every person counts

Data Protection Impact Assessment

CHIEDZA Study

November 2018

Simprints Technology Ltd
Bradfield Centre
Unit 184 Cambridge Science Park
Cambridge CB4 0GA

Data Protection Impact Assessment

CHIEDZA Study

APPROACH

This Data Protection Impact Assessment (DPIA) was conducted by Simprints Technology Limited (Simprints) for its data processing activities as an impact partner of the London School of Hygiene and Tropical Medicine (LSHTM) and the Biomedical Research and Training Institute (BRTI) for the community based interventions to improve HIV outcomes in youth: a cluster-randomised trial in Zimbabwe (CHIEDZA) study in Zimbabwe. This DPIA only covers the data processing activities of Simprints, an independent data controller, and any data processors acting on behalf of Simprints. It does not extend to any data controllers in common nor to any data processors acting on behalf of other data controllers in common.

The methodology used to conduct this DPIA is based on the guidance contained in Article 35, Recital 75, and Recital 90 of the EU's General Data Protection Regulation (GDPR)[1]; the *WP29 Guidelines on DPIA*[2]; the UK Information Commissioner's Office (ICO) website[3]; the DPC's *Draft list of types of Data Processing Operations which require a DPIA*[4]; and CNIL's *Privacy Impact Assessment Methodology*[5]. This DPIA also draws upon risk assessment concepts from the CNIL's *Methodology for Privacy Risk Management*[6], ISO/IEC 27001 standards on Information Security Management Systems[7], ISO 31000 standards on Risk Management[8], and NIST's *Risk Management Guide for Information Technology Systems*[9].

External privacy experts, human rights lawyers, and data security specialists were also consulted in the development of Simprints' DPIA template. All risk mitigation measures have been reviewed and approved by Simprints' acting Data Protection Officer (DPO), Sebastian Manhart, who will also review and reassess this DPIA on a regular basis.

[1] https://gdpr-info.eu/
[2] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
[3] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/
[4] https://www.dataprotection.ie/docimages/documents/DPIA%20DPC.pdf
[5] https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf
[6] https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf
[7] https://www.iso.org/isoiec-27001-information-security.html
[8] https://www.iso.org/iso-31000-risk-management.html
[9] https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01

CONTEXT

Simprints conducts a DPIA for each of its projects due to the scope of its data processing activities. As a UK-based company, Simprints' data processing activities must adhere to the GDPR and is regulated by the ICO. The GDPR in relation to Simprints' processing of biometric, and therefore sensitive, data is especially interesting for a number of reasons. First, it has extraterritorial reach, meaning it applies to EU-registered companies (like us) that process personal data of individuals who are outside the EU (all our project participants), irrespective of whether or not those data enter the EU. Second, it is already seen as the gold standard beyond the EU, with countries such as Japan looking to adopt similar legislation. Third, it is strongly enforceable as it is backed by a strong UK ICO and similar regulatory bodies across Europe. Finally, it is the most advanced and ambitious regulation of its kind and a huge victory for privacy.

The GDPR classifies biometric data as 'special category data' when it is processed 'for the purpose of uniquely identifying a natural person' (Article 9)[10]. As a nonprofit technology company whose mission is to build technology that helps solve global development challenges, Simprints has developed a biometric solution for the 1.1 billion people around the world who lack formal identification and the even greater number of people who lack functional identities for accessing essential services. Accordingly, Simprints processes special category data in all of its projects to help its impact partners deliver and evaluate programmes more effectively and transparently.

Data Governance and Accountability Overview

Data Controller	**Organisation:** Simprints Technology Limited **Location**: United Kingdom
Project Overview	**Name of project**: CHIEDZA Study **Location**: Zimbabwe **Impact partners**: LSHTM, BRTI **Project period**: 1 November 2018 - 31 October 2021
Stakeholders	**Data processor:** Google (USA/Global) **Data controller in common:** LSHTM
Data Overview	**Types of data** (A) Special category: biometric templates (B) Personal, pseudonymised: Globally Unique Identifiers (GUIDs) (C) Personal, non-pseudonymised: geolocation **Data volume**: 54,000 youth clients / survey participants **Data subjects**: youth aged 16 to 24 years **Data retention**: Up to 2 years after the project end date
Data Flows	**Supporting technologies**: Vero fingerprint scanner, Samsung A6 10.1 tablets, Simprints ID, Google Cloud Platform, Google Firebase **Third parties with data access**: Google, LSHTM **International transfers**: USA, Google's global data centers[11], Zimbabwe

