International Journal of Innovative Inventions in Social Science and Humanities

ISSN(print): 3050-6921, ISSN(online): 3050-693X

Volume 03 Issue 11 November 2026

DOI: 10.58806/ijiissh.2026.v3i11n06

Page No: 1534-1545

From Data Protection to Algorithmic Accountability: Rethinking Legal Remedies for AI-Assisted Decisions in Ghana

Dr Godwin Gaduga

Lecturer at Accra Institute of Technology Adjunct Lecturer at Blue Crest University College.

ABSTRACT

Public bodies and private institutions in Ghana increasingly rely on artificial intelligence to allocate credit, screen applicants, select taxpayers for audit and determine eligibility for services, yet the statutes that govern these decisions were enacted for an earlier technological order. This article contends that the resulting deficit is chiefly remedial. The 1992 Constitution guarantees privacy, equality, access to information and administrative justice, and the Data Protection Act, 2012 (Act 843) contains an early African provision on decisions based solely on automated processing; but these instruments do not reliably secure for an affected person the conditions on which an effective remedy depends. Those conditions are notice that an automated system contributed to the decision, reasons sufficient to permit a challenge, a record from which the decision can be reconstructed, review by a person empowered to alter the outcome, and redress proportionate to the harm. The article develops these conditions as the Remedial Chain Test and applies it to the law in force at 29 October 2026. It distinguishes binding law from the proposals in the Data Protection Bill, 2025, the Cybersecurity (Amendment) Bill, 2025 and the Emerging Technologies Bill, and it identifies the evidence that regulators, courts and researchers would require to establish whether the framework operates in practice.

KEYWORDS: Algorithmic Accountability, Automated Decision-Making, Data Protection Act 2012 (Act 843), Administrative Justice, Article 23, Legal Remedies, Human Review, Ghana.

ARTICLE DETAILS

Published On:
16 November 2026

Available on:
https://ijiissh.com/

I. INTRODUCTION

A person in Accra who is refused a loan, excluded from a recruitment exercise, selected for a tax audit or denied a public benefit may well have been assessed, at some stage, by a system that scores, ranks or predicts. For that person, the decisive legal question concerns neither the sophistication of the system nor its commercial origin. It is whether the law enables them to discover what happened, to challenge it and to obtain redress if the decision was wrong. Ghanaian law answers that question only in part. Article 18(2) of the 1992 Constitution protects the privacy of a person's home, property, correspondence and communication, and article 23 requires administrative bodies and officials to act fairly and reasonably, conferring on persons aggrieved by their acts and decisions a right to seek redress before a court or other tribunal.[1] The Data Protection Act, 2012 (Act 843) addresses, in section 41, decisions that significantly affect an individual and are based solely on automated processing, and section 43 entitles an individual to compensation for damage caused by a data controller's failure to comply with the Act.[2]

The incompleteness of this protection matters because the remedy a person actually obtains is determined by the weakest provision in the sequence, whatever the strength of the others. A right to reconsideration of a solely automated decision avails little to a person who was never told that automation was involved. A right of access is of limited value where the controller holds the personal data while the logic of the model remains with a vendor. A constitutional guarantee of fair administrative action is difficult to invoke where the official who signed the decision did little more than confirm a score that no one in the institution could explain. The thesis of this article is that Ghana's principal difficulty in this field is remedial. The legal order already recognises most of the values that

[1]Constitution of the Republic of Ghana 1992, arts 18(2) and 23.

[2]Data Protection Act 2012 (Act 843), ss 41 and 43.

algorithmic accountability requires, but it has not yet organised its institutions and evidentiary practices so that those values reach the individual when harm occurs.

The inquiry is timely. The Data Protection Commission declared 2026 a year of enforcement, and in March 2026 the Minister for Communications, Digital Technology and Innovations announced that government was preparing new data protection legislation addressing artificial intelligence, automated decision-making and cross-border data flows.[3] The Government launched a National Artificial Intelligence Strategy in April 2026 and has described an Emerging Technologies Bill as the intended legal framework for the deployment of artificial intelligence.[4] These developments present an opportunity for reform. They also create a risk that proposals will be mistaken for law, and that institutions will postpone present obligations in anticipation of future ones. The article therefore distinguishes throughout between what binds today, what has been proposed, and what is offered here as recommendation.

Part II sets out the scope of the inquiry, its method and the three categories of authority on which the analysis relies. Part III develops the Remedial Chain Test. Parts IV to VI examine the constitutional, data protection and supporting statutory frameworks in the light of that test, and Part VII considers algorithmic transparency and the conditions of effective human review. Part VIII identifies the structural gaps in the remedies presently available, and Part IX draws on comparative experience. Part X sets confirmed requirements against proposed safeguards, Part XI specifies the evidence needed to evaluate implementation, Part XII advances reform proposals, and Part XIII concludes.

II. SCOPE, METHOD AND CATEGORIES OF AUTHORITY

The subject of the article is the AI-assisted decision, defined as any decision concerning an identifiable individual to which an output generated by a statistical, machine-learning or rule-based computational system makes a material contribution, whether the final act is performed by the system or by an official who relies on it. The definition extends beyond decisions taken solely by automated means. In most institutions, the prevailing arrangement is not full automation; it is a hybrid in which a human signature formally concludes a process whose substance has been largely settled by a score, a flag or a ranking. A remedial framework confined to solely automated decisions would therefore exclude most of the cases in which harm occurs. The article is concerned with the position of the affected person and the remedies available to that person. Questions about how public institutions acquire such systems, and about the constitutional design of institutional answerability more generally, are considered only so far as they bear on remedy.

The method is doctrinal and institutional. The doctrinal inquiry reads the constitutional and statutory text, together with Ghanaian case law where it exists, to identify the obligations that presently bind data controllers and public officials. The institutional inquiry asks how those obligations are, or could be, given effect in the practice of the Data Protection Commission, the Commission on Human Rights and Administrative Justice and the courts. Material from the European Union, the Netherlands, the United Kingdom, Canada and Australia is used to identify solutions that have been tested and failures that have been documented. It is persuasive only and is not treated as authority.

