

SETTLEMENT OF PERSONAL DATA PROTECTION COMPLAINTS IN TANZANIA

PROCEDURAL GUIDE

SEPTEMBER 2026



Authors: Rachel Magege, Anna Kitindi and Abdul Said Naumanga
Reviewers: Dr. Nicksoni Filbert, Advocate Kheri Mbiro and Advocate. Sadiki Sadiki
Citation: Magege, R., Kitindi, A., and Naumanga A.S., (2026) Personal Data Protection Complaints Settlement in Tanzania: Procedural Guide. Tanzania Privacy Professionals Association, Dar es Salaam.



TABLE OF CONTENT

ACKNOWLEDGEMENTS. II
LIST OF ABBREVIATIONS. III
EXECUTIVE SUMMARY. IV

PART I

INTRODUCTIONS AND OFFENCES RELATED TO PERSONAL DATA. 1
 Introduction. 3
 Offences against the PDPC. 4
 Offences against Data Subjects. 5
 Offences relating to Corporates. 8
 General Penalties. 9

PART II

COMPLAINT HANDLING AND ENFORCEMENT FRAMEWORK
UNDER THE PDPA. 11
OVERVIEW OF COMPLAINT HANDLING FRAMEWORK. 12

TIER ONE:

COMPLAINT HANDLING AT CONTROLLER AND/OR
PROCESSOR LEVEL. 14
 Statutory Obligations of Data Controllers and Data Processors 15
 Decisions and Outcomes at Controller Level 15
 Escalation to the PDPC 15
 Substantive Data Subject Rights 16
 Strategic Use of Rights 24
 Representation and Delegated Enforcement 26

TIER TWO:

COMPLAINT PROCEEDINGS WITH THE PDPC 28
 Complaint Settlement Procedures 30
 Pre-Determination Stage 30
 Determination Stage 44
 Post-Determination Stage 54

TIER THREE:

 Procedure for Enforcement of Award. 58
 Appeals. 59

PART III

COMPARATIVE JURISPRUDENCE ON PERSONAL DATA
PROTECTION ENFORCEMENT. 60

REFERENCES 77

ACKNOWLEDGMENTS

We express our sincere appreciation to all individuals and institutions whose support and expertise contributed to the development of this procedural guide.

We extend our gratitude to the leadership of the Tanzania Privacy Professionals Association for their guidance, commitment and continued efforts to advance data protection as well as privacy rights and practices in Tanzania. Their institutional support and vision were instrumental in bringing this publication to fruition. We also thank our external reviewers, Dr. Nicksoni Filbert, Advocate Kheri Mbiro and Advocate Sadiki Sadiki for their expertise, time and effort in making this guide hold standard.

We acknowledge the broader community of data protection stakeholders in Tanzania, whose ongoing work continues to strengthen responsible data governance and protect personal data rights.

LIST OF ABBREVIATIONS

CAP	Chapter
CJEU	Court of Justice of the European Union
ICT	Information and Communication Technology
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EU	European Union
GDPR	General Data Protection Regulations
GN	Government Notice
HR	Human Resources
KEHC	Kenya High Court
KLR	Kenya Law Reports
LR	Law Report
NEMC	National Environment Management Council
ODPC	Office of the Data Protection Commissioner
PDPA	Personal Data Protection Act of Tanzania
PDPC	Personal Data Protection Commission of Tanzania
TLS	Tanganyika Law Society
TPPA	Tanzania Privacy Professionals Association
TZHC	Tanzania High Court
TZS	Tanzanian Shillings

EXECUTIVE SUMMARY

A proper understanding and use of the available complaints settlement procedures can be a powerful engine for data subjects, litigation lawyers and data protection advisers in order to foster data protection growth and the service of justice in Tanzania.

The impact of this procedural guide can be very significant in preventing the misuse and abuse of personal data, generating a greater appreciation of how complaints can be resolved efficiently and identifying existing gaps in practice.

Readers can expect three things:

- I. An analysis of what counts as an offence under the Personal Data Protection Act of Tanzania of 2022;
- II. A thorough breakdown of the complaint settlement processes and enforcement of awards provided; and lastly
- III. Lessons from different dispute settlement bodies regarding data protection justice.

Overall, this procedural guide aims to promote consistent and transparent approaches to complaint settlement in Tanzania's evolving data protection space. By strengthening institutional capacity, whether it be internal complaint settlement departments in companies/offices/organizations, the Personal Data Protection Commission of Tanzania or the High Court of Tanzania, the procedural guide contributes to the broader objective of protecting personal data and the privacy rights of individuals through addressing grievances related to personal data.

PART I

INTRODUCTIONS AND OFFENCES RELATED TO PERSONAL DATA



1. INTRODUCTION AND OFFENCES RELATED TO PERSONAL DATA

A proper understanding and application of available complaints settlement procedures serve as a powerful engine for data subjects, litigation lawyers and data protection advisers, driving both the growth of data protection jurisprudence and the service of justice in Tanzania. This guide was developed as a response to the rapid evolution of the country's digital landscape following the enactment of the Personal Data Protection Act, 2022 of Tanzania (herein **PDPA**) and to bridge the critical gap between statutory rights and procedural realities. Its core objective is to promote consistent, transparent and efficient approaches to dispute resolution by strengthening institutional capacity across all levels - from internal corporate compliance departments to the Personal Data Protection Commission (herein **PDPC**) and the High Court of Tanzania. The significance of this work lies in its utility as a practical shield against the misuse and abuse of personal data, illuminating how grievances can be resolved effectively while systematically identifying existing gaps in current practice.

To achieve this, the guide is structured as a cohesive narrative where each section logically informs the next. It begins with a foundational analysis of what constitutes personal data and offenses under the PDPA. This establishes the legal benchmarks for non-compliance. Recognizing these offenses naturally transitions into the second section, which provides a thorough breakdown of the actual complaint settlement processes, procedural workflows and the subsequent enforcement of awards. Finally, because procedural rules do not operate in a vacuum, the guide culminates in a comparative analysis of diverse dispute settlement bodies. By examining lessons from varied institutional frameworks, this concluding section offers critical insights into how data protection justice is practically meted out, providing readers with a holistic roadmap to navigate and shape Tanzania's evolving data protection landscape.



1.1. Introduction

Personal data means any information that can identify a human being. This can be an image, physical address, biometrics, one's voice, phone number etc. In Tanzania, similar to many other countries, personal data is often collected and processed for many reasons delivery of services, targeted marketing, security, public governance and more. Processing personal data means any operation that includes recording, organizing, structuring, storing, dissemination or erasure.

Personal data is governed by the PDPA. The PDPA establishes the PDPC, lays out proper procedures for collecting and processing data, the liabilities of data collectors and processors and lists the rights of a data subject (the person whose data is collected/processed).

This section examines the specific actions designated as "offences" under the PDPA and its subsequent regulations. While the term "offence" traditionally carries a criminal connotation, a deeper analytical reading of the PDPA reveals a nuanced legislative design: many of these statutory wrongs function fundamentally as civil wrongs or torts rather than traditional crimes - complaints are filed by individual data subjects rather than the State, compensation is paid directly to the aggrieved party rather than criminal fines paid to the State Treasury, etc¹. The six offences addressed in detail below showcase how the PDPA establishes civil liabilities for data misuse, empowering the PDPC to investigate these infractions and, where necessary, refer the matters to a court of competent jurisdiction for civil remedies, enforcement or judicial award. Readers can expect a thorough breakdown of these statutory actions and how they reshape the boundaries between civil liability and regulatory enforcement in safeguarding personal data.

For this procedural guide, the dispute settlement body is the **PDPC**.



¹ Sections 39 – 44 of PDPA address modes of lodging complaints, enforcement and penalty notices, and compensation for breach – all demonstrating civil and tortious frameworks rather than traditional criminal justice models.

1.2. Offences Established under the PDPA

1.2.1 Offences against the PDPC

Actions that may hinder the PDPC's effective functioning are considered an offence. Listed under Section 43 of the PDPA, the following four actions are labelled as offences committed against the PDPC.

1.2.1.1. Hindering the Official Performance of Duties by the PDPC

Such actions include denying access to information or facilities required for an investigation or altering or deleting personal data relevant to investigations.

1.2.1.2. Refusal to Provide Information to the PDPC

Refusing to provide information when asked by the PDPC is an offence. This is because organizations and individuals alike are expected to provide the PDPC with assistance, cooperation and to comply with requests for information or assistance that would enable the PDPC to enforce compliance with data protection principles.

1.2.1.3. Refusal of Premise Entry by the PDPC

To refuse the PDPC entry into any premise or to check systems and documents containing personal data is an offence. The PDPC usually requires such access when conducting on-site inspections and audits, reviewing registration documents, etc.; these are key tools for assessing and enforcing compliance with data protection standards in Tanzania. Under Section 19 of the PDPA, anyone who provides false or misleading information during registration or renewal commits an offence, and will be subject to a TZS 100,000 to TZS 5 million fine, imprisonment for up to five years; or both a fine and imprisonment. After conviction, the court also has the authority to order the forfeiture of devices containing personal data associated with the commission of the offence. These provisions underscore the seriousness of violations, aiming to ensure compliance and safeguard data protection principles.



1.2.1.4. Providing False or Misleading Information to the PDPC

The integrity of the information provided to the PDPC is crucial, as accurate data is fundamental to the PDPC's ability to make informed decisions and assessments regarding compliance with data protection. The PDPA also produced regulations; the Personal Data Protection (Complaints Settlement Procedures) Regulations, 2023 (herein **Complaints Settlement Regulations**) and the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 (herein **Collection and Processing Regulations**). Failure to comply with the instructions provided under both regulations is also a legal offence.

1.2.2 Offences against Data Subjects

1.2.2.1. Unlawful disclosure of personal data

Any disclosure of personal data must align with the original purpose for which the data was collected. A data controller can be a human being, a company/corporate or a public body, and their task is to collect personal data, and oversee the purpose and means of processing said data in accordance with the PDPA. Therefore, they are usually the first point of contact when it comes to matters of handling personal data. If they disclose personal data without a lawful excuse and in a manner that contradicts the original purpose for which the data was collected, then they have committed an offence against the individual whose data they collected.

For example, a hospital collects patient data to provide medical treatment and one day, a staff member shares a patient's diagnosis (without the patient's consent) with a pharmaceutical sales representative for marketing purposes. This is unlawful because the data collected was for treatment, not commercial marketing.

This principle aims to limit the use of personal data to specific, predefined purposes, safeguarding individuals' privacy by restricting the potential misuse of their information.



Personal data must always be handled with the utmost care, confidentiality and respect for privacy. Disclosing personal data unlawfully to anyone counts as an offence.

Similarly, a data processor, (human, company/corporate or public body which processes personal data for and on behalf of the controller and under the data controller's instruction), commits an offence if they disclose any personal data, they are processing without obtaining prior approval from the data controller, and without a lawful excuse.

The PDPA also addresses the unauthorized acquisition and disclosure of personal data by individuals. This includes acquiring personal data without the consent or authority of the data controller or processor and disclosing such information to third parties. Such actions are considered offenses, reflecting the law's stance on protecting personal data from unauthorized access and sharing, which could compromise individual privacy and security.

Moreover, the PDPA criminalizes the act of offering personal data obtained through unauthorised means for sale. This provision targets practices that aim to profit from the unlawful acquisition and sale of personal data, highlighting a commitment to combat the commercial exploitation of confidential information. Section 60(5) of the PDPA clarifies that for the purposes of identifying an offence under Section 60(4), merely advertising that personal data is or might be for sale is considered as making an offer to sell such data.



Individuals and entities found guilty of such offenses face substantial fines and, in some cases, imprisonment. In the case of an individual, they could be fined between TZS 100,000 and TZS 20 million, or they might go to jail for up to ten years or face both consequences. However, for companies or businesses, the fines are much larger, starting at TZS 1 million and going as high as TZS 5 billion. These penalties serve not only

as punitive measures but also as deterrents, reinforcing the importance of compliance with data protection laws and the ethical handling of personal data.

1.2.2.2. Unlawful Destruction, Deletion, Concealment or Alteration of Personal Data:

Any individual found guilty of illegally destroying, deleting, misleadingly concealing, or altering personal data faces significant legal consequences (Section 61 of PDPA). Unlawfully destroying personal data can occur, where to avoid legal consequences of malpractice, a staff member at a clinic intentionally destroys a patient's treatment records. An example of illegal deletion is when a Human Resources (HR) officer receives complaints about harassment and related emails as evidence; to protect a senior manager, the HR officer deliberately deletes those emails from the system. This is an unlawful deletion of personal data intended to obstruct accountability and justice.