[10] https://gdpr-info.eu/art-9-gdpr/
[11] https://www.google.com/about/datacenters/inside/locations/index.html

Purpose and Description of Processing Activities

Biometric (fingerprint) data is collected and processed to enrol and accurately identify participants in projects and programmes. For the CHIEDZA study, Simprints will be used in two ways: to monitor participation of clients in an enhanced HIV and SRH intervention program and to collect data from survey participants during an endline community prevalence survey. Simprints' biometric identification solution adds value by:

- offering greater accuracy than other forms of identification, such as easy-to-lose ID cards or a manual search of clients' names, which can be misspelled or misentered;
- enabling our impact partners to limit the amount of identifying information that needs to be collected from clients, thereby enabling anonymity of clients and ensuring greater protection of their HIV status; and
- facilitating the linking of datasets across time, programs, and communities for ease of monitoring and data analysis. Simprints will conduct an analysis at the end of the project to provide LSHTM/BRTI with coverage and contamination metrics.

Health care providers will register and identify clients using fingerprint identification during routine care throughout a two-year intervention period. At endline, research assistants will conduct a community prevalence survey that measures HIV viral load and assesses SRH knowledge, risks, and behaviors. Since biometric data is classified as 'special category data' under the GDPR, Simprints must have a lawful basis under both Article 6 (consent) and a condition under Article 9 (explicit consent) for its processing activities.

Biometric data is collected from clients and survey participants by a health care provider or research assistant using a tablet, a fingerprint scanner, and Simprints ID. Simprints ID collects only biometric data – in the form of pseudonymised ISO/IEC 19749-2 fingerprint templates[12] – in support of the principle of data minimisation. All other personal data collected for the project, such as names and dates of birth, are collected in the SurveyCTO app and processed by SurveyCTO on behalf of LSHTM.

For each set of biometric templates collected from a data subject, a GUID is generated by the Simprints ID mobile application and passed to SurveyCTO. The GUID is used to link the biometric templates stored in Simprints ID with the personal data stored on SurveyCTO. GUIDs are considered personal, pseudonymised data and are processed by Simprints under the 'legitimate interests' lawful basis. Specifically, **Simprints generates and processes GUIDs so that biometric data and non-pseudonymised personal data can be siloed in separate databases. This is a deliberate security feature designed to prevent biometric data from being easily and directly used to identify individuals.** It also ensures that a breach of LSHTM's database would not expose the biometric data and reduces the likelihood that data will be misused or shared inappropriately.

Enrolment and identification of participants with biometric data can be done completely offline on the tablet. However, to enable matching of biometric templates across multiple health care providers using different tablets, biometric data and GUIDs are also synced to Simprints' cloud platform.

Simprints also collects GPS coordinates to help improve its services. We use consent as our lawful basis for processing geolocation data.

Please see Annex A for data flow diagrams.

[12] https://www.iso.org/standard/50864.html

INHERENT RISK ASSESSMENT

Broadly speaking, there are four threats related to data processing activities[13,14]:

1. Illegitimate access,
2. Unwanted modification,
3. Accidental loss, and
4. Unlawful destruction.

These threats, if they occur, present a risk of harm to the clients / survey participants. A risk assessment considers both the ***severity*** and ***likelihood*** of any risks.

Risk Severity

A DPIA is required for any data processing activities that are 'likely to result in a high risk to the rights and freedoms of natural persons', including the 'processing on a large scale of special categories of data' (GDPR Article 35)[15]. To provide more concrete guidance, the Article 29 Data Protection Working Party outlined nine data processing criteria that are likely to constitute 'high risk'[2]:

1. Evaluation or scoring,
2. Automated-decision making with legal or similar significant effect,
3. Systematic monitoring,
4. **Sensitive data or data of a highly personal nature,**
5. **Data processed on a large scale**,
6. Matching or combining datasets,
7. **Data concerning vulnerable data subjects**,
8. Innovative use or applying new technological or organisational solutions, and
9. Prevention of data subject from exercising a right.

