ILRAJ Position Paper on the Data Protection and Right to Access Information Bill, 2026



A legal reform position for privacy, access to information and accountable data governance

Summary

The Institute for Legal Research and Advocacy for Justice (ILRAJ) supports a law to protect personal data in Sierra Leone. We urge Parliament to amend the Data Protection and Right to Access Information Bill, 2026 before passing it. In its present form, the Bill weakens the right to information Sierra Leoneans already enjoy, and leaves the largest holder of personal data, the Government, mostly outside the new rules.

Our nine positions ask Parliament to:

1. Keep every protection in the Right to Access Information Act, 2013, including independent review of refusals, appeal to the High Court and protection for whistleblowers.
2. Let every citizen make a request orally or in writing, in English, Krio or any local language, without giving a reason.
3. Make the new Authority independent of government, as ECOWAS rules require.
4. Apply the data protection rules to government, with narrow exemptions written into the Act.
5. Give businesses and public services clear and workable grounds for using personal data.
6. Protect fingerprints, face scans, national ID numbers and children's data, stop unwanted marketing, and require prompt notice of data breaches.
7. Fix penalties in the Act itself, and give the Authority the power to fine and the duty to act fairly.
8. Make clear privacy never hides information the public has a right to see, and protect journalists and whistleblowers.
9. Manage the move from the existing Commission to the new Authority with care, and correct the drafting errors.

The paper ends with draft clauses ready for Parliament to adopt.

Why this Bill matters

Every day, Sierra Leoneans hand over personal information to register to vote, obtain a national identification number, register a SIM card, open a bank or mobile money account, see a doctor or pay tax. No law today tells the people holding this information how to use the information, how to keep the information safe, or what to do after a leak. Section 22 of the Constitution protects the home, property and private communications. The Constitution says nothing about personal data held in databases.

The Bill fills this gap, and ILRAJ welcomes the effort. The Bill also does something less visible but equally important. Section 92 repeals the Right to Access Information Act, 2013, and Part X puts a new access to information regime in its place.

The 2013 Act works. The Act scores 126 out of 150 on the Global Right to Information Rating, including 29 out of 30 for appeals. A 2025 evaluation, led by the Right to Access Information Commission with Canada's Centre for Law and Democracy, found the Commission decided appeals within its 15-working-day limit and published its decisions. A new law should build on this record rather than dismantle the record.

Sierra Leone has also made regional commitments. As an ECOWAS member, Sierra Leone is bound by the Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (2010). ECOWAS Heads of State reportedly adopted a revised version at their summit in Lungi on 19 July 2026. Sierra Leone signed the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) in January 2016, and had not ratified the Convention as at the African Union's July 2024 status list.

ILRAJ shares many of the concerns Citizens' Barray set out in its November 2026 position paper. This paper adds further points from a clause-by-clause review of the Bill as published in the Supplement to the Sierra Leone Gazette Vol. CLXVII, No. 62, dated 2 July 2026. All section numbers below refer to the published Bill.

Protect the right to information Sierra Leoneans already have

ILRAJ's position: Parliament should not pass any law which leaves citizens with weaker access to information than the 2013 Act gives them.

A right without a remedy is no right at all. Under the 2013 Act, a citizen refused information complains to the Commission. The public body must prove its actions were lawful (section 44). The Commission decides within 15 days, after hearing both sides (section 45), and holds the powers of a High Court to summon witnesses (section 32(3)). The Commission has power to order release of the information, compensation, or a fine on the public authority (sections 32(4) and 45). Either side then has 45 days to appeal to the High Court (section 46).

The Bill removes this whole chain. Section 86 says only the Authority "may" create an "internal appeal mechanism." Section 87 then asks this mechanism to decide whether "the Authority failed to comply," rather than whether the public body failed. The Bill sets no time limit, no hearing, no power to order release and no appeal to the High Court.

The Bill also opens the door to a reason test. Section 2(b) applies the access to information Parts to any "person, institution or public body that is holding or is in control of information necessary for the enforcement or protection of a right." The 2013 Act applied this condition only to private bodies (section 2(2)). Read literally, section 2(b) lets a public body ask a citizen to prove the information is needed to protect a right. Section 62(1)(a) points the other way, and the conflict will end up in court.

Four further protections disappear with the 2013 Act:

- the duty on every public authority to appoint public information officers (section 28), although sections 63 and 64 of the Bill still give these officers duties
- protection for whistleblowers (section 50)
- protection for officials who act in good faith (section 51)
- the bar on party officials and government office holders serving as Commissioners (section 31(3))

Other African countries show what a strong system looks like. Kenya's Access to Information Act, 2016 says a citizen's right "is not affected by" any reason given, or by what the public body believes those reasons are (section 4(2)). Refusals go to the Commission on Administrative Justice for review, with appeal to the High Court within 21 days (sections 14 and 23(3)). Ghana keeps two separate bodies, a Data Protection Commission and a Right to Information Commission. South Africa, like this Bill, gives one Information Regulator both roles, but the Regulator answers to the National Assembly, and its data protection notices go on appeal to the High Court (sections 39 and 97 of the Protection of Personal Information Act, 2013).

What ILRAJ asks Parliament to do:

- Restore review by the Authority, with the burden of proof on the public body, a decision within 15 working days, binding orders, and appeal to the High Court (draft clauses E and F).
- Rewrite section 2(b) and state plainly no requester needs to give a reason (draft clauses A and B).
- Restore public information officers, whistleblower protection and good faith protection (draft clauses D and M).

