JOURNAL OF POLICIES AND RECOMMENDATIONS

Volume: 5 Issue: 4

(October-December), 2026

ISSN: 2957-4129



KMF PUBLISHERS

www.kmf-publishers.com/jopar/

Contents lists available at KMF Publishers

KMF Journal of Policies and Recommendations

journal homepage: www.kmf-publishers.com/jopar/

Research Article

AI Data Governance Preferences and Intended Professional Compliance in a Bangladesh Legal Sample

Sumaiya Akter[1]; Moumita Akter Mira[1]; Farhan Islam[1]; Kazi Abdul Mannan[2]

[1] Department of Law; [2] Department of Business Administration
Shanto-Mariam University of Creative Technology, Dhaka, Bangladesh

Corresponding Author Sumaiya Akter, Email: sumaiyallkp@gmail.com

ARTICLE INFO

Keywords:
AI governance; data minimisation; compliance intention; legal education; professional confidentiality; privacy; Bangladesh

ABSTRACT

Responsible professional AI use requires both institutional safeguards and individual decisions about data handling, but support for governance principles is not equivalent to demonstrated knowledge or compliance. This study examines that distinction using 385 adult, consenting, AI-aware questionnaire records from Bangladesh. The research team confirms mixed online and in-person collection; 242 respondents are law students. Four governance-preference statements are separated from the single statement of personal compliance intention. Analysis combines item distributions, paired endorsement contrasts, a descriptive count of endorsed governance preferences, rank correlations and adjusted binary and ordinal models. Clear organisational rules receive 76.4% endorsement and high-risk data-protection assessments 75.6%, compared with 54.8% for minimisation, 54.0% for accessible data rights and 51.9% for personal compliance intention. Rules and assessments exceed intention by 24.4 and 23.6 percentage points, respectively; the other two paired differences are not established after correction. Eighty respondents endorse all four governance preferences, of whom 47 endorse personal intention. In the primary binary model, stronger agreement with the rule-preference statement is positively associated with intention, with adjusted odds ratio 1.43 and Holm-adjusted p = 0.042; the association is not retained in ordinal or student-restricted sensitivity analyses. Low block consistency supports item-level interpretation rather than latent knowledge or risk pathways. The contribution is an account of uneven alignment between institutional governance preferences and intended personal conduct, without inferring a measured intention-behaviour gap. Implications prioritise practical data-minimisation tasks, accessible rights procedures and clear allocation of professional responsibility. The study does not measure actual regulatory knowledge, workplace implementation or observed compliance.

Received: 20 September 2026 / Revised: 25 October 2026 / Accepted: 28 October 2026 / Published: 30 October 2026

Copyright: © 2026 by the authors. Licensee KMF Publishers (www.kmf-publishers.com). This open-access article is distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).
DOI: https://doi.org/10.64907/xkmf.v5i4.jopr.2

1. Introduction

Generative AI can assist legal research, drafting and information organisation, but the information entered into a service may concern identifiable clients, counterparties or witnesses. Responsible use therefore depends on decisions about what data are needed, what processing is appropriate and who is accountable for those decisions. A service may offer useful text generation while presenting an unsuitable environment for a particular confidential document. Questions of data governance remain important even where the generated answer is accurate.

Privacy theory helps explain why context matters. Nissenbaum's account of contextual integrity connects privacy to appropriate information flows within particular social settings. Applied to legal work, this directs attention to the movement of information from a professional relationship into a technology service. It does not imply that all AI processing is impermissible. It requires identifying the information, recipients, purposes and governing conditions before assuming that a convenient tool is appropriate.[1]

Bangladesh's Personal Data Protection Act 2026 provides a current statutory context, including provisions concerning disclosure and technical and organisational safeguards. The Evidence Act 1872 separately addresses professional communications and confidential communications with legal advisers. These regimes should not be treated as identical or as automatic answers to every AI-related disclosure question. They nevertheless make the distinction between general support for protection and the practical handling of legal information substantively important.[2]

A person may support clear organisational rules while remaining neutral about an intention to follow data-governance rules in future professional work. Another may intend to comply without endorsing every governance statement presented in a questionnaire. Neither combination necessarily demonstrates inconsistency or misconduct. The statements refer to different actors, actions and contexts: what organisations should do and what the respondent intends to do.

The research problem is how these perspectives align. Much discussion of responsible AI assumes that awareness, favourable governance attitudes and compliance intentions reinforce one another. That is a reasonable proposition to investigate, but it cannot be established simply by reporting a favourable overall average. A questionnaire that combines normative statements and personal intention in one scale may conceal the distinction and create an apparently coherent construct whose meaning remains uncertain.

Legal training adds a further challenge. Familiarity with AI limitations does not establish knowledge of data-processing duties or the ability to apply them to a client file. In particular, agreement that people should have data rights does not demonstrate knowledge of which rights apply, against

[1] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119.

[2] Personal Data Protection Act 2026 (Bangladesh), Act No 63 of 2026, ss 1(3), 16–17 and 44; Evidence Act 1872 (Bangladesh), ss 126–129.

whom, or under what conditions. The study therefore examines governance preferences and self-reported awareness while reserving claims about knowledge and actual compliance for designs that measure them directly.

The article addresses a measurement and inference gap at the boundary between organisational principles and personal conduct. The supplied instrument includes lawful collection rules, minimisation, accessible rights and high-risk assessments, followed by one statement about professional compliance intention. These are relevant topics, but their relevance does not make them interchangeable indicators of governance knowledge. The research contribution depends on preserving their different meanings before estimating relationships.

A second gap concerns the level of evidence. Privacy research distinguishes attitudes, intentions and behaviour, and reviews of the privacy paradox examine the difficulty of interpreting apparent discrepancies. Here, no behavioural observation is available. The defensible task is to describe differences among questionnaire endorsements rather than announce an intention-behaviour gap. This matters because the language of a gap can otherwise turn a descriptive result into an unsupported judgement about professional conduct.[3]

The contextual contribution is evidence from a legally oriented Bangladesh sample, with law students forming its largest component. The database does not establish career stage for every practitioner or current employment in a legal organisation. It is therefore more accurate to study this recorded sample than to label every respondent an emerging legal professional or a decision-maker responsible for organisational AI governance.

The objective is to examine the alignment of AI data-governance preferences with intended professional compliance. RQ1 asks how respondents evaluate the four governance principles and personal intention. RQ2 asks which paired endorsement differences are evident and how personal intention is distributed across combinations of governance preferences. RQ3 asks whether the selected governance statements are associated with intention after limited adjustment and multiplicity correction. RQ4 asks how these estimates change when the ordered outcome is retained or the sample is restricted to students. Supporting analyses examine self-reported privacy awareness and data-use checking.

The distinctive focus is institutional governance endorsement in relation to personal intention, rather than general AI adoption or a single privacy-risk score. The analysis distinguishes broad preference for organisational rules and assessments from minimisation and rights-access preferences. It then asks whether their aggregate and individual relationships with intention tell the same story. This keeps the professional-responsibility question central without assuming that endorsing a norm proves legal understanding.

[3] Spyros Kokolakis, ‘Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon’ (2017) 64 Computers & Security 122.

The study contributes item-level distributions, within-person contrasts and sensitivity analyses matched to the instrument. It also contributes a legally bounded interpretation: current statutory and professional sources contextualise the governance problem, while survey responses remain measures of perceptions. Recommendations concern practical workflows and subsequent evaluation rather than claims that a particular educational or technological intervention has already improved compliance.

Section 2 develops the behavioural, governance and legal foundations. Section 3 describes the data, collection mode, measurement decisions and analytical procedures. Section 4 presents distributions, paired contrasts, governance-preference counts and association models. Section 5 interprets the results against theory and prior research. Section 6 sets out theoretical and practical implications. Section 7 concludes with limitations and future research. Declarations, exact questionnaire wording and OSCOLA references follow.

