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.v3i11n09

Page No: 1589-1610

Beyond Consent: Reconstructing the Legal Foundations of Informational Self-Determination in Ghana's Data-Driven Society

Dr Godwin Gaduga

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

ABSTRACT

This article examines whether consent can still bear the legal and normative weight that Ghanaian data protection law, and the public discourse surrounding it, continue to place upon it in an environment shaped by bundled digital services, pervasive data sharing, behavioural profiling, inferred personal information, identity-linked state infrastructure and increasingly automated decision-making. It contends that the question is usually posed in the wrong form. Ghanaian law does not make consent the sole gateway to lawful processing: section 20(1) of the Data Protection Act, 2012 (Act 843) frames prior consent as the default rule but admits five alternative justifications, and the Act subjects all processing, whatever its basis, to principles of minimality, purpose specification, compatibility, quality, security, openness and data subject participation. The difficulty lies elsewhere. Consent remains the dominant legitimating narrative of the system while performing comparatively little legitimating work, and the alternative bases, in particular the open-textured legitimate interest ground in section 20(1)(e), operate without any statutory balancing discipline. Drawing on article 18(2) of the 1992 Constitution as interpreted in *Cubagee v Asare* and, more recently, in *Gorni v Vodafone Ghana Ltd* (2026), and on a delimited comparison with the European Union, the United Kingdom, Kenya and South Africa, the article reconstructs informational self-determination as a constitutionally grounded and relational entitlement to live under answerable conditions of informational representation, rather than as a succession of individual transactional choices. It proposes an Answerable Processing Framework built on three cumulative requirements of legitimacy, proportionality and answerability, and it distinguishes between obligations that already bind controllers under Act 843 and article 18(2), statutory amendments that should be made to Act 843 or incorporated into the pending Data Protection Bill, regulatory measures available to the Data Protection Commission, and wider institutional reforms. The principal contribution of the article is to demonstrate that a coherent move beyond consent in Ghana depends less on importing foreign doctrine than on giving full effect to the constitutional and statutory resources that Ghanaian law already possesses.

ARTICLE DETAILS

Published On:
16 November 2026

KEYWORDS: Informational Self-Determination, Consent, Data Protection, Article 18(2), Data Protection Act, 2012 (Act 843), Legitimate Interests, Profiling, Inferred Data, Ghana, Comparative Privacy Law.

Available on:
https://ijiissh.com/

I. INTRODUCTION

A. The Problem

When a Ghanaian subscriber registers a SIM card against a Ghana Card, opens a mobile money wallet, installs a digital lending application, enrols on a university portal or accepts the terms of a social media platform, the transaction is almost invariably described in the language of consent. The subscriber is told that she has agreed, that her data will be used in accordance with a privacy notice she has accepted, and that she may change her mind. That description is legally convenient and morally reassuring, because it allows extensive collection, combination and reuse of personal information to be presented as an expression of the data subject's own will. The conditions under which that will is expressed, however, bear little resemblance to a free, informed and specific choice. Mobile connectivity is unavailable without identity linkage; credit is unavailable without access to contacts and

device data; the volume of notices accompanying each service makes careful evaluation unrealistic; and the inferences that will later be drawn about the subscriber's creditworthiness, reliability, health or political sympathies cannot be anticipated at the moment of agreement. The facts of *Gorni v Vodafone Ghana Ltd* demonstrate what is at stake. A law student discovered, through a short code introduced by the telecommunications regulator, that an unknown number and an associated mobile money wallet had been registered against his national identity details without his knowledge, and the respondents' answer was, in substance, that the registration architecture was sound and that anyone with access to his card could have done it.[1]

The question addressed in this article is therefore not whether consent matters, which it plainly does, but whether consent can serve as a *sufficient* foundation for the protection of personal information in Ghana's data-driven society. The question has a doctrinal and a normative dimension. The doctrinal inquiry concerns how consent is positioned within Act 843 and article 18(2) of the 1992 Constitution, what legal work it is required to perform, what work is assigned to the other lawful bases and principles, and where the statutory scheme leaves gaps that consent cannot fill. The normative inquiry concerns the purpose that the protection of personal information ultimately serves, and whether an account of informational self-determination built on individual choice can capture what is at stake when institutions with superior power and knowledge construct, combine and act upon representations of persons.

B. Two Misconceptions

Two misconceptions distort much of the public and professional discussion in Ghana and must be set aside at the outset. The first is the assumption that Ghanaian law makes consent the sole lawful basis for processing, so that every collection or use of personal data requires the data subject's agreement. That assumption is incorrect. Section 20(1) of Act 843 prohibits processing without prior consent *unless* the purpose of the processing is necessary for a contract to which the data subject is a party, is authorised or required by law, is to protect a legitimate interest of the data subject, is necessary for the proper performance of a statutory duty, or is necessary to pursue the legitimate interest of the data controller or of a third party to whom the data is supplied.[2] Much of the processing undertaken by the State, telecommunications operators, banks and employers is therefore lawful, if at all, on grounds other than consent.

The second misconception is the converse assumption that, because consent is only one basis among several, its weaknesses are of marginal importance. That conclusion is equally mistaken. Consent remains the statutory default under section 20(1), the exclusive gateway for direct marketing under section 40(1), one of only two general gateways for the processing of special personal data under section 37(2), a ground on which further processing is deemed compatible with the original purpose under section 25(3)(a), and a ground on which retention beyond the period of necessity may be justified under section 24(1)(d).[3] Where consent is defective, its defects are carried into some of the most sensitive parts of the statutory scheme.

C. Thesis

The article advances three connected claims. The first is that consent in Ghanaian law performs a displacement function. It occupies the rhetorical centre of the system, while the statutory alternatives, and particularly the controller's legitimate interest under section 20(1)(e), carry most of the legal weight without the structured balancing that would make them accountable. Consent is consequently over-relied upon as a justification and under-specified as a legal standard, since Act 843 does not define it and leaves the conditions of its validity to regulations under section 94(1)(b).[4] The second claim is that article 18(2), read through *Cubagee v Asare* and *Gorni*, already supports a fuller conception of informational self-determination than the consent model allows, one that locates the right not only in the individual's power to permit or refuse disclosure but also in the duty of institutions to design, justify and account for the systems through which personal information is processed.[5] The third claim is that privacy protection in Ghana is best strengthened not by abandoning consent but by repositioning it: by confining it to genuinely optional processing, attaching enforceable conditions to its validity, subjecting every non-consensual basis to a proportionality requirement derived from article 18(2) and sections 18 and 19 of Act 843, and securing the scheme as a whole through institutional answerability and effective remedies. The resulting proposal, the Answerable Processing Framework, is developed in Part X.

---

[1] *Elorm Kwami Gorni v Vodafone Ghana Ltd, Attorney-General and National Communications Authority*, Civil Appeal No J4/40/2025 (SC, 25 February 2026) (Mensa-Bonsu JSC, with whom Amadu and Darko Asare JSC agreed; Kulendi JSC concurring; Dzamefe JSC dissenting).

[2] Data Protection Act, 2012 (Act 843), s 20(1)(a) to (e).

[3] Act 843, ss 24(1)(d), 25(3)(a), 37(2)(b) and 40(1).

[4] Act 843, s 94(1)(b), which empowers the Minister, in consultation with the Data Protection Commission, to make regulations specifying the conditions to be satisfied for consent to be given. Section 96, the interpretation provision, contains no definition of consent.

[5] Constitution of the Republic of Ghana, 1992, art 18(2); *Cubagee v Asare* [2018] GHASC 14, [2017-2018] 1 SCGLR 656; *Gorni* (n 1).

D. Contribution and Structure

The article makes four contributions. First, it offers a sustained doctrinal reading of the consent architecture of Act 843 in light of the Supreme Court's decision in *Gorni*, including the significance of the concurring opinion's treatment of aggregated identifiers. Secondly, it identifies several internal tensions in Act 843 that have received little attention, namely the absence of a statutory definition of consent, the unbalanced legitimate interest ground, the divergence between the categories of special personal data in sections 37(1) and 96, and the breadth of the contractual exclusion from the protections against automated decision-making in section 41(4). Thirdly, it develops a conception of informational self-determination that integrates constitutional doctrine with relational accounts of personhood in Ghanaian philosophy, while declining to treat those accounts as a substitute for legal analysis. Fourthly, it offers a reform model that distinguishes clearly between law that already binds and law that ought to be made.

Part II sets out the methodology and Part III distinguishes four senses of consent. Part IV reviews the critical literature, and Part V analyses the Ghanaian constitutional, statutory and judicial framework. Part VI examines the circumstances in which consent is formally obtained but substantively inadequate, and Part VII undertakes the comparative analysis. Part VIII reconstructs informational self-determination, Part IX addresses the principal counterarguments, and Part X sets out the reform model. Part XI identifies unresolved questions and concludes.

II. METHODOLOGY

The article combines four methods, because no single method is adequate to the research question. The first is doctrinal analysis of primary Ghanaian sources. Article 18(2) of the 1992 Constitution, the text of Act 843 as gazette on 18 May 2012, the decisions of the Supreme Court on privacy, and the related legislation governing electronic communications, national identification and credit reporting are examined closely, with attention to structure, internal cross-reference and the interpretive presumptions that Ghanaian courts apply to constitutional and statutory text. Each statutory provision and judicial statement relied upon has been checked against an authoritative text of the instrument or judgment. Where the only accessible source for a development is secondary, as is the case with the reported content of the Data Protection Bill, 2025, that limitation is stated, and no reliance is placed on clause numbering or drafting detail that cannot be confirmed.

The second method is functional comparison. The General Data Protection Regulation of the European Union, the law of the United Kingdom as amended by the Data (Use and Access) Act 2025, and the data protection statutes and leading decisions of Kenya and South Africa are examined not as templates for transplantation but as responses to a common functional problem, namely how processing is to be legitimated when individual choice is weak.[6] The comparison is deliberately limited. The European regime operates within a supranational legal order that recognises data protection as a fundamental right distinct from privacy and supports it with independent supervisory authorities, a specialized court and substantial administrative capacity, none of which can be assumed in Ghana. The caution in the comparative law literature that rules detached from their institutional and cultural setting seldom operate as they did in their place of origin is accordingly treated as a methodological constraint.[7]

The third method is normative reconstruction. The article asks which account of informational self-determination best fits and justifies the existing Ghanaian materials while remaining defensible on its own terms, and it tests competing accounts against difficult cases drawn from identity registration, digital credit, employment, education and automated public administration. The fourth method is philosophical. Because article 18(2) protects persons, and because the question of what a person is cannot be settled by positive law alone, the article draws on the moderate communitarianism of Kwame Gyekye and the work of Kwasi Wiredu to consider whether a relational account of personhood can ground informational self-determination without dissolving the individual right into a collective interest.[8] These traditions are invoked only where they advance a legal argument.

Three limitations should be noted. The article does not report original empirical research and makes no quantitative claims about consent practices in Ghana beyond those stated by courts or public authorities in identified sources. It does not offer a complete account of sectoral regulation in banking, health or education, each of which raises distinct questions. Finally, because the Data Protection Bill, 2025 had not been enacted at the time of writing, the reform analysis in Part X treats the Bill as an opportunity for reform rather than as law.[9]

---

[6] K Zweigert and H Kötz, *An Introduction to Comparative Law* (T Weir tr, 3rd edn, OUP 1998) ch 3.

