



Personal
DATA
Protection
OFFICE

THE REPUBLIC OF UGANDA
IN THE MATTER OF THE DATA PROTECTION AND PRIVACY ACT, CAP 97
COMPLAINT NO: PDPO 096/2025

MUZIRA PATRICK MARK:.....COMPLAINANT

VERSUS

NATIONAL IDENTIFICATION AND REGISTRATION AUTHORITY (NIRA) :.....RESPONDENT

DECISION OF THE PERSONAL DATA PROTECTION OFFICE (PDPO)

Having reviewed the complaint lodged with the Personal Data Protection Office on 11th July 2025, alleging that the National Identification and Registration Authority unlawfully refused the Complainant access to personal data held in the National Identification Register relating to Mr. Kabunga George William and nine other individuals, ten data subjects in all, contrary to the Data Protection and Privacy Act, Cap 97 and the Data Protection and Privacy Regulations, 2021, the decision of the Personal Data Protection Office is as follows:

A. INTRODUCTION

1. This is a complaint lodged with the Personal Data Protection Office (“the Office”) on 11th July 2025 by Muzira Patrick Mark (“the Complainant”), through his advocates, M/s Sebanja & Co. Advocates, against the National Identification and Registration Authority (“NIRA” or “the Respondent”). The complaint was lodged on Form 11, the form prescribed by Regulation 41(2) of the Data Protection and Privacy Regulations, 2021.
2. In substance, the Complainant alleges that NIRA unlawfully refused him access to records held in the National Identification Register relating to Mr Kabunga George William and nine other named individuals, ten data subjects in all, by insisting upon their consent, or in the alternative, a court order, and upon compliance with the Registration of Persons (Access and Use of Information) Regulations, 2015. The Complainant says the records are required to expose allegedly fraudulent claims to the estate of the late Latima Mujankondo Sendagala, and to land at Singo Block 161, Plot 365, Mityana District; to



support an investigation said to be before the Criminal Investigations Directorate at Kibuli vide CRB 229/2023; and to prepare a civil suit. He contends that the refusal contravenes Sections 7(2)(b)(iii), 11(2)(e), 13(3) and 24 of the Data Protection and Privacy Act, Cap 97.

3. NIRA's position, taken in correspondence, is that access to information in the National Identification Register by a person other than a Government Ministry, Department or Agency is governed by Section 67 of the Registration of Persons Act, Cap 332 and the Registration of Persons (Access and Use of Information) Regulations, 2015, which require a duly completed application, payment of the prescribed fee, and the consent of the person whose information is sought, unless a recognised statutory ground for dispensing with consent applies. NIRA maintains that those requirements were not met.
4. PDPO has considered the complaint, the Parties' written submissions, and the annexed materials to their respective responses. This decision is rendered under Regulation 45(2) of the Data Protection and Privacy Regulations, 2021.

B. THE PARTIES/REPRESENTATION

5. The Complainant is an adult Ugandan who describes himself as a grandchild and beneficiary of the estate of the late Daniel Kalumba. He is represented by M/s Sebanja & Co. Advocates, who filed the complaint and the subsequent correspondence on his behalf.
6. The Respondent, NIRA, is the body corporate established by Section 4 of the Registration of Persons Act, Cap 332, and is responsible for the creation, management, maintenance and operation of the National Identification Register as stipulated under Section 5 of the said law. It is a "public body" within the meaning of Section 2 of the Data Protection and Privacy Act, Cap 97, and, in relation to the Register, a "data controller" within that section. NIRA responded to the complaint by a letter to the Office signed by its Manager Compliance and Enforcement; its earlier correspondence on the access request was signed by its Manager Legal and Advisory Services. NIRA did not enter a formal appearance and made no oral submissions; its position is taken from its letters.



7. The persons whose records are sought, Mr. Kabunga George William and nine other named individuals, are not parties to this complaint and have not been notified of it or heard. They are referred to in this decision, only so far as necessary, as “the third-party data subjects”. To protect their rights under the Data Protection and Privacy Act, Cap 97, this decision does not reproduce their national identification numbers, dates of birth or other biographical particulars, and treats the allegations made against Mr. Kabunga as untested allegations only.