Because the field is changing quickly and the risk of mistaking a proposal for law is considerable, each proposition in the article falls within one of three categories. **Confirmed law** comprises constitutional provisions, Acts of Parliament, legislative instruments and judgments binding at 29 October 2026. **Declared policy or proposed law** comprises bills published for consultation, ministerial statements and national strategies, none of which confers enforceable rights until enacted or formally adopted. **Proposed safeguards** are recommendations made in this article or in the scholarly literature that have no present legal basis in Ghana. Where the official consolidated text of a provision could not be confirmed against the Gazette or an authoritative reprint, the relevant note says so.[5]

[3] 'When the Algorithm Recommends, Who Decides?' *Modern Ghana* (2026) <https://www.modernghana.com/news/1527789/when-the-algorithm-recommends-who-decides.amp> accessed 29 October 2026; 'Sam George Announces New Data Protection Bill and Strict Enforcement Measures' (Ghana Chamber of Telecommunications, reproducing GBC, 2026) <https://www.telecomschamber.org/industry-news/sam-george-announces-new-data-protection-bill-and-strict-enforcement-measures/> accessed 29 October 2026.

[4] E Nutsugah, 'Ghana to Invest $250m in AI Centre, Launch National Strategy' *Ghana News Agency* (Accra, 24 April 2026) <https://gna.org.gh/2026/04/ghana-to-invest-250m-in-ai-centre-launch-national-strategy-2/> accessed 29 October 2026; 'Gov't to Lay Emerging Technologies Bill Before Parliament in 2026' *Citinewsroom* <https://citinewsroom.com/2025/11/govt-to-lay-emerging-technologies-bill-before-parliament-in-2026/> accessed 29 October 2026.

[5] Statutory provisions are cited from the texts available through the Data Protection Commission <https://dpc.gov.gh/compliance/>, the Cyber Security Authority <https://www.csa.gov.gh/resources.php> and GhaLII <https://ghalii.org>. Provisions whose consolidated text could not be confirmed are identified in the notes.

III. THE REMEDIAL CHAIN TEST

Data protection law and algorithmic accountability overlap, but they do not coincide. Data protection asks whether personal data is collected, used, retained and secured lawfully, and it confers on the individual rights in respect of that data. Algorithmic accountability asks whether a decision affecting a person can be traced, explained, contested and corrected; its object is the decision. The distinction has practical consequences. A system may process personal data in full compliance with the data protection principles and still produce a decision that is arbitrary, discriminatory or inexplicable. Equally, a decision may be unfair for reasons unconnected with the handling of personal data, such as an ill-chosen threshold or a model trained on a population that does not resemble the people to whom it is applied. The movement described in the title of this article is thus an enlargement of the object of data protection, from the lawful handling of information to the answerability of the institution that acts upon it.

The literature suggests that a narrowly framed right to explanation cannot bear this weight alone. Wachter, Mittelstadt and Floridi argued that the General Data Protection Regulation contains no free-standing right to an explanation of individual automated decisions, and Edwards and Veale observed that even a well-designed right of explanation may not furnish the remedy that affected people need, which is more often a different outcome, a corrected record or an assurance that the error will not recur.[6] Citron's earlier account of technological due process made the related point that automated administration erodes the procedural protections of notice and hearing unless those protections are deliberately built into the design of the system.[7] It follows that remedies should be conceived as a connected sequence, each element of which depends on those before it.

The Remedial Chain Test, which is advanced as an evaluative framework and not as a statement of existing law, holds that an affected person has an effective remedy against an AI-assisted decision only where each of the following five links is present and connected to the next:

1. **Notice:** the person is informed, at or before the time of the decision, that an automated system contributed to it, which system it was, and which institution is answerable for it;
2. **Reasons:** the person can obtain an account of the principal factors that produced the outcome in their case, stated in terms that enable them to identify an error or an improper consideration;
3. **Record:** the institution retains, for a defined period, the inputs, the version of the model, the output, the action taken on it by any official and the reasons recorded, so that a reviewer, regulator or court can reconstruct the decision;
4. **Review:** a person with the authority, competence and time to do so examines the decision on its merits and may alter it, so that review does not merely ratify the output of the system; and
5. **Redress:** where the decision was wrong or unlawful, the person obtains correction, reversal, compensation or another proportionate remedy, and the institution is required to address the cause.

The links are interdependent. Reasons cannot be given where no record was kept; review is ineffective where the reviewer cannot see the reasons; and redress is unattainable where the person never learned that the decision could be challenged. The test also allocates responsibility, because each link can be assigned to an identifiable duty-bearer: the deploying institution for notice and review, the institution and its vendor for reasons and record, and the regulator or court for redress where the institution fails. In this respect, the framework reflects the communitarian conception of responsibility defended by Gyekye, in which rights acquire practical meaning only where the community, here the institution exercising power, accepts correlative duties toward the individual.[8] The following Parts apply the test to each body of Ghanaian law in turn.

IV. THE CONSTITUTIONAL BASIS OF REMEDY

The 1992 Constitution provides the most secure foundation for the chain. It binds the State; it cannot be displaced by contract or by the terms of a vendor's licence, and it confers rights of action that do not depend on any statute concerned with technology. By article 12(1), moreover, the fundamental human rights and freedoms in Chapter Five are to be respected and upheld by all natural and legal persons, as well as by the organs and agencies of government.[9] The question for present purposes is which provisions an affected person can invoke to secure each link. Article 23 is the most important. It requires administrative bodies and administrative officials to act fairly and reasonably and to comply with the requirements imposed on them by law, and it confers on persons aggrieved by the exercise of their acts and decisions a right to seek redress before a court or other tribunal. Article 296 requires that a discretionary power vested in any person or authority be exercised fairly and candidly, without arbitrariness, caprice or bias, and

[6] S Wachter, B Mittelstadt and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76; L Edwards and M Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law and Technology Review 18.

[7] DK Citron, 'Technological Due Process' (2008) 85 Washington University Law Review 1249.

