A Work Project, presented as part of the requirements for the Award of a Master's degree in Management from the Nova School of Business and Economics

ANONYMOUS AND AI-GENERATED INFORMATION REQUESTS: RISKS FOR INSTITUTIONS – A CASE STUDY OF NOVA SBE

LEON SCHNEIDER

Work project carried out under the supervision of:

Leonor Rossi

21-05-2025

Abstract

This thesis uses Nova SBE as an example to examine how public bodies respond to anonymous and artificial intelligence-generated environmental-information requests. Grounded in EU transparency law (Aarhus Convention; Directive 2003/4/EC) and Advocate General Medina's opinion in Case C-129/24, it combines doctrinal analysis with a convenience survey of forty respondents (students, staff and outside stakeholders). Citing overload and privacy concerns, participants rate AI-generated requests as notably riskier than conventional anonymous requests (median 4 vs 3, $p < 0.05$). To protect institutional resilience while maintaining the right of access, the paper suggests statutory clarification, rate-limiting, conditional identity checks.

Keywords

Aarhus Convention, AI-Generated Requests, Anonymous Information Requests, Artificial Intelligence, Data Protection, Digital Information Management, Digital Requests, Directive 2003/4/EC, EU Law, Future Developments, Governance, Information Request Automation, Institutional Misuse, Institutional Risks, Nova SBE, Public Institutions, Regulatory Compliance, Risk Assessment, Transparency

This work used infrastructure and resources funded by Fundação para a Ciência e a Tecnologia (UID/ECO/00124/2013, UID/ECO/00124/2019 and Social Sciences DataLab, Project 22209), POR Lisboa (LISBOA-01-0145-FEDER-007722 and Social Sciences DataLab, Project 22209) and POR Norte (Social Sciences DataLab, Project 22209).

Table of Contents

1 Introduction

Digitalisation has significantly reshaped how institutions interact with the public. As communication channels decentralise, the volume and nature of information requests have evolved. While these developments enhance transparency, they also pose challenges to workflows, data protection, and compliance. Particularly, the rise of anonymous and AI-generated information requests disrupts conventional assumptions about authorship and responsibility, creating practical risks in verification, prioritisation, and resource allocation.

Under the Aarhus Convention and Directive 2003/4/EC, EU public institutions must respond to environmental information requests regardless of whether the applicant identifies themselves. These laws uphold the principle known as interest blindness, which does not imply anonymity or lack of legal personality, according to which access must be granted "without an interest having to be stated" (Directive 2003/4/EC, Art. 3(1)). However, concerns about misuse have intensified the debate. In Case C-129/24, Advocate General Medina considers whether institutions may request names and addresses to safeguard procedural integrity (CURIA, 2025). This thesis explores the impact of anonymous and AI-generated requests using Nova School of Business and Economics (Nova SBE) as a case study. The goal is to assess institutional vulnerabilities and understand how these interactions affect legal certainty, operational capacity, and reputation. The following sections describe the problem context, outline research goals, and introduce the guiding research questions.

1.1 Problem Statement

Public institutions are getting more and more digital information requests, many of which are turned in anonymously or using automated systems. Although anonymity could protect sensitive groups or whistleblowers, unbridled use leads to problems. Especially artificial intelligence-generated requests can overwhelm administrative systems but technically compliant with legal standards enable mass submissions.

This dynamic helps institutions to negotiate challenging trade-offs. They must respect openness rights even while they are effectively controlling resources, protecting data, and identifying abuse. In government of the digital age, the harmony between open access and procedural control is becoming a basic issue.

1.2 Relevance and Research Objectives

Two events drive this study: First, the legal background is still vague. Neither the Aarhus Convention nor Directive 2003/4/EC makes it abundantly clear whether identity disclosure is required. Second, technological change – especially generative artificial intelligence – allows difficultly monitored, scalable, human-like requests.

The thesis aims three-fold:

1. Evaluate requests made anonymously and using artificial intelligence from both legal and operational standpoint.
2. List institutional risk assessments.
3. Look at security measures fit for openness and proportionality.

The thesis mixes empirical data with legal analysis to handle these goals.

1.3 Research Question and Sub-questions

The central research question is:

How do anonymous and AI-generated information requests impact institutions, and what risks arise from this, using Nova SBE as an example?

This question is examined through the following sub-questions:

1. To what extent does EU law, especially the Aarhus Convention and Directive 2003/4/EC, permit anonymous requests?
2. What role does AI play in generating such requests?
3. What risks do stakeholders associate with anonymous and AI-generated submissions?
4. What institutional countermeasures are seen as appropriate?

5. What future trends can be expected in managing digital information requests?

1.4 Structure of the thesis

The thesis consists of six chapters. Chapter 2 provides the theoretical framework by means of a review of legal sources, jurisprudence, and relevant technology. Chapter 3 outlines the methodology, including Nova SBE's survey design and data collection techniques. The results regarding preferred strategies, institutional responses, and risk perception are presented in Chapter 4. Chapter 5 interprets these findings in the context of legal and technological frameworks. Chapter 6 rounds out key insights, policy recommendations, and ideas for next research projects.

Combining legal reasoning with empirical research, the thesis aims to show a whole picture of how institutions could change to accommodate ever more complex and automated forms of public participation.

2 Theoretical Background

This chapter provides the theoretical framework for evaluating the institutional risks presented by information requests produced by artificial intelligence and anonymous users. The thesis follows a structured approach by reviewing the EU legal framework – including the Aarhus Convention and Directive 2003/4/EC – alongside the interpretation provided by Advocate General Medina in Case C-129/24, the technological implications of digitalisation and artificial intelligence, and the resulting institutional risks. All claims are supported by verifiable scientific evidence and aligned with broader academic and legal discourse on digital information governance.

Legal rights and pragmatic restrictions become especially important since digital communication shapes institutional processes increasingly. The chapter aims to show how interactions among regulatory clarity, technological literacy, and organisational readiness shapes responses to new kinds of information access. Particularly underlining how

operationalised in a data-driven and proportionate manner vague legal language – such as the concept of "manifestly unreasonable" – requests must be, the study stresses finding risks and creating mitigating strategies calls for an interdisciplinary knowledge combining law, administrative science, and digital ethics.

Moreover, scholars argue that the practical application of open government concepts must be aware of operational thresholds. Transparency rights could ironically limit democratic participation by compromising the responsiveness and credibility of public authorities should institutions be routinely overwhelmed (Bannister & Connolly, 2011). More thorough analysis of legal frameworks and technological forces will help the following sections deepen the study of these dynamics.