C. EVIDENCE

8. The Complainant relied on the following materials:
- (i) the complaint, Form 11, dated 11th July 2025;
 - (ii) access request forms addressed to NIRA dated 11th June 2025 and 27th June 2025;
 - (iii) a request to the Administrator General dated 10th June 2025;
 - (iv) a letter reinforcing the request dated 20th June 2025;
 - (v) a statutory declaration by the Complainant vide Instrument No. 1750312196170 sworn on 17th June 2025;
 - (vi) a clarification letter dated 8th July 2025 attaching a revised application under the Registration of Persons legal regime and a Uganda Revenue Authority payment registration slip, No. 2260000384093, dated 8th July 2025 in the sum of UGX 50,000 for ten records;
 - (vii) a rejoinder dated 15th August 2025; and annexures, namely a letter from Nakayiza Esther to the Criminal Investigations Directorate requesting transfer of the file, a copy of a purported Letter of Probate, referenced High Court Administration Cause No. 1296 of 2012, a letter from the Registrar of the High Court dated 20th August 2024 stating that the file is not available in the central archives, a petition and Letters of Administration from the Chief Magistrate’s Court at Mityana, Administration Cause No. 176 of 2017, and copies of national identity cards.

9. The Respondent relied on the following materials in support of its response: —



- (i) A letter dated 1st July 2025 vide Ref NIRA/DL/01/07/25/483, and
- (ii) NIRA's response to the Office vide Ref NIRA/DL/01/08/25/075, together with Section 67 of the Registration of Persons Act, Cap 332 and the Registration of Persons (Access and Use of Information) Regulations, 2015.

D. PRELIMINARY MATTERS

10. This decision summarizes the Parties' positions and refers to submitted materials only to the extent necessary for the findings and orders made herein. PDPO does not publish any personally identifiable details, or internal operational documentation that is not necessary for this determination.
11. In determining the issues before it, PDPO assesses the facts on the balance of probabilities and draws reasonable inferences from the documentary record. Where an allegation is pleaded without supporting evidence beyond assertion, PDPO may decline to make an adverse factual finding.
12. The standard of proof does not rise with the seriousness of an allegation; rather, the more serious the allegation, the more cogent the evidence required to establish it. Where the complaint raises an arguable contravention of the Act, the evidential burden rests on the data controller, processor or collector to demonstrate compliance, including, where relevant, the validity of any consent relied on, the necessity of the processing, and the existence of any exemption invoked.
13. The Data Protection and Privacy Act, Cap 97 gives statutory effect to the right to privacy. Article 27 of the Constitution provides:
- (1) No person shall be subjected to—
 - (a) unlawful search of the person, home or other property of that person; or
 - (b) unlawful entry by others of the premises of that person.
 - (2) No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property.



14. That right is, by Article 43 of the Constitution, subject only to such limits as are acceptable in a free and democratic society and as do not prejudice the rights of others or the public interest. The consent regime that the Complainant challenges is an expression, not a denial, of that constitutional value.
15. Decisions of foreign courts and data protection and privacy regulators, and the guidance of bodies such as the European Data Protection Board, do not bind this Office merely because they are foreign or comparative sources. The Office does not, however, ignore them. Where a source states a principle of common law or equity applicable in Uganda, or states a comparative principle that fits the text and purpose of the Data Protection and Privacy Act, Cap 97 and its Regulations, the Office examines the principle, tests it against Uganda's written law and circumstances, and applies or adopts it to the extent appropriate.
16. The Office has also considered the Complainant's allegation regarding the timing of NIRA's response to the Office's notice of 24th July 2025. Since NIRA responded, the Complainant filed a rejoinder on 15th August 2025, and no material procedural prejudice has been demonstrated, the Office has determined the complaint on its merits.

E. ISSUES FOR DETERMINATION

17. PDPO considers that the following **four (4)** issues arise for determination:

Issue 1: Whether the statutory right of access to personal data may be used by one person to obtain another person's data, or is confined to a person's access to his or her own personal data.

Issue 2: Whether NIRA acted unlawfully in requiring the consent of the persons concerned, or a court order, before releasing National Identification Register records to a private applicant.

Issue 3: Whether the exemptions for the investigation of offences and for contemplated court proceedings can be relied upon to compel NIRA to disclose the personal data of third parties without their consent.