[8] K Gyekye, *Tradition and Modernity: Philosophical Reflections on the African Experience* (OUP 1997).

[9] Constitution 1992 (n 1), art 12(1).

in accordance with due process of law. Article 17 guarantees equality before the law and prohibits discrimination on the grounds it lists, and article 21(1)(f) guarantees the right to information, to which the Right to Information Act, 2019 (Act 989) now gives statutory effect.[10]

Article 23 is significant for AI-assisted decisions because it regulates the conduct of the decision-maker, whatever means the decision-maker employs. In *Awuni v West African Examinations Council,* the Supreme Court held that the cancellation of candidates' examination results without affording them a hearing was contrary to the requirements of fairness, and it treated article 23 as giving constitutional force to the rules of natural justice in administrative decision-making.[11] The case is instructive because it concerned an institutional determination, affecting many candidates, founded on a pattern that the institution had detected. That is close in structure to the operation of an anomaly-detection system that flags candidates, taxpayers or claimants. On the reasoning in *Awuni*, the fact that a pattern was identified by software and not by a human examiner would not relieve a public body of the duty to hear the affected person before acting on it. Article 23 therefore supports the notice, reasons and review links as matters of confirmed constitutional law wherever the decision-maker is an administrative body. Article 296 reinforces the review link. An official who adopts a score without understanding its basis, or who applies a threshold mechanically regardless of the facts of the individual case, exercises a discretion that can hardly be described as candid or as conforming to due process.

Article 18(2) bears on the data from which AI-assisted decisions are produced. In *Raphael Cubagee v Michael Yeboah Asare,* the Supreme Court considered the relationship between article 18(2) and the admissibility of a privately made recording, and the decision confirms that privacy arguments are justiciable in the course of civil proceedings.[12] Article 17 is engaged whenever outputs correlate with a protected characteristic, although its application to indirect discrimination produced by an automated system has not been tested in a Ghanaian court. These guarantees are enforceable in the High Court under article 33, and complaints may be brought before the Commission on Human Rights and Administrative Justice under article 218.[13] The constitutional layer is therefore strong at the review and redress links. Its weakness is that it presupposes what it does not secure. A litigant must first know that an automated system was involved and must then obtain enough information about it to frame a claim, and the Constitution does not itself prescribe how either is to be achieved.

V. THE DATA PROTECTION ACT, 2012 (ACT 843)

A. Reach and principles

Act 843 is the most developed source of individual rights relevant to AI-assisted decisions in Ghana. It applies to the State as well as to private persons, since section 91 treats each government department as a data controller.[14] By section 45, it applies to controllers established in Ghana, to controllers established elsewhere that use equipment or processors in Ghana, and to the processing of data originating wholly or partly from Ghana, which brings many foreign providers that process Ghanaian personal data within its scope.[15] The principles in section 17 are accountability, lawfulness of processing, specification of purpose, compatibility of further processing with the purpose of collection, quality of information, openness, data security safeguards and data subject participation.[16] Each translates into an obligation on the person who deploys an automated system. Section 26, which requires personal data to be complete, accurate, up to date and not misleading having regard to the purpose of processing, applies to the data used to produce an individual score. Section 25 restricts the reuse of data collected for one administrative purpose to operate a model serving another. Section 27 requires the controller to ensure that the data subject is aware of the purpose of the collection and of the persons responsible for it.[17] These provisions provide a confirmed foundation for the notice and record links, although they do not, in terms, require disclosure that automated processing will be used to make or support a significant decision.

B. Section 41 and the word solely

Section 41 is the distinctive contribution of the Act. It concerns decisions taken by or on behalf of a controller that significantly affect a data subject and are based solely on processing by automatic means, and it enables the individual to require the controller

[10]Constitution 1992 (n 1), arts 17, 21(1)(f) and 296; Right to Information Act 2019 (Act 989).

[11]*Awuni v West African Examinations Council* [2003-2004] SCGLR 471.

[12]*Raphael Cubagee v Michael Yeboah Asare* (Supreme Court of Ghana, 2018). The full law report citation and the precise holding should be confirmed before publication.

[13]Constitution 1992 (n 1), arts 33 and 218.

[14]Act 843, s 91.

[15]Act 843, s 45.

[16]Act 843, s 17.

[17]Act 843, ss 25 to 27.

to reconsider the decision or to take a new decision on a different basis.[18] The rights of access in sections 32 and 35 enable a data subject to obtain confirmation of the personal data held, and commentators read them as extending to information about the logic of significant solely automated decisions.[19] The section bears a close structural resemblance to section 12 of the United Kingdom's Data Protection Act 1998, under which the controller was required to notify the individual that a decision had been taken on that basis and the individual could then require reconsideration.[20] By framing the remedy as reconsideration, the provision offers affected people something closer to what they usually seek than an abstract explanation would.

Measured against the Remedial Chain Test, however, section 41 has three limitations. The first and most consequential arises from the word *solely*. Where an official considers a score before signing the decision, however briefly, the controller may contend that the decision was not based solely on automated processing, with the result that the protection does not apply to the hybrid decisions that predominate in practice. Any duty of notice that section 41 imposes is subject to the same limitation, because it arises only once a decision falls within the provision. No Ghanaian court has yet construed the word, and the comparative authority considered in Part IX supports a construction that looks to the practical weight of the automated output in the decision, so that the formal participation of an official is not conclusive. The second limitation is that the mechanism depends on the data subject's initiative. The third is that the section prescribes no standard for the reconsideration itself, so that a controller may comply in form by running the same model again on the same inputs.

C. Security and the controller-processor relationship

Section 28 requires a controller to secure the integrity of personal data by appropriate, reasonable technical and organizational measures, to identify reasonably foreseeable risks and to keep its safeguards under review. Section 30 requires the controller to ensure that a processor acting on its behalf complies with those measures, and section 30(4) addresses processors not domiciled in Ghana. Section 31 requires notification of security compromises to the Commission and the data subject as soon as reasonably practicable.[21] For remedy, the significance of these provisions is that they fix responsibility on the controller. An institution that engages a vendor to host and operate a model remains the controller and remains answerable to the affected person for the vendor's processing. It cannot rely on the vendor's control of documentation or logs to excuse a failure to give reasons or to reconstruct a decision.

