectious diseases exist in institutional archives

around the world. IDDO's experience has shown that these scattered resources have the potential to address knowledge gaps in treatment optimisation and inform better research in the future, particularly concerning populations underserved by research, such as children, pregnant women and patients with co-morbidities (for example, malnourished children, patients co-infected with HIV). However, only summary statistics of these studies are usually available, and study methods and data collection have lacked standardisation, making analysis of efficacy and safety between therapeutic interventions or their application across different regions almost impossible.

3: Consultation process

Included in this section

- When and how views are sought
- Who is consulted
- Justification for when it is not appropriate to consult

Summary points

- Consultation and stakeholder engagement regarding reuse of individual patient data is targeted according to specific diseases.
- IDDO utilizes consultation and community engagement at a number of stages during the course of developing a platform for processing data.
- IDDO has established the consultation channels identified below to maximize benefits for communities from which data originate.

Given the nature of data hosted by IDDO, and its role as a Processor, IDDO does not have direct access to data subjects for consultation purposes. Rather, as set out below and elsewhere, IDDO has established ethical, legal and regulatory measures as components of its data governance framework to maximize benefits for communities from which data originate, and to mitigate risk, working directly with Data Contributor institutions as Controllers. It is through this ongoing interaction with those working in or with disease affected communities that we ensure the continued appropriateness of the IDDO data sharing model.

3.1 When and how views are sought

Consultation and stakeholder engagement regarding reuse of individual patient data is targeted according to the specific disease, its geographic endemic areas and the research community engaged in addressing knowledge gaps for countries of data origin. This process is outlined below.

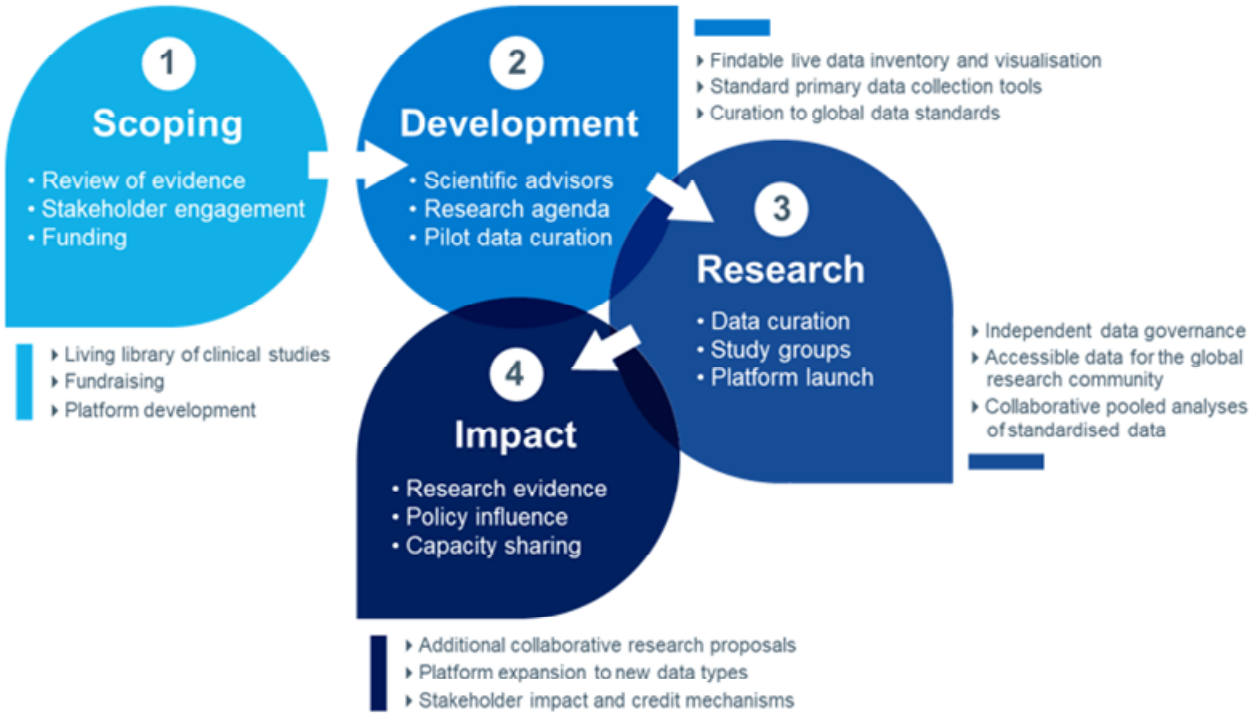


Figure 2 IDDO Roadmap for the equitable development of disease data platforms.

IDDO utilizes consultation and community engagement at a number of stages during the course of developing a platform for processing data to achieve its stated aims (outline in Figure 2 above). The following steps within that process engage in consultation with representatives from disease-endemic communities:

- **Identifying community need:** This initial Phase 1 represents a feasibility study that relies on the participation of the research community for its success. Stakeholder engagement is crucial in determining the viability of a global data platform. It is necessary to ensure community involvement and input on the challenges related to the disease area in question, including their understanding of the political landscape of the given research community. If the research community cannot identify and support the development of such a platform, then the platform will not proceed beyond Phase 1. This assessment will also be informed by the availability of sufficient study data identified through the systematic review.

- **Scientific Advisory Committee:** A critical governance addition for any new platform is the Scientific Advisory Committee (SAC), formed from representatives of the relevant disease research community, and featuring a balance of nationality, gender and research area of expertise. Members of the SAC are initially identified through the extensive stakeholder engagement process conducted during Phase 1 and, as members of the SAC, go on to advise on all technical and research activities undertaken by the platform.

- **IDDO Advisory Board:** The Chair of the SAC for each of IDDO's disease research areas is a member of the IDDO Board who governs IDDO's overall activities and strategic direction.

- **Research Agenda:** As the voice of the relevant disease research community, the SAC leads the development of a Research Agenda containing a list of priority research questions identified by the global research community that could be addressed using data from the platform. The Research Agenda is a key driver in the direction of the platform and is created collaboratively via a transparent process that includes initial development by the SAC members, review by the wider disease expert research community, followed by an open call for comment online. The Research Agenda is updated over time as required, with subsequent development guided by the platform Scientific Advisory Committee and wider research community.

- **Standard Case Report Form:** IDDO works closely with research communities to develop Case Report Form(s) (CRF), tailored for each disease. The CRF does not prescribe what data to collect, but rather provides researchers with a standardised means of recording any data they do choose to collect from a study. By supporting improved data quality at the start of the data lifecycle, CRFs support efficient, scientifically valid generation and reporting of clinical data to streamline development of new treatments, regulatory submission and post-marketing research, as well as enabling data sharing, comparison and aggregation for high-quality, novel research outputs to address knowledge gaps.

- **Data Access Committee:** IDDO's governance framework has been developed with TDR, the Special Programme for Research and Training in Tropical Diseases, hosted by WHO. TDR chairs the independent Data Access Committee, who review applications according to criteria within a Data Access Guidelines document developed by the Committee, and operate in line with their own Terms of Reference, abiding by a Conflict of Interest Policy. Membership of the Data Access Committee is from across relevant fields of global health taking into account a representative balance of skills, disease-specific expertise, geography and gender. Members are appointed through an open nominations process managed by TDR.