Simprints' data processing activities with respect to the CHIEDZA study meet three of these 'high risk' criteria: sensitive data or data of a highly personal nature, data processed on a large scale, and data concerning vulnerable data subjects.

- **Sensitive data**: Because biometric data is unique to each individual and immutable, it is classified as 'highly personal' and sensitive data.
- **Large-scale processing**: Simprints is expected to process biometric data of up to 54,000 people for this project.
- **Vulnerable data subjects:** Privacy and data protection laws are largely absent or inadequate in Simprints' countries of operation. Furthermore, public awareness of privacy rights and data protection responsibilities is generally low. Although Simprints strives to raise awareness about individual privacy rights among the clients / survey participants, we recognise that there may remain a power imbalance between the data subjects and our organisation as a data controller.

Based on these criteria, Simprints' processing of biometric data may result in high risk to the clients / survey participants. Illegitimate access poses a high risk because imposters could misuse the data to identify youth with HIV, which could lead to stigma and discrimination in the community. Likewise, modification, loss, or destruction of the data could prevent the clients from accessing HIV and SRH services to which they are entitled.

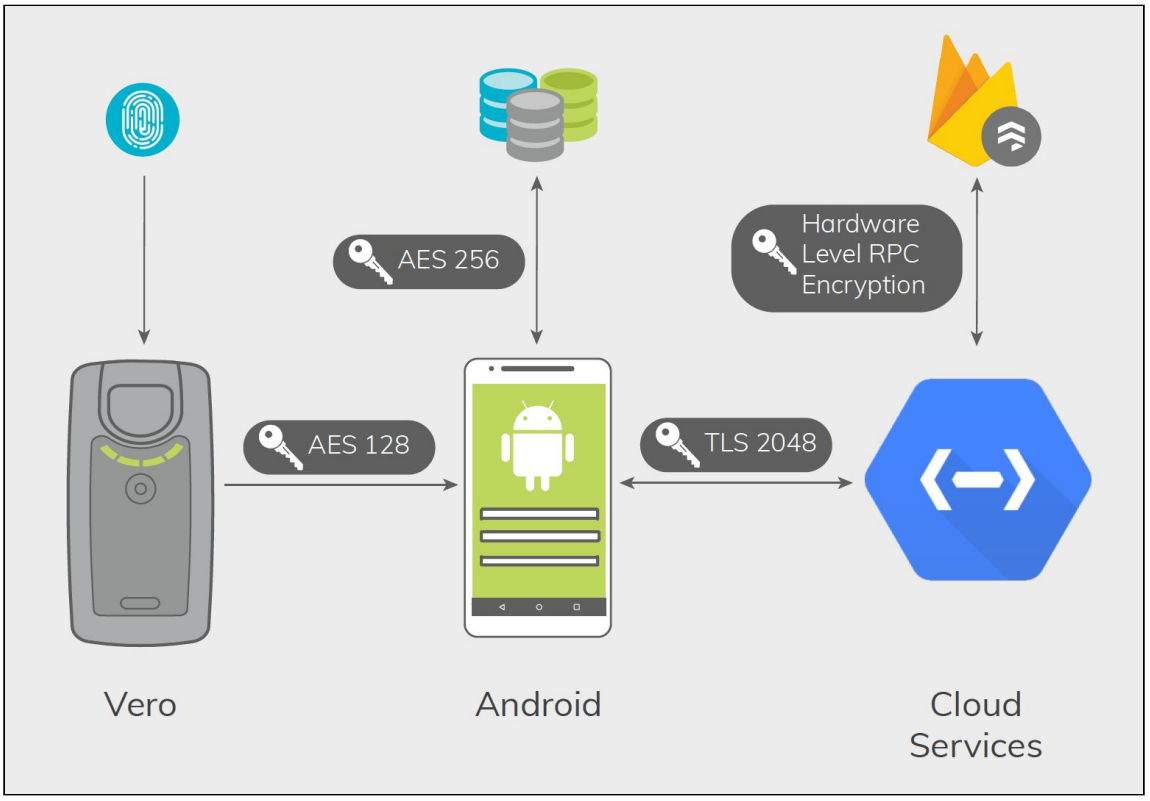
[13] https://www.cnil.fr/sites/default/files/atoms/files/171019_fiche_risque_en_cmjk.pdf
[14] https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing/at_download/fullReport
[15] https://gdpr-info.eu/art-35-gdpr/

Simprints' processing of GUIDs is also considered high risk because they can be used to link biometric templates to personal data stored in a separate database. The processing of GPS coordinates is considered low risk as there is limited risk of harm to participants if geolocation data were inappropriately accessed, modified, loss, or destroyed. The community prevalence survey samples youth between the ages of 18 to 24 regardless of their HIV status, so discovery of an individual's participation would not reveal their status.