D. Remedies under the Act

The Act provides four remedial routes. Under section 33, a data subject may require the correction or deletion of personal data that is inaccurate, irrelevant, excessive, out of date, incomplete or misleading, and the controller must either comply or provide credible evidence in support of the data. Under section 39, a data subject may require a controller to cease processing that causes or is likely to cause unwarranted damage or distress. Under section 43, an individual who suffers damage by reason of a controller's failure to comply with the Act is entitled to compensation.[22] Finally, the Commission, whose functions under section 3 include the investigation and fair determination of complaints, may serve an enforcement notice under section 75 requiring a controller to refrain from contravening the data protection principles.[23] These routes provide the outline of the redress link. In practice, they are weakened by the absence of a published procedure specifying what a complaint to the Commission must contain, the time within which it must be determined and the evidence a complainant may compel, and by the absence, so far as published material discloses, of any Commission determinations on automated decisions to guide controllers.

E. The Data Protection Bill, 2025

The Data Protection Bill, 2025, published for consultation between 20 and 31 October 2025, would repeal Act 843 and replace the Commission with a Data Protection Authority. It would require impact assessments for processing likely to pose risks to data subjects, require data protection by design and by default, mandate the appointment of data protection officers, and confer rights including data portability, erasure and specific rights in relation to automated decision-making.[24] The Minister's statement of March

[18]Act 843, s 41. Secondary summaries differ as to the notice mechanism and the periods prescribed, and the wording should be checked against the gazetted text before reliance.

[19]Act 843, ss 32 and 35; 'What Is Data Protection Act, 2012 (Act 843)?' *OfflistMe* (August 2026) <https://www.offlist.me/what-is-ghana-data-protection-act> accessed 29 October 2026. The extension of access to decision logic is asserted in secondary sources and should be confirmed against the gazetted text.

[20]Data Protection Act 1998 (UK), s 12 (repealed).

[21]Act 843, ss 28, 30 and 31.

[22]Act 843, ss 33, 39 and 43.

[23]Act 843, ss 3, 75 and 76.

[24]Data Protection Bill 2025 (consultation draft) <https://moc.gov.gh/wp-content/uploads/2023/03/DATA-PROTECTION-BILL.pdf> accessed 29 October 2026; Digital Policy Alert, 'Ministry of Communication, Digital Technology and Innovations

2026 indicated that further work was in progress on legislation addressing artificial intelligence and automated decision-making.[25] The Bill is not law. Its final text is unsettled, and controllers remain bound by Act 843 until its repeal takes effect. It nonetheless indicates the direction of policy, and its impact assessment requirement, if enacted with adequate content, would supply much of the record link that Act 843 lacks.

VI. SUPPORTING STATUTES: CYBERSECURITY, ELECTRONIC TRANSACTIONS AND THE LIMITS OF CONTRACT

The Cybersecurity Act, 2020 (Act 1038) establishes the Cyber Security Authority, provides for the designation and protection of critical information infrastructure, regulates cybersecurity service providers and establishes arrangements for responding to incidents.[26] Its contribution to the chain is confined to the record link, but it is a real one. A model whose inputs have been tampered with, or whose outputs have been manipulated, will produce decisions that are wrong for reasons the affected person cannot detect; and an institution that cannot show that its system was secure at the time of the decision cannot show that the decision resulted from the process it describes. Act 1038 confers no individual remedy for harm caused by a decision, and its enforcement mechanisms are regulatory and penal. The Cybersecurity (Amendment) Bill, 2025, published for consultation between 1 October and 14 November 2025, would empower the Authority, among other things, to set and certify security standards for emerging technologies including artificial intelligence. It has been criticized by journalists' associations and civil society organizations concerned about the breadth of the investigative powers it would confer and their compatibility with article 18(2).[27] The Bill is a proposed law, and its parliamentary status should be confirmed at the date of publication.

The Electronic Transactions Act, 2008 (Act 772), as amended by the Electronic Transactions (Amendment) Act, 2012 (Act 838) and by Act 1038, is relevant to remedy in two respects.[28] First, it recognises automated transactions and lays down rules for attributing electronic records to their originator. These provisions support the conclusion that an institution is bound by what its system does on its behalf and cannot disclaim responsibility for an output by invoking the autonomy of the system.[29] Secondly, its provisions on the admissibility and evidential weight of electronic records, read with the Evidence Act, 1975 (NRCD 323), determine whether system logs and model outputs can be proved in legal proceedings. The record link is therefore a matter of the law of evidence as well as of administrative practice.[30] Act 772 does not regulate the substance of automated decisions, and it requires neither explanation nor review.

The arrangements by which an institution acquires an automated system fall outside the scope of this article, but one point concerning them is essential to remedy. The contract between a deploying institution and its vendor cannot diminish the institution's obligations to the affected person, who is not a party to it. The institution remains the decision-maker for article 23 and the controller for Act 843. A contract that leaves the institution without access to the documentation and logs it needs does not excuse a failure to give reasons or to reconstruct a decision; it may instead evidence a failure to adopt the organisational measures required by section 28. Whether a vendor owes a duty of care in tort directly to persons subjected to decisions produced by its system has not been considered by a Ghanaian court.

Closes Consultation on Data Protection Act, 2025' <https://digitalpolicyalert.org/event/34534-ministry-of-communication-digital-technology-and-innovations-closes-consultation-on-data-protection-act-2025-including-data-protection-regulation> accessed 29 October 2026; 'Ghana's Corporate Commercial Outlook 2026' *Mondaq* (16 July 2026) <https://www.mondaq.com/corporate-and-company-law/1818508/ghanas-corporate-commercial-outlook-2026> accessed 29 October 2026.

[25]Ghana Chamber of Telecommunications (n 3).

[26]Cybersecurity Act 2020 (Act 1038).