2.1 Legal Framework

Aarhus Convention and Directive 2003/4/EC regulates access to EU environmental data available inside the EU. Transparency and openness – absolutely required for public involvement in environmental management – are helped to be codified by these tools. Their use, meanwhile, causes challenges in digital environments regarding anonymity, validation, and administrative load. Institutions are not sure whether they have the right to validate identities or limit too high requests. The following sections taken together provide a framework together with an analysis of evolving legal interpretations in view of jurisprudence and doctrinal debate. Though they rely on procedural presumptions anchored in analogues of administration, from a legal-theoretical perspective these tools reflect the EU's commitment to participatory democracy and sustainability. Operating in a digital, high-frequency environment, institutions run across structural mismatches between operational capacity and normative expectations. Researchers such as Meijer and Grimmelikhuijsen (2012) argue that without procedural adaptation, openness rights run the risk of erasing administrative legitimacy rather than enhancing it.

2.1.1 The Aarhus Convention and Directive 2003/4/EC

The Aarhus Convention (UNECE, 1998) guarantees public access to environmental data free from requiring a stated interest. Linking this right into EU law, Article 3(1) of the Directive requires public authorities to provide information to "any applicant" without regard for identify disclosure, Directive 2003/4/EC (European Parliament and Council, 2003). This emphasises transparency, but it offers little procedural guidance for managing either too demanding or anonymous requests. The Directive allows exceptions for obviously illogical or violent demands even though it does not have any criteria for deciding such circumstances (Art. 4(1)(b). This legal ambiguity calls institutional responses in a time of automated and anonymous digital communication under doubt (Zuboff, 2019). Scholarly research reveals the conflict in operational protections against open-access guarantees (Stark, 2020). Comparative study of national implementations exposes several points of view on identity criteria, so increasing the uncertainty.

Moreover, underlined in Article 6 of the Directive is the necessity of any rejection of information under review and the reasoning behind it. This implies that the restriction on access has rather high limits even in technologically developed surroundings. The European Ombudsman has underlined the need of balancing the rights to knowledge with the responsibilities of a good government. Practical examples from countries like Sweden and Austria expose that public bodies sometimes choose case-by-case solutions over set policies, so producing legal uncertainty and inconsistency.

2.1.2 Advocate General Medina's Opinion (Case C-129/24)

Advocate General Medina considered whether national institutions could ask for identity information when responding to requests for anonymous or pseudonymous environmental information in her 2025 opinion in Case C-129/24 (CURIA, 2025). Her logic is limited to Member State laws implementing Directive 2003/4/EC, not particularly relevant to EU

institutions. Regulation (EC) No. 1049/2001 guides requests made to EU institutions by stating that applicants must be a natural or legal person with legal personality if they are able to identify themselves. Medina's proposal that national laws could be compelled to let anonymous requests results in a legal asymmetry: EU institutions could be safeguarded by identity requirements while Member States might not be anymore.

This interpretation has been attacked for contradicting the language of Directive 2003/4/EC, which usually employs the phrase "any person" in a context that presumines identifiable applicants (see footnote 20 of the Opinion). Furthermore supporting her claim with a single doctrinal source (Whittaker, Reid & Mendel, 2023) that contrasts interest-blindness with identity-blindness without reference to national or EU administrative history is the AG.

Two prerequisites for contesting an administrative denial in court, Medina's point of view raises procedural issues at the judicial level since anonymous applicants cannot show authorship of a request or legal capacity. Thus, even if her interpretation might improve access on paper, in practice it could actually compromise legal coherence and enforceability.

2.2 Digitalisation and AI in the Context of Information Requests

Public institutional data collecting and request processing have changed under digitalisation. Web portals and email expose institutions to new vulnerabilities even while they simplify access and help to reduce transaction costs. According to OECD (2021), the technological potential for misuse may undermine these developments. Specifically generative models such as GPT-4 artificial intelligence (AI) reveal this risk. By producing, en masse, grammatically accurate and contextually relevant requests, such models reflect suitable user behaviour (Floridi & Chiriatti, 2020).

This realism makes it challenging to separate strategic or manipulative from actual efforts. Artificial intelligence can help companies with automated triage and data extraction even if public agencies sometimes lack the tools or knowledge to apply such instruments with

effectiveness (Veale et al., 2018). Moreover, absent of fastness are control systems. The European Commission (2020) underlines the need of consistent artificial intelligence anchored in responsibility, human supervision, and openness, although not yet definitely reflected in public administration.

Recent analysis by the Alan Turing Institute (2022) shows that, even if they could increase efficiency, automated moderation systems run the risk of over filtering and supporting bias. This conflict underlines the need of contextual judgement made possible by human-in-loop systems. Public sector innovation also shows that technical departments by themselves cannot outsourced ethical, legal, and participatory aspects of artificial intelligence governance.

Moreover, adding artificial intelligence into administrative procedures creates more governance-related issues than only technical ones. Algorithmic decision-making drives more and more public service delivery; thus, people may lose faith in the neutrality and fairness of results if institutions fail to explain how demands are screened, prioritised, or denied. Keeping credibility in front of rising automation mostly depends on the development of appealing channels and the openness in automated decision systems.

2.3 Institutional Risks from Anonymous and AI-Generated Requests

High volume anonymous submissions and sophisticated automation of requests present dual threats to institutions more and more. These changes question the conventional public administration systems, which were historically intended for slower, traceable, mostly individualised interactions. Institutions must rethink their operational models as digital systems let players send enormous numbers of legally framed but strategically disruptive requests. This part investigates how structural stress on legal compliance, service dependability, and public confidence results from anonymous and artificial intelligence-generated information searches. Based on scholarly literature and regulatory data, it shows how such demands generate both normative and pragmatic conflicts.

2.3.1 Risks of Anonymous Requests

For whistleblowers or in politically delicate circumstances, anonymity can provide protection (Bennett & Raab, 2006). But requests made under anonymity also restrict administrative capacity. Institutions cannot cluster or contextualise requests without clearly identified senders; this leads to inefficiencies. Repeated visits from the same anonymous actor remain unidentifiable, so limiting the ability to discover abuse or implement frequency limits. Moreover, absent from metadata is auditability and responsibility. Public agencies must respond even in situations involving doubt on capacity for follow-up or receipt. These limitations stop Article 4(1)(b) of Directive 2003/4/EC from being applied, so rendering denial for "manifestly unreasonable" requests. Practically, these tests demand evidence of pattern or intent – both concealed by anonymity.