Likelihood of Risk

While the potential impact of a threat is high, there is a **low likelihood of risk** with Simprints' data processing activities.

Firstly, all data are encrypted during processing operations, including collection, transfer, and storage. We ensure the security of all processing using 128-bit encryption between the scanner and the tablet, and SSL/TLS encryption between the tablet and the cloud platform we use, Google Cloud Platform. The fingerprint is stored in an AES 256 database while it is on the tablet, and we use Google's Attestation framework to validate that devices are secure (not rooted) before allowing data storage.



Simprints' API endpoint, which receives information from the partner data collection app, validates the security of the device and Simprints ID using Google's new Safetynet services. This means that only Simprints ID can access our endpoint to validate an API Key, and that rooted or compromised devices will not be able to sign in. With Simprints' robust security measures in place, the likelihood of a threat (illegitimate access, unwanted modification, accidental loss, or unlawful destruction) occurring is low.

Moreover, even if a ***threat*** were to occur, the likelihood of ***risk*** – i.e. harm to the clients / survey participants – remains low. Biometric data, which are the only sensitive, 'highly personal' data processed by Simprints, are pseudonymised to prevent direct identification of individuals if accessed illegitimately. Pseudonymisation is the process of transforming personally identifiable information 'in such a way that

the data can no longer be attributed to a specific data subject without the use of additional information' (GDPR Article 3). In our case, Simprints converts fingerprint images into secure ISO templates (which cannot be reverse engineered into the original fingerprint images) then immediately discards the images. Fingerprint images are never saved, and templates alone are strings of numbers which pose limited risk of misuse. Modification, loss, or destruction of biometric templates could temporarily prevent access to services or systems, but they can be rectified or replaced due to the immutable quality of fingerprints.

GUIDs are also pseudonymised and have no value on their own if accessed illegitimately. The only potential misuse of GUIDs is the linking of biometric templates to individual identities. However, because Simprints does not collect, store, or otherwise process data that can be used to directly identify an individual, GUIDs can only be used to link biometric templates to individual identities if the separate SurveyCTO database containing GUIDs and personal data is hacked at the same time. The likelihood of a bad actor being able to get past both Simprints' and SurveyCTO's data security systems is low. Furthermore, an isolated breach of SurveyCTO's cyber defenses would not expose any Simprints-acquired biometric data.

Modification, loss, or destruction of GUIDs could prevent the Simprints and SurveyCTO databases from 'talking' to one another and temporarily affect the clients' access to services or systems. However, new GUIDs could be generated and used to re-link the two databases.

Overall Risk

Overall, the low likelihood of risk and the high severity of risk involved in Simprints' data processing activities result in an overall **inherent risk** rating of 'medium'. Simprints takes many risk mitigation measures to ensure GDPR compliance and minimise the **residual risk** of its data processing activities.

COMPLIANCE AND RISK MITIGATION MEASURES

Simprints takes privacy and data protection extremely seriously[16,17]. We've adopted a 'privacy by design and default' approach to product development and systems engineering and employ best-practice standards in data security. The compliance and risk mitigation measures adopted by Simprints follow the GDPR's principles of data processing (Article 5)[18], provision of individual rights (Chapter 8)[19], and guidance on international transfers of data (Chapter 5)[20]. Since Simprints uses explicit consent as its lawful basis for processing biometric and geolocation data, we also adhere to the GDPR's very high standards for consent.

Principles of Data Processing

The GPDR specifies 7 principles of data processing, which are paraphrased below, along with a brief description of Simprints' efforts to uphold each principle in practice.