- **Collaborative Study Groups:** A proven model for engagement of researchers in the sharing and reuse of data is IDDO's collaborative Study Group model. Study Groups are formed to address relevant scientific questions identified by the research community through the Research Agenda development process that have not been possible to answer using data from an individual study alone. A description of the study aim is developed with a representative team of experts and a review of the literature is conducted to identify a list of existing relevant data. Corresponding authors are contacted and invited to join the group by sharing their data and contributing to the development of a statistical

analysis plan, as well as all subsequent production of results and publications. The Study Group model is built on principles of equitable data sharing and benefits from the full involvement of researchers who are best placed to understand the context of their data and its interpretation.

- **Dissemination of results:** In service of its goal to build a healthy future for populations most affected by infectious diseases, IDDO also engages with policy leaders in health and open science in order to derive policy influence from its research impact. Operating in between high-level policymakers and the individual researcher in their local context, IDDO provides an invaluable source of information and experience to facilitate improved standards, methods and equitable solutions for global health research using secondary data. In doing so, IDDO seeks to engage with targeted policy actors to support research impact, including government and industry.

- **Capacity sharing:** Since much of the data contributed to the platform comes from low-income settings, it is important to ensure that the countries that generate the data are able to analyse and use it. Therefore, additional resources are applied to capacity sharing, engaging with overseas research networks to provide training, specifically in data management, data sharing and statistics. IDDO has developed training packages to enable online and in-person training, reaching a wider group of partners globally and supporting the development of overseas platforms aligned to IDDO's mission, for shared learning and the exploration of new data types, developing stronger networks for future research collaboration. In addition, IDDO actively supports and hosts regular fellowships for researchers from disease-endemic regions to deliver their research projects utilising data on the IDDO repository.

3.2 Additional consultation

Oxford Tropical Research Ethics Committee (OxTREC): A waiver from ethical review for IDDO's processing and research using secondary analysis of data has been upheld by OxTREC since 2016. This was most recently reviewed in March 2023.

University Information Security Team: Review of IDDO Sub-processors, as listed in the IDDO Sub-processors document.

3.3 Justification for when it is not appropriate to consult

As described above, IDDO does not have direct access to data subjects for consultation purposes, given its role as processer. IDDO has established the consultation channels identified above, alongside ethical, legal and regulatory measures as components of its data governance framework to maximize benefits for communities from which data originate, and to mitigate risk, working directly with Data Contributor institutions as Controllers.

4: Assessment of necessity and proportionality

Included in this section

- The lawful basis for processing
- How the processing achieves IDDO's purpose
- Availability of alternative methods to achieve the same outcome
- How IDDO prevents its processing from evolving beyond original specifications
- How IDDO ensures data quality and data minimization
- The information IDDO gives data subjects and how it supports their rights
- Measures to ensure third-party processors comply
- How IDDO safeguards international transfers

Summary points

- Processing is necessary for the legitimate interests of the Data Contributor to address knowledge gaps in the treatment of infectious diseases.
- Reuse of data for research using secondary analysis is not possible without the processing described in this DPIA.
- IDDO incorporates the UK GDPR International Data Transfer Agreement (IDTA) to safeguard international transfers.

4.1 Lawful basis for processing

The lawful basis for processing personal data at IDDO is legitimate interests (UK GDPR Article 6.1.f), that is, the processing is necessary for the legitimate interests of the Data Contributor as Controller seeking to address knowledge gaps in the treatment of infectious diseases. In line with ICO guidance, carrying out research with appropriate safeguards in place, including all other ethical standards and regulatory requirements, means that a separate Legitimate Interests Assessment process is not required. The condition for processing special category personal data is further covered by UK GDPR Article 9.2.j where processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with UK GDPR Article 89.1.

4.2 How the processing achieves IDDO's purpose

The purposes for IDDO's processing personal data are specified in the IDDO Terms of Data Submission in compliance with the purpose limitation principle (UK GDPR Article 5.1.b). Primarily, the curation and transfer of curated data is essential in order to be able to maximise the utility of existing data to address priority questions in treatment within disease-endemic countries. Without this processing, the data would remain isolated and incompatible, and at risk of loss over time. As an example, while vulnerable populations are included in data hosted by the IDOD repository and require appropriate protection, collating rare

data like this is invaluable for identifying better health measures for these populations, who are chronically underrepresented in clinical studies.

4.3 Availability of alternative methods to achieve the same outcome

Reuse of data for research using secondary analysis is not possible without the processing described in this DPIA. If data are not standardised through a curation process, then they cannot be readily combined for meta-analysis, leaving only siloed and underpowered data from different studies scattered around the clinical research community. Data sharing without this level of processing for interoperability loses any additional value that might have been derived from such data. In the case of IDDO's purpose, the opportunity for new evidence to improve patient treatment and health policy would be lost, or would require delivery of clinical trials which, even if commercially viable, would expose participants, often in vulnerable populations, to unnecessary risks. In addition, anonymised data (as defined by GDPR) simply does not have the granularity and resolution required for scientific analysis. Thus, pseudonymised data are essential for research purposes.

4.4 How IDDO prevents its processing from evolving beyond original specifications

IDDO adheres to the terms of its data governance just like any third party institution. It has no special rights or privileged access to data for research. IDDO's remit and obligations are described in the IDDO Terms of Data Submission.

4.5 How IDDO ensures data quality and data minimisation

Steps are undertaken to ensure data quality and minimization during the following stages of the data flow, as detailed in the IDDO De-identification Procedure:

1. Upon submission of data by the investigators to IDDO's secure data platform.
2. During the data curation process.
3. During external transfer of the curated, de-identified data for research purposes.

Contributors depositing their data are asked to only share pseudonymised data (as defined by GDPR). In addition to this request, an initial check is performed to remove any direct identifiers from the submitted dataset that may have accidentally been submitted before the data enter the curation workflow. Once data enter the curation workflow, free text such as comments are examined for any identifying information and removed if found. Date of birth is removed and only age retained. Country of data collection is retained. Institution names are provided to the data recipient (but not linked to individual patient data) for the purpose of appropriate participation and attribution of Contributors. Finally, data domains within the available IDDO dataset are shared in a tailored manner according to the variables requested by the researcher. New patient keys will be generated using a random mechanism that will replace the original patient ID

before externally sharing the database. This will ensure that multiple requests from the same research group will not be able to link the databases together.

4.6 The information IDDO gives data subjects and how it supports their rights

As outlined in section 2.14 above, IDDO processes data as instructed by the Controller, the clinical researchers and their institutions who collected the data and managed consent and other ethical processes in the conduct of their studies. IDDO therefore maintains a connection to these patient communities via its relationship with the research community working with them, which includes capacity strengthening for clinical researchers in LMICs to support the responsible management and reuse of patient data. Through its efforts to comply with FAIR principles, IDDO endeavours to make study metadata openly available to identify which study data it hosts in its repository, allowing patients the opportunity to exercise their rights to the data.