Unlawful altering can occur when for instance, a university administrator changes a student's grades in the system, either to unfairly benefit the student or to harm them, without authorization. This is an act of manipulating personal data and misrepresenting a student's academic record. An example of unlawful concealment is when a customer service manager hides or removes complaint records about a faulty product from internal systems to avoid scrutiny.

The consequences include both financial penalties and potential imprisonment. Specifically, the PDPA imposes fines ranging from a minimum of TZS 100,000 to a maximum of TZS 10 million. Additionally, offenders may be sentenced to jail for up to five years, or they could be subjected to both penalties and jail time simultaneously.



This provision underlines the seriousness with which the law views the protection of personal data, emphasizing that such actions not only compromise individual privacy but also potentially inflict harm by manipulating or erasing important personal information.

1.2.2.3. Offences relating to corporates

When a company or corporation commits an offense under the PDPA, both the entity and its officers, who knowingly and willfully allowed the violation, are held accountable. In comparison, commercial matters in Tanzania have seen exceptional cases where Tanzanian courts will hold an individual personally liable, as opposed to the company itself. Such an exception was enforced by the High Court of Tanzania (Commercial Division) in the case of *Musa Shaibu Msangi v. Sumry High Class Ltd and Another* [2016] TLS LR 430. Here, the High Court ordered that if directors are using the company to dodge a clear legal duty (such as paying a court-ordered debt), the court can remove that protection, (legally known as the **corporate veil**) and go after the directors personally.

The same protection can be removed for data protection matters. Section 62 of the PDPA highlights that if directors/officers knowingly allow unlawful data processing, the Commission can hold both the company and individuals liable for contravention of the law.

The inclusion of individual liability alongside corporate accountability serves several purposes. *Firstly*, it acts as a deterrent against complacency or negligence in adhering to data protection standards, emphasizing that individuals cannot hide behind the corporate veil to avoid repercussions for illegal activities. *Secondly*, it reinforces the notion that ethical and lawful handling of data is a personal responsibility for those in positions of power within companies and corporations.



For laws to be effectively enforced, there must be tangible consequences for both corporations and the individuals who guide their actions. By making corporate officers personally liable for offenses, the PDPA aims to ensure higher levels of compliance with data protection regulations, thereby safeguarding personal data from misuse, unauthorized access, and other forms of malpractice. Because the PDPA is still new, there are limited enforcement cases regarding this matter. Most authority now comes

from statutory law and interpretation, as well as comparative cases from the corporate sector.

1.3. General Penalties

Section 63 of the PDPA imposes penalties on individuals or entities that contravene any provision of the PDPA or its regulations, specifically in instances where the Act does not prescribe explicit penalties for a particular offence. This provision serves as a catch-all penalty provision, ensuring that any breach of the PDPA's provisions or its regulations is subject to legal repercussions, even if such breaches are not individually enumerated within the Act.

The penalty for such contraventions is twofold, encompassing both financial and custodial penalties. On the financial side, individuals or entities found in violation of the PDPA or its regulations provisions could be subjected to a fine ranging from a minimum of TZS 100,000 to a maximum of TZS 5 million. This financial penalty is designed to serve as a deterrent against non-compliance with the data protection standards set forth by the PDPA.

On the custodial side, the provision allows for imprisonment of up to five years, reflecting the seriousness with which data protection breaches are treated in Tanzania. In some cases, violators may face both financial penalties and imprisonment, depending on the gravity of the contravention and the court's discretion.

Additionally, the PDPA empowers the court to order the forfeiture of devices containing the personal data involved in the contravention. This aspect of the penalty is aimed at directly addressing the misuse of personal data by removing the means through which such data may have been compromised or exploited. It acts as both a punitive measure against violators and a protective measure to prevent further misuse of personal data.

General penalties stated under the PDPA ensure that all forms of non-compliance are met with appropriate sanctions, highlighting the importance of adhering to data



protection principles to safeguard individuals' personal data against unauthorized use, access or distribution.



PART II

COMPLAINT HANDLING AND ENFORCEMENT FRAMEWORK UNDER THE PDPA



2. COMPLAINT HANDLING AND ENFORCEMENT FRAMEWORK UNDER THE PDPA

2.1. Overview of Complaint Handling Framework

Tanzania's personal data protection system offers a clear mechanism for handling complaints where personal data is misused, unlawfully collected or improperly processed. At the centre of this system is the PDPC, which is responsible for receiving, investigating and resolving complaints from individuals whose data protection rights have been violated².

The complaint handling process is governed by the PDPA, the Complaints Settlement Regulations and the Collection and Processing Regulations. These frameworks provide individuals with a formal way to seek remedies. When a complaint is filed with the PDPC, it examines whether a data controller or processor has complied with the legal principles governing personal data. In doing so, the PDPA serves two key purposes: resolving disputes and ensuring that organizations comply with the law.

These laws set out how complaints are filed, investigated, mediated, heard and resolved. Although the process is administrative, it closely resembles a court process because it includes formal procedures such as submissions, determinations and binding decisions.

The complaint-handling process can be understood in three different tiers. The first step is for the individual to deal directly with the data controller or the processor. PDPA grants individuals several rights, such as accessing their personal data, stopping or limiting its processing, correcting or deleting inaccurate data and objecting to automated decisions.

² Section 7(c) of PDPA.



This stage encourages organizations to resolve complaints internally before the matter escalates to the PDPC.

If the matter is not resolved at the controller/processor level, the second step is for the individual to file a complaint with the PDPC. The PDPC then investigates the complaint, gathers evidence, facilitates mediation and issues a decision. At this stage, the PDPC acts as a neutral decision-maker, ensuring fairness while enforcing compliance.

Thirdly, if a party does not comply with the PDPC's decision, the PDPC can take enforcement action, such as giving penalties. Additionally, any party dissatisfied with the PDPC's decision has the right to appeal to the High Court of Tanzania. This ensures that the data protection system in Tanzania is subject to judicial oversight and remains accountable.

Tanzania's data protection enforcement system follows a step-by-step approach, starting with internal resolution, moving to regulatory intervention and finally allowing court oversight. This structure makes it easier for individuals to seek justice while ensuring that organizations remain accountable for how they handle personal data.



TIER ONE:

2.2. Complaint Handling at Controller and/or Processor Level

While the complaint handling framework under the PDPA has been analytically described as operating through a three-tier structure, it is necessary to examine the procedural mechanism through which rights are enforced at the first tier prior to the involvement of the PDPC.

Under the PDPA, the enforcement of data subject rights does not, in the first instance, begin with lodging a complaint before the PDPC. Rather, the PDPA establishes a system of direct engagement between the data subject and the data controller or processor as the primary mechanism for enforcement.

All individuals have a range of enforceable rights³, including:

- the right to access personal data;
- the right to prevent processing that is likely to cause damage or distress;
- the right to object to the processing of direct marketing;
- rights in relation to automated decision-making; and
- the right to rectify, block, erase, or destroy personal data.

These rights are operationalized through procedures prescribed under the Collection and Processing Regulations, where a data subject is required to submit a formal application to the data controller or data processor using the prescribed forms mentioned in these Regulations.



³ Sections 33-38 of PDPA.

2.2.1. Statutory Obligations of Data Controllers and Data Processors

Upon receipt of an application for the enforcement of a right, the data controller or data processor is under a legal obligation to:

- acknowledge the receipt of the application;
- take appropriate interim or final measures, including suspension, restriction, rectification or erasure of personal data; and
- communicate a reasoned decision within the timeframe prescribed under the Regulations.

2.2.2. Decisions and Outcomes at Controller Level

Following consideration of the application, the data controller or processor may:

- accept the request, and implement the necessary corrective measures; or
- reject the request, upon providing written reasons to the data subject.

The decision at this stage constitutes the first-level determination of the dispute within the personal data protection framework.

2.2.3. Escalation to the PDPC

Where a data subject is dissatisfied with the decision of a data controller or data processor, or where the request is not addressed within the prescribed period, the data subject may escalate the matter to the PDPC by lodging a complaint⁴.

This transition marks the movement from Rights Invocation at Controller Level (Tier One) to regulatory enforcement (Tier Two) within the framework established under the PDPA.

The complaint procedure before the PDPC is therefore not the primary mechanism of enforcement but rather a secondary and supervisory mechanism designed to address:

- failures by data controllers or data processors to comply with the law;
- improper or unlawful decisions at the controller level; and

⁴ Regulation 39 of Complaints Settlement Regulations.



- disputes that cannot be resolved through controller or processor engagement.

This layered approach ensures that regulatory intervention is invoked only where necessary while promoting efficiency and accountability at the level of data controllers and data processors.

2.2.4. Substantive Data Subject Rights

The rights conferred upon data subjects under the PDPA are independent and directly enforceable, which may be invoked against a data controller or data processor without any prescribed order or sequence.

Accordingly:

- a data subject is not required to exhaust one right before invoking another;
- any right may be exercised individually or in combination with other rights; and
- multiple rights may be invoked simultaneously, depending on the nature and urgency of the matter.

Therefore, the choice of which right to invoke is a matter of legal strategy, informed by the facts and circumstances of each case.

2.2.4.1. Right of Access to Personal Data

The right of access is provided under Section 33 of the PDPA, which entitles a data subject to:

- obtain confirmation as to whether personal data relating to him is being processed;
- receive a description of such data;
- understand the purpose of processing; and
- be informed of the recipients or categories of recipients of the data.

Procedure: There is no specific procedure to invoke this right under the Collection and Processing Regulations, but in practice:

- the data subject submits a request to the data controller or processor, orally or in writing, usually by letter/notice (demand notice) or mail.



- the controller is required to respond within a reasonable period, subject to lawful limitations (usually 21 days).

2.2.4.2. Right to Prevent Processing Likely to Cause Damage

Under Section 34 of the PDPA, a data subject may require a data controller or data processor to suspend or not begin the collection or processing of personal data where such processing is likely to cause substantial damage or distress.

The procedure for invoking this right is expressly provided under Regulation 15 of the Collection and Processing Regulations.

- **Submission of Application:** The data subject shall submit an application to the data controller or data processor using **Form No. 4** prescribed under the First Schedule of the Collection and Processing Regulations. A copy of the application shall simultaneously be submitted to PDPC⁵.
- **Immediate Interim Measures (72 Hours Rule)**⁶: Upon receipt of the application, the data controller or data processor is required, within seventy-two (72) hours and without charging any fee, to:
 - a. acknowledge the receipt of the application;
 - b. temporarily suspend the processing of personal data;
 - c. indicate in the system that the data is restricted; and
 - d. where the data has been disclosed to third parties, notify such parties and require them to suspend processing or remove the data from their systems.
- **Final Determination of the Application**⁷: Following the temporary suspension, the data controller or data processor shall, within seven (7) days, consider the application and:

⁵ Regulation 15(2) of Collection and Processing Regulations.

⁶ Ibid.

⁷ Ibid.



- a. accept the application, in which case processing shall be suspended or removed⁸; or
 - b. reject the application, where the request is considered unreasonable, and provide written reasons for such rejection⁹.
- **Escalate to the PDPC:** Where the application is rejected, the aggrieved data subject may, within **fourteen (14) days** from the date of notification of rejection, lodge a complaint before the PDPC in accordance with the applicable complaint settlement procedures¹⁰.
 - **Consequence of Failure to Escalate:** Where no complaint is lodged within the prescribed period (14 days), the data controller or data processor may lawfully resume processing of the personal data in accordance with PDPA.

This right is commonly invoked in situations involving:

- ongoing unlawful processing;
- imminent publication of personal data;
- misuse of personal data that causes harm;
- situations that require urgent intervention to prevent further damage.

This right constitutes an immediate protective mechanism comparable to interim relief in litigation. Its key strategic advantages include:

- the imposition of a mandatory 72-hour suspension obligation;
- the ability to freeze processing before escalation; and
- the creation of a clear procedural pathway for complaint proceedings in cases of non-compliance.

2.2.4.3. Right to Prevent Processing for Direct Marketing

Section 35(1) of the PDPA entitles a data subject to require a data controller to cease processing personal data for direct marketing purposes.

⁸ Ibid.

⁹ Ibid.

¹⁰ Ibid.