Make the law usable by every citizen

ILRAJ's position: A citizen should be able to make a request by speaking, in the language the citizen uses, and receive free help from officials.

Only 48.6 per cent of adults in Sierra Leone read and write, according to World Bank data for 2022. A law which works only on paper will fail most of the people the law exists to protect.

The 2013 Act took this into account. Section 3(3) allowed requests "in English or Krio" by email, fax, post or telephone. Section 3(5) allowed a request in any other local language, with the officer arranging translation into English. Section 3(4) required officers to write down oral requests and give the applicant a copy.

The Bill keeps the rule on oral requests (section 63(4)), but drops Krio and the local languages, and section 63(1)(a) still insists on writing. On the data protection side, a person who wants a company to stop using personal data, stop direct marketing, or review a computer-made decision must send a notice in writing (sections 45 to 47).

Kenya offers a useful model. Its information officers must help any person who is unable to write because of illiteracy or disability, and must write the request down for the applicant (section 8 of the Access to Information Act, 2016).

What ILRAJ asks Parliament to do:

- Allow requests orally or in writing, in English, Krio or any language commonly used in Sierra Leone, with free translation (draft clause C).
- Require free help for persons who are unable to read or write and for persons with disabilities, including sign language and accessible formats (draft clause C).
- Let data subjects exercise their rights orally, through a public information officer, a data protection officer or a regional office of the Authority (draft clause C).
- Require every public authority to appoint and publish its public information officers (draft clause D).

An Authority independent of government

ILRAJ's position: The body which protects citizens' information rights must be able to stand up to ministries, security agencies and large companies. The Bill does not give the Authority this strength.

Section 22 promises independence, then adds the words "except as provided by this Act or any other law." The rest of the Bill shows what those words mean in practice:

- Five of the eight Board seats belong to government bodies: the Attorney-General's Office, the Ministry of Information and Civic Education, the Ministry of Communication, Technology and Innovation, the Bank of Sierra Leone and a law enforcement agency (section 7(2)).
- The Minister nominates the private sector and civil society members.
- The quorum is five (section 8(5)), so the government members alone are able to take every decision.
- The Minister approves Board pay (section 12), makes the regulations (section 90), sets every penalty, grants exemptions (section 5), and receives the annual report before Parliament sees the report (section 26).
- No provision says who appoints the Director-General (section 17), and no provision says how any office holder is removed or heard before removal (sections 13 and 19).
- The Bank of Sierra Leone and the police rank among the largest holders of personal data in the country. Both would sit on the Board of their own regulator.

ECOWAS rules point the other way. Article 16 of the Supplementary Act makes membership of the data protection authority "incompatible with membership of government." Article 15 requires members qualified in law and information technology, and Article 17(2) says members "shall receive no instructions from any Authority." The African Commission's Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019) calls for a transparent and participatory appointment process, a fixed term and accountability to the legislature (Principle 34), and for oversight bodies including human rights and privacy experts (Principle 42).

Other countries show better models. In Kenya, the Public Service Commission advertises the post of Data Commissioner, shortlists and interviews candidates and nominates three, the President nominates one, and the National Assembly approves the appointment, for a single six-year term (sections 6 and 7 of the Data Protection Act, 2019). In South Africa, a National Assembly committee nominates members of the Information Regulator, the Assembly approves them, and the President then makes the appointment (section 41 of the Protection of Personal Information Act, 2013). Nigeria's National Commissioner, by contrast, is appointed on the Minister's recommendation (section 14 of the Data Protection Act, 2023), a model ILRAJ does not recommend.

What ILRAJ asks Parliament to do:

- Rebuild the Board with no serving public officials or party office holders, and let the Sierra Leone Bar Association, civil society, the media and business choose their own nominees (draft clause G).
- Require open, competitive recruitment for the Chairperson, members and Director-General, with Parliament's approval (draft clauses G and H).
- Set fixed terms, and allow removal only for stated causes after a fair hearing (draft clause H).
- Require at least 30 per cent women on the Board, in line with the Gender Equality and Women's Empowerment Act, 2022.
- Let the Authority present its own budget and lay its own annual report before Parliament.

Government must obey the law Parliament makes

ILRAJ's position: The Government holds more personal data than anyone else, from national identification and tax records to health files. The data protection rules must bind government, with only narrow exemptions written into the Act.

Section 3 exempts processing from the whole Act where the data is used:

- for "national security or public interest,"
- "for the prevention or detection of a crime,"
- "for the purpose of an investigation,"
- for the assessment or collection of a tax or duty,
- for an order or judgment of a court, or
- "for the purpose of discharging a statutory function."

Almost everything a Ministry, Department or Agency does is a statutory function. Under section 3, the National Revenue Authority, the police, public hospitals and the national civil registration system would escape every duty in the Act, including the duty to keep data secure, to keep data accurate and to report breaches. "Public interest" has no definition and no limit. No exemption requires the processing to be necessary or proportionate, and the Authority has no oversight of any of them.

The Bill goes further. Section 5 lets the Minister exempt any data controller, or any class of controllers, from the whole Act by statutory instrument, with no criteria and no time limit. Section 31(1)(b)(x) lets the Minister add new purposes for processing sensitive data. Under section 170(7) of the Constitution, such an instrument comes into force 21 days after laying unless two-thirds of Members of Parliament vote to annul the instrument. In practice, Parliament would rarely stop one.

The ECOWAS Supplementary Act applies to processing "by government, local authorities, and public or private legal entities" (Article 3(1)), including processing for public security, defence and criminal investigations, subject only to exemptions set out in law (Article 3(4)). Only purely personal or household activity falls outside the ECOWAS Act altogether (Article 4).