[7] A Watson, *Legal Transplants: An Approach to Comparative Law* (Scottish Academic Press 1974); P Legrand, 'The Impossibility of "Legal Transplants"' (1997) 4 Maastricht Journal of European and Comparative Law 111.

[8] K Gyekye, *Tradition and Modernity: Philosophical Reflections on the African Experience* (OUP 1997) ch 2; K Wiredu, *Cultural Universals and Particulars: An African Perspective* (Indiana University Press 1996).

[9] Published commentary in 2025 and 2026 describes the Bill as having been released for stakeholder consultation in October 2025 and as proposing to repeal and replace Act 843: see Part V.F below.

III. FOUR SENSES OF CONSENT

Much of the confusion surrounding consent arises from treating as a single concept four distinct ideas that share a name. Separating them is a precondition of coherent legal analysis, because the failure of consent in one sense does not entail its failure in the others, and a reform that strengthens consent in one sense may weaken it in another.

A. Consent as a Legal Basis for Processing

In its first sense, consent is a legal basis, that is, a condition which, when satisfied, renders a given act of processing lawful. In this sense, consent is a technical category within a statutory scheme, and its content is whatever the scheme requires. Under section 20(1) of Act 843, it is one of six routes to lawful processing; under section 37(2)(b) it is one of two general routes to the lawful processing of special personal data; and under section 40(1) it must be prior and in writing before personal data may be used for direct marketing.[10] Consent as a legal basis is defined by what it licenses, and it may be valid even where it reflects no considered exercise of autonomy, provided that it satisfies the formal and substantive conditions that the law prescribes. The notable feature of Ghanaian law is that Act 843 prescribes almost no such conditions. It does not state whether consent must be express or may be implied, whether silence or a pre-ticked box suffices, whether consent may be combined with acceptance of contractual terms, whether it must be as easy to withdraw as to give, or whether it may be made a condition of a service for which the processing is not necessary.

B. Consent as an Ethical Ideal

In its second sense, consent is an ethical ideal: the moral transformation by which conduct that would otherwise wrong a person becomes permissible because that person has authorised it. On this view, consent has normative force only when certain background conditions are satisfied. The person must have the capacity to decide, must understand what is being authorised, must be free from coercion and manipulation, and must be choosing among options that are not themselves unjust. The distinction between the first and second senses matters because a legal basis may be satisfied where the ethical ideal is not. A ticked box may be legally sufficient under a permissive regime even though the person who ticked it neither understood nor freely accepted what was done in her name.

C. Consent as an Expression of Autonomy

In its third sense, consent is an institutional expression of autonomy, the means by which the law recognises the individual as the author of decisions about her own life. The Supreme Court drew on this conception in *Cubagee v Asare*, where privacy was described as guaranteeing personal autonomy and the right of a person to control intrusions into the sphere of private life.[11] Autonomy in this sense extends beyond consent. It includes the capacity to form preferences without manipulation, to understand oneself without being defined by the classifications of others, and to participate in the decisions that shape one's informational environment. Consent is one expression of autonomy, but a person may be denied autonomy even where each act of processing has been consented to, as where the accumulated effect of many consents is a profile that constrains her future choices in ways she never contemplated.

D. Consent as a Means of Controlling Information

In its fourth sense, consent is a practical means of control by which an individual attempts to determine who knows what about her. This sense is closely associated with the classical definition of privacy as the claim of individuals to determine for themselves when, how and to what extent information about them is communicated to others, a formulation adopted by the Supreme Court of Canada in *R v Bykovets* and cited with approval by the majority in *Gorni*.[12] As a means of control, consent is only as effective as the individual's capacity to monitor and enforce the limits she has set. That capacity diminishes rapidly once data leaves the original controller, is combined with other data or is used to generate inferences, because consent operates at the point of collection while much of the risk materializes later.

E. The Significance of the Distinction

The four senses can diverge in every combination. Processing may be lawful because consented to while offending the ethical ideal. It may respect autonomy without any consent, as when a public health authority processes data under a statutory duty with transparent safeguards. An individual may also give an informed and voluntary consent while having no practical ability to control what follows. The central error of the consent paradigm is to assume that satisfaction of the first sense secures the other three. The corresponding error of some of its critics is to assume that, because consent fails as a means of control, it should be abandoned as a legal basis. This article argues that consent should be retained as a legal basis, but narrowed and disciplined, and that the protection of autonomy and the securing of control should be assigned to principles, duties and institutions that do not depend on the assumption that individuals can regulate the data economy one transaction at a time.

---

[10] Act 843, ss 20(1), 37(2)(b) and 40(1).

[11] *Cubagee v Asare* [2018] GHASC 14, [2017-2018] 1 SCGLR 656, 664 (Pwamang JSC).

[12] *R v Bykovets* 2024 SCC 6, quoted in *Gorni* (n 1) (Mensa-Bonsu JSC); see also AF Westin, *Privacy and Freedom* (Atheneum 1967) 7.

IV. CRITICAL LITERATURE REVIEW

A. The Origins of Informational Self-Determination

The concept of informational self-determination entered legal discourse through the 1983 census judgment of the German Federal Constitutional Court, which derived from the general right of personality: a right of the individual to decide, in principle, on the disclosure and use of her personal data. The Court grounded that right in the observation that a person who cannot know what is known about her, and by whom, may be deterred from exercising her freedoms.[13] Two features of the judgment are frequently overlooked. It was never a pure consent theory, since the Court accepted that the right could be limited in the overriding public interest on a clear statutory basis, subject to proportionality and to organizational and procedural safeguards. Its concern was also structural as much as individual, because the danger it identified was a society in which citizens modify their conduct because they cannot anticipate how information about them will be used. Rouvroy and Poullet later developed this point, arguing that informational self-determination is best understood as an instrument for securing the conditions of self-development and democratic participation rather than as a property-like right of control.[14]

B. The Critique of Privacy Self-Management

The most influential modern critique of consent is Solove's account of privacy self-management. Solove argues that a regime premised on individuals reading notices and weighing the costs and benefits of each transaction fails for cognitive and structural reasons: people do not read or understand notices, cannot assess cumulative or downstream harms, and confront too many processing entities for individual management to be feasible.[15] Empirical research supports the cognitive limb of that argument. McDonald and Cranor estimated the time required to read the privacy policies a typical internet user encounters in a year and found it to be a substantial fraction of working time, while Acquisti, Brandimarte and Loewenstein documented the uncertainty, context-dependence and malleability of privacy preferences.[16] Solove has since argued that most privacy consent is neither wholly valid nor wholly fictitious, and that the law should treat it as a qualified form of permission that triggers additional duties rather than as a complete transfer of normative authority.[17]

Richards and Hartzog refine the critique by distinguishing the conditions under which consent can function, where requests are infrequent, the stakes are evident and there are incentives to choose carefully, from the conditions of digital life, in which requests are constant, harms are abstract and delayed, and interfaces are designed to secure agreement.[18] Their analysis is of particular relevance to Ghana because it attributes the failure of consent not to individual irrationality but to institutional design. Bietti goes further and contends that consent operates in data protection as a "free pass" that relieves controllers of scrutiny to which they would otherwise be subject.[19]

C. Context, Structure and Relationality

A second body of scholarship challenges the individualism of the consent model more fundamentally. Nissenbaum's theory of contextual integrity holds that privacy is violated when information flows breach the norms of the context in which information was originally shared, so that the relevant question is whether a flow is appropriate rather than whether a person agreed to it.[20] Cohen argues that privacy protects the space necessary for the development of subjectivity, and that the networked information economy erodes that space through forms of modulation and behavioural shaping that individual choice cannot resist.[21] Viljoen's relational theory of data governance bears directly on profiling. Much of the value and harm of data lies not in what it reveals about the person from whom it was collected but in what it allows a controller to infer about others who share relevant characteristics, so that individual consent is, in principle, incapable of governing population-level effects.[22] Wachter and Mittelstadt have shown that

[13] *Volkszählungsurteil* (Census Judgment), BVerfG, 15 December 1983, BVerfGE 65, 1.
[14] A Rouvroy and Y Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in S Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 45.
[15] DJ Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880.
[16] AM McDonald and LF Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 I/S: A Journal of Law and Policy for the Information Society 543; A Acquisti, L Brandimarte and G Loewenstein, 'Privacy and Human Behavior in the Age of Information' (2015) 347 Science 509.
[17] DJ Solove, 'Murky Consent: An Approach to the Fictions of Consent in Privacy Law' (2024) 104 Boston University Law Review 593.
[18] N Richards and W Hartzog, 'The Pathologies of Digital Consent' (2019) 96 Washington University Law Review 1461.
[19] E Bietti, 'Consent as a Free Pass: Platform Power and the Limits of the Informational Turn' (2020) 40 Pace Law Review 307.
[20] H Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010).
[21] JE Cohen, 'What Privacy Is For' (2013) 126 Harvard Law Review 1904.
[22] S Viljoen, 'A Relational Theory of Data Governance' (2021) 131 Yale Law Journal 573.

European data protection law offers weak protection against harmful or unreasonable inferences, and have proposed a right to reasonable inferences to address that gap.[23]

D. African Scholarship

African scholarship approaches these debates from a distinct standpoint. Makulilo's edited collection remains the most comprehensive survey of African data privacy statutes and records how closely many of them, Act 843 included, followed the European Data Protection Directive of 1995.[24] Birhane's account of algorithmic colonization warns that data-driven systems designed elsewhere and deployed in African settings may embed assumptions and extract value in ways that individual consent cannot address.[25] Reviglio and Alunge, writing from an Ubuntu perspective, argue that privacy in African thought is better understood relationally, because the self is constituted through relationships, and that this understanding converges in important respects with the structural critiques advanced in Western scholarship.[26] Ghanaian scholarship specifically concerned with consent under Act 843 remains limited. Much of the existing commentary is directed at practitioners and takes the statutory text at face value, and there has been little sustained analysis of the relationship between section 20 and article 18(2), or of the implications of *Gorni* for the consent paradigm.

E. The Gap in the Literature

Three gaps follow. The first is doctrinal: no account has yet examined how the constitutional recognition of personal data protection in *Gorni* affects the interpretation of the consent and legitimate interest provisions of Act 843. The second is conceptual: the critiques of consent have been developed largely in jurisdictions with mature regulatory capacity, and their prescriptions frequently presuppose sophisticated regulators whose existence cannot be assumed in Ghana. The third is constructive: the literature is stronger in diagnosis than in designing alternatives that are legally coherent within a particular constitutional order. This article addresses each of these gaps.