1. **Lawfulness, fairness, and transparency**. Simprints has identified appropriate lawful bases for processing of personal data, specifically explicit consent for biometric and geolocation data and legitimate interests for GUIDs. We are honest about the data we collect and we handle people's data fairly. We also make comprehensive privacy notices available to ensure that youth participants are properly informed and provided LSHTM/BRTI with community sensitisation materials that explain individual privacy rights, including the right to withhold or withdraw consent.
2. **Purpose limitation**. We have a clear purpose for processing data and it is documented in this DPIA and in our project-specific privacy notices.
3. **Data minimisation**. We collect only biometric templates – not images – from our data subjects, which is the minimum amount needed to enrol and identify them as participants in the project. We generate GUIDs specifically for the purpose of data minimisation, so that no other personally identifiable data need to be processed by Simprints. Geolocation data is collected to help Simprints improve its services. No other personal data is processed by Simprints.
4. **Accuracy**. Simprints' fingerprint scanner and software were designed specifically for 'last mile' contexts and were found to be 228% more accurate using open-source matchers than other comparable systems on people with worn, scarred, or damaged fingerprints. The types of data processed by Simprints (fingerprint templates, GUIDs, and GPS coordinates) allow little to no room for human error.
5. **Storage limitation**. Simprints has a standard policy of retaining data for a maximum of two years after a project's end date. We inform recipients of this at the time of data collection and also have procedures in place for honouring individual requests for erasure before the retention period has passed.
6. **Integrity and confidentiality**. We take a 'privacy by design and default' approach as described above. All our data are encrypted and sensitive data are pseudonymised. Simprints abides by the 'principle of least privilege' and restricts biometric data access to only a few software engineers and to the Chief Technology Officer, who authorises access on an as-needed basis. Access to the data is controlled on the project level with the OAuth 2.0 security standard. In the unlikely event that a single project's security credentials are compromised, this does not compromise other project data or access rights.

[16] https://www.simprints.com/wp-content/uploads/2018/04/Simprints-Privacy-Promise.pdf
[17] https://www.simprints.com/wp-content/uploads/2018/04/The-Case-For-Better-Privacy-Standards-April-2017.pdf
[18] https://gdpr-info.eu/art-5-gdpr/
[19] https://gdpr-info.eu/chapter-3/
[20] https://gdpr-info.eu/chapter-5/

7. **Accountability**. Simprints documents its data processing activities with internal data audit and data inventory tools. We are in the process of recruiting a DPO who will be registered with the ICO and responsible for routinely ensuring all technical and organisational measures are appropriate and well-documented.

Individual Rights

Implicit in the GDPR is the idea that ownership of personal data remains with the data subject (e.g. the client or survey participant), even if they're processed or 'controlled' by a data controller (e.g. Simprints). Accordingly, the GDPR describes 8 individual privacy rights that Simprints complies with and advocates wherever relevant and technically feasible.

1. **Right to be informed**. Simprints provides participants with information about the purpose, nature, and scope of processing at the time of data collection. We use a layered approach to avoid being burdensome, providing only essential information in a short consent text and more comprehensive information in a detailed privacy notice. We worked with LSHTM/BRTI to translate the information into Shona and Ndebele, the local languages, to ensure it is clear, concise, and easy to understand.
2. **Right of access**. We believe that pseudonymised biometric data, geolocation data, and GUIDs have no functional value to the clients as they are simply strings of letters and numbers. Instead, the rights to object and to erasure would be more relevant in our project contexts. Therefore, we have not yet established a mechanism for the clients to exercise their right to access the data we process. We will revisit this decision if we receive any requests from clients to access their data.
3. **Right to rectification**. Geolocation data and GUIDs are not eligible for rectification. Biometric data can be re-collected from a client if requested and linked to the original GUID to replace or 'rectify' the original set of biometric templates.
4. **Right to erasure**. Simprints will honour any requests for data erasure within a month of receiving the request. We can delete data directly from our databases and will inform other stakeholders who have access to the data of the erasure request.
5. **Right to restrict processing**. The right to restrict processing does not apply in all circumstances, and we do not foresee any circumstances in which a client would exercise their right to restrict processing instead of their rights to object and to erasure. Therefore, we have not established a mechanism for clients to exercise their right to restrict processing.
6. **Right to data portability**. Simprints stores biometric data in an internationally- recognised ISO/IEC standard format in order to promote interoperability with other systems. If we receive a verified request from the data owner to transfer the data to another stakeholder, we will share the biometric data in a structured, commonly used and machine readable format (JSON). The right to data portability is limited to data collected from clients and therefore does not extend to GUIDs or geolocation data.
7. **Right to object**. We rely on explicit consent for the processing of biometric and geolocation data. At the time of data collection, we inform clients / survey participants of their right to withhold consent, their right to withdraw consent if they change their mind, and their right to erasure. We require our impact partners to offer an alternative form of enrolment and identification to ensure that clients are not denied access to services if they withhold consent or object to Simprints processing their personal data.
8. **Rights related to automated decision making, including profiling**. Simprints' data processing activities do not involve decision making that is based ***solely*** on automated processing. While Simprints ID uses a matching algorithm to identify individuals by their fingerprints, the decision of whether or not to grant access to services is ultimately made by the health care provider.