Complicating reporting duties and internal recordkeeping, anonymous requests can also influence. Many times, organisations track performance metrics including type frequency or time-to-response for requests. These steps lose accuracy and hence their value for operational improvements without consistent identities. Moreover, the difficulty to verify a user's identity might compromise legal enforceability in cases where false information or suspected harmful data use exists. Researchers like Hood and Margetts (2011) have shown how bad data quality compromises institutional learning and responsibility.

2.3.2 Risks of AI-Generated Requests

Artificial intelligence generated demands carry a certain kind of risk. GPT-4 allows actor mass-production of syntactically varied but substantively identical entries. Usually following legal guidelines, these only meet basic needs and avoid conventional spam filters. Institutions thus show spikes in workload without corresponding public benefit (Backhaus et al., 2018). Legal systems do not distinguish between human and machine origin, which makes public authorities cautious to filter AI content in view of legal consequences.

Furthermore, depending on institutional openness and minimal qualitative interaction, produced by artificial intelligence Requests could show false references, cite invented statistics, or reflect legal arguments, so increasing the verifying costs. Should institutions be judged as unable to sufficiently control such inputs, damage to reputation also runs a risk. Ethical questions complicate response strategies even more. Automation may allow authorised low literate or disabled users. As stated in EU AI ethics guidelines (European Commission, 2020), any protections must thus follow proportionality and non-discrimination. Scalable inclusive tools must be developed by institutions to manage volume without discounting sensitive or artistic voices.

Policy responses should thus consist in tracking demand patterns driven by artificial intelligence and in regular threshold recalibration for human inspection. Pilot projects in Nordic countries combining public transparency reports with technical filters have helped to lower false positives as public confidence has grown. Research by the Centre for Digital Governance (2023) shows that regular stakeholder engagement – such as user surveys or institutional roundtables – can help fine-tune these systems and create legitimacy over time.

If institutions are to sustainably meet these challenges, they must apply forward-looking information governance models including adaptive risk assessments and contingency plans for times of great demand. Public relations demand crisis teams; dynamic capacity balances technical and human resources; and pre-defined escalation levels. Establishing flexible response systems helps businesses to maintain legal compliance and public confidence even in highly demanding, extremely volume environments. For instance, cross-institutional cooperation among data protection authorities, municipalities, and colleges can significantly boost collective resilience even more and support best practices to be always shared and polished. If we are to keep democratic responsibility and openness over time, this cooperative,

modular approach to handling anonymous and artificial intelligence-generated requests could become indispensable in the digital era.

3 Methodology

The methodological approach applied in this chapter to investigate the institutional risks presented by information requests generated by artificial intelligence and anonymous users is clarified. Aimed for a structured survey conducted at Nova School of Business and Economics (Nova SBE), the study employs a mixed-method approach combining qualitative and quantitative aspects. The method was supposed to combine pragmatic feasibility with fit and the stated research objectives of Chapter 1 in a compromise with academic rigour. This chapter is defined in three main divisions: the general research design, the construction and administration of the survey instrument, and the analytical techniques used to grasp the obtained data.

3.1 Research Design

A mainly quantitative research design was chosen considering the exploratory and evaluative character of the research question. This choice is justified by the necessity to gather insights from a wide range of institutional players while letting reasonable data interpretation. The main tool used to gather knowledge, opinions, and perceptions on the ethical, operational, and legal consequences of anonymous and artificial intelligence-generated information searches is the survey. Open-ended fields were added to let respondents discuss elements, so adding qualitative variation and strengthening the empirical basis.

Based on theoretical insights from EU law, administrative theory, and digital governance literature – as described in Chapter 2 – the design follows a deductive logic. From this basis, operationalised guiding questions emerged in the survey tool. The method so combines exploratory empirical mapping with normative frameworks. This reflects accepted advice for applied social research (Creswell, 2014).

The questionnaire was piloted to guarantee both validity and clarity. A limited-scale pilot at Nova SBE came after first internal pre-testing with academic colleagues. The comments led to little changes meant to improve sequencing and simplify language. The project supervisor approved the last edition, which was then distributed using standardised digital tools.

3.2 Survey Design

Designed online in May 2025 over 7 days for a subset of the Nova SBE community, a digital survey served as the main empirical tool for this project. The intention was to compile views from those who interact with public administration, in line of research or in professional or institutional capacity. This environment helps one to concentrate on the apparent hazards and governance expectations concerning information requests resulting from anonymous and artificial intelligence.

The work was aimed at a broad, general audience. To ground responses in a shared institutional environment, however, all participants were asked to evaluate a case study related to Nova SBE. Recruitment came from institutional mail lists and lines of internal communication. Participating was voluntary; all responses were anonymised to ensure GDPR compliance with privacy and data protection policies.

From the 7 days of data collecting, forty valid responses total. Despite it lowers generalisability, the sample size is appropriate for an exploratory case study. For basic descriptive statistics and qualitative interpretation, the number lets; for full-scale inferential testing this is not the case. Ethical permission was acquired following institutional policies for social scientific research.

3.2.1 Structure of the Questionnaire

Five thematic blocks made up the survey form:

1. Information on demographics: age group, professional position, institutional affiliation.
2. Awareness of pertinent legal systems (such as the Aarhus Convention) helps one to be familiar.

3. Opinion of risk: Consensus on possible hazards presented by artificial intelligence-generated requests including anonymous ones.
4. Institutional preferences: Opinions on preferred response choices and governing policies.
5. Normative attitudes: Concerns about identity validation, the difference between human and artificial intelligence searches, and the supposed validity of various access policies.

The questionnaire consisted in closed and open-ended questions. 5-point Likert scales helped most to record scaled responses. Free-text and multiple-choice elements helped to clarify things. The poll was developed with Qualtrics and tuned for desktop and mobile access.

3.3 Data Analysis Methods

Given the small sample size (N = 40), the quantitative work mostly uses descriptive statistics – that is, means ± SD together with absolute and relative frequencies – to aggregate the closed items. Independent-samples t-tests were used to probe subgroups (e.g., experienced vs. novice users); test statistics and p-values for the four hypotheses are reported in Chapter 4 (Table 4.1). Reviewed open-text responses using an inductive thematic analysis modelled by Braun & Clarke (2006). Covering themes including legal uncertainty, administrative burden and ethical issues, the resulting code book shows up in Appendix A and is discussed in Section 4.3, where illustrative quotes link qualitative insights to the survey results.