2. Literature Review and Theoretical Foundation

Governance principles, individual privacy decisions and professional compliance operate at different levels. This section connects them through planned behaviour, protection motivation and privacy calculus while identifying the constructs the questionnaire does not measure. It then considers organisational accountability and the current legal context. The purpose is a coherent basis for exploratory analysis, not a claim that combining several theories automatically yields a validated model.

2.1 Data governance and professional information flows

Data governance concerns the allocation of responsibilities and controls over data collection, use, retention and access. In an AI context, these decisions include selecting appropriate tools, limiting inputs and deciding when review is necessary. The NIST Privacy Framework offers an enterprise-risk perspective on identifying and managing privacy risks. As a voluntary framework, it provides a way to organise these questions rather than establish the legal duties of a Bangladesh practice.[4]

Technical research supplies a bounded illustration of privacy risk: Carlini and colleagues demonstrated extraction of training examples from GPT-2. This does not establish that every hosted AI service retains client inputs for training or exposes

[4] National Institute of Standards and Technology, NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0 (NIST 2020), doi:10.6028/NIST.CSWP.01162020.

them in the same way. It does show why an assessment should identify the particular processing and retention arrangements rather than assume that fluent output implies privacy protection. No extraction attack or service audit is conducted in this study.[5]

The legal setting involves information whose sensitivity may arise from both personal identification and the professional relationship in which it was obtained. Removing a name may not eliminate identification where a narrative includes distinctive facts. Similarly, a provider's general privacy notice may not answer whether a particular professional disclosure is appropriate. Contextual integrity helps frame these information-flow questions without reducing privacy to whether an individual clicked consent.[6]

The questionnaire's governance statements address four different principles. DGC1 concerns clear rules for lawful processing; DGC2 limits collection to what is necessary; DGC3 concerns practical exercise of applicable rights; DGC4 concerns assessments accompanying high-risk deployment. They describe what should occur. None records whether an employer has implemented a policy, whether a deployment is legally high risk, or whether a respondent has completed an assessment.

2.2 Planned behaviour and intended compliance

The Theory of Planned Behavior distinguishes behavioural intention from the attitudes, perceived norms and perceived control that can shape it. It also recognises that intention alone does not guarantee behaviour. This makes it useful for a study of intended adherence to data rules, but only if its components are clearly identified. The present DGC5 item measures a general professional intention; it does not specify a particular workplace procedure or time horizon.[7]

DGC1-DGC4 are not direct measures of perceived social pressure, behavioural control or personal attitudes towards performing a specified act. They are governance preferences. They can motivate exploratory association questions, but cannot support a claim that the full planned-behaviour model has been tested. Likewise, the training field records categories of exposure rather than a validated measure of compliance self-efficacy or policy knowledge.

Empirical information-security research provides a closer organisational comparison. Bulgurcu and colleagues examine rationality-based beliefs and security awareness in relation to policy compliance. Herath and Rao combine protection motivation and deterrence within a compliance framework. These studies

[5] Nicholas Carlini and others, 'Extracting Training Data from Large Language Models' in 30th USENIX Security Symposium (USENIX Association 2021) 2633.
[6] Nissenbaum (n 1).
[7] Icek Ajzen, 'The Theory of Planned Behavior' (1991) 50 Organizational Behavior and Human Decision Processes 179.

support distinguishing a policy-related intention from broad awareness, while also showing that organisational conditions and behavioural beliefs require measurement. Their findings cannot be transferred unchanged to AI-related legal work or to this mixed student and practitioner sample.[8]

2.3 Protection motivation and practical capability

Protection Motivation Theory explains protective responses through appraisals of threats and responses. Rogers's original formulation includes the seriousness and likelihood of harm and the efficacy of a protective response. Later work by Maddux and Rogers incorporates self-efficacy. This is relevant to decisions about sensitive information: recognising a possible exposure may be insufficient if a person does not know how to complete the task safely.[9]

The supplied privacy items do not provide complete measures of threat severity, vulnerability, response efficacy, self-efficacy or response cost. They include worry, reduced willingness, preferences for controls and conditional trust. The analysis therefore uses protection motivation to interpret what remains to be measured, rather than treating a five-item average as a complete threat appraisal. A preference for an assessment does not show that the respondent can carry it out or believes it will be effective.

A practical implication follows for research design. A scenario can ask a participant to choose which parts of a legal document are necessary for a task, identify potentially revealing facts and select an approved processing route. Such performance tasks would measure capability more directly than agreement with a general norm. No such task is included here, so the article does not score respondents as competent or non-compliant.

2.4 Privacy calculus and its limits in legal work

Dinev and Hart's privacy-calculus model links privacy-related risks and trust with willingness to disclose information in e-commerce. It provides a useful account of how individuals may weigh anticipated benefits and costs. Applied cautiously, it suggests why privacy concerns and interest in strong controls can coexist with AI use. These are not necessarily opposing attitudes: a person may value a tool while wanting restrictions on its handling of sensitive information.[10]

Professional legal information creates a boundary for this analogy. A user's private calculation of convenience and risk does not by itself authorise disclosure of information concerning another person. Applicable law, confidentiality and organisational responsibilities constrain the choices available. The article consequently does not

[8] Burcu Bulgurcu, Hasan Cavusoglu and Izak Benbasat, 'Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness' (2010) 34 MIS Quarterly 523; Tejaswini Herath and H Raghav Rao, 'Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations' (2009) 18 European Journal of Information Systems 106.

[9] Ronald W Rogers, 'A Protection Motivation Theory of Fear Appeals and Attitude Change' (1975) 91 Journal of Psychology 93; James E Maddux and Ronald W Rogers, 'Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change' (1983) 19 Journal of Experimental Social Psychology 469.

[10] Tamara Dinev and Paul Hart, 'An Extended Privacy Calculus Model for E-Commerce Transactions' (2006) 17 Information Systems Research 61.

treat a favourable benefit-risk judgement as proof that a data practice is permissible.

Research on privacy behaviour also highlights uncertainty and context dependence. Acquisti, Brandimarte and Loewenstein examine how individuals' preferences and understanding can vary with decision conditions. Solove's analysis of privacy self-management identifies limits to relying on individuals to control complex data uses through consent alone. Together these perspectives motivate examining organisational safeguards alongside personal intention, while keeping the two analytically distinct.[11]

2.5 Governance implementation and accountability

Governance principles become actionable through assigned responsibilities, documented procedures and mechanisms for review. Abraham, Schneider and vom Brocke's structured review distinguishes governance mechanisms and their organisational scope, reinforcing the need to investigate implementation separately from general support for governance. The present questionnaire records neither decision authority nor those mechanisms in operation.[12] Raji and colleagues' internal auditing framework treats accountability as a process across system development and deployment rather than a final checklist. Bovens's account similarly highlights actors who must explain and justify conduct to an appropriate forum. These perspectives direct attention to implementation conditions beyond a respondent's favourable statement about rules.[13]

For legal AI, a procedure might specify approved tools, information that must be removed or retained, supervision for sensitive tasks and a route to report an uncertain disclosure. Such arrangements are proposed examples, not observed characteristics of respondents' workplaces. The distinction is crucial: DGC1 measures preference for clear organisational rules, not actual policy clarity. A positive coefficient for DGC1 therefore cannot establish the causal effect of introducing a policy.

[11] Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and Human Behavior in the Age of Information' (2015) 347 Science 509; Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880.

[12] Rene Abraham, Johannes Schneider and Jan vom Brocke, 'Data Governance: A Conceptual Framework, Structured Review, and Research Agenda' (2019) 49 International Journal of Information Management 424.

[13] Inioluwa Deborah Raji and others, 'Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing' in Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (ACM 2020) 33; Mark Bovens, 'Analysing and Assessing Accountability: A Conceptual Framework' (2007) 13 European Law Journal 447.