[27]Digital Policy Alert, 'Cyber Security Authority Opened Consultation on Draft Cybersecurity (Amendment) Bill' <https://digitalpolicyalert.org/event/34393-cyber-security-authority-opened-consultation-on-draft-cybersecurity-amendment-bill-2025-including-cybersecurity-regulation> accessed 29 October 2026; International IDEA, 'Ghana: October 2025' *Democracy Tracker* <https://www.idea.int/democracytracker/report/ghana/october-2025> accessed 29 October 2026.

[28]Electronic Transactions Act 2008 (Act 772), as amended by the Electronic Transactions (Amendment) Act 2012 (Act 838) and Act 1038 <https://ghalii.org/akn/gh/act/2008/772> accessed 29 October 2026.

[29]Act 772, ss 17 and 21. The section numbers are taken from the arrangement of sections and should be confirmed against the consolidated text.

[30]Act 772, s 7; Evidence Act 1975 (NRCD 323).

VII. ALGORITHMIC TRANSPARENCY AND EFFECTIVE HUMAN REVIEW

A. Three levels of transparency

Transparency comprises distinct duties owed to different audiences, and failure to distinguish them is a common source of weak regulation. System-level transparency concerns public knowledge that an institution uses a particular system, for what purpose and under what governance. Decision-level transparency concerns the factors that produced the outcome in an individual case. Audit-level transparency concerns access by regulators, auditors and courts to the model, its documentation, its data and its logs. Ghanaian law addresses these levels unevenly. System-level transparency is supported by Act 989, which entitles a person to request information held by a public institution, subject to the exemptions the Act provides. A researcher, journalist or affected person may therefore ask whether an institution uses an automated system and on what terms, although the exemptions may limit disclosure and the procedure is slow in comparison with the timescale of an individual decision.[31] Decision-level transparency is supported by the rights of access under Act 843 and, in the case of public bodies, by article 23; but neither instrument expressly requires an institution to disclose, at the time of a hybrid decision, that automation was involved. Audit-level transparency has no dedicated statutory basis beyond the general investigative functions of the Data Protection Commission and the Cyber Security Authority.

B. Human review and automation bias

The most common regulatory response to AI-assisted decisions is to require human involvement, and its most common failure is that the official becomes a ratifier of the output instead of a reviewer of the decision. Research on automation bias has shown for more than two decades that people who supervise automated systems tend to defer to their outputs and to overlook errors the system does not flag. Green's study of policies requiring human oversight of government algorithms concluded that such policies frequently provide false reassurance, because the conditions under which reviewers can correct algorithmic errors are seldom satisfied.[32] This research has two implications for Ghana. It explains the fragility of the word *solely* in section 41, since nominal review can remove a decision from the provision while leaving its substance unchanged. It also suggests that articles 23 and 296 furnish a more exacting standard than the statute, because they ask whether the decision-maker in fact acted fairly, reasonably and candidly, and not merely whether an official was formally involved.

For the Remedial Chain Test, review is effective only where five conditions are met. The reviewer must have authority to depart from the output of the system; access to the information on which the output was based and to the affected person's representations; the competence to evaluate both; sufficient time to do so; and freedom from any formal or informal penalty for departing from the output. Each condition is observable, and Part XI identifies the evidence by which an evaluator could determine whether it is satisfied. The National Artificial Intelligence Strategy launched in April 2026 is described in official and press accounts as committed to responsible and human-centred artificial intelligence, and the Government has announced the establishment of a Responsible Artificial Intelligence Office to oversee its implementation.[33] The Strategy is a statement of policy and confers no enforceable right. Its effect on remedies will depend on whether its commitments are carried into legislation, into binding regulatory guidance, or into institutional practice that a court might regard as informing what fairness requires under article 23.

VIII. REMEDIES IN PRACTICE: THREE STRUCTURAL GAPS

Taken together, Parts IV and V disclose at least six avenues of redress grounded in confirmed law: a request to the controller under sections 32, 33, 35 and 41 of Act 843; a complaint to the Data Protection Commission; a claim for compensation under section 43; an application for judicial review in reliance on article 23; an application to the High Court under article 33 for the enforcement of fundamental rights; and a complaint to the Commission on Human Rights and Administrative Justice under article 218. The difficulty does not lie in the number of these avenues. It lies in three structural features that they share.

The first is that each avenue is reactive and individual. Each requires the affected person to become aware of the harm, to identify the responsible institution, to choose a forum and to bear the cost of proceeding. The harms produced by automated systems, by contrast, are frequently systemic and diffuse, affecting many people to a modest degree, and the comparative experience considered in Part IX shows that harms of this kind may persist for years before any individual challenge succeeds.

The second is that the burden of proof is the decisive obstacle. In a claim under section 43, or an application under article 33, the claimant must establish non-compliance or infringement and must show that it caused the loss. Where the relevant evidence consists of the model, its data and its logs, and these are held by the institution or its vendor, the claimant cannot discharge that burden

[31] Act 989.

[32] LJ Skitka, KL Mosier and M Burdick, 'Does Automation Bias Decision-Making?' (1999) 51 International Journal of Human-Computer Studies 991; B Green, 'The Flaws of Policies Requiring Human Oversight of Government Algorithms' (2022) 45 Computer Law and Security Review 105681.

[33] Nutsugah (n 4); 'Ghana Launches National AI Strategy' *TechAfrica News* (27 April 2026) <https://techafricanews.com/?p=77164> accessed 29 October 2026.

without disclosure, and the ordinary rules of discovery are ill-adapted to technical material of this kind. The record link is accordingly the condition on which every judicial remedy depends.

The third concerns decisions taken by private institutions. Article 23 applies to administrative bodies and administrative officials, and the administrative justice mandate of the Commission on Human Rights and Administrative Justice is directed principally at public services. A person refused credit, insurance or employment by a private institution based on an automated score must therefore rely on Act 843, on the general law and, where a fundamental right is engaged, on article 12(1), which binds natural and legal persons, together with the jurisdiction of the High Court under article 33 and that of the Commission under article 218(c) to investigate violations of fundamental rights by private persons and enterprises.[34] These routes are available, but they lack the procedural guarantees of fair hearing and reasons that article 23 secures against public bodies, although private deployments in credit, insurance and employment are no less consequential than public ones.