V. THE GHANAIAN LEGAL FRAMEWORK

A. Article 18(2) of the 1992 Constitution

Article 18(2) provides that no person shall be subjected to interference with the privacy of his home, property, correspondence or communication except in accordance with law and as may be necessary in a free and democratic society for public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.[27] Three structural features of the provision determine its relationship to consent. First, the right is framed as protection against interference, not as a power of authorization, and consent does not appear in the text. Consent is relevant to article 18(2) because a person who genuinely authorizes a disclosure may not have suffered an interference at all, which is a question of the scope of the right rather than of justification. Secondly, the limitation clause is cumulative. An interference must be in accordance with law and also necessary in a free and democratic society for one of the enumerated purposes. Legality is therefore insufficient on its own, and the necessity requirement imports a proportionality inquiry that corresponds closely to the minimality principle in section 19 of Act 843. Thirdly, by article 12(1), the fundamental rights in Chapter Five bind not only the organs of government but also, where applicable to them, all natural and legal persons in Ghana, and article 33(1) entitles any person who alleges a contravention to apply to the High Court for redress.[28] *Gorni* confirms that this horizontal application extends to telecommunications operators that process personal data.

The objects of protection enumerated in article 18(2), namely home, property, correspondence and communication, do not on their face include personal information as such. The Supreme Court has nonetheless declined to treat the list as exhaustive. In *Cubagee v Asare*, Pwamang JSC described privacy as a broad bundle of rights that defies concise definition, held that the listed objects do not exhaust its scope, and identified within it the individual's right to be left alone and to control intrusions into the sphere of private life.[29] That reading laid the interpretive foundation on which *Gorni* subsequently built.

[23] S Wachter and B Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' [2019] Columbia Business Law Review 494.
[24] AB Makulilo (ed), *African Data Privacy Laws* (Springer 2016).
[25] A Birhane, 'Algorithmic Colonization of Africa' (2020) 17 SCRIPTed 389.
[26] U Reviglio and R Alunge, '"I Am Datafied Because We Are Datafied": An Ubuntu Perspective on (Relational) Privacy' (2020) 33 Philosophy & Technology 595.
[27] Constitution of the Republic of Ghana, 1992, art 18(2).
[28] ibid arts 12(1), 12(2) and 33(1).
[29] *Cubagee v Asare* [2018] GHASC 14, [2017-2018] 1 SCGLR 656, 664.

B. Cubagee and Ackah: Consent Limited by Purpose and Mode

Cubagee concerned a reference under article 130(2) on whether a party to a telephone conversation who secretly recorded it had violated the privacy of the other party. The Court held that he had. Its reasoning is significant for present purposes because it is, at its core, an analysis of the scope of consent. A person who speaks on the telephone consents to an oral exchange with the other party; he does not thereby consent to the conversation being captured in a durable, reproducible and transmissible form. The Court accordingly declined to adopt a one-party consent rule and treated consent as limited by the mode and purpose for which it was given.[30] In *Ackah v Agricultural Development Bank*, the Court again held that the recording and subsequent publication of a telephone conversation breached article 18(2), and Pwamang JSC linked the heightened importance of privacy to the ease with which modern technology enables information to be intercepted, stored, retrieved and transmitted without the subject's knowledge, referring to Act 843 as part of the legislative response.[31]

The principle that emerges from these decisions is that consent under Ghanaian constitutional law is limited by purpose and by mode. Agreement to one use of information does not authorise a different use, and the party relying on an agreement must, in substance, show that the use in question fell within what was agreed. That principle anticipates the purpose specification and compatibility rules in sections 22 and 25 of Act 843 and supplies constitutional support for their strict construction.

C. Gorni v Vodafone Ghana Ltd (2026)

In *Gorni*, the appellant discovered in May 2023, by means of the short code introduced by the National Communications Authority, that a number unknown to him, together with a mobile money wallet, had been registered against his Ghana Card details, and that the number was later removed from his records, again without his knowledge. The High Court dismissed his article 33 application as premature for failure to exhaust the regulator's consumer complaint procedures under the Electronic Communications Regulations, 2011 (LI 1991). The Court of Appeal reversed the High Court on that point but dismissed the claim on its merits for want of sufficient evidence. By a majority of four to one, the Supreme Court allowed the appeal, declared that the first and third respondents had breached the appellant's privacy under article 18, and awarded general damages of GH₵10,000 and costs against the operator alone, describing the damages as nominal because the case was largely public interest litigation.[32]

Four elements of the majority reasoning bear on the consent debate. First, Mensa-Bonsu JSC held that control over one's personal information, including the particulars used to register a SIM, falls within the bundle of privacy rights protected by article 18, and that the misuse of those particulars violated the appellant's autonomy.[33] Personal data is thereby brought within the constitutional guarantee, and the statutory processing rules must now be read in the light of a constitutional right. Secondly, the majority described Act 843 as enacted to give substance to article 18(2), which supports a purposive construction of its provisions and, where they are ambiguous, a construction that best protects the constitutional interest. Thirdly, the majority reframed the evidential question. The Court of Appeal had held that the appellant failed to prove his case. The Supreme Court observed that the records required to prove or disprove the allegation were in the exclusive custody of the respondents, and that the real issue was whether the systems they had designed adequately protected subscribers' privacy. That reframing shifts the analysis from the individual transaction to the institutional architecture, and it implies that a controller which designs and operates a processing system bears a practical burden of showing that the system was adequately safeguarded.[34] Fourthly, the majority relied on sections 17, 18, 20, 28 and 29 of Act 843 in holding that the operator ought to have designed its registration system so as to prevent its agents from commercializing subscribers' information.

The concurring opinion of Kulendi JSC adds a point of wider significance. His Lordship reasoned that individual items of information on a national identity card, such as name, age, height, sex or citizenship, may not be private in isolation, but that their collection, compilation, retention and use as an aggregated set of identifiers gives rise to a duty of confidentiality on the part of the authority that obtains them and of any entity that receives them. He described the statutory regime as neither passive nor merely prohibitory, and as imposing affirmative duties of system design throughout the lifecycle of personal data.[35] This aggregation principle is directly relevant to profiling and inference, because the harm of a profile lies in the combination of data points that are individually innocuous.

Dzamefe JSC dissented. His Lordship treated the appellant's case as one of interference with the privacy of property, held that an assigned telephone number is a regulatory resource conferring only a right of use rather than a proprietary interest, considered that the operator had acted reasonably in removing the number within a short period, and found no evidence of harm or misuse.[36] The

[30] ibid.
[31] *Ackah v Agricultural Development Bank* [2017-2018] 2 SCGLR 1, 73 to 74 (Pwamang JSC), as cited and quoted in *Gorni* (n 1).
[32] *Gorni* (n 1).
[33] ibid (Mensa-Bonsu JSC).
[34] ibid.
[35] ibid (Kulendi JSC) paras 5 and 7 to 11.
[36] ibid (Dzamefe JSC, dissenting).

dissent preserves a narrower and more textually confined reading of article 18(2), and it is a reminder that the constitutional status of personal data does not rest on the express words of the provision. That vulnerability is one reason why the reforms proposed in Part X include express statutory recognition of the interests that the majority protected.

D. The Structure of Act 843

1. Principles. Section 17 requires a person who processes data to take account of the privacy of the individual by applying eight principles: 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. Section 18(1) requires personal data to be processed without infringing the privacy rights of the data subject, in a lawful manner and in a reasonable manner. Section 19 provides that personal data may be processed only if the purpose for which it is to be processed is necessary, relevant and not excessive.[37] These provisions are not lawful bases. They are cumulative conditions that apply to all processing, whatever its basis.

2. Lawful bases. Section 20(1) prohibits processing without the prior consent of the data subject unless the purpose is necessary for a contract to which the data subject is a party, is authorised or required by law, is to protect a legitimate interest of the data subject, is necessary for the proper performance of a statutory duty, or is necessary to pursue the legitimate interest of the data controller or of a third party to whom the data is supplied.[38] In form, consent is the default rule, and the remaining grounds are exceptions; in substance, the exceptions are wide enough to cover most institutional processing. Three aspects of the drafting are significant. The contractual ground is tied to necessity for the contract, which, properly construed, excludes processing that a controller has merely written into its terms. The ground concerning the data subject's own legitimate interest in paragraph (c) is neither confined to vital interests nor, on its wording, tied to necessity, which leaves it open to paternalistic use. The controller's legitimate interest ground in paragraph (e) contains no express requirement that the interest be weighed against the rights and interests of the data subject. Article 6(1)(f) of the GDPR, by contrast, makes legitimate interests subject to the overriding interests or fundamental rights and freedoms of the data subject.[39]

3. Objection. Section 20(2) provides that, unless otherwise provided by law, a data subject may object to the processing of personal data, and section 20(3) requires the person processing the data to stop when an objection is made.[40] On its face, the provision confers an unusually strong right, because it is not confined to particular lawful bases and is not subject to any countervailing showing by the controller. In practice it operates as a general right of withdrawal from processing that is not otherwise required by law. It is also little used, in part because the Act does not require controllers to inform data subjects of its existence: the collection notice prescribed by section 27(2) refers to the rights of access and rectification but not to the right to object.

4. Special personal data. Section 37(1) prohibits, unless the Act otherwise provides, the processing of personal data relating to a child under parental control or to the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or criminal behaviour of an individual, and section 37(2) permits such processing where it is necessary or where the data subject consents.[41] The definition of special personal data in section 96 is framed differently. It refers to race, colour, ethnic or tribal origin, political opinion, religious or similar beliefs, physical, medical or mental health or DNA, sexual orientation, and the commission or alleged commission of offences and related proceedings. Neither list refers to biometric data other than DNA. Consequently, the fingerprints and facial images captured during SIM registration and national identification are not, on the face of the Act, special personal data, although they are among the most consequential identifiers held about any person in Ghana.

5. Purpose, compatibility and retention. Section 22 requires personal data to be collected for a specific purpose, explicitly defined and lawful, and section 23 requires the data subject to be made aware of that purpose. Section 25(1) confines further processing to the original purpose, and section 25(2) requires the controller to consider the relationship between the purposes, the nature of the data, the manner of collection, the likely consequences for the data subject and the contractual relationship between the parties. Section 25(3) then deems further processing compatible in listed circumstances, the first of which is the consent of the data subject.[42] Section 24 prohibits retention beyond the period necessary for the purpose, subject to exceptions that again include consent. Consent therefore functions as a means of setting aside the purpose limitation and retention principles, which magnifies the consequences of any weakness in its validity.

[37] Act 843, ss 17, 18(1) and 19.
[38] ibid s 20(1).
[39] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1 (GDPR), art 6(1)(f).
[40] Act 843, s 20(2) and (3).
[41] ibid s 37(1) and (2).
[42] ibid ss 22, 23, 24 and 25.

6. Rights. The Act confers rights to confirmation and description of data held (section 32), to correction and deletion (section 33), to information about processing, including, where processing is the sole basis of a decision that significantly affects the individual, the logic or rationale behind the decision (section 35(1)(d)), to prevent processing likely to cause unwarranted damage or distress (section 39), to prevent processing for direct marketing (section 40), and in relation to automated decision-making (section 41).[43] Two limitations substantially reduce the protective value of these rights in precisely the contexts in which consent is weakest. Section 35(2) excludes the duty to disclose the logic or rationale of a decision where the data constitutes a trade secret. Section 41(4) excludes from the protections against automated decision-making any decision made in the course of considering whether to enter into a contract with the data subject, with a view to entering into such a contract, in the course of performing a contract, or for a purpose authorised or required by or under an enactment. The automated credit decision, the paradigm of consequential algorithmic judgment in Ghana's digital economy, falls squarely within that exclusion.