AI literacy supplies another related but separate dimension. Long and Magerko's competencies framework addresses understanding and critical evaluation of AI. The present literacy items include verification, confidentiality precautions and human oversight, but they do not test whether a respondent can recognise a prohibited data flow. General AI literacy, privacy awareness and professional governance knowledge should consequently remain separate targets for future measurement.[14]

2.6 Legal context and comparative guidance

The Personal Data Protection Act 2026 is the relevant current Bangladesh statute for this legal discussion. Sections 16 and 17 address disclosure restrictions and security safeguards, subject to the Act's provisions. Section 1(3) specifies commencement arrangements, including delayed commencement for specified sections, and section 44 addresses repeal and savings. The article therefore does not describe every institutional or enforcement mechanism as already operational, or rely on the superseded ordinance as the current statute. The English title is used descriptively; the official Bangla text is authoritative.[15]

The Evidence Act's provisions concerning professional communications add a distinct context. Section 126 restricts disclosure by advocates within its scope and contains exceptions; sections 127-129 address related protections and circumstances. These provisions are not a comprehensive AI-use code. They show why evaluating an information flow in legal work can require more than a generic privacy preference. The present survey does not determine whether any specific disclosure is privileged or lawful.[16]

For comparison, the GDPR expressly articulates data minimisation, protection by design and impact assessment within its own scope. The ABA's Formal Opinion 512 discusses professional responsibilities associated with generative-AI tools, including confidentiality and competence. Neither is stated as generally binding Bangladesh law. They provide comparative examples of translating broad principles into professional and organisational questions, with applicability dependent on the relevant jurisdiction and facts.[17]

The legal discussion is current manuscript context, not evidence that respondents knew or were assessed against those instruments. Fieldwork dates are unavailable, so the study cannot attribute answers to exposure to a specific legal reform. Its claims concern recorded preferences and intentions rather than compliance with a doctrinal knowledge test.

[14] Duri Long and Brian Magerko, 'What Is AI Literacy? Competencies and Design Considerations' in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (ACM 2020) 1.

[15] Personal Data Protection Act 2026.

[16] Evidence Act 1872.

[17] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, arts 5, 25 and 35; American Bar Association Standing Committee on Ethics and Professional Responsibility, Generative Artificial Intelligence Tools (Formal Opinion 512, 29 July 2024).

2.7 Exploratory propositions and framework

Four exploratory propositions organise the primary adjusted analysis. E1 expects stronger preference for clear lawful-processing rules to be positively associated with personal compliance intention. Conceptually, both concern the desirability of rule-governed AI use, although they refer to different actors. E2 expects minimisation preference to be positively associated with intention, because limiting unnecessary information is a concrete governance principle. Neither proposition assumes that a respondent has experienced an organisational policy or performed a minimisation task.

E3 expects support for accessible data rights to relate positively to compliance intention, linking individual commitment with the usability of rights protections. E4 expects support for high-risk assessments to relate positively to intention, reflecting a shared orientation towards oversight. The alternative is that these preferences remain weakly aligned because their actors, specificity and practical demands differ. The analysis reports that possibility rather than treating a positive relationship as inevitable.

Figure 1 specifies the four governance-preference predictors and the DGC5 outcome, with formal training and student status as limited adjustments. Separate paired comparisons ask whether endorsement rates differ, and a descriptive count shows how many of the four norms each respondent endorses. This count is not a validated knowledge scale and is not entered as a latent predictor. The propositions were developed for exploratory reanalysis; no preregistered causal, mediation or moderation model is claimed.

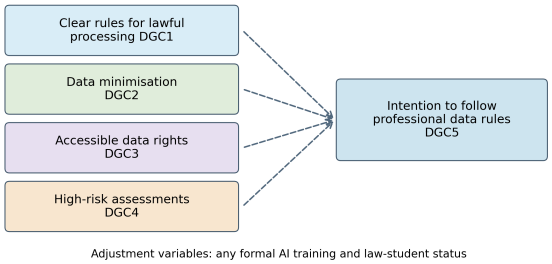

Figure 1. Exploratory framework for governance preferences and compliance intention

Dashed links denote estimated associations, not causal effects. The primary binary outcome is DGC5 endorsement; ordinal sensitivity retains its observed response categories. Predictors describe governance preferences, not actual workplace policies. Knowledge and observed compliance are not measured.

3. Methodology

The study uses a cross-sectional adult questionnaire database supplied as real data. The analytical design follows the wording and measurement properties of the available statements. This section separates documented eligibility, the collection mode confirmed by the research team and details not recoverable from the workbook. Its purpose is to support reproducible analysis without attributing knowledge, behaviour or professional status that the instrument did not establish.

3.1 Design and unit of analysis

One record represents one respondent. The questionnaire captures agreement statements at one point rather than observing a workplace intervention or following compliance over time. It supports descriptive and conditional association analysis, but not causal claims that awareness or institutional rules produce compliance. Observational reporting principles inform the disclosure of eligibility, screening, missingness, analysis decisions and limitations. They do not supply information absent from the research record.[18]

3.2 Population and data provenance

The Group 5 workbook contains README, Data and Codebook sheets. The Data sheet includes 385 rows of responses and 35 variables. Every record indicates consent, age of at least 18 and relevant AI awareness. The recorded categories include law students, law graduates, advocates or legal professionals and other relevant respondents. Career stage, employer policy, current professional AI use and authority over data processing are not established. The sample is therefore described as legally oriented rather than uniformly employed or emerging professionals.

The research team supplied the numerical records as real responses. Consistent with its clarification for these project workbooks, the two Codebook entries containing “synthetic” are treated as clerical labelling errors. Respondent_ID is a row index, and the contextual-text field is excluded from analysis. This treatment neither uses comments as qualitative evidence nor converts the index into a participant identifier. Numerical conclusions are calculated directly from the substantive response fields.

3.3 Collection mode sampling and sample size

The team confirms mixed online and in-person collection for this study. Exact collection dates, invitations, recruitment sites and mode-specific counts were not supplied. Selection probabilities and a complete sampling frame are not documented, so the article does not claim random recruitment, a population response rate or national representativeness. Mode differences cannot be estimated because respondent-level mode is not recorded.

The analytical sample is N = 385, including 242 law students. Cochran’s large-population calculation using 1.96, p = 0.50 and precision 0.05 gives approximately 384.2 and rounds upwards to 385. This is a numerical benchmark rather than evidence of a five-percentage-point population margin of error for the realised design. All 385 observations remain in the primary analysis. No undocumented invitation target, pilot exclusion or prospective model-power calculation is inserted.[19]

[18] Erik von Elm and others, ‘The Strengthening the Reporting of Observational Studies in Epidemiology (STROBE) Statement: Guidelines for Reporting Observational Studies’ (2007) 4 PLOS Medicine e296.

[19] William G Cochran, Sampling Techniques (3rd edn, John Wiley & Sons 1977).

3.4 Questionnaire and analytical roles

Twenty substantive items form four nominal blocks: AI literacy, data-protection awareness, privacy-risk/adoption statements and governance/compliance. Categories run from 1 strongly disagree to 5 strongly agree. No item is reverse-coded. Table 1 identifies the focal distinction between organisational preferences and personal intention; Appendix A gives all analysed wording. Item sources are the supplied Codebook, not claimed validated adaptations of the theoretical literature.

Table 1. Governance preferences and personal compliance intention

Code	Statement focus	Analytical interpretation
DGC1	Clear rules for lawful processing	Organisational preference; focal predictor
DGC2	Only necessary data collected	Minimisation preference; focal predictor
DGC3	Accessible exercise of applicable rights	Rights-process preference; focal predictor
DGC4	Assessments for high-risk deployment	Assessment preference; focal predictor
DGC5	Intend to follow rules in legal work	Personal intention; model outcome

Source: supplied Group 5 Codebook. Exact wording appears in Appendix A. Theory informs interpretation; exact items are not claimed as validated adaptations. Preferences do not establish actual organisational implementation or knowledge.