IX. COMPARATIVE LESSONS

Article 22 of the European Union's General Data Protection Regulation confers on data subjects a right not to be subject to a decision based solely on automated processing that produces legal effects concerning them or similarly significantly affects them, subject to exceptions accompanied by safeguards that include the rights to obtain human intervention and to contest the decision. In *SCHUFA* the Court of Justice gave the concept of a decision a broad reading, holding that the automated establishment of a probability value by a credit reference agency is itself such a decision where a third party to which it is transmitted draws strongly on it in deciding whether to enter into a contract.[35] The reasoning offers a model for construing *solely* in section 41 of Act 843 by reference to the practical weight of the automated output. The Artificial Intelligence Act adds a regime based on risk. It requires human oversight of high-risk systems under article 14, imposes obligations on deployers under article 26 and, under article 86, gives affected persons a right to clear and meaningful explanations of the role of a high-risk system in decisions that produce legal or similarly significant effects.[36]

In the Netherlands, the District Court of The Hague held in February 2020 that the legislation governing SyRI, a system used to identify individuals at risk of committing welfare and tax fraud, violated article 8 of the European Convention on Human Rights because it lacked the transparency and safeguards required to render the interference with private life proportionate.[37] The judgment shows that a privacy guarantee comparable to article 18(2) can found a challenge to the legal basis of an entire algorithmic programme, and that opacity may itself render an interference unlawful because it prevents both the individual and the court from assessing proportionality. In the United Kingdom, the Court of Appeal in *R (Bridges) v Chief Constable of South Wales Police* held the police use of automated facial recognition unlawful on several grounds, including a breach of the public sector equality duty arising from the force's failure to take reasonable steps to satisfy itself that the software did not exhibit unacceptable bias on grounds of race or sex.[38] That holding places on the deploying public body the duty to investigate bias and treats reliance on the vendor's assurances as insufficient, which accords with the allocation of responsibility under section 30 of Act 843.

Canada's Directive on Automated Decision-Making requires federal institutions to complete an algorithmic impact assessment before deploying an automated decision system, scales the requirements of notice, explanation, human intervention and testing to the assessed level of impact, and requires the assessments to be published.[39] It is an executive instrument, and its relevance to Ghana lies in showing how much of the chain can be constructed without primary legislation. In Australia, the Royal Commission into the Robodebt Scheme reported in July 2023 on an automated debt-raising programme that averaged annual income data to infer overpayments of welfare benefits, placed on recipients the burden of disproving the debts, and continued for years despite internal doubts as to its lawfulness.[40] The scheme failed at every link of the chain. Recipients received no intelligible reasons, could not see how their debts had been calculated, faced slow reviews that frequently confirmed the automated result, and obtained redress only after class proceedings and a royal commission.

[34]Constitution 1992 (n 1), arts 12(1), 33 and 218(c).

[35]Case C-634/21 *OQ v Land Hessen (SCHUFA Holding)* EU:C:2023:957; Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, art 22.

[36]Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L, arts 14, 26 and 86.

[37]*Nederlands Juristen Comité voor de Mensenrechten v The State of the Netherlands* (District Court of The Hague, 5 February 2020) ECLI:NL:RBDHA:2020:1878.

[38]*R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [2020] 1 WLR 5037.

[39]Treasury Board of Canada Secretariat, *Directive on Automated Decision-Making* (2019, as amended).

[40]Royal Commission into the Robodebt Scheme, *Report* (Commonwealth of Australia, July 2023).

X. CONFIRMED REQUIREMENTS AND PROPOSED SAFEGUARDS

The analysis may be drawn together by placing each link of the chain against the three categories of authority described in Part II. The table shows that confirmed law is strongest at the redress link and weakest at the notice and record links. That is the reverse of what an effective remedial system requires, since redress depends on the earlier links being in place.

Link	Confirmed requirement (binding at 29 October 2026)	Declared policy or proposed law	Proposed safeguard
Notice	Act 843 s 27 (purpose and responsible party); s 41 (solely automated decisions only); art 23 for administrative bodies, as applied in *Awuni*	Data Protection Bill 2025 rights on automated decision-making; Emerging Technologies Bill	Disclosure at the time of every AI-assisted decision, naming the system and the answerable institution
Reasons	Act 843 ss 32 and 35 (access); s 41 (reconsideration); arts 23 and 296	Data Protection Bill 2025 automated decision rights	Duty to state the principal factors in terms a person can contest
Record	Act 843 ss 17, 26 and 28; Act 772 attribution and admissibility; Act 1038 duties for critical information infrastructure	Data Protection Bill 2025 impact assessments and data protection by design; Cybersecurity (Amendment) Bill 2025 AI security standards	Minimum logging and retention standard; published algorithmic impact assessments for public deployments
Review	Act 843 s 41 (solely automated decisions only); arts 23 and 296	National AI Strategy 2026; Responsible AI Office	Five-condition standard of effective review; *solely* construed by reference to practical weight
Redress	Act 843 ss 33, 39, 43 and 75; arts 12(1), 33 and 218; judicial review	Data Protection Bill 2025 penalty framework and Data Protection Authority	Evidential presumption where the record is not kept; collective complaints; published determinations

Two qualifications apply to the middle column. The bills listed there have completed public consultation but, so far as public sources disclose at the date of writing, have not been enacted, and their final texts may differ from the consultation drafts. The National Artificial Intelligence Strategy and the Responsible Artificial Intelligence Office are commitments of policy whose legal effect will depend on what Parliament, the regulators and the courts make of them.

XI. EVIDENCE NEEDED TO EVALUATE IMPLEMENTATION

A framework that exists only on paper cannot be distinguished from one that operates in practice unless the evidence that would reveal the difference is collected, and no Ghanaian institution at present publishes systematic data on AI-assisted decisions. The table identifies, for each link of the chain, the evidence that would show whether the link functions, the institution likely to hold that evidence, and the means by which it could be obtained under present law.