7. Exemptions. Section 60(1) exempts processing from the provisions of the Act for purposes of public order, public safety, public morality, national security or public interest, and section 60(2) provides that, subject to article 18(2), a certificate signed by the Minister is prima facie evidence of exemption. Section 61 exempts processing for the prevention or detection of crime, the apprehension or prosecution of offenders and the assessment or collection of taxes.[44] Read literally, section 60(1)(e) would permit almost any processing to be removed from the Act by invocation of the public interest. That reading cannot be sustained now that *Gorni* has placed personal data within article 18(2). A statutory exemption cannot authorise an interference that exceeds what the constitutional limitation clause permits, and the exemption must therefore be construed as available only where the processing is in accordance with law and necessary in a free and democratic society for a legitimate aim. The express reference to article 18(2) in section 60(2) supports that construction.

8. Enforcement and remedies. Section 43 entitles an individual who suffers damage or distress through a controller's contravention of the Act to compensation, subject to a defence of reasonable care. The Commission may serve enforcement notices under section 75, conduct assessments on request under section 77 and make determinations under section 78, and sections 88 and 89 create offences of purchasing, knowingly obtaining or disclosing, and selling personal data.[45] Section 91 provides that the Act binds the Republic and that each government department is to be treated as a data controller.

E. Related Statutory and International Framework

Act 843 operates alongside sectoral instruments that bear directly on consent. The Electronic Communications Act, 2008 (Act 775) and the Electronic Communications Regulations, 2011 (LI 1991) govern the subscriber registration environment considered in *Gorni*, including the regulator's complaints procedures.[46] The National Identity Register Act, 2008 (Act 750) establishes the identity system on which SIM, financial and public service registration now depend, and Act 843 repealed several of its information provisions.[47] The Credit Reporting Act, 2007 (Act 726) is integrated with Act 843 through sections 36 and 90 of the latter. The Cybersecurity Act, 2020 (Act 1038) regulates security and incident response, and section 34 of Act 843 preserves the rights conferred by any legislation relating to the right to information, which now includes the Right to Information Act, 2019 (Act 989). At the regional level, Ghana has ratified the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention), which entered into force in June 2023, and is bound as a member of ECOWAS by the Supplementary Act on Personal Data Protection within ECOWAS.[48] Section 87 of Act 843 requires the Commission to perform the data protection functions necessary to give effect to the international obligations of the Republic.

F. Regulatory Practice and the Pending Bill

The Data Protection Commission has publicly described 2026 as a year of enforcement of Act 843 and, in December 2025, launched a privacy seal intended to certify compliant organizations.[49] At the launch of Data Protection Week in 2026, the Deputy Minister responsible for communications was reported as stating that the Commission had observed instances of personal data being shared

[43] ibid ss 32, 33, 35, 39, 40 and 41.
[44] ibid ss 60 and 61.
[45] ibid ss 43, 75, 77, 78, 88 and 89.
[46] Electronic Communications Act, 2008 (Act 775); Electronic Communications Regulations, 2011 (LI 1991) regs 119 to 130, as cited in *Gorni* (n 1).
[47] National Identity Register Act, 2008 (Act 750); Act 843, s 98(1).
[48] African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014, entered into force 8 June 2023); Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (2010).
[49] Ghana News Agency, 'Data Protection Commission acquires vehicles to boost nationwide enforcement' (21 August 2026) <https://gna.org.gh/2026/08/data-protection-commission-acquires-vehicles-to-boost-nationwide-enforcement/> accessed 31 October 2026; International Trade Administration (US Department of Commerce), 'Ghana: Information Technologies Data Protection' (market intelligence note) <https://www.trade.gov/market-intelligence/ghana-information-technologies-data-protection> accessed 31 October 2026.

without consent, resulting in unauthorized digital loans and financial distress.[50] The evidential value of such statements is limited, but they reveal regulatory priorities. The regulator's own description of harm centres on unauthorized sharing, which is a failure of purpose limitation and security as much as a failure of consent.

The Data Protection Bill, 2025 was released for stakeholder consultation in October 2025. According to published commentary, it would repeal and replace Act 843, establish a Data Protection Authority with enhanced enforcement powers including the power to impose administrative fines, extend territorial scope to foreign controllers that offer goods or services to, or monitor, persons in Ghana, broaden the definition of personal data to include online identifiers and location data, add biometric data to the special categories, and introduce rights to erasure and data portability together with requirements of impact assessment and legitimate interest assessment.[51] Because the authoritative text has not been enacted and may change, these features are treated in this article as proposals, and no reliance is placed on the numbering or drafting of particular clauses.

VI. THE LIMITS OF CONSENT: FORMAL VALIDITY AND SUBSTANTIVE INADEQUACY

Act 843 leaves the conditions of valid consent largely unspecified. This Part examines the circumstances in which that omission matters most, namely those in which consent may be formally obtained, in the sense that the data subject has clicked, signed, or otherwise signified agreement, while remaining substantively inadequate to justify the processing it is said to authorise. Six recurring situations may be identified in the Ghanaian context.

A. Unequal Bargaining Power and Dependence on Essential Services

Consent presupposes a genuine option to refuse. Where the service offered is one on which participation in economic and social life depends, such as mobile connectivity, mobile money, banking, utilities, public education, or access to government services, refusal is not a realistic option, and agreement obtained as a condition of access is agreement in form only. The problem is intensified in Ghana by the convergence of essential services on a single identity infrastructure. Once SIM registration, mobile money, banking and many public services are linked to the Ghana Card, a decision to obtain a service is no longer a discrete transaction but an entry into an interconnected system whose boundaries the data subject cannot see. Precision about the legal position is nonetheless required. Where processing is mandated by law, as subscriber registration was during the national SIM registration exercise described in *Gorni*, the appropriate lawful basis is section 20(1)(b) or (d), not consent. To describe such processing as consensual is a category error that obscures the controller's actual obligations. The objection is not that mandatory processing is unlawful but that it is misdescribed, and that the language of consent is then used to justify additional processing that is not mandatory but is attached to the mandatory collection.

B. Bundled Permissions

Bundling occurs where a data subject is required to accept, by a single act, processing for several purposes of which only some are necessary for the service. A digital lending application that requires access to a borrower's contacts, messages and location as a condition of considering a loan application illustrates the practice. Some of that processing may be necessary for the contract under section 20(1)(a). Much of it, particularly access to contacts that are later used to pressure third parties during debt recovery, is not. Where consent to unnecessary processing is made a condition of the service, the data subject's agreement does not reflect a choice about that processing, and treating it as a lawful basis allows the controller to avoid the necessity requirement that would otherwise apply. The regulator's reported concern about unauthorized digital loans arising from the sharing of personal data without consent indicates that the problem is not hypothetical.[52]

C. Information Asymmetry

Section 23 of Act 843 requires a controller to take the necessary steps to ensure that the data subject is aware of the purpose of collection, and section 27(2) specifies the information to be given, including whether the supply of data is discretionary or mandatory and the consequences of failing to supply it.[53] These are valuable obligations, but awareness of a stated purpose is not the same as

[50] 'Data Protection Week launched in Accra: Ghanaians urged to guard personal data' *Ghanaian Times* (Accra, 2026) <https://ghanaiantimes.com.gh/2026-data-protection-week-launched-in-accra-ghanaians-urged-to-guard-personal-data/> accessed 31 October 2026.

[51] Bentsi-Enchill, Letsa & Ankomah, 'Ghana's Corporate Commercial Outlook 2026' (Legal 500, 2026) <https://www.legal500.com/intelligence/ghana/corporate-commercial-law/ghanas-corporate-commercial-outlook-2026> accessed 31 October 2026; D Akwaboah, 'Understanding the Data Protection Bill, 2025: Key Highlights for Businesses and Individuals' *The Business & Financial Times* (Accra, 21 November 2025); KA Owusu-Darko, 'The Data Protection Bill 2025: A Stronger Shield, What Is It Meant to Enable?' *The Business & Financial Times* (Accra, 20 May 2026) <https://thebftonline.com/2026/05/20/the-data-protection-bill-2025-a-stronger-shield-what-is-it-meant-to-enable/> accessed 31 October 2026.

[52] *Ghanaian Times* (n 50).

[53] Act 843, ss 23 and 27(2).

understanding what the processing will involve. Notices are commonly long, expressed in technical or legal language, available only in English, and presented on small screens at the moment when the data subject is most anxious to proceed. Linguistic diversity and differing levels of literacy compound the asymmetry. A consent that is informed only for persons literate in English and familiar with the conventions of privacy notices is not meaningfully informed for a large part of the population. The difficulty lies not in any incapacity of individuals but in conditions of presentation that make understanding improbable and leave the risk of misunderstanding on the weaker party.

D. Downstream Uses and Inferred Information

The most fundamental limitation of consent is temporal. Consent is given at the point of collection, but the significance of data depends on what is subsequently done with it. A data subject who supplies her transaction history to a mobile money provider cannot anticipate that it will be combined with airtime purchases, location patterns and social graph data to infer her creditworthiness, reliability or probable income or, in some systems, characteristics that would constitute special personal data if disclosed directly. Whether inferences are themselves personal data under Act 843 has not been judicially decided, but the statutory definition points strongly to an affirmative answer. Section 96 defines personal data as data about an individual who can be identified from the data, or from the data or other information in the possession of, or likely to come into the possession of, the data controller.[54] An inference attached to the record of an identified borrower is data about that individual and is, once so attached, subject to the principles in sections 17 to 26, including the requirement in section 26 that data be complete, accurate, up to date and not misleading. The aggregation reasoning in the concurring opinion in *Gorni* supports this conclusion: if the combination of individually innocuous identifiers generates obligations, so too must the inferences that such combination is designed to produce.

Consent cannot govern inference, because the data subject does not know what will be inferred and the controller frequently does not know either until a model has been trained. A further complication is that inferences about one person are often derived from data about others, so that a borrower's profile may be shaped by the repayment behaviour of people in her contact list or her locality. In such cases, as Viljoen's analysis anticipates, the persons most affected by the processing are not parties to any consent.

E. The State and Institutional Surveillance

Where the controller is the State or a body exercising public functions, consent is a particularly unsuitable basis. The relationship is one of authority, the data subject cannot take her custom elsewhere, and refusal may carry legal or practical consequences. Act 843 recognises, through sections 20(1)(b) and (d), that most public processing rests on law or statutory duty. Those bases, however, are only as protective as the laws on which they rest, and article 18(2) requires an interference to be not merely authorised by law but necessary in a free and democratic society. A statutory duty to collect data does not establish that every use of the data collected, or every linkage of one public database with another, is necessary. The consent paradigm offers little assistance in this setting, and the protective work must be done by the requirements of legality, necessity and purpose limitation and by institutional oversight.

F. Children

Section 37(1)(a) treats data relating to a child under parental control as special personal data which, on the face of section 37(2), may be processed only where necessary or with consent.[55] The Act does not specify who may consent on a child's behalf, the age at which a child's own consent becomes relevant, or how parental consent relates to the child's developing autonomy. Schools, examination bodies, health providers and digital platforms routinely process children's data, and reliance on parental consent in those settings raises distinct problems of representation, since the interests of parent and child may diverge and the child will live with the consequences of the processing long after the parent's decision.