There is no specific procedure to invoke this right under the Collection and Processing Regulations, but in practice:

- the data subject submits a request to the data controller or processor, orally or in writing, usually by letter/notice (demand notice) or mail.
- the controller or processor is required to cease such processing upon receipt of the request.
- If a data subject is willing for the data controller or processor to use his/her personal data for pecuniary benefits, the data controller or processor shall prepare the agreement in accordance with the Law of Contract Act¹¹.

2.2.4.4. Rights in Relation to Automated Decision-Making

Under section 36(1) of the PDPA, a data subject has the right not to be subjected to a decision which significantly affects him where such decision is based solely on the automated processing of personal data.

This provision protects data subjects from decisions made without human involvement, particularly when such decisions have legal, financial, or reputational consequences.

Procedure: Regulation 19 of the Collection and Processing Regulations imposes mandatory obligations on a data controller or data processor when automated decision-making is involved.

Mandatory Notification: Where a decision is made solely by automated means and significantly affects the data subject, the data controller or data processor shall notify the data subject in writing regarding such processing¹².

Content of Notification¹³: The notification must include:

- basic information about the processing and its intended purpose;
- specific requirements to ensure transparency and uniformity in processing;

¹¹ Section 35(2) of PDPA.

¹² Regulation 19(1) of Data Collecting and Processing Regulations.

¹³ Ibid.



- the procedure used to store the personal data; and
- any effects likely to arise from the processing and how such effects will be handled.
- the right of the data subject to object to the use of their personal data in commercial advertisements.

The data subject retains the right to object to the use of personal data in automated decision-making; and/or reject the decision made solely by automated means¹⁴. Upon such objection or rejection, the data controller or data processor is required to reconsider the decision using appropriate lawful means, including human intervention.

Practical Application: In practice, this right may be invoked when:

- a data subject is adversely affected by automated decisions (e.g. denial of services, profiling outcomes, or exclusion from opportunities);
- the data controller fails to provide notification or adequate disclosure; or
- the decision is made without meaningful human involvement.

Such circumstances may give rise to a complaint before the PDPC on the following grounds: unlawful processing, lack of transparency, and violation of data subject rights

2.2.4.5. Right to Rectification of Personal Data

The right to rectification entitles a data subject to require a data controller or data processor to correct personal data that is inaccurate, outdated, incomplete, or misleading.

In the event of a complaint,

- The data subject shall submit an application using **Form No. 5** prescribed under the First Schedule of the Collection and Processing Regulations;

¹⁴ Ibid.



- The application may be accompanied by supporting documents necessary to justify the requested rectification;
- A copy of the application must be submitted to the PDPC.

(i) Determination by Controller or Processor

- Under regulation 16(3) of the Collection and Processing Regulations, the data controller or data processor shall, within **fourteen (14) days** from the date of receipt of the application either accept and rectify the personal data or reject the application.
- Where the application is rejected, the controller or processor shall notify the data subject in writing, providing reasons for the rejection¹⁵.

Where the application is rejected, no response is provided within the prescribed timeframe, or the rectification is inadequate, the data subject may escalate the matter by lodging a complaint before the PDPC in accordance with the Complaint Settlement Regulations.

Upon receipt of the copy of application Form No. 5, the PDPC may:

- order rectification of personal data;
- block or restrict the processing
- order for the erasure or destruction of the data.

Further, where rectification or related action is taken, the data controller or data processor is required to notify third parties to whom the data had previously been disclosed of such rectification or correction¹⁶. It is important to know that this right is commonly invoked where:

- personal records are factually incorrect;
- data used for decision-making is outdated;

¹⁵ Regulation 16(4) of Collection and Processing Regulations.

¹⁶ Section 38(4) of PDPA.



- inaccuracies negatively affect the legal, financial, or reputational interests of the data subject.

2.2.4.6. Right to Erasure or Destruction of Personal Data

The right to erasure or destruction of personal data arises under Regulation 17 of the Collection and Processing Regulations, which entitles a data subject to require a data controller or data processor to erase or destroy personal data where:

- the data is no longer necessary for the purpose for which it was collected;
- the data subject has withdrawn consent¹⁷;
- the data subject no longer wishes the processing to continue;
- the data is used for commercial purposes against the wishes of the data subject;
- the processing is unlawful; or
- erasure is required by law.

(a) Procedural Enforcement

(i) Application for Erasure: The data subject shall submit an application using **Form No. 6** prescribed under the First Schedule of the Collection and Processing Regulations. A copy of the application shall be submitted to the PDPC¹⁸.

(ii) Determination by Controller or Processor: The data controller or data processor shall, within **fourteen (14) days**, consider the application and they may either accept the request and erase or destroy the data; or reject the application¹⁹. Where the application is rejected, the controller or processor shall notify the data subject in writing, providing reasons for such rejection²⁰.

(iii) Statutory Limitations: The right to erasure shall not be exercised where the processing of personal data is necessary for:

¹⁷ Regulation 17(1)(b) of Collection and Processing Regulations.

¹⁸ Ibid.

¹⁹ Ibid.

²⁰ Ibid.



- the exercise of the right to freedom of expression and information;
- compliance with legal obligations; or
- the performance of duties in the public interest or within the scope of governmental authority.

(iv) Escalation to the PDPC:

The data subject may lodge a complaint before the PDPC in accordance with the Complaints Settlement Procedures, if the application is rejected, no response is provided, or erasure is not properly affected,

2.2.4.7. Right to Compensation

The right to compensation is provided under Section 37 of the PDPA, which entitles a data subject to compensation if he suffers damage because of a contravention of any provision of the PDPA by a data controller or processor.

A data subject is entitled to compensation when:

- there has been a contravention of the PDPA;
- the rights of the data subject have been infringed; and
- the damage suffered relates to the unlawful processing of personal data, where “damage” includes both financial loss and non-financial harm arising from the contravention.

(a) Liability Framework: The PDPA establishes a clear liability regime as follows:

A data controller shall be liable for damage caused by the processing of personal data. A data processor shall be liable where she/he has failed to comply with obligations imposed under the PDPA or acted contrary to the lawful instructions of the data controller.

However, a data controller or data processor shall not be liable if it proves that it is not in any way responsible for the event giving rise to the damage.



(b) Procedural Enforcement

(i) Initiation of Claim

The right to compensation is enforced through complaint proceedings before the PDPC, where the data subject alleges contravention of the PDPA and resulting damage.

(ii) Determination by the PDPC

If the PDPC is satisfied that the data subject has suffered damage and such damage resulted from a contravention of the PDPA, it may order compensation to be paid to the data subject and issue additional corrective measures, including the rectification, blocking, erasure, or destruction of personal data.

(c) Practical Application

This right is typically invoked in cases involving:

- unlawful disclosure of personal data;
- misuse of personal images or information;
- data breaches that result in financial or reputational harm;
- continued processing, in violation of the data subject's rights.

The right to compensation represents the ultimate enforcement mechanism in the personal data protection framework. Its strategic significance includes:

- transforming regulatory violations into monetary liability;
- providing a direct remedy to affected data subjects; and
- strengthening the deterrent effect of the PDPA

2.2.5. Strategic Use of Rights

The rights conferred upon data subjects under the PDPA are not only independent but may also be strategically combined to achieve effective enforcement outcomes.

In practice, exercising a single right may not always be sufficient to fully address violations of personal data protection principles. Accordingly, a data subject may invoke



multiple rights either simultaneously or in succession, depending on the nature, urgency, and complexity of the matter.

2.2.5.1. Concurrent Invocation of Rights

A data subject may invoke more than one right simultaneously, particularly where the situation requires immediate intervention and substantive resolution.

For example:

- i. a request to prevent processing may be submitted together with a request for erasure or destruction of data where the processing is both ongoing and unlawful; or
- ii. a request for access to personal data may be combined with a request for rectification where inaccuracies are suspected.

Concurrent invocation enables the data subject to prevent further harm, secure relevant information and pursue appropriate remedies without any unnecessary delays.

2.2.5.2. Sequential Invocation of Rights

In certain circumstances, rights may be invoked sequentially, particularly where further information is required before pursuing substantive remedies.

For instance, a data subject may first invoke the right of access (Section 33) to obtain information regarding the processing of personal data and thereafter invoke the right to rectification or erasure (Section 38) based on the information obtained.

Sequential invocation is particularly appropriate in cases where the nature or extent of processing is unclear or evidentiary support is required prior to escalation.

2.2.5.3. Factor Considerations in the Use of Rights

The choice of whether to invoke rights individually, concurrently, or sequentially depends on several factors, including:



- the urgency of the situation;
- the risk of ongoing or imminent harm;
- the availability of information regarding the processing; and
- the desired outcome (whether immediate protection, corrective action, or evidentiary clarification).

In urgent cases, priority may be given to rights that provide immediate protection, while in complex matters, an evidentiary approach may be adopted before pursuing substantive remedies.

2.2.6. Representation and Delegated Enforcement

Under Regulation 18 of the Collection and Processing Regulations, data subject rights may be exercised not only by the data subject personally but also by a duly authorized person acting on his behalf.

Where such authorization is granted, the data controller or data processor is required to handle the matter in a manner that safeguards the best interests of the data subject.

In cases involving a child, the controller or processor must additionally ensure that:

- the person exercising the right is properly identified;
- the processing complies with the applicable legal framework; and
- the parent or guardian is informed of the associated risks and safeguards.

Where a right is exercised through an authorized person:

- proof of authorization may be required by the data controller or data processor;
- the controller or processor may decline to act on the request pending verification of such authority; and
- the request shall only be processed upon satisfaction that the representative has a valid legal basis to act on behalf of the data subject.

This provision is particularly relevant in situations involving:

- legal representation by advocates or a duly authorized person;



- representation of minors;
- cases involving incapacity or inability of the data subject; and
- institutional or collective enforcement of rights.



TIER TWO:

2.3. Complaint Proceedings with the PDPC

However, where such invocation of data subject rights at the level of data controllers/processors fails to result in compliance, the matter ceases to be a private compliance issue and crystallizes into a dispute capable of regulatory determination. Prior invocation of rights serves as evidence of attempted compliance resolution, non-compliance or refusal by the controller or processor constitutes the factual and legal basis of the complaint, and the dispute transitions from private enforcement to formal regulatory adjudication.

A dispute is deemed to arise when:

- the data controller or data processor fails to respond within the prescribed timeframe;
- the request is expressly rejected;
- the response is inadequate or incomplete, or the data subject remains aggrieved by the outcome.

Upon the occurrence of any of the above, the data subject acquires the right to escalate the matter to the PDPC by lodging a complaint under Regulation 36 of the Collection and Processing Regulations.

Accordingly, the legal basis for lodging complaints with the PDPC arises from two principal, though interrelated, circumstances, as follows:

- **Violations of the PDPA and Data Protection Principles:** Where a data subject or any affected person considers that the collection, use, storage, disclosure or any other form of processing of personal data contravenes these statutory requirements, such a person is entitled to lodge a complaint before the PDPC. This position is further reinforced under Section 39 of the PDPA, which



empowers the PDPC to receive and investigate complaints relating to violations of personal data protection principles.

- **Decisions of Data Controllers or Processors:** In addition to direct violations of the PDPA, complaints may arise from the way a data controller or processor handles issues related to personal data, while responding to the exercise of data subject rights.

The regulatory framework recognizes that a data subject may first engage a data controller or data processor in seeking the enforcement of their rights²¹, including requests for rectification, erasure, restriction or objection to processing. Where such requests are rejected, inadequately addressed, or handled in a manner inconsistent with the requirements of the PDPA, the right to escalate the matter to the PDPC arises.

Regulation 36 of the Collection and Processing Regulations affirms this position by permitting a data subject who is aggrieved by the decision of a data controller or data processor to submit a complaint to the PDPC in accordance with the applicable complaint procedures under the Complaints Settlement Regulations.

Complaints falling within this category, therefore, arise not merely from abstract dissatisfaction but from a demonstrable failure by a data controller or data processor to act in accordance with the law, particularly in the context of decision-making, response to complaints, or handling of personal data.

Taken together, these provisions establish that the right to lodge a complaint before the PDPC is triggered by any form of non-compliance with the personal data protection framework, whether arising from direct violations of statutory principles or improper, unlawful, or inadequate handling of personal data by data controllers or data processors.

²¹ Part III of Collection and Processing Regulations.



2.3.1. Complaint Settlement Procedures

The settlement of personal data protection disputes before the PDPC is structured as a sequential, multi-stage process designed to ensure both procedural fairness and regulatory effectiveness.

For analytical clarity, the process comprises three core stages:

- **Pre-Determination Stage** – involving the preparation of pleadings, investigation and mediation mechanisms aimed at early resolution;
- **Determination Stage** – involving formal hearing and determination of the complaint; and
- **Post-Determination Stage** – involving enforcement, compliance, and challenge mechanisms such as review and appeal.