DGC5 is the primary outcome. DGC1-DGC4 are focal predictors in their original coding. DPA4 supplies a self-description concerning data collection, storage and processing; DPA3 reports checking information before sensitive use. These two support selected correlations but are not combined into an objective governance-knowledge score. Other privacy and literacy items provide descriptive context. Training and student status are adjustments rather than proxies for verified expertise.

3.5 Measurement assessment and pilot documentation

No verifiable pilot or cognitive-interview report accompanied the materials. A completed pilot and specific item revisions are therefore not asserted. Alpha is calculated separately for the four five-item blocks as a diagnostic. Its values range from 0.183 to 0.312. Alpha does not itself establish dimensionality or validity, but these results do not support reliable reflective composites. Their heterogeneous content also requires caution: preferences, intentions, risk concern and claimed practices are not equivalent response types.[20]

The analysis retains individual statements rather than deleting items to improve a coefficient. No latent loadings, composite reliability, AVE, HTMT or indirect paths are reported without an estimated and defensible measurement model. This choice limits

[20] Klaas Sijtsma, ‘On the Use, the Misuse, and the Very Limited Usefulness of Cronbach’s Alpha’ (2009) 74 Psychometrika 107.

interpretation to what each statement asks. It does not remove single-item measurement error or establish that the items form validated alternative constructs.

3.6 Screening and descriptive analysis

All focal items and model variables are complete and within range; the Data sheet has no blank cells. Nine AI-tool responses are the valid category “None”, not missing data. No exact duplicate is detected after excluding row index and contextual text. Seven respondents give one constant answer across the five DGC statements, but none does so across all 20 substantive items. These seven remain because block-level agreement alone does not establish inattentiveness. Timing and dedicated attention-check information are unavailable.

Endorsement combines categories 4 and 5; not endorsed includes neutral as well as disagreement. Counts, percentages, means and SDs describe responses, with pointwise Wilson intervals for selected proportions. Four exact McNemar tests compare each governance preference with DGC5, with Holm correction across the four tests. Pointwise difference intervals use 10,000 respondent bootstrap resamples. The count of endorsed DGC1-DGC4 preferences is a descriptive checklist summary, not a competency score.[21]

3.7 Association models and sensitivity analysis

Six selected Spearman correlations retain ordered item scores, with pointwise percentile intervals from 3,000 respondent bootstrap resamples and Holm correction within that family. A binomial logistic model estimates DGC5 endorsement using the four governance statements, adjusted for any formal AI training and law-student status. Odds ratios use HC0 robust sandwich covariance. A separate Holm family covers the four focal coefficients. Each original item score is assumed linear in the log odds; adjustment does not establish absence of confounding.[22]

Ordinal logistic sensitivity analysis retains the five observed DGC5 categories, including one strongly disagree response. Its common-slope assumption is not independently established, and pointwise intervals use observed information. A student-only binary model omits status and repeats four-coefficient correction. The analyses overlap and are not independent replications. No causal effect, mediation, moderation or deployable prediction model is estimated. Interpretation considers estimates, uncertainty and specification rather than nominal p-values alone.[23]

[21] Edwin B Wilson, ‘Probable Inference, the Law of Succession, and Statistical Inference’ (1927) 22 Journal of the American Statistical Association 209; Quinn McNemar, ‘Note on the Sampling Error of the Difference between Correlated Proportions or Percentages’ (1947) 12 Psychometrika 153; Sture Holm, ‘A Simple Sequentially Rejective Multiple Test Procedure’ (1979) 6 Scandinavian Journal of Statistics 65; Bradley Efron and Robert J Tibshirani, An Introduction to the Bootstrap (Chapman & Hall 1993).

[22] David W Hosmer Jr, Stanley Lemeshow and Rodney X Sturdivant, Applied Logistic Regression (3rd edn, John Wiley & Sons 2013); Halbert White, ‘A Heteroskedasticity-Consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity’ (1980) 48 Econometrica 817; Holm (n 21).

[23] Peter McCullagh, ‘Regression Models for Ordinal Data’ (1980) 42 Journal of the Royal Statistical Society Series B 109; Ronald L Wasserstein and Nicole A Lazar, ‘The ASA Statement on p-Values: Context, Process, and Purpose’ (2016) 70 American Statistician 129.

3.8 Ethics and participant protection

Participation was voluntary and based on informed consent, with anonymity and the opportunity to discontinue questionnaire completion. All analysed records contain affirmative consent and adult eligibility. The questionnaire did not require names, and results are presented in aggregate. Optional contextual text is excluded, avoiding quotation of potentially identifying material. Data requests should be limited to de-identified numerical fields and handled subject to confidentiality and applicable requirements.

No study-specific formal approval or exemption was identified in the supplied materials or clarification. None is claimed, and consent is not presented as a substitute for any applicable review requirement. Researchers retain responsibility for participant protection regardless of institutional review arrangements. The distinction between stopping before submission and removing an anonymous record afterwards is retained: a completed response may not be reliably identifiable for later withdrawal.

4. Results

Results describe specific governance preferences and intended professional conduct. They distinguish the frequency of agreement, within-person contrasts and conditional associations between responses. N = 385 unless stated otherwise. Endorsement does not establish legal knowledge or observed compliance, and not endorsed includes neutral answers. This distinction is especially relevant to DGC5, where neutrality is common.

4.1 Recorded sample profile

Law students account for 242 respondents (62.9%), graduates for 71 (18.4%), advocates or legal professionals for 42 (10.9%) and other relevant respondents for 30 (7.8%). Table 2 reports status and training because these are the model adjustments. No formal AI training is recorded for 225 respondents, a short orientation for 106 and a course or certified training for 54.

Table 2. Recorded status and formal AI training

Measure	Category	Count (%)
Status	Law student	242 (62.9%)
	Law graduate	71 (18.4%)
	Advocate or legal professional	42 (10.9%)
	Other relevant respondent	30 (7.8%)
Training	No	225 (58.4%)
	Yes, short orientation	106 (27.5%)
	Yes, course or certified training	54 (14.0%)

N = 385. Student-restricted n = 242. Recorded status does not verify career stage, current professional AI use or organisational decision authority.

The age categories are 18-20 years, 64 (16.6%); 21-23, 163 (42.3%); 24-26, 81 (21.0%); 27-30, 44 (11.4%); and 31 or above, 33 (8.6%). There are 200 male responses, 173 female responses, seven prefer-not-to-say responses and five other responses. Dhaka accounts for 166 records, district towns 86, other city corporations 74, upazila or rural areas 55 and other locations four. Weekly or daily AI use totals 275 (71.4%). Duration records 20 never-users while frequency records 15; these fields are not treated as identical measures or proof of professional AI use.

4.2 Governance preferences and compliance intention

Table 3 presents the full distributions of DGC1-DGC5. Preference for lawful-processing rules is endorsed by 294 respondents (76.4%), with mean 4.04. Preference for high-risk assessments is endorsed by 291 (75.6%), also with mean 4.04. Their identical means do not imply identical distributions or respondent-level agreement.

Table 3. Governance preferences and intention distributions

Item	Counts 1 / 2 / 3 / 4 / 5	Mean	SD	Endorsed n (%)	95% CI (%)
DGC 1	0 / 8 / 83 / 181 / 113	4.04	0.77	294 (76.4%)	71.9 to 80.3
DGC 2	4 / 24 / 146 / 166 / 45	3.58	0.82	211 (54.8%)	49.8 to 59.7
DGC 3	3 / 36 / 138 / 167 / 41	3.54	0.83	208 (54.0%)	49.0 to 58.9
DGC 4	0 / 8 / 86 / 175 / 116	4.04	0.78	291 (75.6%)	71.1 to 79.6
DGC 5	1 / 36 / 148 / 152 / 48	3.55	0.84	200 (51.9%)	47.0 to 56.9

N = 385. Categories 1-5 run from strongly disagree to strongly agree. Endorsed = 4 or 5. Wilson intervals are pointwise and do not correct sample-selection bias. Means and SDs are descriptive.