G. Conditions of Substantive Adequacy

These situations allow the conditions that consent must satisfy, if it is to bear legitimating weight, to be stated. Consent is substantively adequate only where it is (i) voluntary, in that refusal is a real option without detriment disproportionate to the processing refused; (ii) specific, in that it relates to identified purposes rather than to open-ended categories; (iii) comprehended, in that the information on which it is based was presented in a form and language reasonably capable of being understood by the person concerned; (iv) granular, in that distinct purposes may be accepted or refused separately; and (v) revocable, in that it may be withdrawn as easily as it was given and withdrawal halts the processing, as section 20(3) already requires in the case of objection. None of these conditions is foreign to Ghanaian law. Voluntariness and specificity follow from the conception of consent in *Cubagee*; comprehension follows from sections 23 and 27(2); granularity follows from the requirement in section 22 those purposes be specific and explicitly defined; and revocability follows from section 20(2) and (3). What Ghanaian law lacks is an authoritative statement that consent which fails these conditions is not consent for the Act.

[54] ibid s 96 (definition of 'personal data').
[55] ibid s 37(1)(a) and (2).

VII. COMPARATIVE ANALYSIS AND THE LIMITS OF TRANSPLANTATION

A. The European Union

The European framework is constitutionally distinctive in a respect that bears directly on consent. Article 8 of the Charter of Fundamental Rights recognises a right to the protection of personal data separate from the right to respect for private life in article 7, and article 8(2) requires personal data to be processed fairly for specified purposes based on the consent of the person concerned or some other legitimate basis laid down by law.[56] Consent is therefore one legitimate basis among several at the level of primary law, and the GDPR reflects that position by listing six lawful bases in article 6(1) without any hierarchy among them. What the GDPR adds, and Act 843 lacks, is a demanding definition of consent and a set of conditions for its validity. Article 4(11) defines consent as a freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or by a clear affirmative action. Article 7 places on the controller the burden of demonstrating consent, requires withdrawal to be as easy as the giving of consent, and provides in article 7(4) that, in assessing whether consent was freely given, utmost account must be taken of whether the performance of a contract is made conditional on consent to processing that is not necessary for that contract. Recital 43 adds that consent is unlikely to provide a valid basis where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority.[57]

The Court of Justice has applied these provisions strictly. In *Planet49*, it held that consent is not validly given by means of a pre-ticked checkbox which the user must deselect in order to refuse.[58] In *Meta Platforms v Bundeskartellamt*, it held that a dominant market position does not of itself prevent a user from validly consenting but is an important factor in assessing whether consent was freely given, and that it is for the operator to demonstrate that it was. It further held that processing for personalized advertising was not objectively indispensable to the performance of the contract and could not rest on the contractual ground, and that reliance on legitimate interests for such processing requires a strict balancing that takes account of users' reasonable expectations.[59] In *SCHUFA*, the Court held that the automated establishment of a credit score is a decision based solely on automated processing within article 22, where a third party to which the score is transmitted draws strongly on it in deciding whether to enter into a contract.[60]

Two lessons follow for Ghana. The first is that consent can be retained as a meaningful basis only if it is accompanied by conditions of validity and if the alternative bases are construed strictly enough to prevent controllers from evading those conditions by reclassifying their processing. *Meta* is instructive precisely because it closes the contractual and legitimate interest routes of evasion at the same time as it tightens the requirements of consent. The second lesson is cautionary. The European approach depends on well-resourced supervisory authorities, a supranational court able to resolve questions of interpretation authoritatively, and administrative fines large enough to influence corporate behaviour. The Data Protection Commission operates under very different conditions, and a reform that imported European standards without the corresponding enforcement apparatus would create obligations without consequences.

B. The United Kingdom

The United Kingdom retained the GDPR in domestic form after its withdrawal from the European Union, supplemented by the Data Protection Act 2018, and has since amended it by the Data (Use and Access) Act 2025. Two amendments are relevant. The 2025 Act introduces a new lawful basis of recognized legitimate interests in article 6(1)(ea) of the UK GDPR, together with an annex listing purposes, including national security, public security, defence, emergencies, the prevention of crime and safeguarding, for which a controller other than a public authority performing its tasks may process personal data without undertaking the balancing test that article 6(1)(f) otherwise requires.[61] The Act also replaces the general prohibition on solely automated significant decisions in article 22 with a recast regime in articles 22A to 22D, which permits such decisions on a wider range of bases subject to safeguards that include the provision of information, the opportunity to make representations, human intervention and the ability to contest the decision, while maintaining stricter limits for special category data.[62]

The British experience confirms that movement beyond consent is under way, but it also shows that such movement may weaken as well as strengthen protection. Recognized legitimate interests reduce reliance on consent by specifying in advance purposes for which processing is presumptively justified, at the cost of removing case-by-case balancing for those purposes. Since section 20(1)(e) of Act 843 already lacks any balancing test, the British model serves Ghana as a warning against further relaxation rather than as a template. The safeguard-based approach to automated decision-making is more promising, because it relocates protection from the moment of consent to the moment of decision.

---

[56] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 7 and 8.
[57] GDPR (n 39) arts 4(11), 6(1) and 7, and recitals 42 and 43.
[58] Case C-673/17 *Bundesverband der Verbraucherzentralen v Planet49 GmbH* EU:C:2019:801.
[59] Case C-252/21 *Meta Platforms Inc v Bundeskartellamt* EU:C:2023:537.
[60] Case C-634/21 *OQ v Land Hessen (SCHUFA Holding AG)* EU:C:2023:957.
[61] Data (Use and Access) Act 2025, s 70 and sch 4, inserting UK GDPR art 6(1)(ea) and Annex 1.
[62] ibid s 80 and sch 6, inserting UK GDPR arts 22A to 22D, which were brought into force in February 2026.

The British courts have also considered the remedial dimension. In *Lloyd v Google LLC*, the Supreme Court held that compensation under section 13 of the Data Protection Act 1998 required proof of material damage or distress and could not be awarded on a uniform representative basis for loss of control of data as such.[63] The contrast with *Gorni* is notable. The Supreme Court of Ghana awarded damages under article 33 for breach of the constitutional right without requiring proof of consequential harm, on the footing that the purpose of the award was to vindicate the principle. Ghanaian law may therefore be better placed than English law to recognise loss of control over personal information as itself a compensable injury, at least where the constitutional route is invoked.

C. Kenya

Article 31 of the Constitution of Kenya, 2010 guarantees the right not to have information relating to one's family or private affairs unnecessarily required or revealed, a formulation that incorporates necessity into the right itself. The Data Protection Act, 2019 lists consent alongside other lawful bases and attaches conditions to consent, including that the controller bears the burden of proving it and that the data subject may withdraw it at any time.[64] Its most consequential provision in litigation has been section 31, which requires a data protection impact assessment before processing that is likely to result in a high risk to the rights and freedoms of data subjects. In *Republic v Joe Mucheru, ex parte Katiba Institute*, the High Court quashed the decision to roll out the Huduma Namba identity card for failure to conduct such an assessment and ordered that one be carried out before further processing.[65] Earlier, in *Nubian Rights Forum v Attorney-General*, the High Court had allowed the national integrated identity system to proceed only subject to an adequate legal and regulatory framework, and had found the proposed collection of DNA and GPS coordinates intrusive and unnecessary.[66]

The Kenyan experience is the closest comparator to Ghana's because it arises from a national digital identity programme. Its principal lesson is that, in identity systems, the protective work is done not by consent, which is unavailable or meaningless where enrolment is effectively compulsory, but by review of necessity and by prior impact assessment enforced through judicial review. Act 843 contains no general duty of impact assessment. Its closest analogue is the assessable processing regime in section 57, which depends on the Minister specifying the relevant categories by executive instrument.[67]

D. South Africa

The Protection of Personal Information Act 4 of 2013 is the African statute most closely comparable in structure to Act 843. Section 11(1) permits processing only where the data subject consents or the processing is necessary for a contract, complies with a legal obligation, protects a legitimate interest of the data subject, is necessary for the performance of a public law duty, or is necessary for the legitimate interests of the responsible party or of a third party. That list corresponds almost exactly to section 20(1) of Act 843. The difference lies in the surrounding provisions. The South African Act defines consent in section 1 as a voluntary, specific and informed expression of will by which permission is given for processing, places the burden of proving consent on the responsible party, and permits a data subject to object on reasonable grounds to processing based on legitimate interests or public duties. It also regulates automated decision-making in section 71.[68] The comparison shows that the deficiency in Ghanaian law is not structural. Act 843 already has an appropriate architecture; what it lacks is the definitional and procedural detail that makes the architecture effective. Nigeria's Data Protection Act 2023 reflects the same regional pattern, combining a list of lawful bases with express conditions for valid consent.[69]

E. What May and May Not Be Transplanted

The comparative materials support four conclusions about transplantation. First, conditions of validity for consent, including a definition, a burden of proof on the controller and a rule against making services conditional on unnecessary consent, may be adopted without difficulty, because they elaborate principles already implicit in *Cubagee* and in sections 20, 22 and 27 of Act 843 and require no new institution. Secondly, a balancing requirement for legitimate interests may be adopted and is arguably already implied in section 20(1)(e) by sections 18(1)(a) and (c) and 19, since a controller cannot process in a reasonable manner and without infringing the data subject's privacy rights if it has not weighed its interest against those rights. Thirdly, impact assessment may be adopted, but its value depends on the availability of review; the Kenyan cases suggest that Ghanaian courts, exercising their jurisdiction

[63] *Lloyd v Google LLC* [2021] UKSC 50, [2022] AC 1217.
[64] Constitution of Kenya, 2010, art 31; Data Protection Act, 2019 (Kenya), ss 30 and 32.
[65] *Republic v Joe Mucheru, Cabinet Secretary, Ministry of Information Communication and Technology and others, ex parte Katiba Institute and another* [2021] KEHC 122 (KLR) (14 October 2021).
[66] *Nubian Rights Forum and others v Attorney-General and others* [2020] eKLR (Consolidated Petitions Nos 56, 58 and 59 of 2019, 30 January 2020).
[67] Act 843, s 57.
[68] Protection of Personal Information Act 4 of 2013 (South Africa), ss 1, 11 and 71; Constitution of the Republic of South Africa, 1996, s 14.
[69] Nigeria Data Protection Act 2023, ss 25 and 26.

under article 33 and in judicial review, could perform that function where regulatory capacity is limited. Fourthly, neither the enforcement model of the European Union nor the deregulatory instruments of the United Kingdom should be adopted without adaptation. The former presupposes regulatory capacity that Ghana has yet to develop, and the latter would further relax a regime that already lacks discipline at the point where discipline is most needed.