Although presented as distinct phases, these stages operate within a continuous procedural framework governed by the PDPA and the Complaints Settlement Regulations.

2.3.2. Pre-Determination Stage

The pre-determination stage constitutes the initial and foundational phase of dispute resolution. It is primarily concerned with establishing the factual and legal basis of the complaint and exploring the possibility of an early, non-adversarial resolution.

This stage is characterized by three principal processes – Preparation of pleadings, Investigation of the Complaint, and Mediation Proceedings.

Unlike the determination stage, which is adjudicatory in nature, the pre-determination stage is inquisitorial and facilitative, allowing the PDPC to actively engage with the dispute while encouraging a consensual resolution.



2.3.2.1. Preparation of Pleadings and Procedure for Filing Complaints

Complaint settlement proceedings before the PDPC are initiated and conducted through a structured set of pleadings that allow the parties to formally present their claims and responses.

Although complaint proceedings before the PDPC are administrative in nature, they incorporate procedural elements commonly associated with civil litigation, including the submission of written pleadings. These pleadings serve to clarify the issues in dispute and guide the subsequent stages of investigation, mediation and hearing.

The principal pleadings in personal data protection complaints consist of **the complaint**, **the defense**, and **the reply to the defense** (if any).

- **Nature and Legal Basis of a Complaint**

A complaint constitutes the initiating pleading in personal data protection dispute proceedings before the PDPC. It is the formal mechanism through which a person alleges a violation of personal data protection principles or challenges a decision made by a data controller or processor regarding personal data.

The right to lodge a complaint is established under Regulation 4(1) of the Complaints Settlement Regulations.

Under this provision, a person or group of persons who considers that there has been a violation of personal data protection principles or who is dissatisfied with a decision of a data controller or data processor may submit a complaint to the PDPC.

Through the complaint, the complainant sets out the material facts, legal basis of the complaint, and relief sought, thereby formally initiating the complaint settlement procedure before the PDPC.



- **Complaint Document (Form No. 1)**

A complaint must be submitted using **Form No. 1** prescribed under the schedule of Complaints Settlement Regulations. Form No. 1 serves as the official complaint document through which the PDPC receives and registers complaints.

In practice, complaints are usually filed electronically through the complaint portal of the PDPC via their website²², where the complainant completes the digital version of Form No. 1 and uploads the supporting documentation.

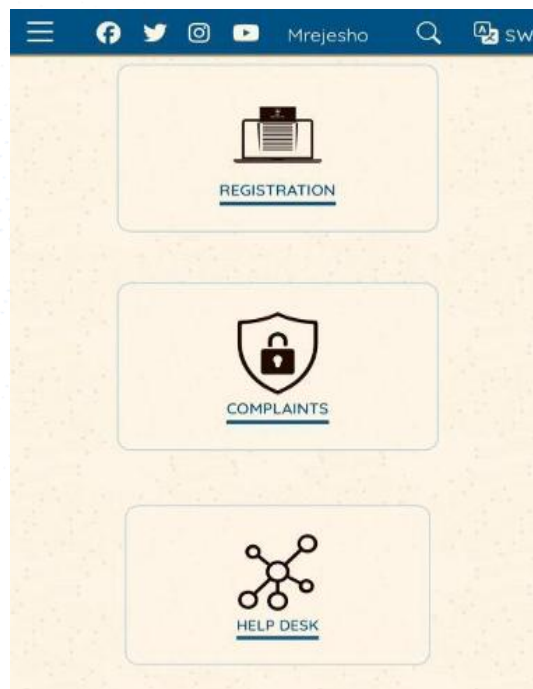


Figure 1: The PDPC's online system

The complaint form generally requires the following information:

1. Complainant Information – identity and contact details of the complainant.
2. Respondent Information – details of the data controller or data processor against whom the complaint is lodged.

²² <https://dataprotection.pdpc.go.tz/complaint-form-one>.

3. Complaint Details – description of the alleged violation of personal data protection principles.
4. Resolution and Redress Sought – the remedy sought from the PDPC.
5. Relevant Documents – supporting evidence attached to the complaint.
6. Declaration – confirmation of the accuracy of the information provided.

These requirements ensure that the PDPC receives sufficient factual and documentary information necessary for the preliminary assessment of the complaint.

- **Time Limit for Filing a Complaint**

The filing of complaints is subject to a statutory time limitation introduced under the **Personal Data Protection (Complaints Settlement Procedures) (Amendment) Regulations, 2025**, published under **GN No. 407 of 2025 (the Amendment)**.

Regulation 4(1) of the Complaints Settlement Regulations was amended by **Regulation 2(a) of the Amendments** to require a complaint to be filed within twenty-one (21) days from the date on which the complainant becomes aware of the violation of personal data protection principles or from the date of the decision of the data controller or processor. This time limit applies to all complaints except those arising under Regulation 15 of the Data Collection and Processing Regulations.

- **Oral Complaints**

The Regulations recognize that not all complainants may submit written complaints. Under Regulation 4(2) of the Complaints Settlement Regulations, a complaint may be presented orally to the PDPC. In such cases, the PDPC is required to reduce the complaint into writing using Form No. 1, and the complainant must sign the recorded complaint.

- **Group Complaints**

The Regulations also allow for representative or group complaints. Under the amended Regulation 4(3) of the Complaints Settlement Regulations, a complaint may be filed by a group of persons affected by the same conduct.



To file such complaints, the following documents must accompany the complaint: a list of the names and signatures or thumbprints of the affected persons; and minutes of the meeting authorizing the filing of the representative complaint. Group complaints provide an avenue for addressing the collective violation of personal data protection rights.

- **Language of Complaint.**

Complaints can be submitted in Kiswahili or English²³.

2.3.2.2. Preliminary Scrutiny and Rejection

Upon receipt of a complaint, the PDPC must evaluate the complaint to determine whether it complies with the requirements of the law **within five days**²⁴.

During this stage, the PDPC verifies whether:

- the complaint complies with the prescribed form requirements,
- the complaint falls within the jurisdiction of the PDPC, and
- the complaint complies with the requirements of the PDPA and the applicable regulations.

If the PDPC is satisfied that the complaint meets the statutory requirements, it proceeds to deal with the complaint.

Within five days of the evaluation of the complaint, the PDPC may reject a complaint where, upon evaluation, it is satisfied that the complaint does not meet the statutory or procedural requirements necessary for further consideration.

The PDPC may reject²⁵ a complaint where:

- the complaint does not disclose a legal cause of action concerning personal data protection;

²³Regulation 4(4) of the Complaints Settlement Regulations.

²⁴Regulation 2(c) of the Amendments, amending Regulation 4(5) of the Complaints Settlement Regulations.

²⁵Regulation 5(1) of the Complaints Settlement Regulations.



- the complaint is filed outside the prescribed time limit;
- the subject matter of the complaint is pending before a court, tribunal, arbitration panel, or other quasi-judicial body;
- the complaint does not relate to matters governed under the PDPA; or
- the complainant lacks legal standing to lodge the complaint.

Where the PDPC rejects a complaint, it is required to notify the complainant of the decision in writing **within seven (7) days** from the date of the decision and provide the reasons for the rejection²⁶. The rejection of a complaint does not permanently bar the complainant from pursuing the matter further.

A complainant may submit a new complaint regarding the same matter²⁷, provided that the new complaint complies with the requirements of the PDPA and the subsequent regulations.

A complainant who is dissatisfied with the PDPC's rejection of the complaint may apply for a review of the decision to the PDPC under **Section 48 of the PDPA**, usually by way of an official letter, since there is no prescribed form in that regard.

The review mechanism serves as an important safeguard within the complaint settlement framework by allowing complainants to challenge decisions that reject their complaints.

2.3.2.3. Service of Summons, Defense and Reply Procedure

(a) Service of Summons and Notification to Present Defense

Regulation 6 of the Complaints Settlement Regulations governs the procedure for service of summons.

²⁶ Ibid.

²⁷ Ibid.



This stage arises after the PDPC has completed the evaluation of a complaint under Regulation 4(5) and is satisfied, pursuant to Regulation 4(6), that the complaint complies with the requirements of the PDPA and subsequent regulations.

In such circumstances, the PDPC is mandated, within a period not exceeding **seven (7) days**, to issue and serve a summons upon the respondent in **Form No. 2** set out in the schedule of the Complaint Settlement Regulations, requiring him to present his defense. This step formally joins the respondent to the proceedings and initiates the adversarial phase of the complaint process.

(b) Modes of Service

(i) Personal Service: The summons may be served directly to the respondent or their authorized representative. Service under this mode is evidenced by acknowledgement through the signing and returning of a copy of the summons to the PDPC.

(ii) Service by Registered Mail: The summons may be sent to the respondent by registered mail, and proof of service is established through a return receipt.

(iii) Substituted Service by Publication: Where service cannot be affected through ordinary means, the PDPC may order substituted service by publication in two newspapers of general circulation within the country. One published in Kiswahili and the other in English. This mode is only permissible when the PDPC is satisfied that:

- the respondent is evading service; or
- service cannot be affected through ordinary means; and
- there is written confirmation from a local government authority of unsuccessful attempts at service.

2.3.2.4. Defense to Complaint

Timeframe for Filing Defense

Under **Regulation 7(1) of the Complaints Settlement Regulations**, the respondent is required to submit a defense within a period not exceeding **twenty-one (21) days** from



the date of receipt of the summons²⁸. This timeframe ensures that the respondent is afforded a reasonable opportunity to prepare and present their case.

This is what they must do:

- specifically answer each allegation of fact contained in the complaint;
- admit or deny allegations based on knowledge; and
- avoid general or evasive denials.

This requirement ensures that the defense is substantive and enables the PDPC to clearly identify the issues in dispute.

Consequences of Failure to File Defense

Under **Regulation 7(3) of the Complaints Settlement Regulations**, failure to submit a defense within the prescribed period is ***deemed a waiver of the respondent's right to appear and participate*** in the proceedings before the PDPC, and the PDPC may proceed to hear and determine the complaint ***ex parte***.

This provision operates as a procedural sanction designed to prevent undue delay in the resolution of complaints and ensure that proceedings are not frustrated by the non-participation of a duly notified respondent.

The operation of Regulation 7(3) of the Complaints Settlement Regulations was illustrated in **Abdul Said Naumanga v Mi Casa Company Limited**²⁹. In this matter, the respondent failed to file a defense within the prescribed period of 21 days, the PDPC deemed such failure as a waiver of the right to participate, and the complaint proceeded to be heard and determined ***ex parte***.

²⁸ Regulation 7(1) of Complaints Settlement Regulations.

²⁹ Complaint No. PDPC/CMP/014/2024.



The PDPC expressly affirmed that: *“where a respondent fails to present a defense as required, he is deemed to have waived his right to appear and participate, and the proceedings may continue in his absence”*.

Therefore, failure to file a defense may result in the loss of the opportunity to challenge evidence or raise defense; ex parte proceedings may lead to adverse findings based solely on the complainant’s case; and the burden effectively shifts to the respondent to later seek relief through an application to set aside the ex parte decision. Accordingly, the timely filing of a defense is not merely procedural but strategically critical to participation in the adjudicative process.

Setting Aside Ex Parte Proceedings

Respondents who fail to file a defense within time may apply to the PDPC, by way of letter, for an order setting aside the ex parte proceedings³⁰.

2.3.2.5. Reply to Defense

Right to Reply

Upon receipt of the respondent’s defense, the complainant may prepare and submit a reply. This ensures that the complainant is afforded an opportunity to respond to matters raised in the defense. Pursuant to the amendment to Regulation 8 of Complaints Settlement Regulations³¹, the complainant is required to submit a reply to the defense within a period of **seven (7) days** from the date of receipt of the defense.

Purpose of Reply

The reply serves to:

- address new facts or allegations raised in the defense;
- clarify or reinforce the complainant’s position; and
- narrow the issues for determination.

³⁰ Regulation 7(4) of Complaints Settlement Regulations.

³¹ Regulation 3 of GN N0 407 of 2025 “the Amendment.”



2.3.2.6. Amendment of Pleadings

Under Regulation 12(1) of the Complaints Settlement Regulations, either the complainant or the respondent may, upon showing sufficient cause, be allowed to amend a complaint, defense, or reply to the defense.

(a) Requirement for Leave

The amendment of pleadings is not automatic. It is subject to approval by the PDPC and the requirement that the opposing party be afforded an opportunity to respond to amended pleadings. This ensures compliance with the principles of natural justice and procedural fairness.