This descriptive-plus-t-test approach fits the exploratory character of the study since its goal is pattern detection and insight generating instead of wide statistical generalisation.

4 Empirical Results

This chapter presents the empirical results of the Nova SBE survey together with interpretations grounded on theoretical considerations developed in Chapters 1 through 3. The focus is on how institutional stakeholders assess related risks, view anonymous and artificial intelligence-generated information requests, and which governance policies they would want. References to

relevant scholarly literature improve every component and relate to past presumptions. Combining empirical and conceptual knowledge is supposed to enable one to evaluate the limits and acceptance of transparency in the digital age. Moreover, this chapter aims to contribute to the ongoing debate on digital governance by clarifying the conditions under which openness transforms from a strength into a vulnerability.

4.1 Participant Profile

The poll comprised 40 answered responses from many stakeholder groups. The sample consisted in largely students (37 %) and external professionals (60 %) as Figure I (Appendix A) shows. The largest age range shown in Figure II (Appendix B) is 30–39 followed by 20–29. This group reflects the reality of Nova SBE as a graduate school with a young, technologically fluent population even while it comprises operational and governance staff with direct institutional responsibilities. Such variety is essential since, as Meijer and Grimmelikhuijsen (2012) point out, personal experience with governance systems and institutional role influence how legitimate and transparent one views are. Including respondents with administrative and academic background guarantees that the data reflects operational problems as well as normative preferences. This range provides a strong basis for evaluating trade-off between institutional resilience and openness. Eventually, considering the intended scope of this case study, the response rate – though small – offers relevant exploratory information. Future studies employing a stratified sampling method could help to confirm these findings in institutional settings.

4.2 Knowledge and Attitudes toward Anonymous Requests

The first poll block looked at knowledge of EU laws, especially the Aarhus Convention and Directive 2003/4/EC. According to results, 62% of respondents knew nothing about EU law allowing requests for anonymous environmental information. This is consistent with past presumptions on low legal literacy in spheres related to digital rights. Still, 35% of respondents

thought anonymous requests were reasonable, while 32% turned them down and 33% stayed not sure. This almost equal implies that, despite legal protection, anonymity remains a divisive subject at institutional level.

Four hypotheses were developed so that one could methodically investigate these trends:

- H1: Those who believe that AI-generated requests pose more perceived risk are more likely to favour tougher rules.
- H2: Acceptance of anonymous requests corresponds favourably with awareness of legal provisions about anonymity.
- H3: Professional status—that of administrative against student—predicts variations in the support for identity verification techniques.
- H4: Support of technical countermeasures is favourably correlated with perceived risk (AI or anonymous).

This divide reflects the "transparency paradox" Bannister and Connolly (2011) describes: institutional acceptance does not always follow from legal openness. Research by Grimmelikhuijsen (2012) underline even more how trust and perceived relevance mediate the effects of transparency. Regarding Nova SBE, operational uncertainty and low awareness seem to compromise normal openness. One view is that anonymity questions accepted responsibility rules, particularly in administrative environments where personal attribution is central. Still, as Craig and Ludloff (2016) highlight, anonymity protects whistleblowers and underprivileged voices as well. Institutions could thus have to strike a balance between official legal compliance and internal procedures strengthening confidence in anonymous systems. This could include better rights communication or tiered verification processes maintaining access while controlling usage risk. Further research, including those by Roberts (2010), emphasises the need of institutional culture in mediating legal guarantees, a component probably relevant to Nova SBE as well.

4.3 Risk Perception of Anonymous and AI Requests

Participants were asked to rate the apparent institutional risk related with two request forms on a 5-point Likert scale. AI-generated requests rated as 4 or 5 in risk accounted for 68% of all requests, far higher than 45% for anonymous ones. Figures IV and V (Appendices C and D) highlight this clear discrepancy.

Respondents connect artificial intelligence searches with high volume, unverifiability, and automation – all components impacting a loss of procedural control. These problems reflect a general shift in legal entitlement from openness to transparency as a managed resource.

Scholarly-wise, this is in line with Veale et al. (2018), who underline that artificial intelligence generates systematic uncertainty into public administration especially in cases of limited monitoring capacity. Moreover, Floridi and Cowls (2019) warn of the "black box effect" in algorithmic governance: institutions struggle to validate the origin, intent, or legitimacy of AI-driven contacts. The high-risk ratings shown here confirm that these problems are operational rather than abstract. One respondent noted, "AI might be a solution for public access," but "only if we control its volume and validate its sender."

By contrast, anonymous requests produced more contradictory answers. Some participants underlined their democratic value – that "not everyone can afford to reveal their identity" – while others concentrated on abuse possibility. This diversity suggests that contextual dependent anonymity is not intrinsically problematic. Literature by Tsoukas (1997) and O'Neil (2016) supports this: institutions must see anonymity as a governance variable rather than a binary one. Practically, this can mean risk-based triaging systems weighing request content, volume, and verifiability to establish procedural depth. Moreover, institutional clarity about procedural protections – such as post-hoc audits or metadata recording – may help to reduce the claimed trade-off between openness and control.

4.4 Institutional Response Preferences

From a pre-defined list, responders could select several protective actions to look at how institutions should handle matters. Most often used ones were rate restrictions (55%), CAPTCHA-style protections (59%), and identity verification (64%). Just 14% of respondents believe that, independent of source, all requests should be handled equally. Figure 5 (Appendix E) separates these preferences based on stakeholder role: Staff wanted protections; students welcomed open systems more readily. This difference captures what Meijer (2014) observes as "role-dependent transparency expectations." Students want access, but staff members typically give procedural integrity first importance. These findings suggest that systems of governance must consider segmentation of stakeholders. For example, while compliance officials focus on audit trails, communication staff may give responsiveness first importance.

The data also support OECD (2021) conclusions stressing the need of layered defences for digital institutions. One-size-fits-all rules cannot apply in a hybrid environment of human and machine-generated interactions. Open comment responders proposed tiered response systems, institutional artificial intelligence policies, and AI-detection filters. One wrote, "We need digital customs, like a firewall for requests." Another underlined that volume is not the only issue; "It's also the uncertainty: who's asking? For what exactly? Using the knowledge, what will they do? These comments underline the qualitative as well as quantitative character of risk assessment. Institutions worry about consequences and legitimacy just as much as about overload. As Bovens et al. (2014) argue, procedural legitimacy is preserved not by access but by clarity, responsibility, and proportionality in response. The decisions shown here support a modular governance approach in which content, frequency, and credibility indicators match request handling. Future application should give technical viability top importance as well as communication clarity.