VIII. RECONSTRUCTING INFORMATIONAL SELF-DETERMINATION

A. Two Conceptions Rejected

Two conceptions that have attracted support in Ghanaian and comparative debate cannot bear the weight required of them. The first is the control conception, according to which informational self-determination consists simply in the individual's power to decide who may collect and use information about her. That conception rightly places the individual at the centre, but it collapses into the consent paradigm whose limitations are set out in Part VI, and it has nothing to say about processing that is lawfully undertaken without consent, which accounts for most processing. The second is the ownership conception, according to which personal data is the property of the data subject, who may license or sell it on terms of her choosing. Published commentary indicates that the Data Protection Bill, 2025 contains a data ownership provision, and the idea has an intuitive appeal in a legal culture in which property rights are well understood.[70] Its difficulty is that property is, above all, alienable. A regime founded on data ownership would invite data subjects to transfer their rights under the very conditions of dependence, asymmetry and bundling that render consent inadequate, and would convert the problem of illegitimate processing into a question of the price at which it was purchased. The dissent in *Gorni*, which treated the case as one concerning property in a telephone number, shows how a proprietary framing can narrow rather than enlarge the protection afforded by article 18(2).

B. The Proposed Conception

The conception defended here holds that informational self-determination is the entitlement of every person to live under answerable conditions of informational representation. Institutions that collect, combine and act upon information about persons inevitably construct representations of them in the form of records, profiles, scores, classifications and inferences that stand in for the person in decisions concerning credit, employment, education, security and public services. The entitlement does not require that the person control every such representation, which would be neither possible nor, in a functioning society, desirable. It requires that the conditions under which representations are made be answerable to the person represented and to the public. The entitlement has three dimensions.

The first is authorship. The person retains standing to participate in the making of representations about her: to know that they exist, to supply and correct the information on which they rest, to contest their accuracy and the inferences drawn from them, and to refuse genuinely optional processing. Consent is one expression of authorship, but so are the rights of objection, access, correction, information and contestation in sections 20(2), 32, 33, 35, 39 and 41 of Act 843.

The second is integrity. Representations must remain faithful to their purpose and to the person represented. This dimension draws together purpose specification and compatibility under sections 22 and 25, minimality under section 19, quality under section 26 and limits on retention under section 24, and it requires inferences to meet the same standards as collected data. An inaccurate, out-of-date, or misleading answer is not acceptable because it was generated rather than supplied.

The third is answerability. Institutions that construct representations must be able to justify them, disclose the basis on which they are made, demonstrate that their systems are designed to prevent misuse, and provide effective remedies when those systems fail. In this dimension, the conception departs most clearly from the consent paradigm. Under that paradigm, the data subject's agreement transfers responsibility to the data subject. Under the conception proposed here, responsibility remains with the institution that holds power over the representation, whatever the data subject has agreed.

C. Constitutional Foundations

This conception is not an external theory imposed on Ghanaian law. It offers the most coherent account of what the Supreme Court has already decided. *Cubagee* grounds privacy in autonomy and self-identity and limits consent by purpose and mode.[71] *Gorni* holds that control over personal information forms part of the constitutional guarantee, treats the adequacy of the controller's systems as the decisive question, and describes Act 843 as giving substance to article 18(2); its concurring opinion recognises that aggregation generates duties that individual data points do not.[72] Each of these propositions corresponds to a dimension of the proposed conception: autonomy and correction to authorship; purpose-limited consent and aggregation to integrity; and system design and the allocation of the evidential burden to answerability. Article 15(1), which provides that the dignity of all persons shall be

[70] Owusu-Darko (n 51), describing a data ownership provision in the Bill. The text of that provision has not been verified against an enacted instrument.
[71] *Cubagee* (n 29).
[72] *Gorni* (n 1).

inviolable, supplies a further foundation, because a person who is governed by representations that she cannot know, contest or correct is treated as an object of administration rather than as a bearer of dignity.[73] Article 12(2), which makes the rights in Chapter Five subject to respect for the rights and freedoms of others and for the public interest, explains why the entitlement is to answerable conditions rather than to control. The public interest may justify processing that the individual would refuse, but only through processes that remain answerable to her.

D. Relational Personhood without Collectivism

The proposed conception draws support from a relational understanding of the person with deep roots in Ghanaian philosophy. Gyekye's moderate communitarianism holds that persons are constituted in and through community and cannot be understood apart from their relationships, while maintaining, against radical communitarianism, that the individual retains rights and a capacity for self-assertion that the community may not override.[74] Wiredu likewise emphasized that personhood in Akan thought has a normative dimension, attained through conduct within a network of social relations rather than conferred by biology alone.[75] Two consequences follow for informational self-determination. First, a relational account explains why many informational harms are not purely individual. Reputation, the value of which the majority in *Gorni* invoked at the opening of its judgment by reference to a good name, exists only in the perceptions of others.[76] An inference about one person derived from data about relatives or contacts affects all of them, and the misuse of a national identity number implicates the integrity of a system on which the entire community relies. Secondly, the moderate character of Gyekye's position guards against the opposite error. Recognition of the relational dimension of personal information does not entitle the State or a corporation to treat individual data as a communal resource to be exploited in the name of collective benefit. The individual remains the primary bearer of the right, and the interest of the community is expressed through the requirement that processing be answerable rather than through the subordination of the person to the aggregate.

E. The Principles Reconsidered

On this conception, the established principles of data protection acquire more determinate content. Lawful processing requires not merely the identification of a basis under section 20(1) but a demonstration that the basis chosen genuinely fits the processing, so that processing necessary for a contract is not recast as consent and processing that serves the controller's interest is not recast as contractual necessity. Purpose limitation requires each representation to be traceable to a specified purpose, so that the generation of new inferences constitutes further processing subject to section 25. Data minimization under section 19 applies to inference as well as to collection, so that a controller may not generate inferences that are excessive in relation to its purpose. Transparency requires disclosure of the existence, categories and principal logic of consequential representations, subject to a narrowly construed trade secret limitation that cannot be used to deny the data subject an intelligible account of the reasons for a decision. Accountability requires controllers to document and be able to demonstrate compliance, which, after *Gorni,* includes the capacity to produce the records on which an allegation of misuse depends. Individual rights operate as instruments of authorship and must be capable of practical exercise, which requires that data subjects be informed of them, including the right to object. Institutional power is addressed by imposing heavier burdens of justification on controllers whose market or governmental position renders consent least meaningful. Effective remedies require both individual redress, through section 43 and article 33, and structural redress, through enforcement notices and judicial orders directed at the design of processing systems.

F. The Remaining Role of Consent

Consent retains an important but limited role. It is the appropriate basis where processing is genuinely optional, where the data subject has a real choice, and where the processing is not necessary for any other recognized purpose, as in the case of optional marketing, voluntary participation in research, non-essential personalization, and the processing of special personal data outside the circumstances in which it is necessary. In those contexts, consent is an exercise of authorship and should be respected. Consent cannot, however, legitimize processing that would otherwise fail the requirements of necessity, proportionality and integrity, nor can it relieve a controller of responsibility for systems that it designs and operates. On this account, consent is a permission granted within a protective framework, not a substitute for that framework.

IX. COUNTERARGUMENTS

A. Operational Feasibility

The first objection is practical. Ghana's data economy includes large multinational platforms and telecommunications operators, but also small enterprises, schools, clinics, churches, cooperatives and informal traders that process personal data without legal

[73] Constitution of the Republic of Ghana, 1992, art 15(1).
[74] Gyekye (n 8) ch 2.
[75] Wiredu (n 8).
[76] *Gorni* (n 1) (Mensa-Bonsu JSC), opening the majority opinion with lines from Shakespeare's *Othello* on the value of a good name.

departments or compliance budgets. Requiring all of them to conduct balancing tests, document legitimate interests, assess the validity of consent and design systems for answerability may impose costs disproportionate to the risks they create, and obligations of that kind may simply be ignored, to the detriment of respect for the law. The objection has force, and it explains why the proposals in Part X are graduated. The conception defended here does not require identical procedures of every controller. It requires that the burden of justification increase with the scale, sensitivity and consequences of the processing and with the power of the controller relative to the data subject. A small clinic processing patient records under a duty of confidentiality is in a very different position from a national mobile money operator profiling millions of customers, and the law can reflect that difference through templates, sectoral codes and thresholds without abandoning the principle. The present regime is not, in any event, free of cost. The costs of weak protection are borne by data subjects rather than by controllers, as the facts of *Gorni* show.

B. The Public Interest

The second objection is that an emphasis on answerability will obstruct legitimate public functions, including the census and official statistics, public health surveillance, the targeting of social protection, revenue collection and the administration of justice. That objection misunderstands the proposal. Article 18(2) expressly contemplates interference for public safety, the economic well-being of the country, the protection of health and the prevention of crime, and Act 843 provides bases for processing under law and statutory duty as well as exemptions for crime, taxation, health and research. The proposal accepts all of these. It requires only that the public interest be established through law that is accessible and precise, that the interference be necessary and proportionate, and that public institutions be able to account for what they do. Those requirements do not obstruct public administration; they are conditions of its legitimacy in a constitutional democracy. The proposal does, however, reject the literal reading of section 60(1)(e) under which an unspecified appeal to the public interest removes processing from the Act altogether, because that reading cannot be reconciled with article 18(2) after *Gorni*.

C. Security

The third objection is that strong privacy protection impedes security, and in particular the prevention of fraud, money laundering and cybercrime, which were among the stated justifications for the national SIM registration exercise. *Gorni* itself answers this objection. The harm in that case arose because the registration system lacked the safeguards that Act 843 requires, so that agents were able to attach identities to numbers without the knowledge of the persons concerned. The majority recognized that the misuse of identity documents in mobile registration creates precisely the risks of fraud and wrongful attribution that registration was intended to prevent. Data protection and security are therefore interdependent rather than competing values. A system that collects identity data without adequate safeguards does not enhance security; it creates a new and valuable target. Properly understood, the security argument supports stronger answerability rather than weaker.

D. Innovation

The fourth objection is that heightened obligations will deter investment and innovation in Ghana's digital economy, particularly in financial technology and artificial intelligence, and will disadvantage local enterprises in competition with foreign firms. Three responses may be made. First, the present regime is already permissive in several respects, notably in the unbalanced legitimate interest ground and the contractual exclusion from the protections against automated decision-making, so that the proposals would bring Ghanaian law closer to the standards that internationally active firms already observe elsewhere. Secondly, legal uncertainty itself deters responsible investment, and clear conditions of validity and balancing criteria reduce that uncertainty. Thirdly, the sustainability of digital services depends on public trust, and where data subjects reasonably suspect that their information will be shared, sold or misused, adoption will be slower and less secure. The regulator's concern with unauthorized digital lending suggests that the absence of discipline is already imposing costs on the legitimate digital economy.

E. The Limits of Individual Control and the Charge of Paternalism

The fifth objection comes from the opposite direction. If consent is unreliable, it may be said, the proposal risks paternalism, because it substitutes the judgment of legislators, regulators and courts for that of individuals about what processing is acceptable and so diminishes the autonomy that informational self-determination is meant to protect. The objection would be decisive against a proposal that removed individual choice, but it does not apply to the present one. The conception defended here retains and strengthens consent where consent is meaningful, preserves and extends the rights through which individuals participate in their own representation, and confines the substitution of public judgment to cases in which individual choice is structurally unavailable, as in compulsory identity systems, or structurally unreliable, as in bundled terms imposed by dominant providers. In those cases, insistence on consent does not respect autonomy; it assigns an impossible task to the weaker party. Respect for autonomy requires that individuals be asked only those questions that they can meaningfully answer.