4.7 Measures to ensure third-party processors comply

Third-party processors i.e. Data Recipients are required to first apply for data to the independent Data Access Committee, stating not only the proposed research, but how the research will align with IDDO's aims in relation to disease-endemic countries, as outlined in the IDDO Data Access Guidelines. If approved for access, Data Recipients receive data following signature by the institution of a legally-binding data use agreement, which complies with EU and UK GDPR.

4.8 How IDDO safeguards international transfers

The IDDO Data Use Agreement incorporates the UK GDPR International Data Transfer Agreement (IDTA). IDDO uses the approved IDTA issued under Section 119A of the UK DPA 2018. Exporters can use the IDTA as a transfer tool in order to comply with GDPR Article 46 when making restricted transfers to countries without EU GDPR adequacy. Before transferring data, the parties will complete and sign the IDTA. IDDO's International Transfer Risk Assessment is appended to this DPIA.

5: Identification and assessment of risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
RISK 1: Access to raw data prior to de-identification procedure by unauthorized persons, leading to risk of re-identification	Possible	Significant	Low
RISK 2: Access to curated data after de-identification procedure by unauthorized persons prior to transfer, leading to risk of re-identification	Remote	Significant	Low
RISK 3: Access to curated data after de-identification procedure by unauthorized persons after transfer, leading to unauthorized secondary use and/or risk of re-identification	Possible	Significant	Medium
RISK 4: Risk of non-compliance with GDPR through IDDO Sub-processors	Possible	Significant	Low
RISK 5: Risk of non-compliance with GDPR through international transfers	Remote	Significant	Low

6: Measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved** Yes/no
RISK 3	Data are hosted, accessed and analysed remotely from a central server (Secure Research Environment). While this would eliminate the risk of use or transfer of data for unapproved purposes it is deemed unfeasible to implement while maintaining equity of access to data for those in lower-resource settings, and would be disproportionately costly to implement.	Reduced	Low	No

7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Jolyon Harris Senior Operations and Development Manager, IDDO	Overall responsibility for integrating actions back into project planning, based on annual review cycle.
Residual risks approved by:	Philippe Guerin Director, IDDO	
DPO advice provided:	Kelvin Bageire, Information Governance Officer, Nuffield Department of Medicine	
Summary of DPO advice: DPIA not required for IDDO as Processor but valid as internal IDDO documentation of data governance.		
DPO advice accepted or overruled by:	Jolyon Harris	
Comments: DPO advice accepted.		
Consultation responses reviewed by:	Matthew Brack Senior Programme Manager, IDDO	
Comments: Serving as lead contact at IDDO for data governance implementation.		
This DPIA will kept under review by:	Matthew Brack Senior Programme Manager, IDDO	Annual review cycle with sign off by NDM Information Governance Officer.

APPENDIX: International Transfer Risk Assessment

Before relying on UK GDPR Article 46 for international transfers of data, a risk assessment is required as held by the Court of Justice of the EU in the Schrems II decision (CJEU - C-311/18). The ICO's Transfer Risk Assessment (TRA) tool has therefore been utilised to assess risk associated with international transfers of data. Such transfers may then be handled sufficiently via the TRA and the IDTA included in the IDDO Data Use Agreement.

ICO TRA tool

Our guidance on international transfers details the requirement to carry out transfer impact assessments (TRAs). As set out in that guidance, there are different ways to carry out a TRA in order to meet legal requirements under the UK GDPR.

This ICO TRA tool is just one method that can be used to carry out a TRA but there are others, including the approach proposed by the EDPB. It is important that you keep a record of your assessment.

- You can use this template TRA tool to record your TRA. Importantly:
- You do not have to use this template. You can record your answers to the 6 questions in other ways.
- We have designed this template for a straightforward transfer, that is one where information is going only to one importer located in one destination country. You can adapt it for more complex personal information flows.
- Before using this TRA tool you should refer to our guidance to decide if and when a TRA is required in respect of your transfer.
- You may want to seek professional data protection advice to review your assessment.

The Appendix contains additional materials which may be helpful:

- A list of UK GDPR special category data.
- A list of typical categories of personal information with an initial risk score.
- Examples of extra steps and extra protections you may consider putting in place, which may be of assistance when carrying out this risk assessment.

Question 1: What are the specific circumstances of the restricted transfer?

Q1 Q2 Q3 Q4 Q5 Q6

Action required for Question 1:

Use Table 1 to document the specific circumstances of the transfer.

How do we complete this action?

- It is important that you record the **specific circumstances of the restricted transfer** including details of the importer, details of the people who the information is about, duration of the transfers, existing protections in place for the information and the categories of personal information being transferred.
- Use Table 1 to document this.
- If you are planning to use the IDTA as your transfer mechanism, you will need much of the same information. You can cross refer to other documents, such as the IDTA.

TABLE 1: Specific circumstances of the restricted transfer

Details of the importer You may refer to other documentation here, such as the description included in the IDTA or other Article 46 transfer mechanism.	
(1) Name of importer: Who is the personal information going to?	Data Recipient signing IDDO Data Use Agreement and IDTA
(2) Destination country (or countries) of	Countries without EU GDPR adequacy decision

the personal information:	
(3) Status of the importer: See our guidance on controllers and processors for more information	☐ controller ☒ processor or sub processor ☐ joint controller
(4) Importer's organisation: What kind of organisation is the importer?	**The data importer's business or organisation is:** Please tick all that apply ☐ Commercial ☐ Public sector ☒ Not for profit ☐ Regulated in the destination country – add type of business (eg financial services, legal services, healthcare): ☒ Other relevant features - add details: Research institution ☐ Part of a multi-national group - add name of group: ☐ Large business (but not multi-national) - add details of size of group: ☐ Small business or sole trader - add details of size of business:
(5) Importer's relevant activities What will the importer be doing with the information? Think about **why** the importer is using the personal information that will be transferred. You may be able to re-use a description of the importer's activities as set out in your service	**The importer's activities or services that are relevant to the transfer are:** The Data Recipient has the right to use the Dataset solely for the purposes of the Research which shall be conducted by the Research Team as per Schedule 2 of the signed IDDO Data Use Agreement, and only for the specific purpose(s) of the transfer, as set out under clauses 2.5, and 3.2 of that agreement.

contract with the importer. For example: "The importer is supplier of software solutions. It is supplying a software package to the exporter and will host the importer's customer information on its servers in the US."	