International Transfers of Data

Some of our partners, service providers, and technology vendors may pass information outside of the EEA into jurisdictions where privacy laws, obligations, and rights may vary. For such transfers, we ensure that appropriate assurance checks and measures are put in place to protect individuals' privacy. We maintain records of where all personal data is and how it is protected. These provisions exceed the regulatory requirements in all of the countries we work in, where often standards are nascent or non-existent.

Simprints uploads data to Google Firebase, which hosts data in the United States, and Google Cloud Platform, which hosts data in many locations around the world[21], including Europe, North America, South America, and Asia. Google Firebase and Google Cloud Platform have been certified[22] as compliant with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework for transfer of data to the United States, and more generally, the EU has recognised the U.S. as providing adequate protection[23]. For its international data transfers to the rest of the world, Google Cloud Platform has agreements and safeguards in place as a data processor of Simprints:

> 'European Union Data Protection Authorities have confirmed that Google Cloud's EU Model Contract Clauses fully meet the requirements to legally frame transfers of data from the EU to the rest of the world, in accordance with EU Data Protection Directive 95/46/EC...In practice, this compliance finding enables our customers in most EU countries to rely on Google Cloud EU Model Contract Clauses for the international transfer of data without further authorizations, and simplifies the processing of national authorizations in other countries, where required.[24]'

Simprints also shares GUIDs with LSHTM, who may transfer, store, or access the data in Zimbabwe. The transfer of data to the United States is covered by the EU's adoption of an adequacy decision[25], i.e. that the United States offers an adequate level of protection. Simprints includes the model EU contract clauses in its partner contracts, which are standard contractual clauses that have been approved by the GDPR for the transfer of data to data controllers established outside of the EU/EEA. The transfer of data to Zimbabwe is covered by these clauses.

Consent

The GDPR defines **valid consent** as 'freely given, specific, informed, and...[indicated by] clear, affirmative action' (Article 4)[26]. Simprints has made every effort to ensure that its consent process meets the high standards set by the GDPR. The CHIEDZA team has secured a waiver of parental consent from the appropriate regulatory body in Zimbabwe for youth clients / survey participants under 18 years of age. We use a layered approach to avoid overburdening the clients / survey participants and worked with LSHTM/BRTI to translate the consent text and privacy notice into Shona and Ndebele.

At the time of data collection, the health care provider or research assistant reads a short consent text which includes the following information:

- Type of personal data being collected (i.e. fingerprint and geolocation data)
- Purpose of processing

[21] https://www.google.com/about/datacenters/inside/locations/index.html
[22] https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI
[23] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
[24] https://services.google.com/fh/files/misc/google_cloud_data_transfer_wp.pdf
[25] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
[26] https://gdpr-info.eu/art-4-gdpr/

- Who will have access to the data
- Right to object and right to erasure
- Prompt to opt-in

If the client / survey participant has additional questions, the health care provider or research assistant will then read the comprehensive privacy notice. In addition to the information contained in the short consent text, the privacy notice also provides the following information:

- Explanation of the fingerprinting procedure
- GUID generation, storage, and sharing
- International transfer of data and data protection mechanisms
- Data retention period
- Promise that data will not be shared with the government
- Right to withhold consent
- Alternative method of enrolment/identification
- Process for requesting erasure of data
- Simprints' contact information

It is important to note that we do 'bundle' certain terms of consent, which may call into question the 'freely given' aspect of consent. Specifically, we ask clients / survey participants to consent to both Simprints and our partner having access to GUIDs and biometric data, rather than choosing which data controller (if not both) may have access to the data. This decision was made because data that is restricted only to Simprints would invalidate the purpose of data processing; without the sharing of GUIDs with LSHTM, the biometric templates would not be able to be matched to individuals. Likewise, it would be impossible to facilitate data access for our partners if Simprints were not granted access to the data ourselves.