(b) Mode of Applying for Amendment

A party seeking to amend a pleading must submit a formal application in writing, usually by way of a letter to the PDPC and specify the nature and basis of the proposed amendment. This requirement ensures that amendments are properly documented and subjected to procedural scrutiny.

(c) Timeframe for Amendment

Where leave to amend is granted, the amendment must be affected within the time specified by the PDPC and in any event, such a period shall not exceed **seven (7) days**. This amendment introduced a mandatory upper limit and prevented undue delays in the progression of proceedings.

(d) Right of Response to Amended Pleadings

Regulation 12(1) further requires that the opposing party be given an opportunity to respond to the amended pleading and such response must be made within a reasonable time prior to the hearing. This preserves procedural balance and ensures that no party is prejudiced by late-stage amendments.



2.3.2.7. Investigation of Complaint

The investigation of complaints is grounded in Section 40 of the PDPA and Regulation 13 of the Complaints Settlement Regulations (as amended). These provisions collectively establish the PDPC's mandate to inquire into complaints and determine whether regulatory intervention is warranted.

(a) Commencement of Investigation

Following the amendment to Regulation 13(1), the PDPC is required, upon receipt of a defense or reply (where applicable), to examine the complaint and satisfy itself that the complainant has a legitimate interest in the matter and the complaint is not frivolous or without basis.

This marks a shift from a purely procedural trigger to a substantive threshold test, introducing an early filtering mechanism into the process.

(b) Notice of Investigation

Prior to commencing the investigation, the PDPC must issue a formal Notice of Investigation to the respondent in **Form No. 3**, as prescribed under the Complaints Settlement Regulations.

This requirement operationalizes Section 40 of the PDPA, ensuring that the respondent is formally notified of the complaint and that the scope and existence of the investigation are clearly communicated.

(c) Nature and Scope of Investigation

The investigation stage is not merely administrative; it is a fact-finding and evaluative process through which the PDPC does the following:

- examines the conduct of respondents;
- assesses compliance with the PDPA and applicable standards; and
- determines whether further regulatory action is necessary.



Where the complaint is found to have merit, the PDPC may require the respondent to consider or reconsider the complaint within fourteen (14) days, reinforcing the corrective nature of this stage.

(d) Confidentiality of Investigation

Pursuant to Section 41 of the PDPA, all investigations must be conducted in a manner that preserves the confidentiality of the data.

This obligation serves multiple functions:

- protecting sensitive personal data;
- safeguarding the integrity of the investigation; and
- maintaining trust in the regulatory process.

(e) Powers of the PDPC During Investigation

The investigative authority of the PDPC is principally derived from Sections 42 and 44 of the PDPA.

These provisions confer broad, quasi-judicial powers, including:

- the power to summon individuals to appear before the PDPC;
- the power to receive evidence, whether on oath, by affidavit, or otherwise;
- the power to enter premises and inspect data processing activities;
- the power to seize devices or materials containing personal data where necessary; and
- the power to examine, extract, or copy documents and records.

Additionally,

- a. The PDPC may require representations from both the complainant and the respondent;
- b. No person may withhold relevant personal data based on other laws; and
- c. Documents obtained must be returned within the prescribed timeframe upon request.



Under **Section 44**, the PDPC may also engage third parties or authorities to assist in investigations and vest such persons with equivalent investigative powers. Collectively, these powers position the PDPC as an active investigative authority, rather than a passive adjudicator.

(f) Procedural Remedies During Investigation

While the investigation stage is primarily inquisitorial, circumstances may arise in which the PDPC issues directions or interim determinations that affect the rights or obligations of the parties.

In such cases, the PDPA provides a mechanism for reviewing the PDPC's decisions or directions under **Section 48 of the PDPA**. It is important to note that the review mechanism applies only where the PDPC has issued a decision or direction capable of legal effect and does not extend to purely administrative or investigative steps.

2.3.2.8. Mediation Proceedings

Mediation is governed by Regulation 14 of the Complaints Settlement Regulations, which establishes it as a mandatory and integral component of the pre-determination stage. Its primary objective is to facilitate the amicable resolution of disputes without resorting to formal adjudication.

(a) Mandatory Mediation Window

The PDPC is required to attempt mediation within **thirty (30) days** from the date of filing the complaint.

This introduces a structured opportunity for settlement, ensuring that parties are given a realistic chance to resolve disputes early.



(b) Role of the Mediator

The PDPC designates an officer to act as a mediator, whose role is to:

- facilitate communication between the parties;
- clarify issues in dispute; and
- guide negotiations towards a mutually acceptable outcome.

The mediator does not impose a decision but operates as an impartial facilitator.

(c) Recording of Settlement

Where mediation is successful, the agreement must be reduced to writing using **Form No. 4** prescribed under the Schedule of the Collection and Processing Regulations, signed by the parties, and submitted to the PDPC. This ensures the clarity, certainty, and formal recognition of the agreed-upon terms.

2.3.2.9. Effect of Mediation Settlement

(a) Conversion into Award

A mediated settlement, once adopted by the PDPC automatically assumes the status of an award. This is a critical provision as it transforms mediation from a voluntary process into a legally binding outcome.

(b) Issuance of Award

The PDPC must formally issue the award within **twenty-one (21) days** from the receipt of the settlement agreement (Form No. 4).

(c) Legal Significance

The combined effect of Regulations 14(5) and 15 of the Complaints Settlement Regulations is that:

- mediation is not merely conciliatory;
- it is an enforceable dispute resolution mechanism; and
- it operates as a functional equivalent of adjudication, where successful.



(d) Relationship Between Investigation and Mediation

Mediation is not an independent stage; rather, it is embedded within and dependent on the investigation process.

Accordingly:

- investigation provides a factual and legal context;
- mediation leverages that context to facilitate settlement; and
- failure of mediation results in a referral to a hearing under Regulation 16 of the Collection and Processing Regulations.

2.3.3. Determination Stage

The determination stage constitutes the formal adjudicative phase of the complaint settlement process before the PDPC. It is triggered upon the failure of mediation and represents the point at which the dispute transitions from a facilitative process to a quasi-judicial determination.

This stage is governed primarily by **Part IV of the Complaints Settlement Regulations**, which establishes the procedural framework for the conduct of hearings, reception of evidence and determination of complaints.

2.3.3.1. Referral of Complaint to Hearing

Where mediation fails, the complaint is formally referred to the PDPC for hearing, and the PDPC must, within seven (7) days, notify the parties through a summons (Form No. 5) that the matter has been scheduled for hearing. This step marks a procedural transition from negotiation to adjudication.

2.3.3.2. Complaints Hearing Committee

Following an investigation and if an attempt at mediation is unsuccessful, the PDPC is tasked with forming a **Complaints Hearing Committee**. The PDPC appoints a Complaints Hearing Committee consisting of three members with expertise in:

- law;



- personal data protection; and
- information and communication technology (ICT)

This multidisciplinary composition reflects the technical and legal complexities of data protection disputes.

2.3.3.3. Amicus curiae

While the Committee is composed of these three experts, it has the flexibility to involve additional persons with specific expertise related to the complaint at hand as a friend of the committee to assist them reaching a just decision³².

2.3.3.4. Appearance, Consequences for Non-Appearance, and Remedy

Regarding representation during the hearings, the parties involved in the complaint have several options. Under Regulation 17(4), a party may appear:

- in person;
- through an advocate; or
- through an authorized representative

Proof of Authority³³

Where representation is used, the representative must produce proof such as:

- power of attorney;
- letter of authorization; or
- other prescribed documentation

Non-Appearance of Parties³⁴

Regulation 18 governs the consequences of failure to appear. In the event where both parties do not appear at the hearing, the complaint may be dismissed. However, where the complainant fails to appear, the complaint may be dismissed but where the

³² Regulation 17(3) of Collection and Processing Regulations.

³³ Regulation 17(5) of Collection and Processing Regulations.

³⁴ Regulation 18(1)–(3) of the Complaints Settlement Regulations.



respondent fails to appear, the PDPC may proceed with ex parte hearing upon application by the complainant.

Setting Aside Orders

A party affected by dismissal or ex parte orders during hearing may apply to PDPC, **within 30 days**, in writing (by way of letter) to set aside such orders upon showing sufficient cause³⁵.

2.3.3.5. Adjournments

During the hearing of the complaint, a party may apply to the committee for adjournment (orally or in writing) under Regulation 19 of the Complaint Settlement Regulations. The committee may grant adjournment where sufficient cause is shown, as the PDPC retains the discretion to refuse unjustified requests.

2.3.3.6. Participation of Third Parties in Proceedings

In addition to the primary parties (the complainant and the respondent), the complaint settlement framework under the PDPC permits the participation of third parties if the circumstances require it.

Such participation arises through two distinct procedural mechanisms, namely:

- third-party proceedings under Regulation 9 of the Complaint Settlement Regulations; and
- intervention under Regulation 20 of the Complaint Settlement Regulations.

These mechanisms serve different legal purposes but collectively ensure the proceedings before the PDPC are comprehensive, fair, and capable of determining all relevant issues.



³⁵ Regulation 18(4) of the Complaints Settlement Regulations.

(A) Third-Party Proceedings

Under Regulation 9(1) of the Complaints Settlement Regulations, a respondent who claims to be a person not originally a party to the complaint may apply to the PDPC for leave to present a third-party notice.

This mechanism enables the respondent to bring into the proceedings any person:

- against whom a claim arises out of the same subject matter of the complaint; and
- whose involvement is necessary for the complete and effective determination of liability.

Its core function is to avoid multiplicity of proceedings, ensure that liability is properly allocated, and enable claims for contribution, indemnity, or related relief to be determined within the same proceedings.

(i) Application to file Third-Party Notice

The respondent must initiate the process by filing a written application to file a Third-Party Notice to the PDPC. The application must contain:

- the name and address of the proposed third party;
- the nature of the complainant's claim against the respondent;
- the stage of the proceedings; and
- the nature of the respondent's claim against the third party, including its connection to the complaint.

(ii) Determination of Application for Leave

The PDPC shall grant leave to the respondent to file a third-party notice only where it is satisfied that:

- the claim against the third party is related to the subject matter of the complaint; and
- in light of all the circumstances, it is reasonable and appropriate to join a third party.



The PDPC retains the discretion to impose terms and conditions when granting such leave.

(iii) Third-Party Notice

Upon granting leave, the respondent shall present a third-party notice, which must comply with Regulation 9(4) of the Complaints Settlement Regulations.

The notice must expressly state:

- the nature of the complainant's claim against the respondent;
- the nature of the respondent's claim against the third party;
- the relief sought against the third party;
- the timeframe within which the third party must file a defense; and
- the consequences of failure to file a defense.

(iv) Service of Third-Party Notice

The PDPC is tasked with serving the third-party notice on the third party and the complainant using the modes of service prescribed under Regulation 6(2) of the Complaints Settlement Regulations.

(v) Defense by Third Party

A third party who wishes to dispute the claim must file a defense within **fourteen (14) days** from the date of service of the notice³⁶. Failure to file a defense within this period exposes the third party to default consequences.

(vi) Directions and Trial of Third-Party Liability

Where a third party files a defense, the PDPC shall fix a date for issuing directions³⁷. At this stage, the PDPC determines whether a proper question exists to be tried regarding the liability of the third party. If satisfied, the PDPC may order that the issue of liability

³⁶ Regulation 9(6) of the Complaint Settlement Regulations.

³⁷ Regulation 10 of the Complaints Settlement Regulations.



be tried together with the main complaint; or separately, at or after the hearing of the complaint.

Where the PDPC is not satisfied that a triable issue exists, it may:

- decline to proceed against the third party; or
- make such orders as the nature of the complaint may require.

(vii) Default and Ex Parte Award Against Third Party

There is a critical enforcement mechanism where a third party fails to comply with procedural obligations.

Default arises where the third party:

- fails to file a defense within the prescribed fourteen (14) days; or
- having filed a defense fails to appear at the directions stage.

In such circumstances, and where the respondent is found liable in the complaint, the respondent may file an ex parte application seeking an award against such third party. Upon consideration of the application and ex parte proof of the respondent's claim, the PDPC may issue a binding award against the third party in respect of the relief sought³⁸.

Generally, third-party procedures transform complaint proceedings from a bilateral dispute into a multiparty adjudicative process, ensuring that liability is not only determined but also correctly distributed.