Details of the people the information is about You may refer to other documentation here, such as the description in the IDTA or other Article 46 transfer mechanism.	
(6) Categories of people: Who is the personal information about? Think about who the personal information being transferred is about. Click in the box next to all of the categories of people who are included in the personal information being transferred. You may make appropriate amendments or add specific details to any of the categories or click "other" and add your own categories at the end.	**The personal information transferred is about the following categories of people:** Confirm if the people are either or both: ☒ adults (who are not vulnerable) ☒ children or vulnerable adults Tick all the categories that apply: Each category includes current, past and prospective people the information is about. If any of the following is a business or organisation, it includes their staff. ☐ staff including volunteers, agents, temporary and casual workers ☐ customers and clients (including their staff) ☐ suppliers (including their staff) ☐ experts and witnesses ☐ advisers, consultants and other professional experts ☒ patients ☐ students and pupils

	☐ members or supporters ☐ shareholders ☐ relatives, guardians and associates of the person the information is about ☐ complainants, correspondents and enquirers ☐ offenders and suspected offenders ☒ children and vulnerable adults ☐ other (please provide details of other categories of people the information is about):
(7) Volume How much personal information are you transferring?	For each person: the number of personal information categories (you can count these when you complete Table 2): 2 (estimated based on possible inclusion of children and vulnerable adults). For each transfer: the number of people the information is about See Schedule 1 of the signed IDDO Data Use Agreement (state if estimated or actual). Over the term of your contract or arrangement, the total number of people the information is about See Schedule 1 of the signed IDDO Data Use Agreement (state if estimated or actual).

Duration You may refer to other documentation here, such as the description in the IDTA or other Article 46 transfer mechanism.	
(8) Frequency of transfers How often will these transfers occur? Think about how often information will be transferred to, or accessed in, the destination country. Delete and complete the wording as appropriate.	How often is a transfer made: • once

(9) Duration of arrangement with importer How long can the importer receive or access the information for? You may cross-refer to a separate contractual provision here, or to a mechanism to determine the duration of the relationship (if your contract may be extended, or terminated early).	2 years

Protections for the transferred personal information You may refer to other documentation here, such as the description included in the IDTA or other Article 46 transfer mechanism.	
(10) Format of the personal information What is the format of the transferred personal information? For example, is it plain text or encrypted?	The data are de-identified and presented in .csv files. "De-identification" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject. De-identification goes further than Pseudonymisation to reduce the risk of re-identification in accordance with best practice, thus getting as close to Anonymous Information as possible.
(11) Transfer process How are you sending the personal information? For example, are you transmitting it by email, website encryption or secure file transfer protocol (SFTP)? Or does the transfer involve remote access to personal information stored in the UK?	Remote access to personal information stored in the UK.

(12) Exporter's technical and organisational measures What other technological and organisational security measures will **you** put in place to protect the personal information before transfer? Is the personal information pseudonymised?	By the exporter before transfer: See IDDO Technical and Organisational Measures
13) Importer's technical and organisational measures What other technological and organisational security measures will the **importer** have in place to protect the personal information once it has been received?	By the importer after receipt: The Data Recipient shall take all practicable steps whilst such information is in its possession or control to prevent access thereto by any person not so entitled under the signed IDDO Data Use Agreement. They will further ensure that the Dataset is used in compliance with all Applicable Regulations, including without limitation, the UK Data Protection Act 2018, the European Convention on Human Rights and Biomedicine (1997) (including its additional protocols) and international best practices, standards and guidance, in particular relevant documents published by the World Health Organization. In particular, they will implement appropriate security measures to ensure the security of the Dataset, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that Dataset. In assessing the appropriate level of security, the Recipient shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for data subjects. In particular the Recipient shall store the Dataset only on encrypted, access-limited, password-protected computers and/or servers. Any duplication of the Dataset must be fully documented such that all versions can be fully and permanently deleted on completion of the Term or earlier termination of this Agreement. The Recipient shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(14) Categories of personal information	
What type(s) of personal information are you transferring?	**Please complete the first column of Table 2 in Question 2 to record this information**

Question 2: What is the level of risk to people in the personal information you are transferring?

Q1 **Q2** Q3 Q4 Q5 Q6

Action required for Question 2:

Use Table 2 to assign a risk level to the personal information you are transferring.

How do I complete this action?

Using the information you recorded at Question 1, you must now **assign a risk level** to the personal information you are transferring.

We have set out below a description of what is a low, moderate and high harm risk, if the personal information is misused or lost.

- List in Table 2 below the categories of personal information you are transferring (you should have done this as part of Q1, Table 1 (14)). In the Appendix, there is a list of typical categories of personal information with an initial risk score (low, moderate or high harm risk). We recommend you use this as the starting point for assessing the risk level.
- UK GDPR specifies that certain types of personal information known as special category data need extra protection. There is a list of special category data in the Appendix. Special category data also includes types of information that can be used to infer any of the information on that list. For example, a photograph showing you attending a medical clinic which treats only a specific type of illness, is special category data because you can infer from that photograph that there is a high chance you have this illness.
- Consider if there are any factors that may increase or reduce that initial risk score. You can use Table 2 to keep a record of those factors. We have suggested some relevant factors, but there may be more.
- Give each category of personal information you are transferring a risk score (in the final column of Table 2). Take into account the initial risk score, any aggravating or mitigating factors identified, and the descriptions of the risk levels.

- At this stage you don't need to worry about the destination country.
- You may be able to reduce the risk score by making changes to the information you are transferring or adding in security protections before transferring it. If you wish to do so, make these changes and repeat Question 1 and 2.

Once you have completed Table 2, proceed to Decision point A to record your results.

Low harm risk	Unlikely to cause more than inconsequential financial harm, physical harm, mental harm or distress. Minimal actions required to put it right (if any), such as an apology.
Moderate harm risk	Unlikely to cause more than minor financial harm, physical harm, mental harm or distress. Some actions needed to put this right, such as proactively seeking the return of information or stopping its unauthorised spread. If this was a data breach, you may need to inform the ICO, but not the people the information is about.
High harm risk	Likely to cause significant financial harm, physical harm, mental harm or distress. Urgent action is required to put this right and minimise the harm caused. If this was a data breach, you would need to inform the ICO and the people the information is about.

TABLE 2: Personal information risk level

Note: This table is editable. Insert rows to add more categories if needed. You may add notes below the Y/N response to explain your decision.

Category of personal information **List the categories.**	**Initial risk score** **(low, moderate or high**	**Aggravating factors that tend to increase risk level**	**Mitigating factors that tend to reduce risk level**	**Other factors**	**Final risk score** - Risk of harm to the people the information is

The Appendix sets out a list of examples of categories and the ICO initial risk score.	**harm risk**	Information is confidential	Person the information is about is a child or vulnerable adult	Large volume of information about each person	You can infer special category data from this information	Information is in the public domain	**Before transfer** information is encrypted, pseudonymised or similar, and importer does not have the key		about (use key above)
Age / DOB	**Low**	Y	Y	N	N	N	Y	DOB removed	**Low harm risk**
Gender	**High**	Y	Y	N	N	N	Y		**Low harm risk**
Medical records	**High**	Y	Y	Y	Y	N	Y		**Moderate harm risk**
Medication records	**High**	Y	Y	Y	Y	N	Y		**Moderate harm risk**
Location data	**High**	Y	Y	N	N	N	Y	Minimised to country or district level	**Low harm risk**

Decision point A (select relevant option):

Based on your assessment in Table 2, the level of risk to people in the categories of personal information you are transferring is:

1. ☐ **All** the categories of personal information we are transferring are a **low harm risk**.

