GHANA

Cross-Border Sharing of Data

This section reviews the rules as required by data protection law in the cross-border sharing of personal data. The rules on the cross-border sharing of personal data under data protection law do not exist in a vacuum, and therefore other important information that must be followed when sharing personal data is discussed. This information, however, is comprehensive as it relates to the cross-border sharing of personal data.

The relevant national health research regulations as they relate to the cross-border sharing of personal data are reviewed. These national health research regulations set out the required legal and ethical conditions that must be met when processing personal data for research. Applicable national legal and ethical documents are listed, but the discussion only specifies the requirements as they relate to the cross-border sharing of personal data for research. The guide does not treat the legal and ethical requirements generally required for research, and therefore users of this guide must consult with these documents to ascertain these requirements and to ensure that they are met.

An overview of the data protection law is provided. This includes what data the law applies to, the categories of data, the key individuals in the DPA, the key principles required to be met in the processing of personal data, and the rights of data subjects. This is an overview only to help users to understand *some* of the requirements of the DPA and to begin to assist users in navigating the DPA. It is not comprehensive, and users of the DPA must consult it to understand all relevant and applicable requirements to be met, and to understand any exceptions that may be in place for research. This is necessary as all these requirements must be met in the processing of personal data for research, in addition to the requirements on cross-border sharing of data.

The section provides users with a comprehensive description of the requirements to be met in the cross-border sharing of personal data for research. It sets out all the necessary conditions that must be met to legally share data across borders for research.

In countries where no data protection law is in force, the necessary national legal and ethical requirements, as they relate to the cross-border sharing of data, are presented.

The cross-border sharing of data is governed by several legal and ethical regulations, all of which must be met prior to the sharing of data for research. The Data Protection Act is in force. It is a general data protection law that applies to the processing (i.e., use) of personal data in all sectors. Therefore, it is not a regulation that was introduced to regulate research. However, as research

processes vast quantities of personal data, the Data Protection Act applies. It is only one of several laws that must be met when transferring data for research.

Health Research Regulations and Cross-Border Data Sharing

In addition to this national law, several international treaties and conventions have been signed. Of importance in this domain are the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) and the Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS ('the ECOWAS Data Protection Act'). Ghana has ratified the Malabo Convention.

The relevant national legislation and guidelines are the:

- Council for Scientific and Industrial Research (CSIR) Act
- Public Health Act
- Standard Operating Procedures of CSIR Institutional Review Board

These set out the legal and ethical requirements that must be met for the conduct of research in Ghana. They set no additional requirements to be met in the cross-border flow of data for research.

Data Protection Act

In addition to these legal and ethical requirements, the Data Protection Act applies to the processing of all personal data, but because of the importance of research, special provisions are in place for research. The conditions must all be met for research. In addition, extra conditions must be met prior to the transfer of personal data across borders.

Some of the techno-legal terms used in this Act are discussed below. This is not a thorough assessment of the Data Protection Act as it applies to research, but rather an overview of some of the key terms and conditions that must be met in the processing of personal data for research.

The Main Actors Defined in the Data Protection Act

	Legal definition	Layman explanation
Data subject	An individual who is the subject of personal data.	The person to whom the data relates.
Data controller	A person who either alone, jointly with other persons or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed.	The person who decides what the data will be used for in research. Legal responsibility falls on the PI *and* on the research institution (as employer).
Data processor	In relation to personal data, any person other than an employee of the data controller who processes the data on behalf of the data controller.	Someone who is not directly employed by the data controller but who processes personal data under the direction of the data controller. The person may be a consultant, for example.
Data Protection Commission	The Commission established under the Act.	The independent body established to monitor and enforce compliance with the law.
Data supervisor	A professional appointed by a data controller in accordance with the Act to monitor the compliance by the data controller in accordance with the provisions of the Act.	An individual in an organisation who is appointed to advise and promote compliance with the law.
Foreign data subject	Data subject information regulated by laws of a foreign jurisdiction that is sent into Ghana from a foreign jurisdiction wholly for processing purposes.	

Health professional	A registered medical practitioner or a recognised traditional healer or any person who is registered to provide health services under any law for the time it is in force.	
Recipient	A person to whom data is disclosed including an employee or agent of the data controller or the data processor to whom data is disclosed while processing the data for the data controller. However, it does not include a person to whom disclosure is made with respect to a particular inquiry pursuant to an enactment.	
Third party	In relation to personal data, a person other than (a) the data subject, (b) the data controller, or (c) any data processor or other person authorised to process data for the data controller or data processor.	

Categories of Data Listed in the Data Protection Act

	Legal definition	Layman explanation
Personal data	Data about an individual who can be identified: (a) from the data, or (b) from the data or other information in the possession of, or likely to come	Data about a particular person that can identify him or her.

	into the possession of, the data controller.	
Special personal data	Personal data which consists of information that relates to (a) the race, colour, ethnic or tribal origin of the data subject; (b) the political opinion of the data subject; (c) the religious beliefs or other beliefs of a similar nature of the data subject; (d) the physical, medical, mental health or mental condition or DNA of the data subject; (e) the sexual orientation of the data subject; (f) the commission or alleged commission of an offence by the individual; or (g) proceedings for an offence committed or alleged to have been committed by the individual, the disposal of such proceedings, or the sentence of any court in the proceedings.	Personal data about a particular person, such as health data and genetic data, and which receives additional legal protection.