Nigeria shows how to draft a narrow exemption. Section 3(2) of the Nigeria Data Protection Act, 2023 relieves processing for criminal investigations, national security, journalism and legal claims from some duties, but the principles, the lawful grounds, the duty to appoint a data protection officer and the duty to report breaches still apply. The Nigeria Data Protection Commission also has power to issue a guidance notice where exempt processing risks breaching the principles (section 3(4)).

What ILRAJ asks Parliament to do:

- Keep the household exemption, and delete the rest of section 3 and the whole of section 5 (draft clause I).
- Replace them with exemptions from named duties only, where compliance would prejudice national security, crime prevention, tax collection or court proceedings, and only where the processing is authorised by law, necessary and proportionate (draft clause I).
- Keep the core duties, especially security, accuracy and breach reporting, for all processing (draft clause I).
- Remove the Minister's power to add grounds for processing sensitive data.

Workable rules for businesses and public services

ILRAJ's position: Strong protection and workable rules go together. A law businesses are unable to follow will be ignored, and ignored rules protect nobody.

The Bill makes consent the starting point for all processing. Section 38(1) says a data controller or processor "shall not process personal data unless consent is given by the data subject at the start of collecting the data." Section 39 lists the only alternatives: state functions, state services and licences, compliance with a law or court order, medical emergencies, epidemics, disasters, and employment.

Two grounds every modern data protection law includes are missing. The first is performance of a contract with the data subject. The second is the legitimate interests of the business, balanced against the rights of the individual. The drafters knew of both, since sections 29(1)(d) and 35(2)(a) refer to "legitimate interests," and section 45(6) refers to contracts.

The effect is serious. A bank, insurer, telecoms operator, landlord, school or private clinic must obtain consent simply to hold the information needed to serve a customer. Section 38(2)(e) lets the customer withdraw consent at any time, which would force the business to stop. Businesses will respond by making consent a condition of service, which defeats the rule in section 38(2)(a) requiring consent to be "freely given."

Three other provisions add to the burden:

- Section 83(1)(a)(i) makes storing or disclosing personal data "without the explicit consent of the data subject" a crime. A ministry relying on section 39 would commit an offence by storing data section 39 allows.
- Every data controller and processor must register (section 50) and renew registration every year (section 51), even a small shop, although section 16(1)(f) already gives the Authority power to set thresholds.
- Every data controller and processor must submit a privacy design policy to the Authority for approval and publish the policy "on his website" (section 55). Most small businesses in Sierra Leone have no website.

Children need protection, but section 36 goes too far in one direction and not far enough in another. Every use of the data of a person under 18 needs a parent's or guardian's consent, with no other ground. Schools, hospitals, examination bodies and child protection services would need parental consent for routine work, and a 17-year-old would be unable to agree to any online service.

The ECOWAS Supplementary Act waives consent where processing is needed for a legal obligation, a public interest task, a contract, or the vital interests of the data subject (Article 23(2)). Kenya (section 30 of the Data Protection Act, 2019), Nigeria (section 25 of the Data Protection Act, 2023) and South Africa (section 11 of the Protection of Personal Information Act, 2013) all recognise both contract and legitimate interests. Nigeria limits legitimate interests where they override the rights of the individual or fall outside what the individual would reasonably expect (section 25(2)).

What ILRAJ asks Parliament to do:

- Replace sections 38 and 39 with one clear list of lawful grounds, including contract and legitimate interests with a balancing test (draft clause J).
- Redraft section 83 to punish processing without any lawful ground, rather than processing without consent.
- Require registration only above thresholds set by the Authority, with certificates valid for several years.
- Replace prior approval of privacy design policies with a duty to keep records available to the Authority on request.
- Allow other lawful grounds for children's data, keep the best interests test, and set an age for consent to online services.

Everyday protections for citizens

ILRAJ's position: Citizens give their fingerprints, face scans, ID numbers and phone details to vote, register SIM cards, open mobile money accounts and receive services. The law should protect them at each of these points.

Fingerprints, face scans and ID numbers. Article 12 of the ECOWAS Supplementary Act requires prior authorisation from the data protection authority before anyone processes biometric data, genetic data or national identification numbers. The Bill lists biometric and genetic data as sensitive, but requires no prior authorisation for any of them.

Marketing messages. Section 46 lets a person stop direct marketing only by sending a written notice, so companies are free to keep sending messages until the person writes. Worse, section 46(5) defines direct marketing as material "directed to a particular institution." The UK law the clause was copied from says "particular individuals" (section 11(3) of the UK Data Protection Act 1998). As drafted, section 46 protects no

individual at all. Article 34 of the ECOWAS Supplementary Act prohibits direct marketing to a person who has not given "prior consent," and South Africa requires consent for electronic marketing, with a narrow exception for existing customers (section 69 of the Protection of Personal Information Act, 2013).

Decisions made by computers. Under section 47, a person must first send a written notice before a data controller has to make sure a decision is not taken solely by computer. Section 47(4) then exempts decisions about contracts and any decision "authorised or required by or under any law." Loan approvals, insurance, recruitment and social benefits all fall outside the protection. Article 35(2) of the ECOWAS Supplementary Act states "no decision that has legal effect on an individual shall be based solely on processing by automatic means."

Data breaches. Section 61 covers only data "accessed or acquired" by an unauthorised person, so loss, destruction, alteration and ransomware attacks fall outside. Affected persons need be told only within a "reasonably practical period," and need not be told at all where the company says their identity "cannot be established" (section 61(1)(b)), or where safeguards "may include encryption" (section 61(6)). Failure to notify carries no penalty. Only failure to keep breach records is an offence (section 61(9)).