Issue 4: Whether the Complainant is entitled to the remedies sought.

F. RESOLUTION OF ISSUES

Issue 1: Whether the statutory right of access to personal data may be used by one person to obtain another person's data, or is confined to a person's access to his or her own personal data.

Submissions of the Complainant

18. The Complainant relied on Section 24(1) of the Data Protection and Privacy Act, Cap 97 and Regulation 35 of the Data Protection and Privacy Regulations, 2021. He placed particular reliance on Section 24(4)(b), and submitted that the disclosure of personal data relating to another individual is permitted where it is reasonable in all the circumstances. On that basis, he contended that NIRA wrongly denied him access to the records he requires to verify the alleged fraud.

Submissions of the Respondent

19. NIRA treated the request as an application by a person who is not the data subject, governed by the Registration of Persons Act, Cap 332 and the Registration of Persons (Access and Use of Information) Regulations. NIRA did not address Section 24 of the Data Protection and Privacy Act, Cap 97.

Determination

20. The Complainant's argument under this issue turns on whether Section 24 creates a right of access to one's own personal data, or whether it can be used by one person to obtain the personal data of another. The starting point is the language of Section 24 itself.



21. Section 24(1) provides that a data subject who provides proof of identity may request a data controller to confirm whether it holds personal data about that data subject, to give a description of the personal data held, and to provide the identity of a third party or category of third party who has or has had access to the information. Section 24(2) requires the request to be made in the prescribed form and manner. Section 24(3) allows the data controller to require sufficient information to identify the person making the request and to locate the data requested by that person.
22. Section 24(4) then deals with a specific problem that may arise in the course of responding to a valid access request made by a data subject. It provides that where the controller is unable to comply with the request without disclosing data related to another individual who may be identified from the information, the controller shall not comply with the request unless the other individual consents to the disclosure, or it is reasonable in all the circumstances to comply without that consent, or the disclosure is compelled by a court order.
23. Regulation 35 of the Data Protection and Privacy Regulations, 2021 confirms that interpretation. Regulation 35(1) provides that a request by a data subject to a data controller to confirm whether the controller holds personal information on that data subject shall be made in Form 8 in Schedule 1. Regulation 35(2) provides that, for purposes of Section 24(1) of the Act, the data subject satisfies the proof of identity requirement by providing a national identification card or alien's identification card, a passport or other travel document, or a driver's licence.
24. Read literally and purposively, Section 24 and Regulation 35 confer a right exercisable by a data subject in respect of that data subject's own personal data. Section 24(4) is not an independent gateway by which a stranger may obtain another person's personal data. It is a protective provision that applies where a controller is dealing with a valid access request by a data subject and discovers that compliance with that request would necessarily disclose data related to another identifiable individual.



25. The interpretation is supported, as persuasive authority only, by **Durant v Financial Services Authority [2003] EWCA Civ 1746**. In that case, the English Court of Appeal held, in construing a similar subject access framework under the United Kingdom Data Protection Act 1998, that a data subject access request is concerned with information constituting the requester's own personal data. It is a right which exists to enable an individual to check whether his or her own personal data is held and processed lawfully and accurately; it is not to be used as a means of obtaining information for litigation against others. The Office adopts that reasoning as persuasive and consistent with the text and purpose of Section 24 of the Data Protection and Privacy Act, Cap 97.
26. Applied to the present complaint, the Complainant is not the data subject in respect of the NIRA records he seeks. The records relate to Mr. Kabunga George William and nine other data subjects. The Complainant has not presented a request made by those data subjects, nor proof of identity supplied by them for purposes of Section 24(1) and Regulation 35. He cannot convert their personal data into his own personal data by asserting an interest in verifying suspected fraud.
27. The Complainant's reliance on Section 24(4)(b) therefore fails at the threshold. The "reasonableness" test in Section 24(4)(b) arises only where a controller is dealing with a valid access request by a data subject for that data subject's own personal data, and where compliance with that request would necessarily disclose data related to another identifiable individual. There is no such request here.
28. The Office therefore finds that the right of access under Section 24 of the Data Protection and Privacy Act, Cap 97 is a right of access by a data subject to his or her own personal data. It does not entitle the Complainant to obtain the personal data of the named third parties. This issue is resolved against the Complainant and is not upheld.