Data minimisation receives 211 endorsements (54.8%) and mean 3.58; accessible data rights receives 208 (54.0%) and mean 3.54. Personal compliance intention receives 200 endorsements (51.9%), with pointwise interval 47.0%-56.9% and mean 3.55. The DGC5 distribution includes one strongly disagree, 36 disagree, 148 neutral, 152 agree and 48 strongly agree responses. Thus, 148 of the 185 non-endorsements are neutral, limiting any interpretation that non-endorsement indicates an intention to violate rules.

Supporting responses also vary by wording. Understanding that AI inputs may create privacy risks receives 275 endorsements (71.4%), while understanding collection, storage or processing receives 177 (46.0%). Checking privacy or data-use information receives 284 (73.8%), and avoiding sensitive personal information in public tools 222 (57.7%). Confidentiality precautions under safeguards receive 297 (77.1%), and support for meaningful human oversight 299 (77.7%). These self-reports are not performance-based knowledge or data-handling assessments.

4.3 Measurement and screening results

Alpha is 0.312 for literacy, 0.207 for data-protection awareness, 0.183 for privacy-risk/adoption and 0.278 for governance/compliance. The diagnostics do not support interpreting the nominal blocks as reliable reflective constructs. The focal DGC block's distinction between organisational principles and personal intention is therefore retained in all subsequent analyses. No latent knowledge-to-compliance pathway is estimated.

All records meet the recorded consent, adulthood and AI-awareness criteria. There are no focal missing values, and all 385 observations contribute to the paired and primary adjusted analyses. Retaining the seven constant-DGC respondents avoids imposing an undocumented exclusion rule. These checks identify what the workbook permits; they do not reconstruct recruitment or independently audit the circumstances of each questionnaire response.

4.4 Paired governance and intention contrasts

Table 4 compares each organisational principle with personal intention. Lawful-rule preference exceeds intention by 24.4 percentage points, with bootstrap interval 18.2-30.6 and adjusted p below 0.001. Assessment preference exceeds intention by 23.6 points, with interval 17.1-30.1 and adjusted p below 0.001. These differences concern statements about different actors and actions, not changes in the same behaviour over time.

Table 4. Paired differences between governance preferences and intention

Preference – intention	Preference only / intention only	Difference pp	95% CI pp	Holm p
DGC1 – DGC5	132 / 38	24.4	18.2 to 30.6	<0.001
DGC2 – DGC5	100 / 89	2.9	-4.2 to 9.9	0.934
DGC3 – DGC5	93 / 85	2.1	-4.7 to 8.8	0.934
DGC4 – DGC5	138 / 47	23.6	17.1 to 30.1	<0.001

N = 385; pp = percentage points. Exact McNemar tests corrected across four comparisons. Pointwise intervals use 10,000 respondent bootstrap resamples. Different actors and wording preclude interpretation as an intention-behaviour gap or treatment effect.

The minimisation-intention difference is 2.9 points, with interval −4.2 to 9.9 and corrected p = 0.934. The rights-access-intention difference is 2.1 points, with interval −4.7 to 8.8 and corrected p = 0.934. Neither comparison establishes a net difference, and neither is an equivalence test. The pattern is therefore specific: two governance preferences exceed intention substantially, while the other two have similar marginal endorsement within the uncertainty of these contrasts.

Joint counts show why the pairs should not be reduced to their margins. For rules and intention, 162 endorse both, 132 rules only, 38 intention only and 53 neither. For assessments and intention, the counts are 153 both, 138 assessments only, 47 intention only and 47 neither. Minimisation and intention have 111 both, 100 minimisation only, 89 intention only and 85 neither. Rights and intention have 115 both, 93 rights only, 85 intention only and 92 neither.

4.5 Breadth of governance preferences and personal intention

Table 5 shows how many of the four governance statements each respondent endorses and the distribution of intention within those groups. This summary preserves the count as a descriptive property. It does not imply that all four principles have equal legal weight or that a higher count constitutes more knowledge.

Table 5. Breadth of governance endorsement and personal intention

Norms endorsed	Group n (%)	Intention yes n	Intention no n	Within-group yes %	95% CI (%)
0	9 (2.3%)	2	7	22.2	6.3 to 54.7
1	43 (11.2%)	17	26	39.5	26.4 to 54.4
2	118 (30.6%)	66	52	55.9	46.9 to 64.6
3	135 (35.1%)	68	67	50.4	42.0 to 58.7
4	80 (20.8%)	47	33	58.8	47.8 to 68.9

N = 385. Count covers DGC1-DGC4; it is a descriptive checklist, not a validated knowledge or competence scale. Intention yes = DGC5 category 4 or 5; no includes

neutrality. Wilson intervals are pointwise. The zero-norm group has only nine records; no trend test is claimed.

Eighty respondents (20.8%) endorse all four principles; 47 of these endorse intention and 33 do not. Among the remaining 305 respondents, 153 endorse intention. The within-group intention proportions rise from 22.2% in the nine-person zero-endorsement category to 55.9% at two, decline to 50.4% at three and reach 58.8% at four. The zero category is small and its interval is wide. No monotonic trend, dose-response relationship or validated progression is inferred from this table.

4.6 Selected ordinal associations

Table 6 reports the six selected rank correlations. None remains below 0.05 after correction. The largest is checking privacy/data-use information with intention, rho = 0.133, with corrected p = 0.055. Rules and intention have rho = 0.121 and corrected p = 0.089. These estimates describe small bivariate associations, with family-adjusted p-values interpreted separately from pointwise intervals.

Table 6. Selected ordinal associations with compliance intention

Pair	Spearman ρ	95% CI	Raw p	Holm p
DGC1 / DGC5	0.121	0.022 to 0.218	0.018	0.089
DGC2 / DGC5	0.031	-0.070 to 0.131	0.548	0.548
DGC3 / DGC5	0.109	0.013 to 0.200	0.033	0.130
DGC4 / DGC5	0.062	-0.038 to 0.163	0.228	0.455
DPA4 / DGC5	0.096	-0.002 to 0.192	0.061	0.183
DPA3 / DGC5	0.133	0.033 to 0.224	0.009	0.055

N = 385. Pointwise percentile intervals use 3,000 respondent bootstrap resamples. Holm correction covers six correlations. DPA3 records claimed checking; DPA4 records claimed understanding of processing. Neither is an objective knowledge measure.

Rights access and intention have rho = 0.109, assessments and intention 0.062, minimisation and intention 0.031, and data-processing awareness and intention 0.096. Their corrected p-values range from 0.130 to 0.548. The results do not establish a strong general awareness or governance-preference relationship with intention. They also do not establish the absence of every potentially relevant relationship, especially given the single-item and self-report limitations.

4.7 Adjusted binary model

The primary model contains 200 intention endorsements and 185 other responses. It converges, with predictor VIFs from 1.009 to 1.034. Table 7 gives adjusted odds ratios, pointwise HC0 intervals and correction across the four governance coefficients. The adjustment fields concern recorded training and student status, not verified organisational conditions.

Table 7. Adjusted binary model of personal compliance intention

Predictor	aOR	95% CI	Raw p	Holm p
Lawful-processing rules DGC1	1.43	1.09 to 1.87	0.011	0.042
Data minimisation DGC2	1.07	0.83 to 1.38	0.603	1.000
Accessible rights DGC3	1.19	0.93 to 1.53	0.175	0.526
High-risk assessments DGC4	1.09	0.84 to 1.41	0.533	1.000
Any formal AI training	0.92	0.61 to 1.40	0.697	—
Law-student status	0.83	0.54 to 1.26	0.382	—

N = 385; intention endorsements = 200; other responses = 185. Item estimates are per one-point increase, with HC0 robust pointwise intervals. Holm correction covers four focal coefficients. Training/status references: no training and non-student. aOR = adjusted odds ratio. Rule preference does not measure implemented policy.