Link	Evidence that the link functions	Likely holder	Route under present law
Notice	Inventory of automated systems used by public institutions; standard notices given to affected persons; proportion of decisions in which notice was given	Ministries, agencies, Responsible AI Office	Act 989 request; parliamentary question
Reasons	Sample reasons letters for AI-assisted decisions; documentation held by institutions; success rate of access requests under ss 32 and 35	Deploying institutions, vendors	Act 843 access request; Act 989 request; disclosure in litigation
Record	Logging and retention policies; impact assessments; security audit reports for systems forming part of critical information infrastructure	Institutions, Data Protection Commission, Cyber Security Authority	Act 989 request (subject to exemptions); investigative powers of the regulators

Link	Evidence that the link functions	Likely holder	Route under present law
Review	Override rates; reviewer caseloads and time per case; training records; whether an override must be justified	Deploying institutions	Act 989 request; academic study with institutional cooperation
Redress	Number and outcome of s 41 requests, complaints to the Commission, enforcement notices, s 43 claims, judicial review and art 33 applications, and CHRAJ complaints	Data Protection Commission, courts, CHRAJ	Published annual reports; court records; Act 989 request

The override rate, meaning the proportion of system outputs altered on human review, is the most informative single indicator of whether review is effective. A rate close to zero across a large number of decisions does not by itself prove that review is a formality, since the system may be accurate; but it should prompt inquiry into whether reviewers have the authority, information and time to disagree. A rate that varies widely between reviewers suggests inconsistency in the standard being applied. Outcome data disaggregated by region, sex, age and other relevant characteristics is equally important, because a claim of indirect discrimination under article 17 cannot be assessed without it, and its collection must itself comply with the provisions on special personal data in section 37 of Act 843. Two cautions should be noted. The absence of complaints is not evidence of compliance, since a regulator that receives none may be observing an absence of harm or simply an absence of notice. Further, much of the evidence identified is held by institutions with an interest in withholding it, so the adequacy of mechanisms such as requests under Act 989 can be judged only after they have been tested.

XII. PROPOSALS FOR REFORM

The proposals that follow are proposed safeguards in the sense defined in Part II. They are arranged according to the instrument capable of implementing them, beginning with measures available under existing law, because much of the chain can be constructed without awaiting the bills considered above.

Four measures could be adopted immediately. First, the Data Protection Commission could issue interpretive guidance stating that a decision is based solely on automated processing where the automated output is determinative in practice, and that review which fails to satisfy the five conditions identified in Part VII does not remove a decision from section 41. Such guidance would not bind a court, but it would inform the Commission's enforcement and indicate the standard controllers are expected to meet. Secondly, the Commission could interpret section 27 as requiring a controller to inform the data subject that automated processing will be used to make or support a significant decision, since that is a material aspect of the purpose and manner of the processing. Thirdly, the Responsible Artificial Intelligence Office, or the Ministry pending its establishment, could publish a register of automated systems used by public institutions, stating for each its purpose, the answerable official and a summary of any impact assessment, and thereby supply the system-level transparency on which the other links depend. Fourthly, the Commission could publish anonymized summaries of complaints and enforcement notices concerning automated decisions, establishing a body of guidance where none presently exists.

Five further measures would require legislation, for which the Data Protection Bill and the Emerging Technologies Bill are the natural vehicles. Protection should extend beyond solely automated decisions to decisions significantly assisted by automated systems, so that the duties of notice, reasons and review are triggered by the practical contribution of the system. Algorithmic impact assessments should be required for public deployments and for private deployments in domains of high impact, and summaries of them should be published. Minimum requirements for logging and retention should be prescribed, sufficient to reconstruct the inputs, the version of the model, the output, the action of any official and the reasons for a defined period. An evidential presumption should provide that, where an institution has failed to keep the record the law requires, any disputed fact concerning the manner in which the decision was reached is to be resolved against it, so that the record link is enforced through the redress link. Finally, the law should permit representative and collective complaints to the regulator, since the harms in question are frequently systemic, and it should define the respective responsibilities of the proposed Data Protection Authority, the Cyber Security Authority and any Emerging Technologies Agency, so that each link has an identifiable regulator and the affected person is not referred from one body to another.

The courts require no new text. In proceedings for judicial review of AI-assisted decisions, they could build on *Awuni* to hold that fairness under article 23 requires disclosure of the part played by an automated system and an opportunity to respond to its output,

and that a discretion exercised by the mechanical adoption of a score is neither candid nor in accordance with due process under article 296.[41] The existing constitutional text can support these developments without amendment.

XIII. CONCLUSION

Ghana does not confront AI-assisted decision-making in a legal vacuum. Its Constitution guarantees privacy, equality, access to information and administrative justice; its data protection statute addressed automated decisions at an early stage; and its cybersecurity and electronic transactions statutes provide for the security of the systems through which decisions are now made and for the attribution of what those systems produce. What the legal order lacks are the connecting obligations that convert these guarantees into usable remedies: a duty to disclose that an automated system has contributed to a decision, a standard for the reasons that must then be given, a requirement to keep the record from which the decision can be reconstructed, a conception of review that excludes mere ratification, and a system of redress that does not founder on a burden of proof the affected person cannot discharge. The Remedial Chain Test identifies where those obligations are missing and supplies a standard against which present practice and pending legislation can be measured. Its principal lesson is that the sequence of reform matters. Stronger penalties and compensation, on which the pending bills place emphasis, will achieve little while notice and record remain weak, because a remedy that cannot be triggered or proved affords no protection. A regulator that issues guidance on section 41, and a court that reads article 23 as requiring disclosure of automated involvement, can each strengthen the chain now, within existing law, while Parliament deliberates. The shift from data protection to algorithmic accountability is ultimately a shift from the protection of information to the protection of the person who is judged by means of it, and Ghana's framework should be measured by whether that person can learn what happened, be heard by someone able to change the outcome, and obtain redress when the process has failed them.