Issue 2: Whether NIRA acted unlawfully in requiring the consent of the persons concerned, or a court order, before releasing National Identification Register records to a private applicant.



Submissions of the Complainant

29. The Complainant submitted that requiring consent from persons whom he suspects of fraud is impractical and self-defeating. He contended that the Data Protection and Privacy Act, Cap 97 permits disclosure without consent where the disclosure is necessary for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law, or for the preparation or conduct of court proceedings. On that basis, he argued that NIRA's insistence on consent, or a court order, wrongly obstructed his ability to verify the alleged fraud and protect his interests.

Submissions of the Respondent

30. NIRA submitted that access to the National Identification Register by a person other than a Ministry, Department or Agency of Government is governed by Section 67(3) of the Registration of Persons Act, Cap 332 and the Registration of Persons (Access and Use of Information) Regulations. NIRA's position is that a private applicant must submit the prescribed application, state the purpose for which the information is required, pay the prescribed fee, and provide the consent of the person to whom the information relates in Form 2, unless a recognised no-consent ground applies. NIRA further submitted that no such ground was demonstrated in this case.

Determination

31. The issue is whether NIRA contravened the Data Protection and Privacy Act, Cap 97 by requiring the Complainant to comply with the special access legal regime governing the National Identification Register before it could release personal data relating to third parties.

32. Section 67(3) of the Registration of Persons Act, Cap 332 provides that a person other than a Ministry, Department or Agency of Government may access information in the Register only in accordance with Regulations issued by the Board after consultation with



the Minister. The relevant Regulations are the Registration of Persons (Access and Use of Information) Regulations, 2015.

33. Regulation 3 of those Regulations requires a person who wishes to access or use information in the Register to apply to NIRA in Form 1. The application must state, among other things, the particulars of the person whose information is required, the applicant's address, the capacity in which the applicant acts where the request is made on behalf of another person, and the purpose for which the information is required. Where the application concerns information of an individual contained in the Register, Regulation 3(3) requires the application to be accompanied by the consent of the person to whom the information relates. That consent must be in Form 2. Regulation 4 requires payment of the prescribed fee.
34. The Regulations also recognise limited cases where access may be permitted without consent. Regulation 3(6) allows NIRA to permit access without the person's consent where the access or use is required by law, or is necessary for reasons of public order, public safety, public morality, national security, public interest, or any other circumstance the Authority may deem fit.
35. The confidentiality of the Register is reinforced by the Registration of Persons Act, Cap 332 itself. Section 61 requires registration officers and persons processing personal data on behalf of NIRA to treat that information as confidential and not disclose it unless required by law. Section 81 makes unauthorised disclosure, submission or transfer of data from the Register an offence.
36. The Complainant's argument assumes that the consent exceptions in Section 7(2) of the Data Protection and Privacy Act, Cap 97 displace the consent requirement in the Registration of Persons access legal regime. They do not. Two settled principles of statutory interpretation explain why. The first is harmonious construction, where two statutes can reasonably be read together as a coherent scheme, they should be so read. The second is the maxim **generalalia specialibus non derogant**, meaning that general provisions do not derogate from special provisions.



37. The classic statement of that maxim appears in **Seward v The Owners of the Vera Cruz (1884) 10 App Cas 59**, a decision of the House of Lords. The principle is that where general words in a later enactment are capable of sensible application without disturbing an earlier or more specific enactment dealing with the same subject, the specific regime is not taken to have been overridden in the absence of a clear legislative intention to that effect. The Office adopts that principle as consistent with the Ugandan statutory scheme.
38. Applying those principles, the two statutes cohere rather than conflict. The Registration of Persons Act, Cap 332 and the Registration of Persons (Access and Use of Information) Regulations, 2015 are the special regime governing access to information in the National Identification Register. The Data Protection and Privacy Act, Cap 97 is the general personal data protection and privacy statute. The general does not sweep away the special. Rather, the two regimes march together. Section 7(1) of the Data Protection and Privacy Act, Cap 97 establishes consent as the general basis for lawful collection or processing of personal data. Regulation 3(3) of the 2015 Access and Use Regulations applies that same protective principle specifically to Register information.
39. Section 7(2) of the Data Protection and Privacy Act, Cap 97 may make processing without consent lawful where the statutory conditions are met. But it does not create an independent right for a private person to compel NIRA to disclose another person's Register data outside the procedure established under Section 67 of the Registration of Persons Act, Cap 332 and Regulation 3 of the 2015 Access and Use Regulations. Where disclosure from the Register is sought without consent, the applicant must still bring the request within Regulation 3(6), a court order, a formal request by a competent investigative or prosecuting authority, or another clear legal obligation requiring disclosure.
40. On the facts, the records sought are information held in the National Identification Register, and the Complainant is not a Ministry, Department or Agency of Government. His request was therefore governed by Section 67(3) of the Registration of Persons Act, Cap 332 and Regulation 3 of the 2015 Regulations. NIRA was entitled to require a proper