In all other respects, Simprints takes great care to ensure that consent is 'freely given', even going so far as to turn down any projects that might deny access to services for refusing or withdrawing consent. Early in the project planning process, we worked with LSHTM to ensure that the clients are able to use an alternative form of enrolment and identification (an ID number) to participate in the project activities.

Summary

The GDPR is arguably the broadest and most rigorous data protection law in the world. At Simprints, we are proud to demonstrate how GDPR can be applied by the biometrics and international development industries to advance privacy for people around the world.

The GDPR compliance and risk mitigation measures we've taken reduce the inherent risk severity from high to medium. The likelihood of risk was originally low and remains low. Therefore, the overall residual risk is low to medium. We describe Simprints' ongoing initiatives to further mitigate residual risks in the next section.

RESIDUAL RISKS AND RECOMMENDATIONS

The GDPR applies to organisations operating within the EU as well as to global organisations that offer goods and services to people in the EU. Its guidance is intentionally broad as it must be appropriate for all sectors that collect personal data, from small businesses to multinational corporations. As a result, many of the GDPR's components are vaguely-defined and subject to interpretation.

As a UK-based nonprofit social enterprise that works predominantly in developing countries, Simprints does not the fit the typical profile of the types of companies that the GDPR was designed for. Some of the GDPR's standards are difficult and, at times, impractical to apply to Simprints' project contexts. Yet, we regularly go above and beyond the privacy practices established in the biometrics and international development industries, taking great care to emphasise privacy and data protection with our partners and project participants.[27] We insist on being data controllers to enable the siloing of biometric data from other personally identifiable data in an effort to safeguard the clients' / survey participants' identities. Nonetheless, there remain some residual risks to Simprints' data processing activities with regard to the CHIEDZA study, which are outlined below along with recommended actions and priority status.

A priority status of 'high' indicates that Simprints' is actively taking steps to implement the recommended action within a quarter. A priority status of 'medium' indicates that Simprints is planning to implement the recommended action within one or two quarters. A priority status of 'low' indicates that Simprints is considering implementing the recommended action and may build it into activities in future quarters.

Residual Risk	Recommended Action	Priority
We do not inform the clients / survey participants of their **right to access data** or have a mechanism in place to provide data access.	None. As explained in the **Individual Rights** section above, we believe this is low risk in our project contexts and accept this risk. We will reconsider this if we receive a request for data access.	N/A
We ask the clients / survey participants to consent to both Simprints and LSHTM having access to the data, which is considered 'bundled' consent and may call into question whether consent is 'freely given.'	None. As explained in the **Consent** section above, it is not feasible to grant only one data controller in common access to the data.	N/A
We do not collect the clients' / survey participants' contact information and would not be able to inform them directly in case of a personal data breach.	None. In case of a personal data breach, we would work with our partners to inform the clients / survey participants of the breach. We intentionally collect only biometric data and no other personally identifiable information in an effort to protect individual privacy. We think the benefits of this outweigh the risks.	N/A
Under the layered approach, the **privacy notice** is made available to clients / survey participants,	Display the privacy notice more prominently, e.g. on a poster or given as handouts.	Low – We provide tailored community sensitisation materials to our partners,

27 https://www.simprints.com/wp-content/uploads/2018/06/Small-Company-Big-Ethics-Privacy-Law-Business-June-2018.pdf

but it is only provided upon request.		which emphasise privacy and consent.
Simprints' has not yet appointed a full-time, independent **DPO**.	Recruit a full-time DPO (this is already in progress).	Medium – We have an acting DPO (the COO) that is trained in privacy, but there may be a conflict of interest.
We are in compliance with GDPR requirements but wish to go further in **promoting privacy** in our project contexts and in the Tech4Dev space.	Establish an Integrity Council (consisting of experts in privacy, data security, law, ethics, and/or research) to advise Simprints on all matters of privacy and ethics.	Low - This is not mandated by the GDPR. It is a step above and beyond the requirements.