(B) Intervention Proceeding

There is a formal mechanism through which a person who is not originally a party to a complaint may apply to participate in the proceedings as an intervener³⁹.

³⁸ Regulation 11(2) of the Complaints Settlement Regulations.

³⁹ Regulation 20 of the Complaints Settlement Regulations.



The right to intervene is available to any person with an interest in the complaint at any stage prior to the conclusion of the hearing.

The underlying objective of this provision is to ensure that proceedings before the PDPC are inclusive and informed by all materially affected interests and decisions are made based on a complete factual and legal matrix.

(i) Application for Intervention

An application for intervention must be made formally and in writing to the PDPC and must contain the following mandatory particulars:

- the date of application;
- the complaint number;
- the title of the complaint;
- the name, postal and physical address of the intervener;
- a concise statement of the matter in issue affecting the intervener;
- the party whose position the intervener intends to support; and
- the grounds for the application, together with supporting documents.

This requirement ensures that the application discloses the legal and factual basis of the interest claimed and the relevance of the intervener's participation in the dispute.

(ii) Notification and Right to Object

Upon receipt of the application, the PDPC shall notify all existing parties to the proceedings and any party to the complaint may file an objection to the intervention within **seven (7) days** from the date of receipt of such notice.

This procedural safeguard ensures that the intervention is subject to adversarial scrutiny and that frivolous, duplicative, or prejudicial interventions are filtered out at an early stage.



(iii) Determination of Application (Test for Intervention)

Under Regulation 20(4) of the Complaints Settlement Regulations, the Committee is required to assess whether the applicant is directly affected by the outcome of the complaint or the applicant's interest in the outcome is established and legally recognizable.

Therefore, the threshold is not merely abstract or speculative but a demonstrable, proximate, and substantive interest in the subject matter of the dispute. Where the Committee is satisfied that such interest exists, it may grant the application pursuant to Regulation 20(5) of the Complaints Settlement Regulations, subject to such terms and conditions as it considers appropriate.

(iv) Statement of Intervention

Where leave to intervene is granted, Regulation 20(6) of the Complaints Settlement Regulations imposes a mandatory obligation on the intervener to file a statement of intervention **within seven (7) days** from the date of the grant.

The statement must contain:

- particulars of the intervener, including relevant complaint details;
- the material facts of the complaint as they relate to the intervener;
- a succinct presentation of the facts and legal arguments supporting the intervention;
- the relief sought by the intervener; and
- a list and copies of the supporting documents relied upon.

This document functions as the intervener's primary pleading, defining the scope and basis of their participation.

(v) Reply To the Statement of Intervention

When a Statement of Intervention is filed with the PDPC, the existing parties to the complaint may file a **response** to the statement of intervention, jointly or severally **within**



seven (7) days from the date of receipt of the notice of application for Intervention from the PDPC. This ensures that the intervener's position is subjected to adversarial testing and that procedural balance between parties is maintained.

(vi) Role in Final Determination

Following the conclusion of the hearing, the Committee shall prepare and submit recommendations to the PDPC, considering the participation and submissions of all parties, including the intervener.

2.3.3.7. Procedural Flexibility and the Use of Other Laws

The complaint settlement framework under the PDPC is characterized by a degree of procedural flexibility designed to ensure that disputes are resolved effectively, fairly, and without undue technical rigidity.

At the determination level, Regulation 17(10) of the Complaints Settlement Regulations confers upon the Complaints Hearing Committee the authority to regulate its own procedure in circumstances where the Regulations do not expressly provide for a particular procedural issue. This provision recognizes the quasi-judicial nature of the proceedings before the PDPC and allows the Committee to adopt appropriate procedural mechanisms necessary for the just determination of complaints.

Such discretion enables the Committee to adapt its procedures to the specific circumstances of each case, including matters relating to the reception of evidence, conduct of proceedings, and management of the hearing process, provided that the principles of fairness and natural justice are observed.

Complementing this procedural flexibility, Regulation 30 of the Complaints Settlement Regulations vests the PDPC with broader residual powers to take any action that is necessary and permitted under the PDPA or any other relevant law to effectively and completely adjudicate on matters before it.



This provision has two significant implications.

- It allows the PDPC to fill procedural gaps where the Regulations are silent.
- It permits the application of other relevant legal frameworks, including the principles of civil procedure and administrative law, where appropriate.

Taken together, Regulations 17(10) and 30 establish a flexible and adaptive adjudicative system in which the PDPC is not constrained by strict procedural technicalities but is instead guided by the overarching objective of achieving substantive justice in personal data protection disputes.

Example;

A practical illustration of this procedural flexibility arose in ***Naumanga v. Mi Casa Company Ltd***, where parties rely on these provisions to address a procedural gap relating to the mode of taking evidence.

In this case, one of the witnesses was located outside the jurisdiction and could not physically attend the hearing. In the absence of express provisions under the Regulations governing remote testimony, the Committee was invited to exercise its discretion under Regulation 17(10) and adopt the procedures provided under the **Judicature and Application of Laws (Remote Proceedings and Electronic Recording) Rules, 2021**.

The request sought to allow the witness to testify through virtual means, thereby ensuring that material evidence was not excluded solely because of logistical constraints. This approach underscores the functional role of Regulation 17(10) as a mechanism for importing appropriate procedural frameworks where necessary and demonstrates how the PDPC may facilitate access to justice while maintaining procedural integrity.

2.3.3.8. Transition to Determination

Upon conclusion of the hearing, the Committee prepares recommendations, and the PDPC proceeds to issue a formal award.



2.3.4. Post-Determination Stage

The post-determination stage constitutes the final phase of the complaint settlement framework under the personal data protection regime. It commences upon the issuance of an award by the PDPC and is primarily concerned with the implementation, realization, and possible challenge of the award.

At this stage, the dispute transitions from adjudication to execution and post-adjudicative control, where the rights and obligations determined by the PDPC are either:

- enforced and realized by the successful party; or
- challenged or reconsidered by the aggrieved party.

Accordingly, the post-determination phase operates through a dual structure: enforcement mechanisms, aimed at giving practical effect to the award and corrective mechanisms, including review and appeal, are aimed at ensuring the legality, fairness, and accountability of the decision.

An award issued by the PDPC represents a final and binding determination of the rights and obligations of the parties concerning the complaint. Although rendered within a quasi-judicial administrative framework, such an award possesses the legal character of a decree of the High Court capable of execution and is not merely declaratory in nature.

2.3.4.1. Issuance of Award

The PDPC shall, upon receiving recommendations from the Complaints Hearing Committee, consider the same and issue a written award in respect of the complaint⁴⁰. It is the functional equivalent of a judgment in civil proceedings, albeit within an administrative framework.

An award represents:

- the final determination of the complaint;

⁴⁰ Regulation 21 of Complaints Settlement Regulations.



- the PDPC's findings on:
- liability;
- compliance with the PDPA; and
- entitlement to remedies.

Types of Reliefs and Remedies in an award

The PDPC is empowered to grant a range of remedies, including:

- **Corrective Measures:** These include orders requiring the respondent to rectify or correct personal data, suspend or restrict processing, erase or remove personal data, and destroy unlawfully processed data.
- **Compensation:** Under Section 37 of the PDPA, the PDPC may order compensation where there has been a contravention of the PDPA, and the data subject has suffered damage as a result. Damage includes financial loss and non-material harm, including reputational or privacy-related injury.
- **Ancillary Direction:** The PDPC may issue any other direction necessary to secure compliance or remedy the effects of unlawful processing.

2.3.4.2. Enforcement Notice

Where non-compliance is identified, Regulation 22 of the Complaints Settlement Regulations empowers the PDPC to issue an enforcement notice. The notice may require the respondent to take specific corrective actions and report compliance within 7 days and not more than 21 days. An enforcement notice operationalizes the award and creates a binding compliance obligation on the respondent.

2.3.4.3. Penalty Notice

Where a respondent fails to comply with an enforcement notice the PDPC may issue a penalty notice under Regulation 23 of the Complaints Settlement Regulations.

The penalty is part of the award and may include administrative fines or compensation orders, depending on the nature of the breach.



2.3.4.4. Taxation of Costs

Where costs are awarded, Regulation 27 of the Complaints Settlement Regulations governs their recovery through taxation proceedings before the PDPC. The successful party is required to file a bill of costs for taxation in accordance with the **Advocates Remuneration and Taxation of Costs Rules of 2015**⁴¹.

The PDPC examines, verifies, and assesses the bill of costs and determines whether the claimed costs are reasonable and properly incurred. Under Regulation 27(3) of the said Regulations, an aggrieved party may appeal the decision on taxation to the High Court.

2.3.4.5. Review of Decision

The power of review is conferred under Section 48 of the PDPA and Regulation 25 of the Complaints Settlement Regulations. Review constitutes an internal reconsideration mechanism, allowing the PDPC to revisit its own decisions or directions. It may be initiated upon application by an aggrieved party; or on the PDPC's own motion.

The purpose of the review is to correct errors, consider new or overlooked material and ensure that the decision accords with the law and justice.

- Procedure and Timeframes
 - An application for review must be lodged within twenty-one (21) days from the date of the award;
 - The application shall be made using Form No. 8.
 - Upon receipt, the PDPC shall determine the review within fourteen (14) days.
 - Upon review, the PDPC may affirm, vary, or alter the decision or revoke the decision entirely.

N.B.: The review must be conducted by officers different from those involved in the original determination to ensure impartiality.

⁴¹ Regulation 27(2) of Complaint Settlement Regulations.



The functional significance of a review is to be:

- a corrective and self-regulatory mechanism;
- a means of enhancing administrative fairness and accuracy; and
- a preliminary filter before resorting to judicial appeal.



TIER THREE:

2.4. Judicial Enforcement and Appeal

2.4.1. Procedures for Enforcement of Awards

Regulation 24 of the Complaints Settlement Regulations establishes the legal framework for the enforcement of the Award. An award of the PDPC is enforceable as if it were an order of the High Court⁴². This provision confers judicial enforceability on the award and access to formal execution mechanisms available under court processes.

Enforcement is initiated by the award holder in the following manner:

- the award holder shall apply to the High Court for the registration of the award.
- the application is made by way of a formal letter, accompanied by the award.
- upon registration the award assumes the status of a High Court decree, and
- becomes enforceable through established execution procedures.

Once registered, enforcement may be effected through attachment and sale of property, garnishee proceedings, or any other lawful execution mechanism available under civil procedure. This ensures that non-compliance with the award attracts coercive legal consequences.

The enforcement mechanism serves to:

- transform the PDPC's decision into a practically realizable remedy;
- ensure compliance with orders relating to:
- compensation;
- rectification or erasure of data; and
- alteration of data processing practices; and
- reinforce the authority and credibility of the PDPC.

⁴² Regulation 27(2) of Complaint Settlement Regulations.

⁴² Regulation 24(1) of Complaint Settlement Regulations.



2.4.2. Appeals

- Appellate Structure: The legal framework in Tanzania provides two principal avenues of appeal to the High Court:
 - Appeals under Section 49 of the PDPA: This applies to the administrative actions of the PDPC, including enforcement notices, penalty notices and regulatory directions.
 - Appeals under Regulation 26: This applies specifically to awards issued under Regulation 21.
- Timeframe for Appeal: An appeal must be filed within twenty-one (21) days from the date of the decision. This time limit is mandatory and ensures procedural efficiency and the finality of the proceedings.
- Nature of Appeal: An appeal to the High Court constitutes a process of judicial review and adjudication, whereby the Court examines the legality, correctness, and propriety of the PDPC's decision.
- The Court may uphold, vary or set aside the decision.

The post-determination stage represents the point at which adjudicative outcomes are either transformed into enforceable rights or subjected to legal scrutiny. Therefore, it is the stage where the authority of the PDPC is both realized and tested.



PART III

COMPARATIVE JURISPRUDENCE ON PERSONAL DATA PROTECTION ENFORCEMENT



3. COMPARATIVE JURISPRUDENCE ON PERSONAL DATA PROTECTION ENFORCEMENT

The personal data protection enforcement frameworks in Tanzania, Kenya, and the European Union (EU) share a common parentage in the principles of the EU General Data Protection Regulations (GDPR), yet their procedural and substantive jurisprudence has developed at markedly different speeds and depths. Tanzania enacted the PDPA in 2022, with operative Regulations following in 2023. Kenya preceded Tanzania by four years through the Data Protection Act No. 24 of 2019, while the EU has administered the GDPR since 25 May 2018. The resulting disparity in jurisprudential depth creates both a practical necessity and a legitimate basis for PDPC to draw on comparative precedents when exercising its procedural flexibility under Regulations 17(10) and 30 of the Complaint Settlement Regulations.