F. Institutional Capacity

The final objection is that the proposal presupposes institutions, namely a well-resourced regulator and courts familiar with data processing, that Ghana does not yet fully possess. The objection is partly correct, and the reform model in Part X responds to it in two ways. It gives priority to measures that can be implemented through existing institutions, including the judicial interpretation of Act 843 in light of article 18(2), and it identifies the courts, exercising their jurisdiction under article 33 and in judicial review, as a complementary forum of accountability where regulatory enforcement is limited. *Gorni* shows that the Supreme Court is able and willing to examine the architecture of processing systems, and the Kenyan identity cases show that judicial review of impact assessment duties is practicable in an African constitutional order with comparable resources.

X. A MODEL FOR GHANA: THE ANSWERABLE PROCESSING FRAMEWORK

A. Three Cumulative Requirements

The framework proposed here organizes the protection of personal information around three cumulative requirements that any act of processing must satisfy. Each corresponds to a dimension of the conception defended in Part VIII and is grounded in existing Ghanaian law, although each would be strengthened by the reforms set out below.

The requirement of legitimacy. The controller must identify the lawful basis that genuinely fits the processing and must be able to show that the conditions of that basis are satisfied. Processing mandated by law rests on section 20(1)(b) or (d) and may not be presented as consensual. Processing said to be necessary for a contract must be objectively necessary for its performance, not merely provided for in its terms. Processing based on the legitimate interest of the controller or of a third party under section 20(1)(e) must withstand a weighing of that interest against the rights and reasonable expectations of the data subject. Processing based on consent must satisfy the conditions of substantive adequacy stated in Part VI.G.

The requirement of proportionality. Even where a lawful basis exists, the processing must be necessary, relevant and not excessive for its purpose under section 19, compatible with the purpose of collection under section 25, limited in duration under section 24 and accurate under section 26. These requirements apply to inferences as fully as to collected data. Where processing interferes with privacy within the meaning of article 18(2), it must also be necessary in a free and democratic society for one of the enumerated purposes. Consent may satisfy the requirement of legitimacy, but it cannot by itself satisfy the requirement of proportionality: a controller cannot render excessive processing proportionate by obtaining consent to it.

The requirement of answerability. The controller must be able to account for the processing to the data subject, to the regulator and to a court. That requires documentation of the basis relied upon and of any balancing undertaken; disclosure of the existence and principal logic of consequential representations; system design that prevents foreseeable misuse, as sections 28 and 29 require and as *Gorni* applied them; the practical availability of the rights of access, correction, objection and contestation; and the capacity to produce, when challenged, the records on which an allegation of misuse depends. Where the controller cannot account for its processing, the presumption should operate against it.

B. Existing Obligations

Much of the framework can be applied now, without legislative change. The propositions set out in the table below represent the author's reading of existing law. Some are settled by the statutory text or by *Gorni*; others are interpretive arguments that a court could adopt but has not yet expressly endorsed, and they are identified as such.

Proposition	Legal source	Status
Consent is one of six lawful bases, not the sole basis	Act 843, s 20(1)	Settled by statutory text
Processing mandated by law rests on law or statutory duty, not on consent	Act 843, s 20(1)(b) and (d)	Settled by statutory text
Consent is limited by the purpose and mode for which it was given	*Cubagee*; Act 843, ss 22 and 25	Settled in principle
Personal data falls within article 18(2), which binds private controllers	*Gorni*; Constitution, arts 12(1) and 18(2)	Settled by the majority in *Gorni*
Controllers owe affirmative duties to design systems that prevent misuse	Act 843, ss 17, 28 and 29; *Gorni*	Settled by *Gorni*
Where relevant records are in the controller's exclusive custody, the controller bears a practical burden of producing them	*Gorni*	Settled by *Gorni* on its facts
A data subject may object to processing not otherwise required by law, and processing must then cease	Act 843, s 20(2) and (3)	Settled by statutory text

Proposition	Legal source	Status
Controllers must notify the Commission and data subjects of security compromises	Act 843, s 31	Settled by statutory text
Legitimate interest processing must be weighed against the rights of the data subject	Act 843, ss 18(1)(a) and (c), 19 and 20(1)(e); art 18(2)	Interpretive argument
The contractual ground requires objective necessity	Act 843, s 20(1)(a)	Interpretive argument supported by the text
Inferences attached to an identifiable person are personal data subject to the quality principle	Act 843, ss 26 and 96; *Gorni* (Kulendi JSC)	Interpretive argument
The public interest exemption is available only where article 18(2) is satisfied	Act 843, s 60(1)(e) and (2); art 18(2)	Interpretive argument supported by the text

C. Proposed Statutory Amendments

The following amendments are proposed either to Act 843 or, more realistically, for incorporation into the Data Protection Bill, 2025 before its enactment. They are proposals and not statements of existing law.

1. **Definition and conditions of consent.** Consent should be defined as a freely given, specific, informed, and unambiguous indication of agreement by a clear affirmative act. The statute should place the burden of proving consent on the controller, require withdrawal to be as easy as the giving of consent, and provide that consent is not freely given where the provision of a service is made conditional on consent to processing that is not necessary for that service. These provisions would codify what *Cubagee* already implies and what the South African and Kenyan statutes already provide.
2. **Balancing of legitimate interests.** Section 20(1)(e) should be made subject to the condition that the interest is not overridden by the rights and freedoms of the data subject, with statutory factors including the reasonable expectations of the data subject, the relationship and imbalance of power between the parties, the vulnerability of the data subject, the involvement of children and the safeguards adopted. Public authorities should not be permitted to rely on this ground in performing their public functions, and the British model of recognized legitimate interests should not be adopted.
3. **Inferred data.** The definition of personal data should state expressly that it includes information inferred or derived about an identifiable individual, and data subjects should have a right to contest the accuracy and reasonableness of inferences used in decisions that significantly affect them.
4. **Special personal data.** Sections 37(1) and 96 should be consolidated into a single list, to which biometric data processed for the purpose of uniquely identifying a person should be added. The provisions on children's data should specify who may consent on a child's behalf and should require processing to be in the best interests of the child.
5. **Automated decision-making.** The contractual and statutory exclusions in section 41(4) should be replaced by a regime of safeguards applicable to all significant automated decisions, including credit decisions, guaranteeing notice, an intelligible explanation of the principal factors, the opportunity to make representations, meaningful human review and a right to contest the decision. The trade secret limitation in section 35(2) should be narrowed so that it cannot be used to deny an individual an intelligible account of the reasons for a decision.
6. **Impact assessment.** A general duty to conduct and document a data protection impact assessment before high-risk processing should be enacted, with mandatory assessment for identity systems, the linkage of public databases, large-scale profiling and biometric processing, and with publication of summaries in respect of public sector systems.
7. **Notice of the right to object.** Section 27(2) should be amended to require that data subjects be informed at the time of collection of the right to object under section 20(2).
8. **Exemptions.** Section 60(1)(e) should be repealed or confined to specified purposes, all exemptions should be made expressly subject to necessity and proportionality, and ministerial certificates should be reviewable on their merits.
9. **Remedies.** The statute should recognise that loss of control over personal data caused by a contravention is itself compensable, permit representative proceedings on behalf of affected data subjects, and empower the regulator to make structural orders directed at the design of processing systems.
10. **Data ownership.** Any data ownership provision should, if retained at all, be drafted to confer rights of protection and participation rather than a power of alienation, and should be made expressly subordinate to the principles of necessity and proportionality.

D. Regulatory Measures Available Now

Several significant measures do not require primary legislation. Section 86(1) of Act 843 obliges the Commission to provide guidelines and promote good practice, and section 94(1)(b) already empowers the Minister, in consultation with the Commission,

to prescribe by regulation the conditions to be satisfied for consent to be given. Guidance and regulations made under these provisions could give effect to the conditions of substantive adequacy and to a structured assessment of legitimate interests without awaiting the Bill. Section 57 permits the Minister to specify categories of assessable processing by executive instrument, and identity linkage, credit scoring, biometric processing and large-scale profiling are obvious candidates. The Commission could develop sectoral codes with the Bank of Ghana for digital lending, with the National Communications Authority for subscriber registration and telecommunications, and with the responsible authorities for education and health. It could also set standards for layered notices in Ghanaian languages as well as English. Finally, its declared enforcement priorities could be directed towards bundled consent, interface designs that manipulate agreement, the harvesting of contact lists for debt recovery and the commercial misuse of identity data, using enforcement notices under section 75 and assessments under section 77.

E. Institutional Reforms

The framework also requires institutional change. The independence of the regulator should be strengthened. Section 10 of Act 843 permits the Minister to give policy directives to the Commission's Board, an arrangement that is difficult to reconcile with the requirement of an independent national protection authority in the Malabo Convention and with the Commission's role in supervising public sector controllers.[77] Section 91(3) requires each government department to designate a data supervisor. That requirement should be fully implemented, and a public register of significant public sector databases, and of the linkages between them, should be maintained. The judiciary would benefit from specialised training in data processing and from rules of procedure for privacy claims under article 33 that reflect the allocation of the evidential burden in *Gorni*. Coordination is needed among the Data Protection Commission, the National Communications Authority, the Bank of Ghana, the Cyber Security Authority, the National Identification Authority and the Commission on Human Rights and Administrative Justice, so that controllers subject to overlapping regimes face consistent requirements and data subjects are not referred from one forum to another. Lastly, the capacity of civil society and the legal profession to bring representative and public interest litigation should be supported since, as *Gorni* illustrates, systemic failures frequently come to light through individual litigants acting in the public interest.

XI. UNRESOLVED QUESTIONS AND CONCLUSION

A. Unresolved Questions

Several questions remain open. The first concerns the durability of *Gorni*. The decision was given by a panel of five, with a reasoned dissent that adopts a narrower reading of article 18(2), and its holding that personal data falls within the constitutional guarantee has not yet been considered by a larger bench. Whether the aggregation reasoning in the concurring opinion will be treated as part of the ratio in later cases is equally uncertain. The second concerns the relationship between the constitutional route under article 33 and the statutory regime administered by the Commission. In *Gorni*, the Court of Appeal and the Supreme Court accepted that a data subject need not first exhaust the telecommunications regulator's complaints procedure before seeking constitutional redress, but the extent to which courts will defer to, or require recourse to, the Commission's processes under Act 843 has not been settled. The third is whether inferences are personal data within section 96. The textual argument advanced in Part VI is strong, but the point remains undecided, and its resolution will determine whether much of the profiling economy is subject to the principles of the Act. The fourth question concerns collective interests. If, as the relational account suggests, many informational harms are borne by groups rather than by individuals, Ghanaian law must determine whether and how groups, communities or representative organizations may assert those interests, and whether standing under article 33 extends to them. The fifth concerns cross-border processing. Section 45 applies the Act to processing of information originating in Ghana, but the practical capacity to hold foreign controllers to account remains limited, and the reported localization and transfer provisions of the Bill raise questions of proportionality and feasibility. The sixth concerns the training of artificial intelligence systems on personal data, a form of further processing whose compatibility with the original purpose under section 25, and whose justification under section 20(1)(e), Ghanaian law has not addressed. The seventh concerns the right to object under section 20(2) and (3). Read literally, it permits any data subject to halt any processing not otherwise required by law, and the courts have not yet had to decide whether it is as absolute as its terms suggest or whether it is subject to implied limits where processing rests on contract or legitimate interest.