Rule preference has adjusted odds ratio 1.43, interval 1.09-1.87, raw p = 0.011 and Holm p = 0.042. This is the sole focal coefficient retained below 0.05 in the primary specification. Minimisation has adjusted odds ratio 1.07, rights access 1.19 and assessments 1.09; their pointwise intervals include one. Training has adjusted odds ratio 0.92 with interval 0.61-1.40, and student status 0.83 with interval 0.54-1.26. None is interpreted as a causal educational or workplace effect.

4.8 Sensitivity and proposition assessment

The ordinal model retains all five intention categories, including the single strongly disagree response. Its rule-preference estimate is 1.26, interval 0.98-1.61 and adjusted p = 0.283. Table 8 compares the focal estimates with the student-only binary model. Neither sensitivity analysis retains a focal coefficient after its four-test correction.

Table 8. Ordinal and student-restricted sensitivity estimates

Predictor	Ordinal aOR (95% CI)	Ordinal Holm p	Student aOR (95% CI)	Student Holm p
Lawful-processing rules DGC1	1.26 (0.98 to 1.61)	0.283	1.39 (0.99 to 1.97)	0.237
Data minimisation DGC2	1.05 (0.83 to 1.33)	0.896	0.97 (0.68 to 1.38)	1.000
Accessible rights DGC3	1.22 (0.97 to 1.52)	0.283	1.08 (0.78 to 1.50)	1.000
High-risk assessments DGC4	1.10 (0.86 to 1.39)	0.896	1.03 (0.74 to 1.43)	1.000

Ordinal N = 385; DGC5 counts: strongly disagree 1, disagree 36, neutral 148, agree 152, strongly agree 48. Common slopes assumed; observed-information intervals. Student binary n = 242; endorsements = 121; HC0 intervals. Separate Holm families cover four focal coefficients in each model. Analyses overlap.

Among 242 students, 121 (50.0%) endorse intention. Their rule-preference estimate is 1.39, interval 0.99-1.97 and adjusted p = 0.237. The corresponding full-sample binary estimate is therefore a specification-dependent association rather than a uniformly retained result. E1 is supported only in the primary binary specification; E2-E4 are not retained there.

Descriptively, the most evident pattern remains the contrast between rules/assessments and intention, alongside lower endorsement of minimisation and rights access.

5. Discussion

The principal finding is uneven alignment between institutional governance preferences and intended professional compliance. Clear rules and assessments receive markedly more endorsement than personal intention, while minimisation and rights access do not show the same contrast. The adjusted rule association is positive in one specification but is not retained in the ordinal and student-only analyses. Interpretation must therefore distinguish descriptive asymmetry from a stable behavioural explanation.

5.1 Institutional preferences and personal intention

The 24.4-point rules-intention difference and 23.6-point assessments-intention difference concern different subjects: organisations or deployments on one side, and the respondent's prospective conduct on the other. A person can favour institutional rules without identifying a relevant professional situation in which to state a personal intention. Equally, neutrality may reflect uncertainty about what the rules entail. These are plausible interpretations, not explanations measured by the questionnaire.

Planned-behaviour theory clarifies the next research step. An intention should be specified in relation to an action and context, with relevant attitudes, perceived norms and control measured separately. DGC5 is broad and future-oriented, especially for students without established professional responsibilities. The present contrast should consequently not be called proof that favourable attitudes fail to become behaviour. Neither actual conduct nor the full set of intention antecedents is measured.[24]

Information-security compliance research provides an organisational comparison, where awareness and beliefs are studied in relation to policy adherence. Its relevance is the need to examine an identifiable policy, practical constraints and respondents' relationship to an organisation. The current preference for clear rules is not equivalent to experiencing such rules. Future legal-AI research should record the policy environment before drawing conclusions about implementation.[25]

[24] Ajzen (n 7).
[25] Bulgurcu, Cavusoglu and Benbasat (n 8); Herath and Rao (n 8).

5.2 Minimisation and rights access require specific interpretation

The lower endorsement of minimisation and rights access distinguishes this study from a generic claim that governance receives uniformly strong support. However, the study cannot establish that respondents oppose either principle or lack knowledge of it. Both statements contain many neutral responses, and neither is a scored doctrinal question. A vague understanding of necessary data, uncertainty about applicable rights or a response to the wording could each matter; none is directly observed.

The professional significance lies in the concrete tasks behind those principles. Minimisation requires identifying what information is needed for a purpose, not merely expressing concern about confidentiality. Rights access requires a process through which a person can act, not only a statement that rights matter. Comparative GDPR provisions show how these ideas can be articulated within a legal framework, but their legal applicability must be assessed separately from the survey preferences.[26]

Protection motivation provides a useful question about capability: can a respondent carry out the protective response and does the response seem feasible? The present data lack self-efficacy and response-cost measures. A scenario-based exercise could test whether participants can remove unnecessary identifying facts, choose an appropriate tool and identify a route for a rights request. The implication is to investigate capability, not infer it from the endorsement percentages.[27]

5.3 Awareness self-reports do not establish governance knowledge

The 73.8% endorsement of checking data-use information is higher than the 46.0% endorsement of understanding that AI services may collect, store or process user data. These different statements were not included in the corrected paired-test family, so the comparison is descriptive. It illustrates why the nominal awareness block should not automatically be scored as a coherent knowledge construct. Claimed checking is not demonstrated comprehension, and a statement about understanding is not an objective test.

AI literacy research identifies competencies for understanding and evaluating systems, while privacy-behaviour research emphasises context and uncertainty. Together these perspectives support distinguishing confidence, reported practice and correct performance. A respondent may report checking a notice without successfully recognising its implications for a legal task. Future instruments should evaluate what is understood and how it affects a specific decision.[28]

[26] General Data Protection Regulation.
[27] Rogers (n 9); Maddux and Rogers (n 9).
[28] Long and Magerko (n 14); Acquisti, Brandimarte and Loewenstein (n 11).

Solove's critique of privacy self-management supplies an institutional qualification. Even informed users may face complexity that is difficult to manage individually. Educational responses should therefore be accompanied by approved tools, clear responsibilities and practical assistance. The survey cannot estimate the relative effectiveness of those measures, but its mixed response types make it particularly important not to assign responsibility exclusively to an individual's claimed awareness.[29]

5.4 Interpreting the conditional rule association

The primary binary model's rule coefficient remains below 0.05 after correction, while the selected rank association and the two sensitivity models do not. These results are not logically contradictory: the models use different outcome information, adjustment and uncertainty criteria. They do mean that a general statement of robust association would be too strong. The most precise description is a positive adjusted binary association that is not uniformly retained across specifications.