4.5 Hypothesis Testing

Four hypotheses formulated from the theoretical framework were tested using descriptive and inferential statistics. H1 hypothesised that those who felt great risk connected to artificial intelligence would also support robust control. Although mean values followed the expected trend, a t-test turned up no significant correlation ($p = 0.705$). Once more, nothing of significance ($p = 0.327$). H2 looked at whether knowledge of EU anonymity rights, or legal awareness, affected acceptance of anonymous requests. H3 investigated whether status, that is, student against staff, predicted support for identity checks – also negligible – $p = 0.868$.

Only H4 yielded a noteworthy result ($p = 0.005$) looking at whether risk perception matched support for technical protections. This suggests that while general attitudes could be nebulous, particular risk issues become preferences for action. Policy preferences, as Oliver (2013) notes, crystallise most powerfully around concrete hazards. These outcomes validate risk-based institutional design as a practical governance tool.

While only one hypothesis shows relevance, overall, the direction of results supports significant theoretical assumptions. Views of risk and trust first help to mediate transparency preferences (Grimmelikhuijsen & Welch, 2012). Second, the stakeholder roles affect the normative expectations of transparency (Lidskog et al., 2011). Third, legal knowledge by itself does not ensure institutional legitimacy until deeply ingrained in operational capacity and strategic clarity (Curtin & Meijer, 2006).

Future studies on request handling systems should look at field experiments, cross-national comparisons, or bigger samples. Moreover, including requests produced by artificial intelligence into public-sector operations demands long-term observation since first impressions might change with exposure. Still, the Nova SBE case study offers a current perspective of how institutional governance interacts with digital transformation. Its findings

especially relate to companies handling similar challenges in balancing legitimacy, automation, and involvement.

Taken together, the findings offer an empirical foundation for the interpretative discussion in Chapter 5, where more specific analysis of the implications of these conclusions for institutional design, stakeholder involvement, and policy framing is conducted.

5 Discussion

This chapter addresses the implications of the empirical results in view of the legal and conceptual frameworks discussed in Chapter 2. The focus is on how institutions such as Nova SBE see and manage risks related to artificial intelligence-generated information searches including anonymous data. Connecting stakeholder responses to current legal interpretations and governance literature helps the chapter to highlight significant challenges and consider their institutional relevance. The objective is to derive proportionate and operationally feasible solutions balancing the need of procedural protections with the transparency obligations in progressively digital demand environments. Four dimensions define the discussion: interpretation of results, theoretical alignment, institutional consequences, and observed constraints.

5.1 Interpretation of Findings

The poll results expose several points of view on the validity and feasibility of requests generated by means of anonymous and artificial intelligence. Though anonymity was generally accepted in theory, searches carried out using artificial intelligence were seen as more problematic. Respondents underlined functional issues including more work and resource burden over more general legal questions. This implies that official legal status does not define more how institutional tolerance is developed than perceived intention and operational cost.

Especially many of the respondents agreed with identity verification in cases of suspected abuse but disagreed with general policies. This exposes a proportional attitude to openness:

institutional value should not be lost even if it should be maintained. Underlines the need of low-friction, adaptive defences, support of rate-based controls, request limits, and CAPTCHAs. "Anonymous access is important – but not if it means paralysing our systems," one respondent summed up this balance rather succinctly. Institutions must thus match sensible capacity limits with protections.

These results expose a dynamic between operational manageability and democratic access that defines digital governance gradually more and more in conflict. Public institution design defines their legitimacy in remaining open but defendable as they come across growing automated interaction.

5.2 Relation to Theoretical Background

The empirical results answer the legal interpretation Advocate General Medina presents in Case C-129/24. Medina contends under the Aarhus Convention and Directive 2003/4/EC that although public authorities may verify identity in cases of suspected procedural abuse, anonymous access is a fundamental right. This point of view matches the conditional safeguards respondents would want. It also advances a change from strict interpretation towards risk-responsive government.

Article 4(1)(b) of the directive lets authorities reject "manifestly unreasonable" requests; it provides no clear definition of such unreasonableness in digital environments. Medina's point of view closes this disparity by supporting sensible precautions and contextual judgement. Institutions are thus let to step in when overwhelmed without straying from openness criteria. Legal ambiguity does, however, often discourage action in practice. Many businesses are reluctant to turn down demanding requests concerning legal challenges or damage of reputation. Moreover, the poll results support academic points of view according to which openness is a sociotechnical process. Researchers such as Veale et al. (2018) and Zuboff (2019) warn as detailed in Chapter 2 that artificial intelligence can skew institutional involvement by hiding

masking manipulation as civic participation. Janssen and Kuk (2016) also contend that institutional capacity must change in line with legal requirements and technical tools. From this point of view, theoretical concepts need to be translated into workable governance structures while Nova SBE participants' responses show how anchored in feasibility and responsiveness.

5.3 Implications for Institutions

The rise of requests made anonymously and using artificial intelligence forces companies to reconsider how they handle digital interaction. Companies who have always been obliging consumers of requests now have to monitor, assess, and rank vast volumes of possibly automated data. This calls not only new tools but also fresh ideas of governance. Scalable, context-sensitive systems must actively maintain open access; it cannot be guaranteed just by non-discrimination.

If Nova SBE received hundreds of semantically identical AI-generated requests in a short period of time, for example, the administrative load would most likely be more than it could manage. Staff members running the risk of delay or inconsistency would be under pressure to give response strategies top priority without clear direction. Such overload could erode public confidence, especially in cases where the institution is seen as unduly restrictive or unresponsive. Preventive systems thus must forecast volume and intent rather than only formal compliance.

Survey participants quietly agreed with this viewpoint. Appropriate countermeasures included internal coordination, temporary identity verification, and technical filtering. Most importantly, they preferred flexible government over global policies. This suggests that in procedural design, transparency and justice define legitimacy rather than rigidity. Institutions that justify protective actions and apply them in line are more likely to retain the trust of their employees.

5.3.1 Identified Risks

The studies highlight some key risks. First, operational strain from mass donations made by artificial intelligence may overwhelm limited institutional resources. These demands might theoretically follow legal guidelines even though they lack great civic intent. Second, legal doubt on identity confirmation creates uncertainty. Institutions worry especially about running legal conflicts or violating transparency rules without precedents or procedural clarity.