While data protection law does not usually apply to anonymised data, the Data Protection Act does not explicitly exclude anonymised data from the ambit of its provisions. Data that is not personal data can be shared.

To determine whether the data you are sharing is no longer individually identifiable, it is important to make an assessment. This can, however, be challenging. Unfortunately, the Data Protection Act does not define or use the terms anonymisation, de-identification or pseudonymisation, nor is there

is there guidance from the Regulator on these points. The data controller may wish to follow the guidance set out to be followed under the GDPR on how to make an assessment to determine whether data has been anonymised – including anonymisation techniques.

The test for anonymisation is always objective, but it can be interpreted in two ways: context-specific (relative approach) or context-agnostic (absolute approach).

Accordingly, the test for determining whether data is anonymised can be approached in two ways:

1. **Context-Agnostic Test**: Is there anyone in the world who can identify the data subject from the data? This test assesses whether any individual, regardless of context, could identify the data subject.
2. **Context-Specific Test**: Can a specific holder of the data identify the data subject from the data? This test evaluates whether the specific data recipient, given their context and resources, can identify the data subject.

The choice of approach affects the treatment of pseudonymised data. For example:

1. **Context-Agnostic Test**: If Data Controller A sends pseudonymised data to Data Controller B (with A retaining the means to identify individuals), the dataset is not considered anonymised.
2. **Context-Specific Test**: If Data Controller A sends pseudonymised data to Data Controller B, the dataset *might* be considered anonymised in the hands of Controller B. However, a test is necessary to determine whether the dataset is indeed anonymised for Data Controller B.

The first test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to Controller B, the dataset would not be anonymous.

The second test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to Controller B,

the dataset *may* be anonymous in the hands of Data Controller B. A test would be needed to determine whether the dataset is anonymous in the hands of Data Controller B.

Key Principles That Must be Met in Terms of the Data Protection Act

1. *Accountability:* This is not defined but is required. Generally, under data protection law, this will include keeping a record of processing activities and demonstrating compliance.
2. *Lawfulness of processing:* Personal data must be processed without infringing the privacy rights of the data subject, and must be done lawfully and reasonably. In addition, the data controller or data processor processing the personal data of foreign data subjects must ensure that personal data is processed in compliance with data protection legislation of the foreign jurisdiction from which the personal data originated.
3. *Specification of purpose:* Personal data must be collected only for a purpose which is specific, explicitly defined and lawful and which is related to the functions or activity of the person. A data controller who collects data must take the necessary steps to ensure that the data subject is aware of the purpose for the collection of the data.
4. *Compatibility of further processing with purpose of collection:* Where a data controller holds personal data collected in connection with a specific purpose, further processing of the personal data must be for that specific purpose.
5. *Quality of information:* A data controller who intends to process personal data must ensure that the data is complete, accurate, up to date and not misleading, having regard to the purpose for the collecting or processing of the personal data.
6. *Openness:* This is not defined but is required. Generally, under data protection law, this requires providing a data subject with information on the processing of his/her personal data.
7. *Data security safeguards:* A data controller must take the necessary steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate, reasonable, technical and organisational measures to prevent loss, damage or unlawful access.
8. *Data subject participation:* This is not defined but is required.

Data Subject Rights in Terms of the Data Protection Act

Data subjects have rights that the data controller must protect. These rights are the:

1. *Right to access:* The data subject has a right to request a data controller to confirm whether the data controller holds personal data about the data subject. This includes the right to request a data controller to give a description of the personal data which is held by a third party including the identity of all third parties with access to the information of the data subject.
2. *Right to correct personal data:* The data subject may request the data controller to correct or delete personal data about the data subject in their possession that is inaccurate, irrelevant, excessive or outdated.
3. *Right to prevent processing:* A data subject must have the right to require the data controller to cease or not begin processing of personal information for a specified purpose or in a specified manner.
4. *Right to prevent processing of personal data for direct marketing:* A data controller must not process the data subject's information for direct marketing purposes without the prior consent of the data subject.
5. *Rights in relation to automated decision-taking:* A data subject is entitled to require the data controller to ensure that any decisions taken by or on behalf of the data controller which significantly affect him/her are not based solely on processing by automatic means.
6. *Rights in relation to exempt manual data:* A data subject has the right to require the data controller to rectify, block, erase or destroy manual data which is inaccurate or incomplete or to cease holding such data in a manner which is incompatible with the legitimate purposes pursued by the data controller.

Cross-Border Data Sharing

When considering the cross-border sharing of data for research, all the provisions of the Data Protection Act must be met. The Act has no specific requirements on cross-border data sharing. Therefore, a researcher who wants to transfer personal data outside Ghana must comply with the general principles and regulations in the Act.