Transfers abroad. Section 42 applies only to "a data processor based in Sierra Leone," so data controllers sending data abroad face no rules. No body decides which countries offer adequate protection, and no contract-based safeguards exist for businesses using cloud services abroad.

What ILRAJ asks Parliament to do:

- Require the Authority's prior approval before processing biometric data, genetic data or national identification numbers, unless an Act of Parliament authorises the processing with safeguards (draft clause K).
- Require prior consent for electronic marketing, and correct the definition to "particular individuals" (draft clause L).
- Protect every person from decisions with legal or similar effects made solely by computer, with a right to an explanation and human review (draft clause Q).
- Define a personal data breach fully, set a firm deadline for telling affected persons, require public notice through radio and newspapers where persons are impossible to identify, and make failure to notify an offence (draft clause P).
- Apply the transfer rules to all data controllers and processors, and allow transfers with approved contract terms or on necessity grounds.

Penalties set by Parliament, and a regulator with real powers

ILRAJ's position: Parliament, not a Minister, should decide the punishment for breaking this law. The Authority also needs the power to fine, and the duty to act fairly when using the power.

No offence in the Bill carries a penalty. Sections 45(5), 46(4), 50(8), 61(9), 81(2), 82(2), 83(5), 84, 85(1) and 88(3) each leave the penalty to "such penalty as the Minister may, in consultation with the Authority, prescribe." Until the Minister acts, a court has no sentence to impose. Later, penalties would change by ministerial instrument rather than by Act of Parliament. The 2013 Act took the better course, fixing maximum fines and prison terms in the Act itself (sections 32(8), 47 and 48). Those fines were set at ten million leones for individuals and one hundred million leones for companies. Since the Bank of Sierra Leone removed three zeros from the currency on 1 July 2022, the same figures are worth NLe 10,000 and NLe 100,000, so Parliament should set fresh amounts.

The Authority also has no power to fine anyone, although section 20(1)(c) speaks of "administrative sanctions." Article 19(1)(i) of the ECOWAS Supplementary Act expects the authority to "impose administrative and financial sanctions on data controllers." Other countries set clear limits:

- Kenya: up to five million shillings or one per cent of annual turnover, whichever is lower (section 63 of the Data Protection Act, 2019).
- Nigeria: for data controllers of major importance, the greater of ten million naira or two per cent of annual gross revenue (section 48 of the Data Protection Act, 2023).
- South Africa: administrative fines of up to R10 million (section 109 of the Protection of Personal Information Act, 2013), and prison terms of up to ten years for the most serious offences (section 107).

Three further gaps need attention:

- Section 16(1)(d) lets officers "enter premises occupied by a data controller or data processor" with no warrant. The Cyber Security and Crime Act, 2021 requires a High Court warrant before search and seizure of computer data (section 10). The Authority should meet the same standard.
- Section 88(3) makes breach of a Code of Practice a crime. Codes are guidance the Authority issues without Parliament's approval, and should not carry criminal liability.
- No section gives a right of appeal from the Authority to the courts. Kenya allows appeal to the High Court (section 64), Nigeria allows judicial review within 30 days (section 50), and South Africa allows appeal to the High Court within 30 days (section 97).

What ILRAJ asks Parliament to do:

- Fix maximum fines and prison terms in the Act, with amounts suited to the new leone (draft clause T).
- Give the Authority power to issue enforcement notices and administrative penalties linked to turnover, only after notice and a hearing (draft clause R).
- Require a High Court warrant for entry and search, except with the occupier's consent (draft clause S).
- Remove criminal liability for breach of a Code of Practice.
- Provide a right of appeal to the High Court from every decision of the Authority (draft clause F).

Privacy must not become secrecy

ILRAJ's position: Privacy protects people. Privacy should never protect public officials from scrutiny, or punish the journalists and whistleblowers who expose wrongdoing.

The Bill pulls in two directions. Section 68(1) requires every public authority to publish the monthly pay of its officers (paragraph (j)) and the details of beneficiaries of subsidy programmes (paragraph (l)). Section 71(1)(e) requires every public contract, with the contractor's name and the contract sum, to be published in the Gazette. Yet section 83 makes disclosing personal data without "explicit consent" a crime. The Bill nowhere says which rule wins. An official who wishes to hide a payroll or a contract list would point to section 83.

Whistleblowers lose the protection section 50 of the 2013 Act gave them. The 2013 Act protects any person who releases information on wrongdoing, in the reasonable belief the information is accurate, from dismissal, discrimination or reprisal. Principle 35 of the African Commission's 2019 Declaration calls on

states to protect any person who discloses wrongdoing in the public interest from "civil, criminal, administrative or employment-related" sanctions.

Journalists receive no protection either. Section 25(1) of the Constitution guarantees the freedom "to receive and impart ideas and information without interference." Yet the Bill would apply every consent, notice and registration duty to a newsroom investigating corruption. Article 32 of the ECOWAS Supplementary Act permits processing "for the purposes of journalism" under the ethical rules of the profession. Kenya (section 52 of the Data Protection Act, 2019), Nigeria (section 3(2) of the Data Protection Act, 2023) and South Africa (section 7 of the Protection of Personal Information Act, 2013) all protect journalistic, literary and artistic work.