Third, institutions thought to be either too liberal or too repressive damage reputation. Some would view protective acts as censorship or, alternatively, as inaction resulting from incompetence. Maintaining institutional credibility calls for the right mix. Moreover, aggravating these risks are divided internal governance and technical inertia. Administrative, legal, and IT departments running without coordination can lead to inconsistent filtering or response policies. From this follows legal exposure, inefficiencies, and a declining confidence among stakeholders.

To help to offset this, institutions must rely on well-defined escalation paths and centralised systems. Digital resilience cannot be reached just with technology; it calls for internal alignment, shared responsibility, and ongoing adaptation.

5.3.2 Possible Risk Mitigation Strategies

The results compel one to counsel a layered mitigating strategy. First to early block highly volume or suspicious entries, institutions should use automated tools including pattern detection, IP filtering, and CAPTCHAs first. These systems reduce load by letting authorised users' access. Second, conditional identity verification should only be carried out under exactly defined criteria – that is, when demand frequency or content points to possible abuse.

Thirdly, obviously, dashboards and transparency reports should show institutional response strategies and thresholds. Indicating control helps one to get confidence and discourage violence. Fourth, cooperative policy development guarantees that, with input from legal

academics, data security experts, and civil society, governance strategies remain legitimate, reasonable, and flexible. Sort this input to foster group responsibility.

Fifth, training and internal capacity building are quite vital. Staff members should be conversant with relevant legal frameworks, escalation rules, digital request systems. Institutions should also endeavour on projects like the Open Government Partnership (OGP) and evaluate their policies in line with those of other businesses. This promotes best practice identification, improves consistency, and guarantees congruence with international criteria.

Especially fit for lead in this field are colleges like Nova SBE. Their capacity for research, independence, and multidisciplinary reach helps them to be test beds for smart transparency. Apart from enhancing institutional credibility, creating internal AI-triage systems would help professors and students to establish resilience using technology.

5.4 Limitations of the Research

There are some limits in this research. It revolves mostly on one institution – Nova SBE – that reduces generalisability. Other public authorities or companies might follow different legal, cultural, or infrastructure guidelines. The survey's framework consisted in hypothetical situations, like answering 1,000 weekly questions. These are helpful, but under real overload conditions these could not reflect actual behaviour or stress reactions.

The paper also examines anticipated, not observed, artificial intelligence-generated requests. It evaluates data entered in real time not automatically. It thus ignorance of real system burden or algorithmic trends. Future studies might solve this by means of live simulations or audit institutional reactions under controlled stress levels.

The evolving legal scene adds still another limitation. EU case law on anonymous digital access is yet unknown as of right now. In particular with regard to identity verification, new laws could either expand or limit institutional discretion. Legislative changes – especially under projects

aiming at digital governance – may also influence procedural guidelines. Thus, depending on the time, the importance of the results of this study may vary.

Still, this chapter adds in a relevant way concepts on institutional capacity, open access, and digital risk management. anchored in resilience, adaptability, and proportionality, it challenges public institutions and universities to rethink how they apply openness in reality.

6 Conclusion and Outlook

Public institutions now face fresh difficulties with the growing frequency of anonymous and artificial intelligence-generated information searches. Investigating these developments from both a legal and empirical standpoint, this thesis has shown conflicts between institutional stability and openness responsibilities. Although present EU law guarantees access rights without identity disclosure, the operational reality clearly shows the need of protective systems. Chapter 6 addresses the main conclusions, responds to the research question, generates pragmatic recommendations, and lists next areas of study. Taken together, these viewpoints seek to support a balanced, legally sound, technologically informed approach to digital information governance.

6.1 Summary of Key Findings

With Nova SBE as a case study, this thesis investigated public institution reactions to artificial intelligence-generated information searches including anonymity. While legal systems including the Aarhus Convention and Directive 2003/4/EC provide wide access rights – including the right to anonymity – these rights can contradict institutional needs for responsibility and operational manageability. Especially with reference to automated mass requests, which can overwhelm systems, lower responsiveness, and erode trust, the empirical data confirm that staff members and students both see great risks. Furthermore, underlined by the legal research is growing conflict between pragmatic procedural protections and normative transparency obligations. Advocate General Medina's (Case C-129/24) point of view provides

a possible middle ground that so gives institutions a legally valid basis for protective measures by allowing identity verification under specific criteria. At last, the study shows that adaptive governance determines whether institutional resilience or openness is more appropriate.

6.2 Answer to the Research Question

Institutions respond differently depending on artificial intelligence and information searches produced by anonymous users. Legally, they challenge the boundaries of open-access policies that do not yet clearly separate coordinated abuse from actual public interest. Operationally, many institutions today lack technical capacity, personnel, and time needed to handle these demands. Institutions run the danger of looking either opaque if they ignore these expectations or unprofessional if overburdened from a reputation standpoint. The Nova SBE case shows how precisely, fairly, and transparently policies define the apparent validity of institutional responses. Although they must respect the legal right to access environmental data under anonymity, institutions basically need useful tools to properly control access to it. Consequently, the legal obligation should be seen in view of risk, volume, and institutional capacity instead of implying perfect availability.

6.3 Recommendations for Institutions

Given the observed challenges, public agencies should manage requests received anonymously or via artificial intelligence using proactive strategies. First helping to avoid overload without sacrificing access rights are technical protections including CAPTCHA systems, IP monitoring, and rate-limiting support. Second, institutions should build a tiered response model whereby they demand identity verification just when specific indicators, such high-frequency, templated, or pseudonymous requests, point to usage. Third, artificial intelligence should be considered as a tool for support as well as a threat; for instance, it can help classify requests, spot trends, and simplify responses. Fourth, institutional policies must be legally sound and well-documented so that any departure from perfect openness could have a logical basis. Not least of all, by means

of cross-sectoral communication with peers, authorities, and digital rights organisations, institutions should help to create best practices. This approach can protect fundamental liberties and preserve institutional capability in the digital era.

6.4 Future Research Directions

Extending the conclusions of this thesis, next studies should widen the field of inquiry and deepen it. Comparative legal study among EU countries offers a good road map for several Aarhus Convention implementations and evaluates how identity management is really managed. Moreover, longitudinal studies tracking institutions during times of great demand – especially from automated sources – may expose details on institutional resilience and adaptation. Technical research is another area of interest: assessing and benchmarking automated public institution filtering systems to split between approved and illegal digital interaction. By looking at how users view institutional legitimacy when identity is required or requests are limited, behavioural research could help to even more clarify things. Development of responsive, fair, and strong models of information governance will depend on interdisciplinary studies combining legal analysis, administrative science, and generally digital ethics depending on other disciplines.