application, the prescribed fee, and the consent of the persons concerned, unless a recognised no-consent basis was established.

41. The Complainant's concern that seeking consent from suspected fraudsters would be impractical is understandable. However, that concern does not by itself displace the statutory safeguards. The lawful routes for disclosure without consent include a court order, a formal request by a competent investigative or prosecuting authority, or a clear basis satisfying Regulation 3(6). The Complainant's own assertion of suspected fraud does not, without more, compel NIRA to disclose third-party personal data directly to him.
42. The Office therefore finds that NIRA did not act unlawfully, and did not contravene the Data Protection and Privacy Act, Cap 97, merely by requiring the Complainant to comply with the Registration of Persons access legal regime before releasing third-party personal data from the National Identification Register. This issue is resolved against the Complainant and is not upheld.

Issue 3: Whether the exemptions for the investigation of offences and for contemplated court proceedings can be relied upon to compel NIRA to disclose the personal data of third parties without their consent.

Submissions of the Complainant

43. The Complainant submitted that Section 7(2)(b)(iii) of the Data Protection and Privacy Act, Cap 97 permits processing without consent where it is necessary for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law. He also relied on Section 11(2)(e)(i) and (iv), which permit collection from another source where necessary for the investigation of an offence or for court proceedings that have commenced or are reasonably contemplated. He further relied on Section 13(3)(e), which relieves a collector from notifying the data subject where the sought information relates to the preparation or conduct of court proceedings. Finally, he invoked Section 34 of the

Access to Information Act, contending that disclosure is required in the public interest because the records may reveal a substantial contravention of the law.

Submissions of the Respondent

44. NIRA did not file detailed submissions specifically addressing the statutory exemptions invoked by the Complainant. Its position, taken from its letters, was that access to information in the National Identification Register is governed by the special legal regime under Section 67 of the Registration of Persons Act, Cap 332 and the Registration of Persons (Access and Use of Information) Regulations, 2015, and that the Complainant had not met the requirements of that regime.

Determination

45. The issue is whether Sections 7(2)(b)(iii), 11(2)(e), 13(3), of the Data Protection and Privacy Act, Cap 97, and Section 34 of the Access to Information Act create a right in the Complainant to compel NIRA to disclose the personal data of third parties without their consent.

46. Sections 7, 11 and 13 of the Data Protection and Privacy Act, Cap 97 must be read according to their language and purpose. Section 7(1) states the general rule that personal data shall not be collected or processed without the prior consent of the data subject. Section 7(2) then provides that personal data may be collected or processed without consent in specified circumstances, including where the processing is authorised or required by law, or where it is necessary for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law.

47. Section 11 deals with the source from which personal data may be collected. Its general rule is that personal data must be collected directly from the data subject. Section 11(2) then permits collection from another person, source or public body in specified circumstances, including where collection from another source is necessary for the prevention, detection, investigation, prosecution or punishment of an offence, or for



proceedings before a court or tribunal that have commenced or are reasonably contemplated.