Next step: You may proceed with the restricted transfer. This is because no matter what the response might be to the next questions, the nature of the personal information and the circumstances of the transfer means the risk of harm to people is low. You can record this as the final decision for your TRA.

2. ☒ **All** the categories of personal information we are transferring are **low harm risk** and **moderate harm risk**. (None is **high harm risk**)

Next step: go to Question 3.

3. ☐ **All or some** of the categories of personal information we are transferring are a **high harm risk**.

Next step: go to Question 3.

Additional notes: In addition to the measures described in the IDDO Technical and Organisational Measures, data minimisation measures to mitigate risk are described in the IDDO De-identification Procedure. Further measures to protect data subjects after transfer are detailed in the IDDO Data Use Agreement signed by the Data Recipient.

Question 3: What is a reasonable and proportionate level of investigation, given the risk level in the personal information and the nature of your organisation?

Action required for Question 3:

- Use Tables 3 and 4 to decide what is a reasonable and proportionate level of investigation of the destination country.
- Carry out and record the findings of your investigation.

How do I complete this action?

To decide the level of investigation required, you must consider three factors:

- Factor 1: the risk level in the personal information you identified at Question 2 (at Decision point A).
- Factor 2: the size of your organisation and therefore the resources available to you. Use the data protection fee tiers as a guide - organisations who are required to pay a Tier 1 or Tier 2 data protection fee are considered an SME for the purpose of this question.
- Factor 3: The total volume of personal information you are transferring. Transfers are high volume if you are sending a significant amount of personal information either in one transfer or in a number of recurring transfers.

Use the investigation matrix in Table 3 to decide the level of investigation required. The 3 levels of investigation are set out in Table 4. Make a note of which level of the investigation you are going to conduct and your reasons why this is reasonable and proportionate.

Carry out your investigation. First read Questions 4 and 5 below, because you will use the results of your investigation to answer those two questions.

If some or all of the personal information is high harm risk and you do not want to carry out a level 3 investigation, then at Decision Point B select "LEVEL 3 investigation Option (ii)", and follow the instructions. It means you can carry out a level 2 investigation for your low and moderate risk data only, and that you can transfer the high harm risk data only if an exception applies (considered in Question 6).

TABLE 3: Investigation matrix

Business size	**All** the personal information we are transferring is **low harm risk**	**All** of the personal information we are transferring is **low harm risk** and a **moderate harm risk**	**All or some** of the personal information we are transferring is **high harm risk**
SME	No further investigation necessary. You may make your restricted transfer (see Decision point A).	☒ **Level 1 investigation**	☐ If you are transferring a **low** volume of personal information = **Level 2 investigation** ☐ If you are transferring a **high** volume of personal information = **Level 3 investigation**
Large business		☐ **Level 2 investigation**	☐ **Level 3 investigation**

TABLE 4: Levels of investigation

Level 1 investigation	**Level 2 investigation**	**Level 3 investigation**
Resources to use (Level 1): Consider: • your own knowledge of the destination country, including its legal system, respect for the rule of law and its human rights record; • the latest Foreign Commonwealth and Development Office Human Rights and	**Resources to use (Level 2):** **In addition to the resources in the previous column**, you should carry out further internet-based research about the destination country, using reputable websites. This may include: • additional human rights reports issued	**Resources to use (Level 3):** **Option (i):** **In addition to using the resources in the previous two columns**, you should conduct a detailed analysis about the treatment of human rights in the destination country.

Democracy Report; • the relevant Department for International Trade's Exporting country guides; and • at least one human rights report, such as those published by charitable organisations (eg Amnesty International Reports on the state of the world's human rights). You should always bear in mind what other influences may impact these reports, and therefore how much you can rely on them.	by charitable organisations; • human rights reports from other governments (eg US State Department's Country reports on human rights practices); and • newspaper reports. You should always bear in mind what other influences may impact these reports, and therefore how much you can rely on them.	You may need professional advice for this level of investigation. **Option (ii):** Mark all high harm risk data as "significant risk data", and carry out a Level 2 investigation for the rest of the information. You will not need to answer Question 5. Follow the instructions in Decision Point B.

Decision point B: Make a note of the level of the investigation you are going to carry out, and your reasons why this is reasonable and proportionate.

☒ **LEVEL 1 investigation**

☐ **LEVEL 2 investigation**

☐ **LEVEL 3 investigation Option (i)**

☐ **LEVEL 3 investigation Option (ii)** Go to Decision point E(2) and tick that all your high harm risk data is both human rights risk data and enforceability risk data.

Carry out a level 2 investigation for your low and moderate risk data. Answer Question 4 and complete Decision point C for the low and moderate risk data only.

You do not need to answer Question 5. This is because low and moderate risk data cannot be enforceability risk data.

This means you can only transfer the high harm risk data if an exception applies (considered in Question 6).
Additional notes: Additional protection measures have been outlined at Decision Point A (above). Further to these, every data transfer must be preceded by a Data Access Application that details ethics approvals for the intended research. Ethics approvals and associated scientific methodology are verified by an independent Data Access Committee, overseen by TDR, the Special Programme for Research and Training in Tropical Diseases, hosted at the World Health Organization (WHO). In this manner, each application for data receives objective assessment by qualitied third-party reviewers.

Question 4: Is the transfer significantly increasing the risk for people of a human rights breach in the destination country?

Q1 Q2 Q3 **Q4** Q5 Q6

Action required for Question 4:

- Based upon your investigation and the specific circumstances of the transfer, decide whether by making the transfer you are making the human rights risk worse for the people the information is about. This could be by making it more likely that a human rights breach will happen or by making it more severe if it did happen.
- The increase in risk must be clear and meaningful and linked to your transfer.
- Use Table 6 to record your investigation and to make your risk assessment.

How do I complete this action?

- You must consider the specific circumstances of the transfer and any other relevant factors which you can reasonably know, imply or predict. For example, do you know or is it likely that any of the people the information is about are citizens or residents of the destination country, is it reasonably possible they will travel to the destination country?
- Consider whether by making the transfer you are making the human rights risk worse for the people the information is about, by making it more likely that a human rights breach will happen or making it more severe if it did happen.
- Human rights are basic rights and freedoms for every person in the world. In the modern world they are founded on the Universal Declaration of Human Rights (adopted by the United Nations in 1948). This formed the basis of the European Convention of Human Rights (ECHR). Table 5 provides a summary of the key human rights taken from simplified ECHR.
- Use Table 6 to record the findings of your investigation and make your risk assessment

- If you have concerns that the transfer is significantly increasing the risk of a human rights breach for people, consider whether you can take any extra steps or put in place extra protections. The Appendix has examples and extra steps and protections for you to consider. If so, update your responses in in this TRA tool taking those extra steps and protections into account, and repeat this Question 4.