AUTHORISATION

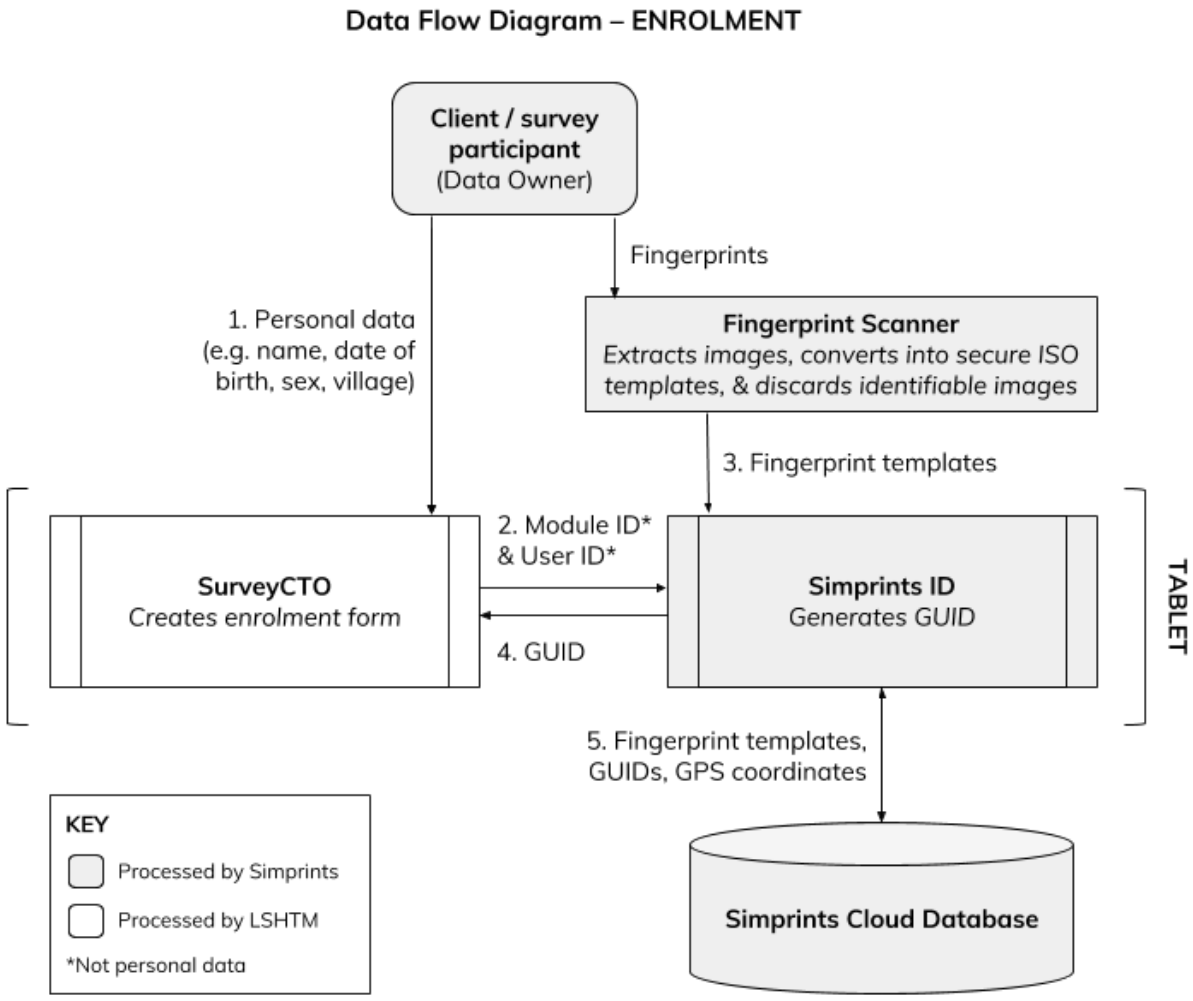
The measures in this DPIA and the residual risks have been approved by:

03.12.2018

Sebastian Manhart
Chief Operating Officer & Acting DPO
Simprints Technology Ltd.

Date

Annex A. Data Flow Diagrams



Data Flow Diagram – IDENTIFICATION