What ILRAJ asks Parliament to do:

- Make clear the data protection Parts never block publication of the public duties, pay and contracts of public officials, or of any information the Act requires public bodies to publish (draft clause N).
- Restore protection for whistleblowers, with any contract term silencing a protected disclosure made void (draft clause M).
- Add an exemption for journalism, literature and art, tied to a recognised code of ethics, while keeping the duty to keep data secure (draft clause O).

A clean transition and a clean text

ILRAJ's position: The move from the existing Commission to the new Authority should protect staff, pending cases and citizens' rights. The text Parliament passes should be accurate.

Section 91 transfers only the "assets, including funds and administrative records" of the "Right to Access Information Authority." No body of this name exists. The 2013 Act established the Information Commission (sections 1 and 30), known in practice as the Right to Access Information Commission. Section 91 says nothing about the Commission's staff, the Commissioners' remaining terms, complaints and appeals already pending, contracts, debts or approved publication schemes. Section 92(1) repeals "The Right to Access to Information Act, 2013," while the correct title is "The Right to Access Information Act, 2013."

The publication schemes matter. Section 8(6) of the 2013 Act gave public authorities seven years from their first scheme to meet every proactive disclosure duty. Section 68(6) of the Bill repeats the seven-year window. Unless the Act saves the existing schemes, public authorities would restart the clock in 2026.

The Bill also gives businesses and public bodies no time to prepare. Data protection laws elsewhere allow a transition period, and the EU General Data Protection Regulation, for example, applied two years after adoption.

The printed Bill contains more than 35 drafting and printing errors. Examples include:

- two sections numbered 20
- a definition of direct marketing aimed at "a particular institution" (section 46(5))
- wrong cross-references in sections 1, 38, 40, 45, 51, 52, 57, 61, 66, 73, 74 and 79
- paragraphs missing or lettered twice in sections 4, 33, 44 and 50
- stray page numbers, and the word "DRAFT," printed inside sections 1, 4, 27, 30, 31, 36, 44 and 45

ILRAJ has prepared a full schedule of these errors and will share the schedule with the Committee on request.

What ILRAJ asks Parliament to do:

- Replace section 91 with a full transitional provision covering staff, Commissioners, pending matters, assets, liabilities and publication schemes (draft clause V).
- Correct the title of the 2013 Act in section 92.
- Give data controllers a period of [12] months to comply and [6] months to register (draft clause V).
- Refer the Bill to the Law Officers' Department for a full technical revision before third reading, and use gender-neutral language such as "Chairperson."

How other African countries do it

On independence, fines, lawful grounds, journalism and appeals, the Bill falls behind the laws of Kenya, Nigeria and South Africa.

Feature	This Bill	Kenya	Nigeria	South Africa
Data protection regulator	Data Protection and Right to Access Information Authority	Office of the Data Protection Commissioner	Nigeria Data Protection Commission	Information Regulator
Access to information oversight	The same Authority	A separate body, the Commission on Administrative Justice	A separate law, the Freedom of Information Act, 2011	The same Information Regulator
How the regulator is chosen	Five of eight Board seats held by government bodies, two more nominated by the Minister. No rule on who appoints the Director-General	Public Service Commission recruits and nominates three, President nominates one, National Assembly approves. Single six-year term	President appoints on the Minister's recommendation. Five years, renewable once	National Assembly nominates and approves, President appoints. Up to five years, renewable
Administrative fines	None	Up to KES 5 million or 1 per cent of annual turnover, whichever is lower	For controllers of major importance, the greater of ₦10 million or 2 per cent of annual gross revenue	Up to R10 million
Contract and legitimate interest grounds	Neither	Both (section 30)	Both (section 25)	Both (section 11)
Journalism exemption	None	Yes (section 52)	Yes (section 3(2))	Yes (section 7)
Appeal to the courts	None	High Court (section 64)	Judicial review within 30 days (section 50)	High Court within 30 days (section 97)

Ghana, like Kenya, keeps two separate bodies, a Data Protection Commission and a Right to Information Commission. A combined regulator, as in South Africa and in this Bill, works only with independent appointments, separate procedures for each right, and appeal to the courts.

New provisions ILRAJ proposes

The clauses below turn ILRAJ's positions into legislative text. Section numbers refer to the Bill as gazetted. Figures in square brackets are policy choices for Parliament.

Clause A: Application of the access to information Parts (replaces section 2(b))

(b) the right to access information,

(i) to every public authority, and

(ii) to a private body, where the information is necessary for the exercise or protection of a right.

Clause B: No reason required (new section 62A)

62A. (1) A person who applies for information held by or under the control of a public authority shall not be required to give any reason for the application.

(2) A public authority shall not refuse, delay or limit a response to an application because of any reason the applicant gives, or because of what the public authority believes the applicant's reasons to be.

Clause C: Form and language of applications (replaces section 63(1) to (5), and new section 49A)

63. (1) An application to access information may be made orally or in writing, in English, Krio or any other language commonly spoken in Sierra Leone, by any means of communication, including in person, by telephone, by post or by email.

(2) A public information officer who receives an oral application shall reduce the application to writing, read the record back to the applicant, and give the applicant a copy free of charge.

(3) Where an application is made in a language other than English, the public authority shall arrange a translation into English free of charge, and shall communicate with the applicant in the language of the application where reasonably practicable.

(4) A public information officer shall give reasonable assistance, free of charge, to an applicant who is unable to read or write or who has a disability, including by the use of sign language, braille or another accessible format.

(5) An application shall describe the information requested in enough detail to enable the public authority to identify the information, and shall give a means of contacting the applicant.

49A. A data subject may exercise any right under this Part orally or in writing, in person or by any means of communication, and subsections (2) to (4) of section 63 apply to data controllers with the necessary modifications.