REFERENCES

1) Constitution of the Republic of Ghana 1992, arts 18(2) and 23.
2) Data Protection Act 2012 (Act 843), ss 41 and 43.
3) 'When the Algorithm Recommends, Who Decides?' Modern Ghana (2026) <https://www.modernghana.com/news/1527789/when-the-algorithm-recommends-who-decides.amp> accessed 29 October 2026; 'Sam George Announces New Data Protection Bill and Strict Enforcement Measures' (Ghana Chamber of Telecommunications, reproducing GBC, 2026) <https://www.telecomschamber.org/industry-news/sam-george-announces-new-data-protection-bill-and-strict-enforcement-measures/> accessed 29 October 2026.
4) E Nutsugah, 'Ghana to Invest $250m in AI Centre, Launch National Strategy' Ghana News Agency (Accra, 24 April 2026) <https://gna.org.gh/2026/04/ghana-to-invest-250m-in-ai-centre-launch-national-strategy-2/> accessed 29 October 2026; 'Gov't to Lay Emerging Technologies Bill Before Parliament in 2026' Citinewsroom <https://citinewsroom.com/2025/11/govt-to-lay-emerging-technologies-bill-before-parliament-in-2026/> accessed 29 October 2026.
5) Statutory provisions are cited from the texts available through the Data Protection Commission <https://dpc.gov.gh/compliance/>, the Cyber Security Authority <https://www.csa.gov.gh/resources.php> and GhaLII <https://ghalii.org>. Provisions whose consolidated text could not be confirmed are identified in the notes.
6) S Wachter, B Mittelstadt and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76; L Edwards and M Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law and Technology Review 18.
7) DK Citron, 'Technological Due Process' (2008) 85 Washington University Law Review 1249.
8) K Gyekye, Tradition and Modernity: Philosophical Reflections on the African Experience (OUP 1997).
9) Constitution 1992 (n 1), art 12(1).
10) Constitution 1992 (n 1), arts 17, 21(1)(f) and 296; Right to Information Act 2019 (Act 989).
11) Awuni v West African Examinations Council [2003-2004] SCGLR 471.
12) Raphael Cubagee v Michael Yeboah Asare (Supreme Court of Ghana, 2018). The full law report citation and the precise holding should be confirmed before publication.
13) Constitution 1992 (n 1), arts 33 and 218.
14) Act 843, s 91.
15) Act 843, s 45.
16) Act 843, s 17.

[41] *Awuni* (n 11).

17) Act 843, ss 25 to 27.
18) Act 843, s 41. Secondary summaries differ as to the notice mechanism and the periods prescribed, and the wording should be checked against the gazetted text before reliance.
19) Act 843, ss 32 and 35; 'What Is Data Protection Act, 2012 (Act 843)?' OfflistMe (August 2026) <https://www.offlist.me/what-is-ghana-data-protection-act> accessed 29 October 2026. The extension of access to decision logic is asserted in secondary sources and should be confirmed against the gazetted text.
20) Data Protection Act 1998 (UK), s 12 (repealed).
21) Act 843, ss 28, 30 and 31.
22) Act 843, ss 33, 39 and 43.
23) Act 843, ss 3, 75 and 76.
24) Data Protection Bill 2025 (consultation draft) <https://moc.gov.gh/wp-content/uploads/2023/03/DATA-PROTECTION-BILL.pdf> accessed 29 October 2026; Digital Policy Alert, 'Ministry of Communication, Digital Technology and Innovations Closes Consultation on Data Protection Act, 2025' <https://digitalpolicyalert.org/event/34534-ministry-of-communication-digital-technology-and-innovations-closes-consultation-on-data-protection-act-2025-including-data-protection-regulation> accessed 29 October 2026; 'Ghana's Corporate Commercial Outlook 2026' Mondaq (16 July 2026) <https://www.mondaq.com/corporate-and-company-law/1818508/ghanas-corporate-commercial-outlook-2026> accessed 29 October 2026.
25) Ghana Chamber of Telecommunications (n 3).
26) Cybersecurity Act 2020 (Act 1038).
27) Digital Policy Alert, 'Cyber Security Authority Opened Consultation on Draft Cybersecurity (Amendment) Bill' <https://digitalpolicyalert.org/event/34393-cyber-security-authority-opened-consultation-on-draft-cybersecurity-amendment-bill-2025-including-cybersecurity-regulation> accessed 29 October 2026; International IDEA, 'Ghana: October 2025' Democracy Tracker <https://www.idea.int/democracytracker/report/ghana/october-2025> accessed 29 October 2026.
28) Electronic Transactions Act 2008 (Act 772), as amended by the Electronic Transactions (Amendment) Act 2012 (Act 838) and Act 1038 <https://ghalii.org/akn/gh/act/2008/772> accessed 29 October 2026.
29) Act 772, ss 17 and 21. The section numbers are taken from the arrangement of sections and should be confirmed against the consolidated text.
30) Act 772, s 7; Evidence Act 1975 (NRCD 323).
31) Act 989.
32) LJ Skitka, KL Mosier and M Burdick, 'Does Automation Bias Decision-Making?' (1999) 51 International Journal of Human-Computer Studies 991; B Green, 'The Flaws of Policies Requiring Human Oversight of Government Algorithms' (2022) 45 Computer Law and Security Review 105681.
33) Nutsugah (n 4); 'Ghana Launches National AI Strategy' TechAfrica News (27 April 2026) <https://techafricanews.com/?p=77164> accessed 29 October 2026.
34) Constitution 1992 (n 1), arts 12(1), 33 and 218(c).
35) Case C-634/21 OQ v Land Hessen (SCHUFA Holding) EU:C:2023:957; Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, art 22.
36) Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L, arts 14, 26 and 86.
37) Nederlands Juristen Comité voor de Mensenrechten v The State of the Netherlands (District Court of The Hague, 5 February 2020) ECLI:NL:RBDHA:2020:1878.
38) R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058, [2020] 1 WLR 5037.
39) Treasury Board of Canada Secretariat, Directive on Automated Decision-Making (2019, as amended).
40) Royal Commission into the Robodebt Scheme, Report (Commonwealth of Australia, July 2023).
41) Awuni (n 11).