TABLE 5: Human rights risk analysis

Art 1: Obligation to respect human rights	This is the general principle that countries must make sure everyone has these human rights.	**Art 8: Right to respect for private and family life**	You have the right to respect for your private and family life, your home and correspondence (letters, emails, phone calls, texts etc).
Art 2: Right to life	You have the right to life. Take note whether the death penalty is available for certain crimes.	**Art 9: Freedom of thought, conscience and religion**	You have the right to freedom of thought, conscience and religion. You have the right to practise your religion at home and in public and to change your religion if you want.
Art 3: Prohibition of torture	No one has the right to hurt you or torture you, even when you are held by police or armed forces.	**Art 10: Freedom of expression**	You have the right to responsibly say and write what you think and to give and receive information from others. This includes freedom of the press.
Art 4: Prohibition of slavery and forced labour	It is prohibited to treat you as a slave or to impose forced labour on you.	**Art 11: Freedom of assembly and association**	You have the right to take part in peaceful meetings and to set up or join associations -

			including trade unions.
Art 5: Right to liberty and security	You have the right to liberty. If you are arrested you have the right to know why. If you are arrested you have the right to stand trial soon, or to be released until the trial takes place.	**Art 12: Right to marry**	You have the right to marry and to have a family.
Art 6: Right to a fair trial	You have the right to a fair trial before an unbiased and independent judge. If you are accused of a crime, you are innocent until proved guilty. You have the right to be assisted by a lawyer who has to be paid by the state if you are poor.	**Art 13: Right to an effective remedy**	If your rights are violated, you can complain about this officially to the courts or other public bodies.
Art 7: No punishment without law	You cannot be guilty of a crime if your action was not a crime at the time you did it.	**Art 14: No discrimination**	You have these rights regardless of your skin colour, sex, language, political or religious beliefs, or origins.

TABLE 6: Record of investigation and conclusions

Investigation level:	☒ 1 ☐ 2

	☐ 3
Resources used: Make a note here of resources used (see Table 4)	IDDO uses its own and knowledge and investigation of country regulations concerning both research ethics and data protection. This also draws on knowledge from key partners with local operations (e.g. Drugs for Neglected Diseases *initiative* and Médecins Sans Frontières). Furthermore, the context for data use is always considered by the independent Data Access Committee, particularly in light of the latest developments concerning the regulation of clinical research, level of adherence, and the political climate in the destination country.
Key question 1: From your investigation do you have any concerns about any human rights issue?	☒ No concerns. Go to Decision point C and tick C1. ☐ We have concerns, which are: refer to the specific Articles set out above, if you can. Go to Key question 2.
Key question 2: By making this transfer, are you making the risk significantly worse for the people the information is about? By either: • making it more likely that a human rights breach will happen to the people the information is about; or • making the human rights breach more severe if it did happen. The increase in risk must be clear and meaningful and linked to the transfer.	☐ No. Go to Decision point C and tick C2. ☐ Yes. Which categories of personal information cause the increase in risk: ☐ All categories of personal information. Go to Decision point C and tick C3 ☐ Only the following categories of personal information: (please list):

	Go to Decision point C and tick C4.

Decision point C: Read and select the most appropriate response based upon your investigation:

1. ☒ We do not have any concerns about any relevant human rights risk in the destination country for the people the information is about.

Next steps: go to Q5.

2. ☐ We have concerns that there are human rights risks in the destination country, but by making the transfer we are not significantly increasing the risk of a human rights breach in the destination country for the people the information is about.

Next steps: go to Question 5.

3. ☐ We have concerns that the transfer is significantly increasing the risk of a human rights breach in the destination country for the people the information is about, and this applies to all the categories of personal information.

Next steps: Go to Decision point E(3) below and tick "**Yes, all categories of data are human rights risk data**". If at Question 2 you selected a Level 3 Option (ii) investigation, move on to Question 6. Otherwise go to Question 5.

4. ☐ We have concerns that the restricted transfer is significantly increasing the risk of a human rights breach in the destination country for the people the information is about, and this applies only to some categories of personal information.

Next steps: Go to Decision point E(4) below, tick and list "**Yes, the following categories of data are human rights risk data**" and list them. If at Question 2 you selected a Level 3 Option (ii) investigation, move on to Question 6. Otherwise go to Question 5.

Question 5:

(a) Are you satisfied that both you and the people the information is about will be able to enforce the Article 46 transfer mechanism against the importer in the UK?

(b) If enforcement action outside the UK is needed: are you satisfied that you and the people the information is about will be able to enforce the Article 46 transfer mechanism in the destination country (or elsewhere)?

Action required for Question 5:

- Using the resources gathered as part of your investigation and taking into account the specific circumstances of the transfer, consider whether the transfer mechanism can be enforced against the importer in the UK or, if needed, in the destination country.
- Use Table 7 to record your risk assessment.

How do I complete this action?

- To answer question 5 we suggest that you work through the questions in the Table 7 Enforcement questionnaire
- If you have concerns about the enforceability of the transfer mechanism, consider whether you can take any extra steps or put in place extra protections. The Appendix has examples of extra steps and protections for you to consider. If so, update your responses in in this TRA tool taking those extra steps and protections into account, and repeat this Question 5.

TABLE 7: Enforcement questionnaire

<table>
<tr><th>Enforcement risk – Key questions</th><th>Answer</th><th>Notes</th></tr>
<tr><td>1. Are you transferring only personal information that gives rise to a low harm risk or a moderate harm risk (see Question 2)?</td><td>☒ Yes. Go to Decision point D and tick D(1)
☐ No, go to next question</td><td></td></tr>
<tr><td>2. In your investigation into the destination country, have you found any records suggesting there are issues about respect for the rule of law, independence of the Courts and Judges, and the time it takes for cases to be heard?</td><td>☐ No concerns. Go to Decision point D and tick D(2).
☐ Yes (or not sure). Add notes and go to next question.</td><td></td></tr>
<tr><td>3. Is there a high likelihood that the importer will accept the decision of a UK Court or arbitration award? Factors to consider here:
(a) The importer has insurance from a reputable insurance provider that covers payment of claims in a UK Court or a UK arbitration award, without requiring any action to be brought in the destination country. The insurance must be enough to cover all of the potential claims. If this applies, you must check this insurance cover each year.
(b) The importer has provided evidence that in the past it has always accepted decisions of UK Courts or UK arbitration awards.
(c) The importer must comply with professional or similar rules, and you would be able to make a complaint to its oversight body, which would impact its ability to do business.</td><td>first tick if any of the factors apply<table><tr><th>Factor</th><th>Satisfied</th><th>Not satisfied</th></tr><tr><td>(a)</td><td>☐</td><td>☐</td></tr><tr><td>(b)</td><td>☐</td><td>☐</td></tr><tr><td>(c)</td><td>☐</td><td>☐</td></tr><tr><td>(d)</td><td>☐</td><td>☐</td></tr></table>Taking these factors into account answer Question 3. If you are satisfied about one or more of the above factors, it is likely you may answer Yes.
☐ Yes. There a high likelihood that the</td><td></td></tr>
</table>

Enforcement risk – Key questions	Answer	Notes
(d) There are strong commercial reasons for the importer to accept a decision of UK Court or UK arbitration award, even where the claim is substantial.	importer will accept the decision of a UK Court or UK arbitration award. Add notes and go to Decision point D and tick D(3). ☐ No. There is not a high likelihood that the importer will accept the decision of a UK Court or arbitration award. Add notes and go to next question.	
4. Are there any other factors that make it very unlikely you or the people the information is about would have to bring a claim in the destination country to enforce the Article 46 transfer mechanism?	☐ Yes. Set out the factors in the Notes, and go to Decision point D and tick D(4). ☐ No. Go to Decision point D and tick D(5).	