Clause D: Public information officers (new section 62B)

62B. (1) Every public authority shall, within three months after the commencement of this Act, appoint as many public information officers as are necessary to give effect to this Part, at its headquarters and in each regional and district office.

(2) A public authority shall publish the names, offices and contact details of its public information officers, and notify the Authority of them.

(3) Where a public authority fails to appoint a public information officer, the head of the public authority shall perform the functions of a public information officer.

Clause E: Review by the Authority (replaces sections 86 and 87)

86. (1) A person aggrieved by

(a) a refusal, deemed refusal, partial refusal, fee, delay or other decision of a public authority under Part X or Part XI, or

(b) an act, omission or decision of a data controller or data processor in breach of this Act,

may apply to the Authority for review, orally or in writing, within 60 days of the decision or of becoming aware of the breach, or within such longer period as the Authority allows.

(2) The Authority shall give notice of the application to the public authority, data controller or data processor concerned, and give both parties an opportunity to be heard.

(3) The burden of proving compliance with this Act lies on the public authority, data controller or data processor concerned.

(4) The Authority shall decide an application under paragraph (a) of subsection (1) within 15 working days, and an application under paragraph (b) of subsection (1) within 60 days, of receiving the application.

(5) For the purposes of a review, the Authority shall have the powers of a Judge of the High Court to summon witnesses, administer oaths and compel the production of documents.

(6) On a review, the Authority may

(a) order the release of information,

(b) order a data controller or data processor to comply with this Act, including by correcting, erasing or ceasing to process personal data,

(c) order the payment of compensation to the applicant,

(d) impose an administrative penalty under section 16A, or

(e) dismiss the application.

(7) The Authority shall give its decision in writing with reasons, and shall publish its decisions with personal data removed.

(8) A decision of the Authority may be registered in the High Court and enforced as an order of the High Court.

Clause F: Appeal to the High Court (new section 87)

87. (1) A party aggrieved by a decision, order, enforcement notice or administrative penalty of the Authority may appeal to the High Court within 45 days of receiving the decision.

(2) An appeal does not suspend the decision of the Authority unless the High Court orders otherwise.

Clause G: The Board (replaces section 7(2) to (4))

7. (2) The Board shall consist of a Chairperson and six other members, being persons of integrity with knowledge or experience in law, human rights, information and communication technology, records management or public administration, as follows:

(a) a Chairperson, who shall be a retired Justice of the Superior Court of Judicature or a legal practitioner of not less than 15 years' standing,

(b) one person nominated by the Sierra Leone Bar Association,

(c) one person nominated by civil society organisations working on human rights, transparency or digital rights, through a process those organisations determine,

(d) one person nominated by the Sierra Leone Association of Journalists,

(e) one person nominated by business associations, through a process those associations determine, and

(f) two persons with expertise in information and communication technology, cyber security or records management, selected through open and competitive recruitment.

(3) A person shall not be appointed, or remain, a member of the Board if the person

(a) is a Member of Parliament or a member of a local council,

(b) holds office in, or is employed by, a political party,

(c) is a public officer in active service, or

(d) has a financial interest in a business regulated by the Authority which conflicts with the person's duties.

(4) The President shall appoint the Chairperson and the members, subject to the approval of Parliament, from the persons nominated or selected under subsection (2).

(5) A member shall hold office for a term of four years, and is eligible for reappointment for one further term only.

(6) At least 30 per cent of the members of the Board shall be women.

Clause H: Director-General and security of tenure (new sections 17(1A) and 13A)

17. (1A) The Board shall appoint the Director-General through open and competitive recruitment, subject to the approval of Parliament.

13A. (1) The Chairperson, a member of the Board, the Director-General or a Deputy Director-General may be removed from office only for

(a) inability to perform the functions of the office, whether arising from infirmity of body or mind or any other cause,

(b) serious misconduct, or

(c) failure to disclose a conflict of interest.

(2) Before removal, the person shall be informed in writing of the grounds, and given an opportunity to be heard before a tribunal of three persons appointed by the Chief Justice.

(3) The President shall act on the recommendation of the tribunal, and the recommendation shall be laid before Parliament.

Clause I: Exemptions (replaces section 3, and deletes section 5)

3. (1) This Act shall not apply to the processing of personal data by an individual in the course of a purely personal or household activity.

(2) Sections 28(3) to (5), 43 to 49 and 61(1)(b) shall not apply to the processing of personal data where, and to the extent that, compliance would be likely to prejudice

(a) national security or defence,

(b) the prevention, detection, investigation or prosecution of an offence,

(c) the assessment or collection of a tax or duty, or

(d) proceedings before a court or tribunal.

(3) Subsection (2) applies only where the processing is authorised by law, and is necessary and proportionate to the purpose.

(4) Sections 27, 38, 56, 59 and 61(1)(a) apply to all processing, including processing to which subsection (2) applies.

(5) The Authority may inspect processing to which subsection (2) applies, subject to such safeguards for classified information as the Authority and the head of the institution concerned agree, and shall report annually to Parliament on the use of this section.

Clause J: Lawful grounds for processing (replaces sections 38 and 39)

38. (1) A data controller shall not process personal data unless at least one of the following applies:

(a) the data subject has given consent for one or more specific purposes,

(b) the processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject before entering into a contract,

(c) the processing is necessary to comply with a legal obligation of the data controller,

(d) the processing is necessary to protect the vital interests of the data subject or another person,

(e) the processing is necessary for a task carried out in the public interest, or in the exercise of official authority vested in the data controller by law, or

(f) the processing is necessary for the legitimate interests of the data controller or a third party, except where those interests are overridden by the rights and interests of the data subject, in particular where the data subject is a child.