This Part identifies seven key enforcement gaps in Tanzania's current data protection framework and examines the position taken on each in Kenyan, EU, and other comparative jurisdictions. The analysis is structured around concrete legal issues that are either unresolved in Tanzanian jurisprudence or where the existing statutory framework is silent, ambiguous, or untested. The aim is not merely academic comparison but to provide practitioners, PDPC, and regulators with persuasive authority and practical guidance on how to approach these gaps.

It bears emphasis at the outset that the PDPC performs a hybrid quasi-judicial and regulatory role. When hearing and determining complaints between parties, the PDPC performs a statutory adjudicatory function involving the determination of rights and obligations under the PDPA, a character confirmed by the procedural structure of the Complaint Settlement Regulations and by the reviewer's emphasis on accuracy in describing the PDPC's role. The PDPC is not a criminal court and has no jurisdiction to entertain criminal offences established under the PDPA; those are matters for courts of



law and prosecution by the Director of Public Prosecutions. The enforcement issues examined in this Part relate exclusively to breaches of personal data principles and the civil remedial jurisdiction of the Commission.

3.1. The Quasi-Judicial Character of the Commission and the Legality of Its Adjudicatory Powers

Issue: Whether the PDPC's power to investigate and issue binding compensation awards constitutes judicial authority, and whether such powers are constitutionally permissible when vested in a non-court body.

3.1.1. Position in Tanzania

No Tanzanian court has yet directly addressed the constitutional validity of the PDPC's adjudicatory powers. Section 50 of the PDPA expressly authorises the PDPC to order compensation upon determination of a complaint. Regulation 21 of the Complaint Settlement Regulations makes the award binding, and Regulation 24 provides for its registration with the High Court as an arbitral decree enforceable through established civil execution procedures. The PDPA designates the PDPC as the primary forum for personal data disputes, with the High Court exercising an appellate and supervisory role under sections 48 and 49.

The PDPC's dual character regulatory supervisor and statutory dispute adjudicator has not been addressed in any Tanzanian judicial decision. However, the structure mirrors numerous other Tanzanian statutory bodies whose determinations are treated as administrative in nature and subject to review, including the Fair Competition Commission and the National Environment Management Council (**NEMC**). In those contexts, Tanzanian courts have consistently distinguished between administrative adjudication and constitutional judicial authority.



3.1.2. Kenyan Comparative Authority

In *Arunda v Office of the Data Protection Commissioner & another; Data Privacy and Governance Society of Kenya (Interested Party)* (Constitutional Petition E010 of 2025) [2025] KEHC 12262 (KLR) (12 August 2025), the Kenyan High Court (Mwamuye J.) addressed precisely this question. A petitioner argued that the Office of the Data Protection Commissioner (herein **ODPC**) had unconstitutionally assumed the jurisdiction of the High Court by receiving complaints, investigating breaches, and issuing binding compensation awards powers which, the petitioner contended, constituted judicial authority exclusively vested in the High Court under Articles 23(1) and 165(3)(b) of the Kenyan Constitution.

The High Court dismissed the petition. The Court held that the ODPC performs administrative and quasi-judicial functions grounded in the Data Protection Act, not functions amounting to the exercise of constitutional judicial authority. The Court observed that the ODPC's powers are akin to those of other regulatory agencies the Communications Authority, the Competition Authority, and the Kenya Revenue Authority all of which operate under statutes permitting enforcement actions subject to judicial review. The ODPC does not issue declarations of constitutional rights; it investigates factual complaints and applies the statutory framework to provide regulatory redress. The availability of an appeal to the High Court under section 64 of the Data Protection Act was identified as the constitutional safeguard: the ODPC's decisions are administrative determinations, not final judicial orders.

For Tanzania, this reasoning directly supports the PDPC's exercise of its adjudicatory functions. The parallel is close: section 49 of the PDPA provides for appeal to the High Court against the PDPC's decisions, and Regulation 26 provides for appeal against awards precisely the judicial oversight that the Kenyan court identified as constitutionally sufficient.



3.1.3. EU Comparative Context

Under the GDPR, each EU Member State must establish an independent supervisory authority with power to receive complaints, investigate, and issue binding administrative decisions including fines. The Court of Justice of the European Union has consistently upheld these arrangements on the basis that decisions remain subject to judicial review under GDPR Article 78, which guarantees effective judicial remedies against binding supervisory authority decisions. The EU framework treats data protection regulators as administrative bodies performing functions analogous to specialised regulatory tribunals, not courts of law.

This gap in Tanzanian jurisprudence and the absence of any decided case affirming the constitutional legitimacy of the PDPC's adjudicatory powers may leave practitioners uncertain. As Tanzania's jurisprudence develops, the reasoning in *Arunda* and the EU supervisory authority framework provide strong persuasive guidance that the PDPC's powers are constitutionally sound, provided that rights of appeal to the High Court are preserved and exercised.

3.2. Exhaustion of Administrative Remedies: Tanzanian Decisions and Their Limits

Issue: Whether a data subject must exhaust available administrative remedies before the PDPC before approaching the High Court, and what documentary evidence of such exhaustion is required.

3.2.1. Tanzanian Decisions

Two High Court decisions decided on 15 March 2024 establish Tanzania's baseline position but also expose an unresolved tension.



In *Alexander J. Barunguza v Personal Data Protection Commission, Law School of Tanzania & Attorney General*, Misc. Civil Cause No. 56 of 2024 (High Court of Tanzania, Dar es Salaam, 4 October 2024), the High Court (Mango J.) struck out an appeal because the appellant had failed to attach the Commission's prior determinations. The Court held that jurisdiction before the appellate court cannot be presumed and must be established by documentary proof that the statutory administrative process was properly invoked and concluded. Conclusory assertions of compliance are insufficient; documentary proof is required.

In *Fatna Faradji Kayuga v MIC Tanzania (PLC) Ltd*, Civil Case No. 125 of 2023 (High Court of Tanzania, 15 March 2024), the High Court struck out the plaintiff's suit on the ground that the PDPA confers exclusive jurisdiction on the PDPC to receive and determine personal data complaints and to order compensation under section 50. Filing an original suit in the High Court before any PDPC determination was premature. The Court further held that a right of appeal to the High Court against the PDPC's decision is available under section 49, and that a party must exhaust those remedies before resorting to the court.

Together, these decisions establish two limbs of the exhaustion doctrine: (i) the data subject must invoke the PDPC's complaint process before courts can assume jurisdiction; and (ii) evidence of having done so, by exhibiting the PDPC's determinations, is indispensable at the appellate stage.

3.2.2. Where Exhaustion Was Not Required

In *Sayida Daud Masanja Versus Vodacom T. Public Ltd Co.* (Civil Case No. 06 of 2023) [2024] TZHC 1240 (15 March 2024), the High Court held that where a cause of action is framed as a tort of negligence and where the PDPC was not yet operationally established at the time of filing, the court retains original jurisdiction. This decision introduces a nuance: the exhaustion doctrine does not apply where the PDPC's mechanism was unavailable or where the claim is a genuine parallel private law tort.



This tension between the *Kayuga* and *Masanja* lines of authority is an unresolved gap in Tanzanian jurisprudence. The *Kayuga* court's emphasis on the PDPC's power to order compensation as the decisive factor suggests that where the PDPA's remedial framework is adequate and available, exhaustion is mandatory regardless of how the claim is framed.

3.2.3. Kenyan Comparative Authority on Regulatory Timelines

In *Gichuhi & 2 others v Data Protection Commissioner; Mathenge & another (Interested Parties)* (Judicial Review E028 of 2023) [2023] KEHC 17321 (KLR) (12 May 2023), the Kenyan High Court quashed a complaint determination made by the ODPC outside its statutory 90-day period and issued a mandamus requiring readmission and fresh determination within the correct timeframe. This decision confirms that exhaustion operates in both directions: complainants must use the administrative remedy, but the regulator must also observe its own statutory timelines or face judicial correction.

In *Regus Kenya Limited v Data Protection Commissioner & another* (Civil Appeal E472 of 2023) [2025] KEHC 13491 (KLR) (30 September 2025), the Court clarified that Kenya's 90-day statutory period begins from the date of formal admission of the complaint, not from lodgement a distinction that meaningfully extends the regulator's working window. Tanzania's PDPA does not impose an equivalent overarching deadline on the PDPC's final determination, which creates an accountability gap that the PDPC should address through published service delivery standards under its administrative discretion.

3.3. Respondent Silence and Inaction: The Commission's Power to Proceed

Issue: Where a respondent receives notice and summons but fails to respond or appear, can the Commission proceed to determination, and on what legal basis?



3.3.1. Tanzanian Position

In *Abdul Said Naumanga v Mi Casa Company Limited* (Complaint No. PDPC/CMP/014/2024), the PDPC determined a complaint against a Dar es Salaam entertainment establishment that had posted photographs and videos of the complainant, a lawyer, on Instagram without consent. After the company failed to respond to summons or appear at the hearing, the PDPC proceeded ex parte, treating the respondent's silence as a waiver of the right to be heard. The PDPC found in the complaints favour and awarded TZS 20,000,000 in compensation.

This determination confirms the PDPC's authority under Regulations 7(3) and 18(3) of the Complaint Settlement Regulations to proceed where a respondent has been properly served but chooses not to engage. The award is binding, not advisory, and is enforceable as an arbitral decree registered at the High Court.

A critical terminological point: under section 84 of the Arbitration Act and the structure of the Complaint Settlement Regulations, a Commission award, once registered at the High Court, takes the status of a decree not a judgment. Practitioners filing for enforcement of a Commission award must proceed by way of registration and execution of a decree, not by way of enforcement of a judgment.

3.3.2. Kenyan Comparative Authority

In *Regus Kenya Limited v Data Protection Commissioner* [2025] KEHC 13491 (KLR), the ODPC issued enforcement and penalty notices against Regus after the company ignored multiple complaint notifications. The High Court upheld the ODPC's jurisdiction to act against an unresponsive party, confirming that silence does not give rise to procedural prejudice in favour of the respondent. The Court also confirmed that the burden of proving valid consent rests on the data controller; a respondent cannot escape liability by failing to participate.



3.3.3. The Investigative Power and Its Independence from the Defence

A practical question arises whether the PDPC's investigative powers under sections 41-42 of the PDPA are triggered only after receipt of a defence, or whether they may be exercised independently. Regulation 13(3) of the Complaint Settlement Regulations which empowers the PDPC during or after investigation to require a controller to reconsider a complaint within 14 days supports the purposive view that investigative authority is independent of whether a defence has been filed. Where a respondent waives the right to file a defence, the PDPC may investigate without respondent involvement and thereafter appoint a hearing committee to hear the matter *ex parte*. The Kenyan position in *Regus*, where enforcement notices were validly issued against a party that had not engaged at all, reinforces this approach.

3.4. The Scope of Personal Data: Image Rights and the Boundary of the Commission's Jurisdiction

Issue: Whether the unauthorised use of a person's photograph on social media constitutes processing of personal data subject to the PDPC's jurisdiction, and how conflicting administrative and judicial approaches should be reconciled.

3.4.1. Divergent Tanzanian Approaches

In *Nyangoma Mwesingwa v Cecilia Maliganya* (PDPC Complaint No. PDPC/CMP/002/2025), the PDPC held that a minor's photograph published on social media without parental consent constituted personal data and that its publication amounted to unlawful processing. The PDPC applied a broad, purposive interpretation of personal data, emphasising heightened protection for children's data, and ordered removal of the images and payment of compensation.

By contrast, in *Fred Fabian Ngajiro @ Fred Vunjabei vs Multichoice Group Limited and Others* (Civil Appeal No. 32046 of 2024) [2025] TZHC 6615 (28 October 2025), the High Court declined to apply the PDPA to the use of a person's image on television and social media,



finding that no traditional data controller-processor relationship existed and that the relevant conduct did not constitute “processing” as contemplated by the Act.

This divergence represents a significant jurisprudential gap: two bodies applying the same Act to factually analogous situations the unauthorised public dissemination of a person’s image have reached opposite conclusions on the PDPA’s applicability. Until a higher court resolves this conflict, practitioners face uncertainty about the correct forum and the appropriate legal framework for image rights disputes in Tanzania.