Decision point D: Read and select the most appropriate response based on your investigation
1. ☒ We are only sending information that poses a low harm risk or a moderate harm risk. As a result, there is a low likelihood that we and the people the information is about would need to enforce the transfer mechanism in the destination country.
2. ☐ We do not have any concerns about respect for the rule of law, independence of the Courts and Judges, and the time it takes for cases to be heard in the destination country.
3. ☐ There is a high likelihood that the importer would accept the decision of a UK Court or UK arbitration award (considering the factors set out in Table 7 above).

4. ☐ It is very unlikely that we or the people the information is about would have to bring a claim in the destination country to enforce the Article 46 transfer mechanism (considering the factors set out in Table 7 above).

5. ☐ We have concerns that (a) both we and the people the information is about may not be able to enforce the Article 46 transfer mechanism against the importer in the UK; and (b) if enforcement action is needed outside of the UK, we and the people the information is about may not be able to enforce the transfer mechanism in the destination country.

Go to Decision point E(5) and tick that "**All high risk data is enforceability risk data**"

Decision point E: Have you identified any **human rights risk data** at Question 4 or **enforceability risk data** Question 5?

If you are carrying out a Level 3 Option (ii) investigation, then you **must** tick E(2) and you **may** need to tick either 2 or 3 depending on your answers to Question 4.

1. ☒ **No**, we have not identified any because we have ticked:

- A(1);
- Or:
  - one of C(1) or C(2); **and**
  - one of D(1) or D(2) or D(3) or D(4).

You may proceed with the transfer.

2. ☐ **Yes,** all **high risk data** is both human rights risk data and enforceability risk data, because we ticked B(3) Option (ii).

(Optional) list all the categories of high risk data:

3. ☐ **Yes, all categories of data are human rights risk data**, because we ticked C(3).

(Optional) List all categories of data:

4. ☐ **Yes, the following categories of data are human rights risk data**, because we ticked C(4): List the categories of data which, by including in the restricted transfer, you have concerns will significantly increase the risk of a human rights breach in the destination country for the people the information is about:
5. All high risk data is enforceability risk data, because we ticked D(5) (Optional) list all the categories of high risk data:
The human rights risk data and enforceability risk data identified above is your "significant risk data" for Question 6

Question 6: Do any of the exceptions to the restricted transfer rules apply to the significant risk data you have identified?

Q1 Q2 Q3 Q4 Q5 **Q6**

Action required for Question 6:

- Your significant risk data is identified in Decision point E.
- Using our guidance on the exceptions to the international transfer rules, and taking into account the specific circumstances of the transfer, and the type of risk you identified at Decision point E, decide if any of the exceptions apply to the significant risk data.
- You are considering if one of the exceptions applies only for the significant risk data, and on the basis that the Article 46 transfer mechanism provides some (but not all) of the appropriate safeguards and effective and enforceable people's rights.
- You can only rely on these exceptions in very limited circumstances, if it is necessary and proportionate to do so.
- Use Table 8 to record your assessment.

How do I complete this action?

This question assumes you are putting in place the Article 46 transfer mechanism and all the extra step and protections you identified in working through this TRA tool.

To answer question 6 we suggest that you work through the questions in the Table 8 Exceptions checklist.

When thinking about whether the risks are outweighed by the benefits of the transfer, it may help to think about whether it is a human rights risk or an enforceability risk or both (as you identified in Decision point E).

If the exceptions do not apply to **all** the significant risk data, consider if you can take out of your restricted transfer the significant risk data that is not covered by an exception. If so, repeat the TRA tool removing that data.

TABLE 8: Exceptions checklist

Exception	Does the scenario apply?	Which types of significant risk data does the scenario apply to? (You can state **all** if the exception scenario could apply to all the significant risk data.)	Does the benefit of the transfer for this exception, outweigh all the risk(s) you identified in Decision point E	Your reasons
• The person has given their explicit consent to the restricted transfer of the significant risk data.	☐		Not required for this exception	
• The transfer of the significant risk data is necessary for the performance of a contract between you and the person the information is about. Or it is necessary so you can implement pre-contractual measures requested by that person.	☐		☐ Yes ☐ No	
• The transfer of the significant risk data is necessary for you to either perform or enter into a contract with a person, and that contract is in the interests of a separate person	☐		☐ Yes ☐ No	

(who the information is about)				
• The transfer of the significant risk data is necessary for important reasons of public interest.	☐		☐ Yes ☐ No	
• The transfer of the significant risk data is necessary for you or another person or organisation, to establish whether you or a third party has a legal claim or defence, to make a legal claim or to defend a legal claim.	☐		☐ Yes ☐ No	
• The transfer of the significant risk data is necessary to protect the vital interests of a person – this may or may not be the person the information is about. To use this exception the person the information is about must be physically or legally incapable of giving consent to the transfer of their information.	☐		☐ Yes ☐ No	
• The transfer of the significant risk data is from a public register and meets the relevant legal	☐		☐ Yes ☐ No	

requirements about access to that public register.				
• The restricted transfer of the significant risk data is necessary for your compelling legitimate interests. You must read our guidance about the extra requirements for this exception.	☐		☐ Yes ☐ No	

Decision point F: Read and select the most appropriate response based on your analysis:

1. ☐ One or more of the exceptions applies to all the significant risk data. You may proceed with the transfer.

2. ☐ The exceptions do not apply to all the significant risk data. You may **not** proceed with the transfer relying on the Article 46 transfer mechanism.

If you are concerned whether you have reached the right conclusion, you may always seek professional data protection advice to review your assessment.

Additional notes:

include any other information that may be relevant to your analysis, including if you have decided to rely on an exception for certain categories of information, and remove other categories from the scope of the transfer.

Appendix to TRA tool

This Appendix sets out information which may be helpful to you when filling out your TRA Tool. It does not form part of your TRA Tool. You may delete this Appendix from your TRA Tool.

1. List of Special Category Data

Personal information revealing:

- Racial or ethnic origin
- Political opinions
- Religious of philosophical beliefs
- Trade union membership

Processing of genetic data or biometric data for the purpose of uniquely identifying a natural person

Personal information concerning:

- A person's health
- A person's sex life or sexual orientation

Read our guidance on special category data.

2. Categories of Personal Information

Please find below the relevant initial risk scores to apply when listing the different categories of personal information in Table 2 of the TRA tool.