(2) Paragraph (f) of subsection (1) does not apply to processing by a public authority in the performance of its functions.

(3) Where processing is based on consent, the data controller shall be able to show the data subject consented, and the data subject may withdraw consent at any time without affecting the lawfulness of processing before the withdrawal.

(4) Consent shall not be made a condition for the supply of a good or service where the processing is not necessary for the supply.

Consequential amendments: delete section 39, and in section 83(1)(a)(i) replace "without the explicit consent of the data subject" with "without a lawful ground under section 38."

Clause K: Prior authorisation for biometric, genetic and identification data (new section 31A)

31A. (1) Except where an Act of Parliament authorises the processing and provides safeguards for the rights of data subjects, a data controller shall not, without the prior written authorisation of the Authority, process

(a) biometric data, including fingerprints and facial images,

(b) genetic data, or

(c) a national identification number, or other identifier of general application, for a purpose other than the purpose for which the number was issued.

(2) The Authority shall decide an application under subsection (1) within 30 days, and may grant authorisation subject to conditions.

(3) The Authority shall publish a register of authorisations granted under this section.

Clause L: Direct marketing (new section 46A, and replaces section 46(5))

46A. (1) A person shall not use personal data to send direct marketing by telephone call, text message, email, social media message or other electronic communication unless

(a) the data subject has given prior consent, or

(b) the data subject is an existing customer, the marketing concerns similar goods or services, and the data subject was given a simple and free means of refusing at the time of collection and in every message.

(2) Every direct marketing message shall identify the sender and give a simple and free means of stopping further messages.

(3) In this section and in section 46, "direct marketing" means the communication, by whatever means, of advertising or marketing material directed to particular individuals.

Clause M: Protected disclosures (new section 80A)

80A. (1) No person shall be subjected to any civil, criminal, administrative or employment-related sanction, or to dismissal, discrimination or reprisal, for disclosing information on wrongdoing, or on a serious threat to health, safety or the environment, where the person acted in good faith and reasonably believed the information to be substantially true.

(2) A disclosure made to the Authority, the Anti-Corruption Commission, the Audit Service Sierra Leone, the police or a Member of Parliament shall be deemed to be made in the public interest.

(3) A term of any agreement or settlement which prevents a person from making a disclosure protected by this section is void.

(4) A person who imposes a sanction contrary to subsection (1) is liable in damages to the person sanctioned.

Clause N: Public information and privacy (new section 75A)

75A. (1) Nothing in Parts VI to IX or in section 83 prevents a public authority from publishing or disclosing

(a) information required to be published under sections 68 and 71,

(b) the name, title, office, functions, grade and remuneration of a public officer, or

(c) the terms of a contract with a public authority, including the identity of the contractor and the contract sum.

(2) A public authority publishing details of the beneficiaries of a public programme shall limit the details to what accountability requires, and shall not publish information likely to endanger the safety of a beneficiary.

(3) Publication or disclosure under this section is lawful processing for the purposes of section 38.

Clause O: Journalism, literature and art (new section 4A)

4A. (1) Sections 28, 33, 38, 43 to 49 and 50 shall not apply to the processing of personal data solely for journalistic, literary or artistic purposes, where

(a) the processing is undertaken with a view to publication,

(b) the data controller reasonably believes publication is in the public interest, and

(c) the data controller complies with a code of professional ethics recognised by the Independent Media Commission.

(2) Sections 56 and 59 continue to apply to processing under subsection (1).

Clause P: Personal data breaches (amends sections 1 and 61)

(a) Insert in section 1: "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.

(b) In section 61(1), replace "personal data has been accessed or acquired by an unauthorised person or entity" with "a personal data breach has occurred."

(c) Replace section 61(1)(b) with: "(b) communicate the breach to each affected data subject without undue delay, and in any event within [seven] days of notifying the Authority."

(d) Insert after section 61(1): "(1A) Where a data controller is unable to identify or contact an affected data subject, the data controller shall give public notice of the breach, within the period in paragraph (b) of subsection (1), through at least one national radio station, one newspaper of national circulation and the data controller's website, if any."

(e) Replace section 61(6) with: "(6) Communication to a data subject is not required where the personal data was encrypted to a standard approved by the Authority and the key was not compromised."

(f) Replace section 61(9) with: "(9) A data controller or data processor who fails to comply with subsection (1), (1A), (3) or (8) commits an offence."

Clause Q: Automated decisions (replaces section 47)

47. (1) A data controller shall not take a decision which produces legal effects concerning a data subject, or similarly affects the data subject in a significant way, based solely on automated processing, unless the decision is

(a) necessary for entering into or performing a contract with the data subject,

(b) authorised by a law which provides safeguards for the rights of the data subject, or

(c) based on the explicit consent of the data subject.

(2) In every case under subsection (1), the data controller shall inform the data subject of the decision and of the logic involved, and the data subject may, within 21 days, require a review of the decision by a natural person.

(3) The data controller shall complete the review, and inform the data subject of the outcome, within 14 days of the request.

Clause R: Enforcement notices and administrative penalties (new section 16A)

16A. (1) Where the Authority is satisfied a data controller, data processor or public authority has failed to comply with this Act, the Authority may serve an enforcement notice stating the failure, the steps required and the period for compliance, which shall not be less than 14 days.