Nor does the coefficient demonstrate that introducing clear organisational rules causes compliance. DGC1 records a preference about what organisations should have. It does not measure actual policy existence, clarity, enforcement or support. Treating it as a policy intervention would change the variable's meaning. Accountability theory supports examining those institutional features separately, including who explains a decision and who can require a response.[30]

Statistical guidance also cautions against interpreting a near-threshold corrected p-value as a complete verdict. Effect estimates, confidence intervals, measurement and design remain relevant. The ordinal analysis assumes common slopes and contains a sparse extreme category, while the student restriction reduces sample size and changes composition. None alone establishes the definitive mechanism. These results provide a bounded hypothesis for better specified future work.[31]

5.5 Professional confidentiality and governance implementation

The legal context limits a purely individual privacy-calculus account. Information in a legal file may concern people other than the tool user, and a personal judgement that convenience outweighs risk does not determine the permissibility of disclosure. Bangladesh's disclosure/security provisions and professional-communication protections provide relevant legal questions, subject to their scope and exceptions. The survey does not adjudicate a transaction or establish an infringement.[32]

Comparative professional guidance reinforces the practical importance of confidentiality when lawyers use generative tools. The ABA opinion is not a Bangladesh rule, but its identification of competence, confidentiality and supervision illustrates

[29] Solove (n 11).
[30] Bovens (n 13).
[31] Wasserstein and Lazar (n 23); Douglas G Altman and J Martin Bland, 'Absence of Evidence Is Not Evidence of Absence' (1995) 311 BMJ 485.
[32] Personal Data Protection Act 2026; Evidence Act 1872.

how a broad preference can be translated into questions for professional review. A local workflow must identify the applicable duties and the responsible decision-maker rather than copy a foreign checklist without assessment.[33]

Technical AI accuracy and data governance also need separate evaluation. Studies of legal hallucinations examine reliability of outputs, while data-governance questions concern inputs, processing and information flows. A system can produce a correct answer through an inappropriate data practice, or an incorrect answer despite careful handling of inputs. The present survey establishes neither technical performance nor actual data compliance. Both require additional evidence.[34]

5.6 Integrated interpretation

The findings support analysing governance principles and personal intention as related questions that remain empirically and conceptually distinct. The count table does not show a simple monotonic progression, and only one adjusted association is retained in one specification. A model treating broad awareness as an automatic route to compliance would therefore exceed the evidence. The study's contribution is to identify where the questions differ and which relationships merit better measurement.

Organisational processes can provide the setting for that measurement. Internal auditing research and privacy-risk frameworks direct attention to documented decisions, assigned roles and review across an activity's lifecycle. Those processes could be tested in legal education and workplace studies using appropriate safeguards. The present preferences identify priorities for investigation, rather than prove that a particular governance arrangement is implemented or effective.[35]

6. Theoretical and Practical Implications

The results inform a more precise account of responsible professional AI use. They distinguish what respondents believe institutions should do from what they intend to do personally, and both from demonstrated knowledge and actual conduct. The implications below follow that distinction and separate proposals for research and practice from intervention effects not measured in this study.

[33] ABA, Formal Opinion 512 (n 17).

[34] Matthew Dahl and others, 'Large Legal Fictions: Profiling Legal Hallucinations in Large Language Models' (2024) 16 Journal of Legal Analysis 64; Varun Magesh and others, 'Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools' (2025) 22 Journal of Empirical Legal Studies 216.

[35] Raji and others (n 13); NIST, Privacy Framework (n 4).

6.1 Theoretical implications

First, the article refines the meaning of compliance intention within a mixed legal sample. Planned-behaviour theory remains useful, but an organisational "should" statement is not a substitute for a fully specified personal attitude, norm or control measure. A theoretical extension should measure the professional action, context and time horizon before testing whether institutional conditions explain intention or behaviour. The current data motivate that specification rather than validate the complete theory.[36]

Second, privacy calculus requires a professional boundary. Decisions about others' information take place within legal and institutional responsibilities, not simply personal willingness to exchange privacy for convenience. Contextual integrity supplies a complementary account of appropriate information flow. Keeping these perspectives distinct helps explain why an adoption preference and a governance duty should not be treated as the same outcome.[37]

Third, the findings direct attention to the difference between supporting protection and being able to enact it. Protection motivation identifies the importance of response efficacy and capability, while organisational compliance research identifies policy-related beliefs and conditions. Future studies can connect those mechanisms with specific minimisation and rights-access tasks. The present article contributes a sharper measurement agenda rather than a confirmed causal chain.[38]

6.2 Implications for legal education and organisations

Legal educators can use realistic, de-identified scenarios to teach data minimisation. Students can identify the task purpose, distinguish necessary from unnecessary facts, and explain whether a proposed AI input could reveal a person. Assessment should record the quality of that reasoning alongside confidence. A high score on a general attitude statement should not be used as a professional competence credential.

Organisations can translate governance preferences into practical procedures: identify approved tools, specify who can authorise sensitive processing and provide an escalation route for uncertainty. Rights requests should have an identifiable recipient and a usable process. High-risk assessment should connect documented risks to decisions and follow-up, rather than end with agreement that assessments are desirable. These are proposed responses to the measured distinctions, not evidence that respondents' organisations lack or possess such procedures.

The NIST generative-AI profile offers a voluntary basis for thinking about risks and human interaction, while privacy frameworks can help structure data-risk assessment. Local professional and statutory requirements still determine the applicable

[36] Ajzen (n 7).
[37] Dinev and Hart (n 10); Nissenbaum (n 1).
[38] Maddux and Rogers (n 9); Bulgurcu, Cavusoglu and Benbasat (n 8).

responsibilities. Evaluation should examine whether procedures reduce unnecessary disclosure and improve correct handling of requests, with access to human assistance where needed. It should separately monitor technical output reliability, privacy practice and users' confidence.[39]

6.3 Policy and societal implications

Policy communication in Bangladesh can distinguish general governance aspirations from the specific duties, commencement arrangements and mechanisms in the Personal Data Protection Act. Professional confidentiality should be considered alongside, rather than assumed identical to, personal-data protection. The survey is not a compliance audit or a legal-knowledge examination, so it should not be used to estimate the prevalence of infringements.[40]

Research and professional bodies can develop locally reviewed examples of lawful processing, minimisation and rights procedures, then evaluate comprehension and performance. Formal oversight, resources and role allocation matter alongside education. A people-facing rights process should be judged for practical accessibility rather than assumed effective because respondents endorse its principle.

7. Conclusion Limitations and Future Research

This study uses 385 real questionnaire records to examine governance preferences and intended professional compliance in a legally oriented Bangladesh sample. Clear lawful-processing rules and high-risk assessments receive 76.4% and 75.6% endorsement, exceeding personal intention by 24.4 and 23.6 percentage points. Minimisation and rights access receive approximately 54% endorsement and do not show equivalent net contrasts with intention. The pattern therefore differentiates among governance principles rather than establishing a uniform preference-intention divide.

The primary binary model identifies a corrected association between rule preference and intention, but it is not retained in ordinal or student-only analyses. Eighty respondents endorse all four principles, of whom 47 endorse intention. These findings concern response alignment, not demonstrated legal knowledge, workplace policy or observed compliance. The defensible conclusion is that institutional governance preferences and intended personal conduct should be analysed separately before proposing how one may influence the other.

The contribution is a legally contextualised account of measurement and alignment. It replaces a broad knowledge/compliance composite with statements whose meanings remain visible, distinguishes paired

[39] Chloe Autio and others, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1, National Institute of Standards and Technology 2024), doi:10.6028/NIST.AI.600-1; NIST, Privacy Framework (n 4).
[40] Personal Data Protection Act 2026; Evidence Act 1872.

differences from individual association and reports sensitivity rather than selecting only the favourable specification. Substantively, it identifies minimisation and accessible rights as specific areas for capability-based follow-up. The framework connects professional responsibility with organisational implementation while avoiding a claim that self-reported intention establishes actual compliance.

The sample contains 242 students and is not established as representative of all legal professionals. Collection is mixed-mode, but dates, detailed recruitment and mode counts were unavailable. Career stage, employer policy and actual professional AI use are not verified. Self-report, single-item error, heterogeneous blocks and cross-sectional design limit interpretation. Adjustments cover only training and student status; unmeasured experience and institutional conditions may matter. Ordinal common slopes are assumed and one extreme category is sparse. Analyses are exploratory, and no observed behaviour or objectively scored knowledge is available.