3.4.2. Kenyan Comparative Authority

The ODPC has consistently treated photographic images as personal data. In a 2023 enforcement action, the ODPC imposed a penalty of KES 4,550,000 on a school for posting images of minors without parental consent, the highest single penalty issued in that enforcement round. The ODPC has also imposed penalties on restaurants and other commercial entities for posting images of customers or employees without consent. This approach is consistent with the broad definition of personal data under the Kenyan Data Protection Act and reflects the PDPC’s purposive interpretation applied in *Nyangoma Mwesingwa*.

3.4.3. EU Comparative Context: Joint Controllership and the Fashion ID Principle

In *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* (Case C-40/17) [2019] ECLI:EU:C:2019:629 (Court of Justice of the European Union, 29 July 2019), the CJEU held that a German online clothing retailer who embedded a Facebook “Like” button on its website became a joint controller with Facebook in respect of the collection and transmission of website visitors’ personal data. The Court adopted a broad view of joint controllership: where a website operator installs a plugin that causes personal data to be transmitted to a third party, and where the operator derives commercial benefit from that transmission, the operator jointly determines the purpose and means of the processing, even though subsequent processing by the third party is beyond the operator’s control.



This decision has important implications for Tanzania's multi-party data disputes. The PDPC's authority under Regulation 9 of the Complaint Settlement Regulations to permit a respondent to add a third party from whom contribution may be sought is directly consistent with the *Fashion ID* approach: multiple actors may be jointly liable as data controllers, and a respondent cannot escape liability by pointing to a co-responsible third party. The procedure of adding a third party prevents multiplicity of suits and ensures comprehensive accountability in a single proceeding.

3.5. Challenging Non-Admission Decisions: Review, Appeal, and Judicial Review

Issue: Where the PDPC declines to admit a complaint, what recourse is available to the complainant, and in what sequence must remedies be pursued?

3.5.1. Tanzanian Position

Regulation 5(4) of the Complaint Settlement Regulations provides that where a complaint is not admitted following initial review, the complainant may apply for review under section 48 of the PDPA. This is the primary statutory remedy against a non-admission decision. Section 48 grants the Commission power to review its own decisions on application by an aggrieved party or on its own motion, within 21 days of the decision, and requires that the review be conducted by officers different from those involved in the original determination.

Only after exhausting the review mechanism would it be appropriate to consider appeal to the High Court under section 49, and judicial review remains a remedy of last resort available only where no adequate statutory remedy exists. No Tanzanian court has yet decided a case on the specific procedural pathway for challenging a Commission non-admission decision, which represents a practical gap for complainants.



3.5.2. Kenyan Comparative Authority

In *Ceres Tech Limited v Commissioner, Office of the Data Protection Commissioner* (Judicial Review Application 25 of 2024) [2024] KEHC 12833 (KLR) (24 October 2024), the Kenyan High Court struck out a judicial review application filed by a data controller challenging an ODPC determination. The Court held that the applicant had bypassed the statutory appellate route provided under section 64 of the Data Protection Act and that filing for judicial review instead of appeal was an abuse of process. Statutory review and appeal must be exhausted before judicial review will lie.

This principle applies equally to complainants challenging non-admission decisions. In *Republic v Data Protection Commissioner; Hotel Waterbuck Limited* (Judicial Review E011 of 2024) [2025] KEHC 5801 (KLR) (5 May 2025), the High Court reiterated that where statute provides a specific mechanism for seeking a remedy, that mechanism must be followed and judicial review is not available as an alternative route. The Court expressly endorsed its earlier decisions in *Ceres Tech* and held that complaints against ODPC decisions must be channeled through the statutory routes.

3.5.3. Comparative Context: Right to an Effective Remedy

Under GDPR Article 78, individuals have the right to an effective judicial remedy against a supervisory authority that refuses to handle their complaint or fails to inform them of progress within three months. The EU's GDPR Procedural Regulation (Regulation (EU) 2025/2518, entered into force November 2025) further formalises these complainant rights in cross-border cases. The underlying principle that a complainant whose complaint is not admitted must have a clear, accessible, and effective procedural pathway to challenge that decision is equally applicable in Tanzania.

For Tanzanian practitioners, the correct sequence where a complaint is not admitted is: first, apply for review under section 48 and Regulation 5(4); if review is refused or fails, appeal under section 49 to the High Court. Judicial review is available as a final backstop



only where the statutory remedies are inadequate, unavailable, or have been exhausted without relief.

3.6. The Binding Force and Execution of Commission Awards

Issue: What is the legal status and enforceability of a Commission award, and how does it compare to court orders?

3.6.1. Tanzanian Position

A Commission award following complaint determination is binding. It is neither advisory nor recommendatory. Regulation 24(1) of the Complaint Settlement Regulations provides that a party may apply to the High Court to register the award, and upon registration, it is treated as a court decree and may be executed through all available civil execution procedures, including attachment and sale of property and garnishee proceedings.

Two terminological points merit emphasis. First, the award is registered as a **decree**, not as a judgment: practitioners filing registration applications should use the correct characterisation consistent with section 84 of the Arbitration Act, Cap 15 R.E. 2022. Second, while the PDPC may issue enforcement and penalty notices as part of its regulatory (rather than adjudicatory) function, the monetary award arising from a complaint determination is a civil remedy and must not be confused with criminal sanctions under sections 60-63 of the PDPA, which are within the exclusive jurisdiction of criminal courts.

3.6.2 Kenyan Comparative Authority

In *Regus Kenya Limited v Data Protection Commissioner* [2025] KEHC 13491 (KLR), the Kenyan High Court treated the ODPC's enforcement notices and penalty notice as binding legal instruments, reducing the penalty on appeal from KES 5,000,000 to KES 2,500,000 as a matter of proportionality. The Court confirmed that the Commissioner



was within the law in imposing the administrative fine and that the reduction on appeal was a matter of calibrating proportionality, not of invalidating the ODPC's authority. This confirms that data protection authority orders are binding civil determinations subject to proportionate appellate review, a principle directly applicable to Tanzania's PDPC.

3.7. Proportionality in Compensation and Penalty Assessment: An Emerging Gap

Issue: What principles should guide the PDPC in quantifying compensation and sanctions, and how should proportionality be assessed in the absence of legislative guidance?

3.7.1. Current Tanzanian Gap

The PDPA and Complaint Settlement Regulations do not prescribe a detailed methodology for quantifying compensation in personal data breach cases. Section 50 authorises the PDPC to order “appropriate compensation” but provides no further guidance. The award of TZS 20,000,000 in *Naumanga v Mi Casa* was made on the facts without reference to any published quantification criteria. As the volume of complaints grows, the absence of a published methodology creates inconsistency and undermines the predictability of PDPC awards.

3.7.2. Kenyan Comparative Authority

The Kenyan ODPC has imposed fines ranging from KES 250,000 for minor breaches to KES 5,000,000 for systematic violations. In *Regus Kenya Limited* [2025] KEHC 13491 (KLR), the High Court conducted a proportionality analysis balancing: the nature and gravity of the breach (unsolicited marketing communications); the respondent's status as a first-time offender; the need for deterrence; and the commercial context of the relationship between the parties. This multi-factor proportionality analysis provides a practical template for Tanzania's PDPC to adopt in assessing compensation.



3.7.3. EU Framework for Proportionate Penalties

GDPR Article 83 prescribes eight factors for proportionate administrative fines: the nature, gravity, and duration of the infringement; whether it was intentional or negligent; action taken to mitigate damage; the degree of controller or processor responsibility; previous infringements; the degree of cooperation with the authority; the categories of personal data affected; and how the authority became aware of the violation. While Tanzania is not bound by the GDPR, this framework represents the most thoroughly developed comparative methodology for proportionate penalty assessment. The PDPC may, in the absence of domestic legislative guidance, use Regulation 17(10) of the Complaint Settlement Regulations which grants flexibility to adopt appropriate procedures where the Regulations are silent to develop and publish an internal quantification methodology aligned with these comparative principles.

3.8. Legislative and Regulatory Gaps Requiring Development

3.8.1. Cross-Border Processing and Multi-Jurisdictional Enforcement

Tanzania's PDPA does not yet contain a detailed framework governing situations where a data controller is established outside Tanzania but processes the personal data of Tanzanian residents, or where a breach involves controllers or processors in multiple jurisdictions. This gap will become more pressing as digital commerce, mobile banking, and cloud services expand the jurisdictional footprint of data controllers operating in Tanzania. The EU's GDPR Procedural Regulation (Regulation (EU) 2025/2518), which harmonises cooperation mechanisms between EU supervisory authorities in cross-border cases, represents current best practice. Tanzania's PDPC may look to these provisions for guidance on cooperation principles, even in the absence of formal bilateral arrangements.



3.8.2. Consent in the Digital Economy

A recurring theme in Kenyan and EU enforcement is the standard of proof for valid consent to data processing in digital commercial contexts particularly for unsolicited marketing, digital lending, and website analytics. In *Regus Kenya Limited* [2025] KEHC 13491 (KLR), the Court confirmed that the burden of proving consent rests on the data controller, and that the termination of a commercial relationship extinguishes any consent previously given for marketing purposes. As Tanzania's digital economy expands, these consent principles will become increasingly important to PDPC adjudication. The PDPC's published determinations when they address these issues will form the foundation of Tanzania's own jurisprudence in this area.

3.9. Conclusion

Tanzania's personal data protection enforcement framework is in an early but active developmental phase. The PDPC has commenced adjudicatory work, the High Court has begun to define the boundaries of its supervisory jurisdiction and practitioners are navigating a landscape shaped by primary decisions. The seven enforcement gaps and comparative issues examined in this Part illuminate the frontier questions that will define the next phase of Tanzania's data protection development.

The central comparative lesson is that effective enforcement depends on three reinforcing elements: a Commission that exercises its adjudicatory functions with confidence and consistency; a court system that provides principled supervisory oversight without displacing the PDPC's primary jurisdiction; and a body of precedent that gives practitioners and data subjects sufficient certainty to use the system effectively.

Kenya's more mature jurisprudence anchored in a shared legislative heritage provides the most directly persuasive comparative authority for Tanzanian practitioners and adjudicators. The GDPR framework and CJEU decisions provide higher-level conceptual



authority on questions of joint controllership, proportionality in penalty assessment and the constitutional legitimacy of specialist regulatory bodies. Both sources of authority are available to the PDPC under Regulations 17(10) and 30 of the Complaint Settlement Regulations, which grant flexibility to adopt appropriate procedures where the Regulations are silent and to apply general principles of law and equity.



REFERENCES

Legislation

Data Protection Act, 2019 of Kenya

General Data Protection Regulation, EU 2016/679

Law of Contract Act, Cap 345

Personal Data Protection Act, 2022 of Tanzania

Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023

Personal Data Protection (Complaint Settlement Procedures) Regulations, 2023

Judicature and Application of Laws (Remote Proceedings and Electronic Recording) Rules, 2021.

Case Law

Musa Shaibu Msangi v Sumry High Class Ltd and Another [2016] TLS LR 430

Abdul Said Naumanga v Mi Casa Company Limited. Complaint No. PDPC/CMP/014/2024

Alexander J. Barunguza v Personal Data Protection Commission, Law School of Tanzania & Attorney General, Misc. Civil Cause No. 56 of 2024 (High Court of Tanzania, Dar es Salaam, 4 October 2024)

In Fatna Faradji Kayuga v MIC Tanzania (PLC) Ltd, Civil Case No. 125 of 2023 (High Court of Tanzania, 15 March 2024)

Nyangoma Mwesingwa v Cecilia Maliganya, PDPC Complaint No. PDPC/CMP/002/2025

Fred Fabian Ngajiro @ Fred Vunjabei vs Multichoice Group Limited and Others (Civil Appeal No. 32046 of 2024) [2025] TZHC 6615 (28 October 2025),

Sayida Daud Masanja Versus Vodacom T. Public L.t.d Co. (Civil Case No. 06 of 2023) [2024] TZHC 1240 (15 March 2024),

Gichuhi & Others v Data Protection Commissioner; Mathenge & Another [2023] eKLR

Regus Kenya Limited VS Data Protection Commissioner and James Ndungo [2025] KEHC 13491 (KLR):

Fashion ID GmbH & Co KG Versus Verbraucherzentrale NRW, ECLI: EU:C:2019:629,



Ceres Tech Limited v. The Commissioner, Office of The Data Protection Commissioner,
Judicial Review Application Cause No. 25 of 2024

Redempta Akoth Agwanda v. The office of the Data Protection Commissioner, Judicial
Review Application No. E103 Of 2025

Additional Resources

Complaint Form. Retrieved from <https://dataprotection.pdpc.go.tz/complaint-form-one>