48. Section 13 is different. It does not create a power to disclose. It concerns the duty to inform a data subject where personal data is collected. Section 13(3) relieves the data collector or data controller from the duty to inform the data subject in specified circumstances, including where notification would compromise the law enforcement power of a public body responsible for the prevention, detection, investigation, prosecution or punishment of an offence, or where the information relates to the preparation or conduct of court proceedings.
49. The decisive point is that these provisions are permissive processing provisions. Section 7(2) says personal data “may be collected or processed” without consent in the stated circumstances. Section 11(2) says personal data “may be collected” from another source. Section 13(3) merely removes, in defined circumstances, the duty to inform the data subject. None of these provisions says that a data controller or collector “shall disclose” personal data to a private requester. None creates a private right by which one person may compel a controller to surrender another person’s personal data.
50. That conclusion is supported, as persuasive authority only, by the judgment of the Court of Justice of the European Union in **Rīgas satiksme, Case C-13/16**, Judgment of 4th May 2017. The ratio of that case is that data protection and privacy law does not impose an obligation on a data controller to disclose personal data to a private third party merely to enable that third party to bring a civil claim. Such disclosure may be lawful, but only where a structured test is satisfied, there must be a legitimate interest, disclosure must be necessary for that interest, and the data subject’s rights and freedoms must not override that interest. Although *Rīgas satiksme* was decided under a foreign instrument and is not binding on this Office, its reasoning is consistent with the Ugandan Act’s insistence on consent, necessity, proportionality and protection of the data subject. The Office adopts it as persuasive guidance in construing Sections 7, 11 and 13.

51. The investigation of offences exemptions must also be read in light of the institutional framework for criminal investigations and prosecutions. Under Article 120(3) of the Constitution, the Office of the Director of Public Prosecutions may direct the Police to investigate information of a criminal nature, institute criminal proceedings, take over and continue criminal proceedings instituted by another person or authority, and discontinue criminal proceedings before judgment. A private citizen may set the criminal process in motion only through the procedures provided by law, including the route for private complaints under the Magistrates Courts Act, and subject to the supervisory powers of the court and the Office of the Director of Public Prosecutions. The Complainant is not the Police and is not the Office of the Director of Public Prosecutions. The existence of a police reference or complaint does not, by itself, entitle him to step into the place of the investigating or prosecuting authority and demand direct disclosure of another person's Register data.
52. Nor is the Complainant without a lawful route if the information is genuinely required for civil proceedings. The proper route is court supervised disclosure. In **Norwich Pharmacal Co v Customs and Excise Commissioners [1974] AC 133**, the House of Lords held that a person who becomes mixed up, even innocently, in the wrongdoing of another may, in appropriate circumstances, be ordered by a court to disclose information, including the identity of the wrongdoer, to the person wronged. The Office relies on it for the narrow proposition that, where a private litigant seeks third-party information to pursue a civil claim, the appropriate route is an application to a court of competent jurisdiction, not a unilateral demand to the controller.
53. The Complainant's reliance on Section 34 of the Access to Information Act does not alter the conclusion. NIRA is a public body, and records held by NIRA may in principle fall within the Access to Information Act. However, information in the National Identification Register is governed by a special statutory regime under Section 67 of the Registration of



Persons Act, Cap 332 and the Registration of Persons (Access and Use of Information) Regulations, 2015. That special regime prescribes the conditions under which a private person may access Register information, including the consent requirement and the limited no-consent grounds.

54. In any event, the Access to Information Act does not create an absolute right to obtain personal data about another person. Section 5(1) qualifies the right of access where release is likely to interfere with the privacy of another person, and Section 26 protects against unreasonable disclosure of personal information. Section 34 is a public interest override within the Access to Information Act, but it requires a separate balancing exercise, the disclosure must reveal evidence of a substantial contravention of the law, or an imminent or serious public safety, public health or environmental risk, and the public interest in disclosure must outweigh the harm contemplated. It does not, by itself, override the consent and access controls specifically imposed on the National Identification Register.
55. Accordingly, even if the Complainant wished to pursue access under the Access to Information Act, that route would have to be pursued through the machinery of that Act and consistently with the Registration of Persons legal regime and the privacy rights of the affected data subjects. It does not provide an independent basis for this Office, in this complaint under the Data Protection and Privacy Act, Cap 97 to compel NIRA to release third-party Register data directly to the Complainant.
56. It is necessary to confront the Complainant's strongest argument, that the exemptions would be meaningless if a data controller could always insist on consent. The answer is that the data controller does not always have the last word. A data controller who refuses disclosure properly supported by a court order, a formal request from a competent investigating or prosecuting authority, or a statutory obligation requiring disclosure may itself breach the law and become answerable before this Office or another competent forum. But that is not the present case. The exemptions in Sections 7, 11 and 13 support lawful disclosure to, or at the instance of, an authorised actor. They are not a sword by



which a private litigant, relying on his own theory of fraud, may compel direct disclosure of another person's personal data.