Future work should document fieldwork and measure specific professional activities, workplace rules, perceived control and task efficacy. Cognitive interviews can test how respondents interpret necessary data and applicable rights. An independent validation study should separate governance preferences, knowledge, capability, intention and conduct before estimating latent pathways. Experiments can evaluate approved-tool guidance, minimisation practice and rights-request procedures using de-identified scenarios. Longitudinal workplace studies can then examine whether these capabilities and institutional supports predict safer processing, with consent, confidentiality and appropriate oversight. These designs would test the mechanisms that the present responses can only identify for further investigation.

Declarations

Ethical approval and oversight

No study-specific formal ethical approval or exemption was reported in the supplied materials or clarification; none is claimed. Participant protection and the limits of available oversight documentation are described in Section 3.8.

Informed consent

Participation was voluntary and based on informed consent, with anonymity and the opportunity to discontinue questionnaire completion. All analysed records contain affirmative consent and adult-eligibility responses.

Data availability

De-identified numerical data and analytical specifications may be requested from the corresponding author, subject to confidentiality and applicable requirements. Optional contextual text was excluded.

Funding and competing interests

No external funding source or competing interest was disclosed in the materials supplied for this manuscript.

Author contributions

Sumaiya Akter: conceptualisation, preparation of study materials, data organisation and curation, manuscript development. Prof. Dr Kazi Abdul Mannan: conceptual and methodological guidance, supervision, interpretation of statistical findings, critical review and editing. The student project was conducted under his supervision.

Generative AI disclosure

Generative AI assisted literature retrieval, drafting, language editing, organisation and analytical code development. Estimates were computed programmatically from numerical survey responses. Authors retain responsibility for analysis, interpretation, references and reporting.

Bibliography

Abraham R, Schneider J and vom Brocke J, 'Data Governance: A Conceptual Framework, Structured Review, and Research Agenda' (2019) 49 International Journal of Information Management 424

Acquisti A, Brandimarte L and Loewenstein G, 'Privacy and Human Behavior in the Age of Information' (2015) 347 Science 509

Ajzen I, 'The Theory of Planned Behavior' (1991) 50 Organizational Behavior and Human Decision Processes 179

Altman DG and Bland JM, 'Absence of Evidence Is Not Evidence of Absence' (1995) 311 BMJ 485

American Bar Association Standing Committee on Ethics and Professional Responsibility, *Generative Artificial Intelligence Tools* (Formal Opinion 512, 29 July 2024)

Autio C and others, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* (NIST AI 600-1, National Institute of Standards and Technology 2024), doi:10.6028/NIST.AI.600-1

Bovens M, 'Analysing and Assessing Accountability: A Conceptual Framework' (2007) 13 European Law Journal 447

Bulgurcu B, Cavusoglu H and Benbasat I, 'Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness' (2010) 34 MIS Quarterly 523

Carlini N and others, 'Extracting Training Data from Large Language Models' in *30th USENIX Security Symposium* (USENIX Association 2021) 2633

Cochran WG, *Sampling Techniques* (3rd edn, John Wiley & Sons 1977)

Dahl M and others, 'Large Legal Fictions: Profiling Legal Hallucinations in Large Language Models' (2024) 16 Journal of Legal Analysis 64

Dinev T and Hart P, 'An Extended Privacy Calculus Model for E-Commerce Transactions' (2006) 17 Information Systems Research 61

Efron B and Tibshirani RJ, *An Introduction to the Bootstrap* (Chapman & Hall 1993)

Herath T and Rao HR, 'Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations' (2009) 18 European Journal of Information Systems 106

Holm S, ‘A Simple Sequentially Rejective Multiple Test Procedure’ (1979) 6 Scandinavian Journal of Statistics 65

Hosmer DW Jr, Lemeshow S and Sturdivant RX, *Applied Logistic Regression* (3rd edn, John Wiley & Sons 2013)

Kokolakis S, ‘Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon’ (2017) 64 Computers & Security 122

Long D and Magerko B, ‘What Is AI Literacy? Competencies and Design Considerations’ in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (ACM 2020) 1

Maddux JE and Rogers RW, ‘Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change’ (1983) 19 Journal of Experimental Social Psychology 469

Magesh V and others, ‘Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools’ (2025) 22 Journal of Empirical Legal Studies 216

McCullagh P, ‘Regression Models for Ordinal Data’ (1980) 42 Journal of the Royal Statistical Society Series B 109

McNemar Q, ‘Note on the Sampling Error of the Difference between Correlated Proportions or Percentages’ (1947) 12 Psychometrika 153

National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0* (NIST 2020), doi:10.6028/NIST.CSWP.01162020

Nissenbaum H, ‘Privacy as Contextual Integrity’ (2004) 79 Washington Law Review 119

Raji ID and others, ‘Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing’ in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (ACM 2020) 33

Rogers RW, ‘A Protection Motivation Theory of Fear Appeals and Attitude Change’ (1975) 91 Journal of Psychology 93

Sijtsma K, ‘On the Use, the Misuse, and the Very Limited Usefulness of Cronbach’s Alpha’ (2009) 74 Psychometrika 107

Solove DJ, ‘Introduction: Privacy Self-Management and the Consent Dilemma’ (2013) 126 Harvard Law Review 1880

von Elm E and others, ‘The Strengthening the Reporting of Observational Studies in Epidemiology (STROBE) Statement: Guidelines for Reporting Observational Studies’ (2007) 4 PLOS Medicine e296

Wasserstein RL and Lazar NA, ‘The ASA Statement on p-Values: Context, Process, and Purpose’ (2016) 70 American Statistician 129

White H, ‘A Heteroskedasticity-Consistent Covariance Matrix Estimator and a Direct Test for Heteroskedasticity’ (1980) 48 Econometrica 817

Wilson EB, ‘Probable Inference, the Law of Succession, and Statistical Inference’ (1927) 22 Journal of the American Statistical Association 209

Appendix A Questionnaire wording

Table A1 reproduces every statement used in the focal and supporting analyses. Their analytical roles follow the wording rather than a claim of validated scale equivalence.

Table A1. Exact wording of analysed statements

Code	Questionnaire statement
DGC1	Organizations using AI should have clear rules for lawful data collection and processing.
DGC2	AI systems should collect only data necessary for their stated purpose.
DGC3	People should have accessible ways to exercise applicable data rights.
DGC4	Regular data-protection assessments should accompany high-risk AI deployment.
DGC5	I intend to follow data-governance rules when using AI in professional legal work.
DPA1	I understand that information entered into an AI system may create privacy risks.
DPA2	I avoid entering sensitive personal information into public AI tools.
DPA3	I check privacy or data-use information before using an AI service for sensitive tasks.
DPA4	I understand that AI services may collect, store or process user data.
DPA5	I believe users should receive clear information about how their data are used by AI systems.
PPR1	I worry that AI-powered legal platforms may expose personal or confidential information.
PPR2	Privacy concerns reduce my willingness to use AI services for sensitive legal matters.
PPR3	I would be more willing to use an AI platform that offers strong privacy controls.
PPR4	I would prefer an AI legal platform that allows meaningful control over personal data.
PPR5	Trust in data protection affects my intention to adopt AI-powered legal services.
AIL2	I verify important AI-generated information before relying on it.
AIL4	I avoid sharing confidential or sensitive information with AI tools unless appropriate safeguards are in place.
AIL5	I believe meaningful human oversight is necessary when AI affects important legal or rights-related decisions.

Source: supplied Group 5 Codebook. Responses range from 1 strongly disagree to 5 strongly agree. No substantive item is reverse-coded.

DGC5 is the primary model outcome. DGC1-DGC4 are focal predictors. DPA3 and DPA4 support selected correlations; other privacy and literacy statements provide descriptive context. The items do not constitute a scored legal-knowledge test or an audit of observed processing.

Table of Legislation

Personal Data Protection Act 2026 (Bangladesh), Act No 63 of 2026, ss 1(3), 16-17 and 44

Evidence Act 1872 (Bangladesh), ss 126-129

Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, arts 5, 25 and 35