Category of Personal Information	Initial risk score (indicative ICO score)

Name	**Low**
Address & Contact details	**Low**
Age / DOB	**Low**
Gender	**High**
Biometric data	**High**
CCTV, photos and other images (which are not biometric data)	**Moderate**
Race/ethnic origin	**High**
ID documentation, such as passport, national insurance number, ID card, driving licence details	**High**
Medical records	**High**
Medication records	**High**

Name and contact details of GP	**Low**
Name and contact details of specialist medical professionals	**High**
Genetic data	**High**
Current marriage and partnerships	**Moderate**
Marital history	**Moderate**
Details of family and other household members	**Moderate**
Habits	**Low**
Housing	**Low**
Travel details	**Low**
Leisure activities	**Low**
Location Data	**High**

Membership of charitable or voluntary organisations	**Low**
Political opinions	**High**
Religious or philosophical beliefs	**High**
Trade Union membership	**High**
Sex life or sexual orientation	**High**
Free text about an individual, eg in emails, social media, livechat (must assume is SCD)	**High** (may vary depending on circumstances)
Employment and career history	**Low**
Recruitment	**Low**
Termination details	**High**
Attendance records	**Low**

Health and safety records	**High**
Performance appraisals	**Moderate**
Training records	**Low**
Security records	**Low**
Financial account / credit card details	**High**
Income	**Moderate**
Salary	**Moderate**
Assets and investments	**Moderate**
Payments	**Moderate**
Creditworthiness / Credit score	**Moderate**
Loans	**Moderate**

Benefits	**Moderate**
Grants	**Moderate**
Insurance details	**Moderate**
Pension details	**Moderate**
Goods or services supplied	**Low**
Marketing preferences	**Low**
Delivery preferences	**Low**
Licences issues	**Low**
Insurance details	**Low**
Records of unspent criminal convictions and offences	**High**
Records of spent criminal convictions and offences	**High**

Records of DBS checks	**High**
Criminal investigations records	**High**

3. Extra Steps and Protections

Questions 4 and 5 of the TRA tool ask you to consider whether you can take any extra steps and extra protections that will reduce the risks in relation to the restricted transfer.

There are a range of extra steps and protections that you can use, covering additional technical, organisational or contractual protections. Of course these extra steps and protections are over and above the protections which you already have in place, which you will have included in Question 1.

The table below is a **non-exhaustive example list** of measures that you may apply to seek to reduce the risks to the people the information is about, established by your investigation into the destination country. The table references different levels of risk reduction (basic, enhanced, significant) to help you form an overall view of the likely effectiveness of the measures.

To make sure the measures you use are legally binding, you may need to amend the Article 46 transfer mechanism. The effectiveness of these measures in reducing the risk to the person who the information is about will vary depending on the circumstances of the restricted transfer.

Extra Steps and Protections (examples only)

Category	Purpose	Basic Protection	Enhanced Protection	Significant Protection

Category	Purpose	Basic Protection	Enhanced Protection	Significant Protection
Access controls	Either minimises likelihood of a breach of the Art 46 transfer mechanism occurring or reduces risk of harm to the person who the information is about if a breach of the Art 46 transfer mechanism occurs	You will password protect personal information prior to transfer to importer. You will provide the password separately where the importer is to process the personal information beyond storing it.	You will encrypt the personal information prior to transfer using an appropriate encryption solution (i.e. storage encryption / encryption at-rest) and you will implement suitable key management procedures.	You will encrypt the personal information prior to transfer using appropriate encryption solution, you will split the encrypted datasets between multiple parties and you will take measures to ensure the decryption code is retained only by you.
Changes to the personal information	Either minimises likelihood of a breach of the Art 46 transfer mechanism occurring or reduces risk of harm to the person who the information is about if a breach of Art 46 transfer mechanism occurs	You review the purposes and scope of the transfer and further minimise the amount of personal information you transfer (ie only certain data categories), but it is not anonymised or pseudonymised	You minimise the amount of personal information you transfer, apply pseudonymisation techniques to the personal information prior to transfer and the importer does not have access to the additional information.	You only transfer minimal pseudonymised datasets and split them between multiple entities, so that there is a minimal risk that any one party could identify a person. Note: You should also consider anonymisation techniques. If the personal information is effectively anonymised in the hands of a receiver so that it is no longer personal information, the UK GDPR transfer

Category	Purpose	Basic Protection	Enhanced Protection	Significant Protection
				restrictions (and the UK GDPR generally) will not apply to that anonymised information.
Organisational	Reduces risk concerning (i) third party access to personal information outside of legal process in the destination country; and (ii) human rights breach for the person who the information is about in the destination country	Both you and the importer offer regular staff training to raise awareness of data protection and security issues.	The importer does extra internal checks within its organisation to make sure personal information is not being shared with third parties or public authorities, outside of the legal process in the destination country, and the organisation's internal processes. The importer strictly enforces password protocols.	The importer strictly limits access to personal information to certain individuals with role-based access profiles. Where third parties or those without access privileges require access to personal information , they must follow a strict protocol before any personal information is shared more widely. Importer has a strict policy where it receives requests or legal orders for third-party access to personal information.

Category	Purpose	Basic Protection	Enhanced Protection	Significant Protection
Contractual	Additional contractual clauses in transfer mechanism to reduce risk of (i) exporter or the person who the information is about from being unable to enforce contractual rights; and (ii) third party access to personal information outside of legal process in destination country	Importer and/or exporter has an enhanced complaints process for people whose personal information has been subject to a data breach, including a compensation scheme.	If exporter has sufficient financial resources: contractual right for people to bring a claim against the exporter if the importer fails to comply with UK court order or arbitration award. The importer may only comply with a request by a third party or public authority (i) where the legitimate interests of the importer, the requesting party and any other third party override the interests or fundamental freedoms of the person who the information is about ; or (ii) if the request was made in the UK, the disclosure would be lawful and/or in the overriding public interest.	If exporter has sufficient financial resources: contractual right for people to bring a claim against the exporter for any breach of the Article 46 transfer mechanism by importer. Or a contractual right for people to bring a claim against a UK organisation in the same group as the importer (with sufficient financial resources) for breach by the importer. Confirmation and commitment by importer to maintain: • Professional or regulatory status • ICO code of conduct • ICO certification • Reputable security certification If the importer receives a request from a third party

Category	Purpose	Basic Protection	Enhanced Protection	Significant Protection
				or public authority for access to personal information it must: • notify the exporter of the request, order or warrant and provide a copy of it; • ask the law enforcement agency or public authority to redirect its request to the exporter to control conduct of the disclosure; • if applicable, give the exporter the opportunity to withdraw or suspend the transfer; and • challenge the validity of the request, order or warrant and demand that the public authority aims to obtain such information via co-operation with government bodies in each jurisdiction (ie use an alternative

Category	Purpose	Basic Protection	Enhanced Protection	Significant Protection
				established treaty or mechanism to allow government-government sharing of obtain information). • Importer must report monthly to the exporter if it receives no requests, orders or warrants relating to the exported personal information.