57. The Office therefore finds that Sections 7(2)(b)(iii), 11(2)(e), and 13(3) of the Data Protection and Privacy Act, Cap 97, and Section 34 of the Access to Information Act, did not oblige NIRA to disclose the requested records directly to the Complainant without consent, a court order, a formal request by a competent investigative or prosecuting authority, or another clear legal obligation requiring disclosure. This issue is resolved against the Complainant and is not upheld.

Issue 4: Whether the Complainant is entitled to the remedies sought.

58. Having considered the submissions and evidence adduced by the Parties, the Office makes the following determination regarding the orders and remedies sought.

59. The Complainant sought an order directing NIRA to disclose the requested National Identification Register records without requiring the consent of the persons to whom the records relate. He also sought any further relief the Office considers appropriate.

60. The issue is whether, in light of the findings made above, the Complainant has established a legal entitlement to the remedies he seeks.

61. Regulation 45(3) of the Data Protection and Privacy Regulations, 2021 empowers the Office, where it determines that a data collector, data processor or data controller is infringing the rights of a data subject or is in violation of the Act, to serve a notice requiring that data collector, processor or controller to take or refrain from taking specified steps, to refrain from processing personal data, to process personal data only in accordance with specified directions, or to take specified remedial action.



62. That corrective power is triggered by a finding of infringement of a data subject's rights or a violation of the Act. In this complaint, the Office has not found that NIRA violated the Data Protection and Privacy Act, Cap 97 by requiring the Complainant to comply with the special access legal regime governing the National Identification Register. The precondition for a corrective notice compelling disclosure is therefore absent.
63. There is a further and independent obstacle. The principal remedy sought would require NIRA to release third-party Register data directly to the Complainant without consent, without a court order, without a formal request from a competent investigative or prosecuting authority, and without another clear legal obligation requiring disclosure. Such an order would undermine the safeguards imposed by Section 67 of the Registration of Persons Act, Cap 332 and Regulation 3 of the Registration of Persons (Access and Use of Information) Regulations, 2015. It would also risk directing NIRA officers into conduct prohibited by Section 81 of the Registration of Persons Act, which criminalises unauthorised disclosure, submission or transfer of data from the Register.
64. For those reasons, the principal relief is refused not merely as a matter of discretion, but as a matter of law. The Office cannot order a controller to disclose personal data where the statutory basis for disclosure has not been established and where the order would defeat the privacy safeguards that the Act and the Registration of Persons regime protect.
65. The refusal of the principal order does not leave the Complainant without lawful avenues. He may pursue access under the Registration of Persons (Access and Use of Information) Regulations, 2015 and, if access is refused, pursue the appeal route provided under those Regulations. He may also request the Uganda Police Force or the Office of the Director of Public Prosecutions, where appropriate, to make a formal request to NIRA if the information is required for an investigation or prosecution. In addition, he may apply to a court of competent jurisdiction for court supervised disclosure, including, where the legal requirements are met, a Norwich Pharmacal type order.



Personal
DATA
Protection
OFFICE

66. The Office therefore finds that the Complainant is not entitled to the principal remedy sought. The Office declines to order NIRA to disclose the requested third-party personal data directly to him. To the extent the Complainant seeks “any other remedy as the Office may deem fit”, no additional corrective remedy arises because no violation of the Data Protection and Privacy Act, Cap 97 or its Regulations has been established against NIRA.

67. This complaint is accordingly not upheld.

G. Right of Appeal

68. Any party aggrieved by this Decision may appeal to the Minister of ICT and National Guidance within thirty (30) days from the date of notice of this Decision, in accordance with Regulation 46 of the Data Protection and Privacy Regulations, 2021.

Dated this 28th day of May 2026

Baker Birikujja

NATIONAL PERSONAL DATA PROTECTION DIRECTOR