B. Conclusion

Consent has never, in Ghanaian law, been the sole foundation of lawful processing, and in present conditions it cannot be a sufficient one. Act 843 already recognises five alternatives to consent and subjects all processing to principles that do not depend on agreement. The difficulty is that consent continues to dominate the way processing is described and justified, while the conditions of its validity remain undefined and the alternatives, especially the controller's legitimate interest, operate without discipline. The result is a regime in which the weakest form of legitimation is relied upon most heavily, and in which the data subject's formal agreement is used to shift responsibility away from the institutions that hold power over her information.

[77] Act 843, s 10; Malabo Convention (n 48) art 11.

A coherent move beyond consent requires neither its abandonment, which would deprive individuals of one of the few instruments of authorship available to them, nor the wholesale adoption of doctrines developed in jurisdictions whose institutional conditions differ from Ghana's. It requires that consent be repositioned within a framework of legitimacy, proportionality and answerability, and that the constitutional and statutory materials for that framework, which already exist, be given full effect. Article 18(2), as interpreted in *Cubagee* and *Gorni*, protects a person's control over her personal information as part of a broader commitment to autonomy and dignity. Act 843 subjects all processing to principles of minimality, purpose specification, compatibility, quality and security, confers rights of access, correction and objection, and binds the State. The Supreme Court has shown that these provisions can be read as imposing affirmative duties of system design and as placing on controllers the burden of accounting for systems within their exclusive knowledge.

What remains is to complete the structure: to define consent and the conditions of its validity, to subject legitimate interests to balancing, to bring inferred and biometric data within the protective scope of the Act, to extend safeguards against automated decision-making to the contexts in which they matter most, to require impact assessment for high-risk systems, to confine the exemptions, and to equip the regulator and the courts to hold institutions to account. Informational self-determination, so understood, is not the solitary power of an individual to accept or refuse each request for her data. It is the entitlement of every person to live among institutions that must justify, disclose, and answer for the representations they make of her. That entitlement is already implicit in Ghanaian constitutional law, and the task of the next phase of Ghanaian privacy law is to make it explicit and enforceable.

REFERENCES

1) Elorm Kwami Gorni v Vodafone Ghana Ltd, Attorney-General and National Communications Authority, Civil Appeal No J4/40/2025 (SC, 25 February 2026) (Mensa-Bonsu JSC, with whom Amadu and Darko Asare JSC agreed; Kulendi JSC concurring; Dzamefe JSC dissenting).
2) Data Protection Act, 2012 (Act 843), s 20(1)(a) to (e).
3) Act 843, ss 24(1)(d), 25(3)(a), 37(2)(b) and 40(1).
4) Act 843, s 94(1)(b), which empowers the Minister, in consultation with the Data Protection Commission, to make regulations specifying the conditions to be satisfied for consent to be given. Section 96, the interpretation provision, contains no definition of consent.
5) Constitution of the Republic of Ghana, 1992, art 18(2); Cubagee v Asare [2018] GHASC 14, [2017-2018] 1 SCGLR 656; Gorni (n 1).
6) K Zweigert and H Kötz, An Introduction to Comparative Law (T Weir tr, 3rd edn, OUP 1998) ch 3.
7) A Watson, Legal Transplants: An Approach to Comparative Law (Scottish Academic Press 1974); P Legrand, 'The Impossibility of "Legal Transplants"' (1997) 4 Maastricht Journal of European and Comparative Law 111.
8) K Gyekye, Tradition and Modernity: Philosophical Reflections on the African Experience (OUP 1997) ch 2; K Wiredu, Cultural Universals and Particulars: An African Perspective (Indiana University Press 1996).
9) Published commentary in 2025 and 2026 describes the Bill as having been released for stakeholder consultation in October 2025 and as proposing to repeal and replace Act 843: see Part V.F below.
10) Act 843, ss 20(1), 37(2)(b) and 40(1).
11) Cubagee v Asare [2018] GHASC 14, [2017-2018] 1 SCGLR 656, 664 (Pwamang JSC).
12) R v Bykovets 2024 SCC 6, quoted in Gorni (n 1) (Mensa-Bonsu JSC); see also AF Westin, Privacy and Freedom (Atheneum 1967) 7.
13) Volkszählungsurteil (Census Judgment), BVerfG, 15 December 1983, BVerfGE 65, 1.
14) A Rouvroy and Y Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in S Gutwirth and others (eds), Reinventing Data Protection? (Springer 2009) 45.
15) DJ Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880.
16) AM McDonald and LF Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 I/S: A Journal of Law and Policy for the Information Society 543; A Acquisti, L Brandimarte and G Loewenstein, 'Privacy and Human Behavior in the Age of Information' (2015) 347 Science 509.
17) DJ Solove, 'Murky Consent: An Approach to the Fictions of Consent in Privacy Law' (2024) 104 Boston University Law Review 593.
18) N Richards and W Hartzog, 'The Pathologies of Digital Consent' (2019) 96 Washington University Law Review 1461.
19) E Bietti, 'Consent as a Free Pass: Platform Power and the Limits of the Informational Turn' (2020) 40 Pace Law Review 307.
20) H Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press 2010).
21) JE Cohen, 'What Privacy Is For' (2013) 126 Harvard Law Review 1904.

22) S Viljoen, 'A Relational Theory of Data Governance' (2021) 131 Yale Law Journal 573.
23) S Wachter and B Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' [2019] Columbia Business Law Review 494.
24) AB Makulilo (ed), African Data Privacy Laws (Springer 2016).
25) A Birhane, 'Algorithmic Colonization of Africa' (2020) 17 SCRIPTed 389.
26) U Reviglio and R Alunge, '"I Am Datafied Because We Are Datafied": An Ubuntu Perspective on (Relational) Privacy' (2020) 33 Philosophy & Technology 595.
27) Constitution of the Republic of Ghana, 1992, art 18(2).
28) ibid arts 12(1), 12(2) and 33(1).
29) Cubagee v Asare [2018] GHASC 14, [2017-2018] 1 SCGLR 656, 664.
30) ibid.
31) Ackah v Agricultural Development Bank [2017-2018] 2 SCGLR 1, 73 to 74 (Pwamang JSC), as cited and quoted in Gorni (n 1).
32) Gorni (n 1).
33) ibid (Mensa-Bonsu JSC).
34) ibid.
35) ibid (Kulendi JSC) paras 5 and 7 to 11.
36) ibid (Dzamefe JSC, dissenting).
37) Act 843, ss 17, 18(1) and 19.
38) ibid s 20(1).
39) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1 (GDPR), art 6(1)(f).
40) Act 843, s 20(2) and (3).
41) ibid s 37(1) and (2).
42) ibid ss 22, 23, 24 and 25.
43) ibid ss 32, 33, 35, 39, 40 and 41.
44) ibid ss 60 and 61.
45) ibid ss 43, 75, 77, 78, 88 and 89.
46) Electronic Communications Act, 2008 (Act 775); Electronic Communications Regulations, 2011 (LI 1991) regs 119 to 130, as cited in Gorni (n 1).
47) National Identity Register Act, 2008 (Act 750); Act 843, s 98(1).
48) African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014, entered into force 8 June 2023); Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (2010).
49) Ghana News Agency, 'Data Protection Commission acquires vehicles to boost nationwide enforcement' (21 August 2026) <https://gna.org.gh/2026/08/data-protection-commission-acquires-vehicles-to-boost-nationwide-enforcement/> accessed 31 October 2026; International Trade Administration (US Department of Commerce), 'Ghana: Information Technologies Data Protection' (market intelligence note) <https://www.trade.gov/market-intelligence/ghana-information-technologies-data-protection> accessed 31 October 2026.
50) 'Data Protection Week launched in Accra: Ghanaians urged to guard personal data' Ghanaian Times (Accra, 2026) <https://ghanaiantimes.com.gh/2026-data-protection-week-launched-in-accra-ghanaians-urged-to-guard-personal-data/> accessed 31 October 2026.
51) Bentsi-Enchill, Letsa & Ankomah, 'Ghana's Corporate Commercial Outlook 2026' (Legal 500, 2026) <https://www.legal500.com/intelligence/ghana/corporate-commercial-law/ghanas-corporate-commercial-outlook-2026> accessed 31 October 2026; D Akwaboah, 'Understanding the Data Protection Bill, 2025: Key Highlights for Businesses and Individuals' The Business & Financial Times (Accra, 21 November 2025); KA Owusu-Darko, 'The Data Protection Bill 2025: A Stronger Shield, What Is It Meant to Enable?' The Business & Financial Times (Accra, 20 May 2026) <https://thebftonline.com/2026/05/20/the-data-protection-bill-2025-a-stronger-shield-what-is-it-meant-to-enable/> accessed 31 October 2026.
52) Ghanaian Times (n 50).
53) Act 843, ss 23 and 27(2).
54) ibid s 96 (definition of 'personal data').
55) ibid s 37(1)(a) and (2).
56) Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 7 and 8.

57) GDPR (n 39) arts 4(11), 6(1) and 7, and recitals 42 and 43.
58) Case C-673/17 Bundesverband der Verbraucherzentralen v Planet49 GmbH EU:C:2019:801.
59) Case C-252/21 Meta Platforms Inc v Bundeskartellamt EU:C:2023:537.
60) Case C-634/21 OQ v Land Hessen (SCHUFA Holding AG) EU:C:2023:957.
61) Data (Use and Access) Act 2025, s 70 and sch 4, inserting UK GDPR art 6(1)(ea) and Annex 1.
62) ibid s 80 and sch 6, inserting UK GDPR arts 22A to 22D, which were brought into force in February 2026.
63) Lloyd v Google LLC [2021] UKSC 50, [2022] AC 1217.
64) Constitution of Kenya, 2010, art 31; Data Protection Act, 2019 (Kenya), ss 30 and 32.
65) Republic v Joe Mucheru, Cabinet Secretary, Ministry of Information Communication and Technology and others, ex parte Katiba Institute and another [2021] KEHC 122 (KLR) (14 October 2021).
66) Nubian Rights Forum and others v Attorney-General and others [2020] eKLR (Consolidated Petitions Nos 56, 58 and 59 of 2019, 30 January 2020).
67) Act 843, s 57.
68) Protection of Personal Information Act 4 of 2013 (South Africa), ss 1, 11 and 71; Constitution of the Republic of South Africa, 1996, s 14.
69) Nigeria Data Protection Act 2023, ss 25 and 26.
70) Owusu-Darko (n 51), describing a data ownership provision in the Bill. The text of that provision has not been verified against an enacted instrument.
71) Cubagee (n 29).
72) Gorni (n 1).
73) Constitution of the Republic of Ghana, 1992, art 15(1).
74) Gyekye (n 8) ch 2.
75) Wiredu (n 8).
76) Gorni (n 1) (Mensa-Bonsu JSC), opening the majority opinion with lines from Shakespeare's Othello on the value of a good name.
77) Act 843, s 10; Malabo Convention (n 48) art 11.