(2) Where a person fails to comply with an enforcement notice, or the failure is serious, the Authority may, after giving the person written notice of the proposed penalty and an opportunity to be heard, impose an administrative penalty not exceeding the higher of NLe [ ] or [two] per cent of the person's annual turnover in Sierra Leone for the preceding financial year.

(3) In deciding whether to impose a penalty, and the amount, the Authority shall consider the nature, gravity and duration of the failure, the number of persons affected, the harm caused, any steps taken to reduce the harm, any previous failure and the degree of cooperation.

(4) An administrative penalty shall be paid into the Consolidated Fund.

(5) The Authority shall publish every enforcement notice and administrative penalty.

Clause S: Entry and search under warrant (replaces section 16(1)(d))

(d) with the consent of the occupier, or under a warrant issued by a Judge of the High Court on reasonable grounds to suspect a breach of this Act, enter and search premises occupied by a data controller or data processor, and inspect, copy or seize records, data or equipment relevant to an investigation,

Clause T: Offences and penalties (replaces section 85, and deletes section 88(3))

85. (1) A person who commits an offence under this Act for which no other penalty is provided is liable on conviction

(a) in the case of an individual, to a fine not exceeding NLe [ ] or to imprisonment for a term not exceeding [two] years, or to both, and

(b) in the case of a body corporate, to a fine not exceeding NLe [ ].

(2) A person who knowingly obtains, discloses or sells personal data in breach of section 83 is liable on conviction to a fine not exceeding NLe [ ] or to imprisonment for a term not exceeding [five] years, or to both.

Consequential amendments: in sections 45(5), 46(4), 50(8), 61(9), 81(2), 82(2), 83(5) and 84, replace "to such penalty as the Minister may, in consultation with the Authority, prescribe" with "to the penalty in section 85."

Clause U: Data protection officers (new section 57A)

57A. (1) A public authority, and a data controller or data processor whose core activities involve large-scale processing of sensitive personal data or the regular monitoring of individuals, shall designate a data protection officer.

(2) The data protection officer shall advise on compliance, receive requests and complaints from data subjects, and act as the point of contact with the Authority.

(3) The data controller shall publish the contact details of the data protection officer and notify the Authority of them.

Clause V: Transitional provisions (replaces section 91)

91. (1) On the commencement of this Act,

(a) the Information Commission established under the Right to Access Information Act, 2013 is dissolved, and the assets, liabilities, rights, obligations, contracts and records of the Commission vest in the Authority,

(b) every person employed by the Commission becomes an employee of the Authority, on terms not less favourable than those enjoyed immediately before commencement, and

(c) every application, review, appeal or other proceeding pending before the Commission continues before the Authority, and shall be decided under the Right to Access Information Act, 2013.

(2) The Information Commissioner and the Commissioners in office immediately before commencement shall perform the functions of the Board until the Board is constituted under section 7, which shall be within six months of commencement.

(3) A publication scheme approved under the Right to Access Information Act, 2013 continues in force until replaced under section 68, and the period in section 68(6) runs from the date of the first approval of a scheme under the Act of 2013.

(4) A data controller or data processor shall comply with Parts VI to IX within [12] months, and apply for registration within [6] months, of commencement.

ILRAJ's call to Parliament

Honourable Members, you have a rare chance to give Sierra Leone a data protection law for the digital age, and to strengthen a right to information law already admired across Africa. Please do not trade the second for the first.

ILRAJ asks you to pass a final Act which:

- keeps every safeguard of the Right to Access Information Act, 2013, including review, appeal to the High Court and whistleblower protection
- lets every citizen ask for information without giving a reason, by speaking or writing, in English, Krio or any local language
- applies the data protection rules to government, with narrow exemptions set out in the Act
- gives businesses and public services clear lawful grounds to use personal data
- protects biometric data, children's data and citizens' phones and inboxes from misuse
- creates an Authority free of government control, with the power to fine and the duty to act fairly
- leaves penalties to Parliament, not to a Minister
- moves staff, cases and publication schemes from the existing Commission to the new Authority without loss

ILRAJ stands ready to brief the Committee, to share its full schedule of drafting corrections, and to work with the Ministry of Information and Civic Education and the Law Officers' Department on the clauses proposed above.

Issued in Freetown by the Institute for Legal Research and Advocacy for Justice (ILRAJ), November 2026.

Basita Michael Executive Director

Sources

- The Data Protection and Right to Access Information Bill, 2026, Supplement to the Sierra Leone Gazette Vol. CLXVII, No. 62, 2 July 2026
- The Right to Access Information Act, 2013 (Act No. 2 of 2013)
- The Constitution of Sierra Leone, 1991
- The Cyber Security and Crime Act, 2021 (Act No. 7 of 2021)
- Gender Equality and Women's Empowerment Act, 2022 (Act No. 23 of 2022)
- ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS
- Africa Legal, ECOWAS strengthens its data protection framework (7 August 2026)
- African Union, status list of the Convention on Cyber Security and Personal Data Protection
- African Commission, Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019
- Kenya, Data Protection Act, 2019
- Kenya, Access to Information Act, 2016
- Nigeria, Data Protection Act, 2023
- South Africa, Protection of Personal Information Act, 2013
- Ghana, Right to Information Act, 2019 (Act 989), Afriwise summary
- UK Data Protection Act 1998, section 11
- Global Right to Information Rating, Sierra Leone
- RTI Evaluation Report, Sierra Leone (2025)
- World Bank data via FRED, adult literacy rate, Sierra Leone
- Al Jazeera, Sierra Leone launches re-denominated currency (1 July 2022)
- Citizens' Barray, Position Paper on the Data Protection and Right to Access Information Bill 2026 (November 2026)