References

Aarhus Convention. 1998. *Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters*. Geneva: United Nations Economic Commission for Europe.

Backhaus, Klaus, Bernd Erichson, Wolfgang Plinke, and Rolf Weiber. 2018. *Multivariate Analysemethoden: Eine anwendungsorientierte Einführung*. 15th ed. Wiesbaden: Springer Gabler.

Bannister, Frank, and Regina Connolly. 2011. "The Trouble with Transparency: A Critical Review of Openness in e-Government." *Policy & Internet* 3 (1): 1–30.

Bennett, Colin J., and Charles D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. 2nd ed. Cambridge, MA: MIT Press.

Bovens, Mark, Robert E. Goodin, and Thomas Schillemans, eds. 2014. *The Oxford Handbook of Public Accountability*. Oxford: Oxford University Press.

Braun, Virginia, and Victoria Clarke. 2006. "Using Thematic Analysis in Psychology." *Qualitative Research in Psychology* 3 (2): 77–101.

Centre for Digital Governance. 2023. *Digital Trust and Stakeholder Legitimacy*. Working Paper.

Craig, Terence, and Mary E. Ludloff. 2016. *Privacy and Big Data: The Players, Regulators, and Stakeholders*. 2nd ed. Sebastopol, CA: O'Reilly Media.

Creswell, John W. 2014. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 4th ed. Thousand Oaks, CA: Sage Publications.

Curtin, Deirdre, and Albert Meijer. 2006. "Does Transparency Strengthen Legitimacy? A Critical Analysis of European Union Policy Documents." *Information Polity* 11 (2): 109–122.

Directive 2003/4/EC. 2003. "Directive of 28 January 2003 on Public Access to Environmental Information." *Official Journal of the European Communities* 41: 26–32.

European Commission. 2020. *Ethics Guidelines for Trustworthy AI*. Brussels.

European Parliament and Council. 2001. "Regulation (EC) No 1049/2001 Regarding Public Access to European Parliament, Council and Commission Documents." *Official Journal of the European Communities* L 145/43.

Floridi, Luciano, and Massimo Chiriatti. 2020. "GPT-3: Its Nature, Scope, Limits, and Consequences." *Minds and Machines* 30 (4): 681–694.

Floridi, Luciano, and Josh Cowls. 2019. "A Unified Framework of Five Principles for AI in Society." *Harvard Data Science Review* 1 (1): 1–17.

Floridi, Luciano, Josh Cowls, Monica Beltrametti, Raja Chatila, Patrice Chazerand, Virginia Dignum, Christoph Luetge, **et al.** 2018. "AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations." *Minds and Machines* 28 (4): 689–707.

Grimmelikhuijsen, Stephan G., and Eric W. Welch. 2012. "Developing and Testing a Theoretical Framework for Computer-Mediated Transparency of Local Governments." *Public Administration Review* 72 (4): 562–571.

Grimmelikhuijsen, Stephan G., and Albert Meijer. 2012. "Transparency and the Effectiveness of Public Service Delivery: A Literature Review." *Public Performance & Management Review* 36 (1): 89–106.

Hood, Christopher, and Helen Margetts. 2011. *The Tools of Government in the Digital Age*. Basingstoke: Palgrave Macmillan.

Information Commissioner's Office and The Alan Turing Institute. 2022. *Explaining Decisions Made with AI*. London.

Janssen, Marijn, and Gemma Kuk. 2016. "The Challenges and Limits of Big Data Algorithms in Technocratic Governance." *Government Information Quarterly* 33 (3): 371–377.

Krämer, Ludwig, and Charles Badger. 2024. *Krämer's EU Environmental Law*. 9th ed. Oxford: Hart Publishing.

Lidskog, Rolf, Arthur P. J. Mol, and Peter Oosterveer. 2011. "Environmental Risk and Governance: Understanding Socio-Economic and Political Transformations." *Environmental Politics* 20 (6): 810–828.

Medina, Laila. 2025. *Opinion of Advocate General in Case C-129/24, Coillte Cuideachta Ghníomhaíochta Ainmnithe v Commissioner for Environmental Information*. Court of Justice of the European Union.

Meijer, Albert. 2013. "Understanding the Complex Dynamics of Transparency." *Public Administration Review* 73 (3): 429–439.

Meijer, Albert, and Stephan Grimmelikhuijsen. 2012. "Transparency, Trust and Value." *International Review of Administrative Sciences* 78 (1): 50–68.

Meijer, Albert. 2014. "Transparency." In *The Oxford Handbook of Public Accountability*, edited by Mark Bovens, Robert E. Goodin, and Thomas Schillemans, 507–524. Oxford: Oxford University Press.

OECD. 2021. *Digital Government Index: 2021 Results*. Paris: OECD Publishing.

O'Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishing Group.

Oliver, Christine. 2013. "Organizational Responses to Institutional Complexity: Institutional Logics and Organizational Design." *Organization Studies* 34 (3): 403–422.

Roberts, Alasdair. 2010. *The Logic of Discipline: Global Capitalism and the Architecture of Government*. New York: Oxford University Press.

Stark, Bianca. 2020. "Automating Transparency? Algorithmic Systems and Open Government." *Journal of Information Technology & Politics* 17 (2): 123–136.

Tsoukas, Haridimos. 1997. “The Tyranny of Light: The Temptations and the Paradoxes of the Information Society.” *Futures* 29 (9): 827–843.

UNECE. 2014. *The Aarhus Convention: An Implementation Guide*. 2nd ed. Geneva: United Nations.

Veale, Michael, Reuben Binns, and Lilian Edwards. 2018. “Algorithms That Remember: Model Inversion Attacks and Data Protection Law.” *Philosophical Transactions of the Royal Society A* 376 (2133): 20180083.

Veale, Michael, Sara Hajian, Richard Fletcher, Gianluca Misuraca, and Lilian Edwards. 2018. “Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision-Making.” In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Article 440: 1–13. New York: ACM.

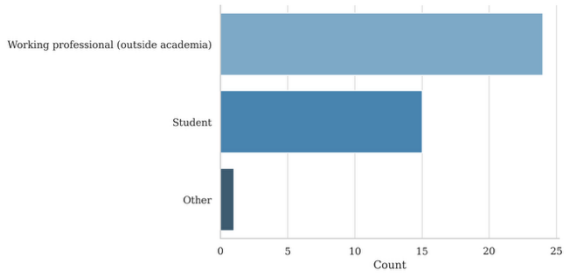
Wachter, Sandra, Brent Mittelstadt, and Chris Russell. 2017. “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR.” *International Data Privacy Law* 7 (2): 76–99.

Whittaker, Daniel, Emily Reid, and Toby Mendel. 2023. *Freedom of Environmental Information: Aspirations and Practice*. Cambridge: Intersentia.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

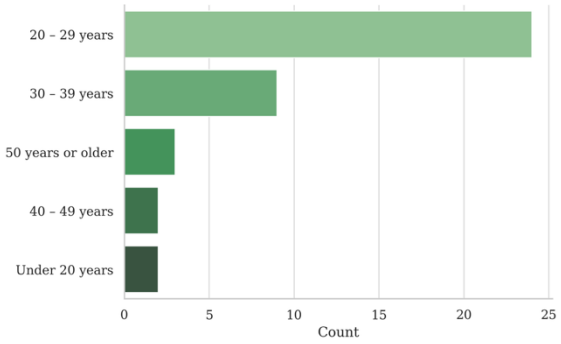
Appendices

Appendix A: Figure I: Respondent Status Profile



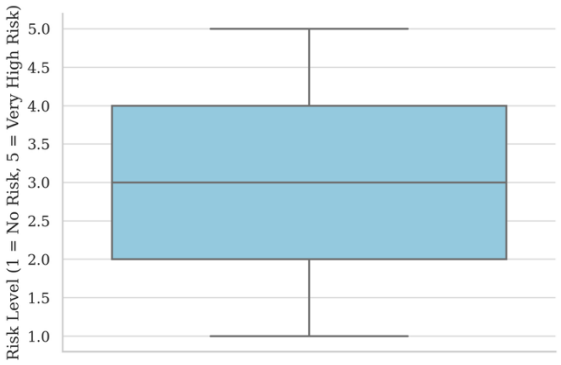
Bar chart, n = 40. Number of respondents by status category: Student (n=15), Working professional (n=24), Other (n=1).

Appendix B: Figure II: Age-Group Distribution of Participants



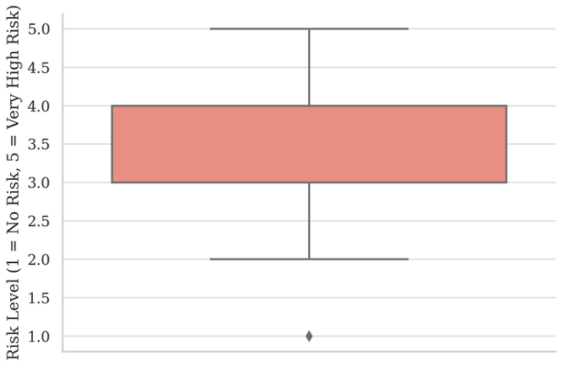
Horizontal bar chart, n = 40. Counts of participants in age brackets: Under 20 years, 20–29 years, 30–39 years, 40–49 years, 50 years or older.

Appendix C: Figure III: Perceived Risk from Anonymous Requests



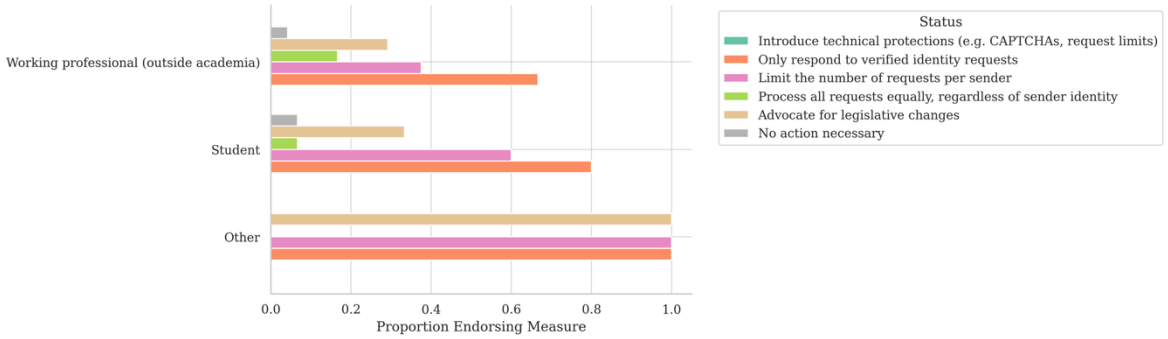
Boxplot, n = 40. Risk level rated on a 5-point Likert scale (1 = No risk, 5 = Very high risk).

Appendix D: Figure IV: Perceived Risk from AI-Generated Requests



Boxplot, n = 40. Risk level rated on a 5-point Likert scale (1 = No risk, 5 = Very high risk).

Appendix E: Figure V: Preferred Institutional Countermeasures by Status Group



Grouped bar chart, n = 40. Proportion of respondents in each status group endorsing countermeasures: introduce technical protections (e.g., CAPTCHA, rate limits); only respond to verified identity requests; limit number of requests per sender; process all requests equally; advocate legislative changes; no action necessary.

Appendix F: Table I: Codebook

Variable name	Question (short)	Response format / values	Recoding / derived	Description
StartDate … RecordedDate	Qualtrics system fields	ISO date-time, seconds, percentages	—	Metadata (start/end time, duration, progress, etc.)
Q1_status	Current status	1 Student · 2 Working professional · 3 Admin/IT staff · 4 Academic staff · 5 Other	—	Demographic
Q2_age	Age group	1 < 20 · 2 20–29 · 3 30–39 · 4 40–49 · 5 50 +	—	Demographic
Q3_awareness	Knows that environmental info requests can be anonymous (EU)	1 Yes · 0 No	—	Prior knowledge
Q4_accept	Thinks anonymous requests are acceptable	1 Yes · 2 No · 3 Unsure	—	Attitude
Q5_riskAnon	Perceived risk from **many anonymous** requests	Likert 1 (None) – 5 (Very high)	—	Risk perception
Q6_riskAI	Perceived risk from **AI-generated** requests	Likert 1 – 5	—	Risk perception
Q7a_captcha	Tech protections (CAPTCHAs, rate limits) selected	0 Not chosen · 1 Chosen	—	Multiple-choice dummy
Q7b_idOnly	Only respond to verified IDs	0/1	—	—
Q7c_limitSender	Limit number per sender	0/1	—	—
Q7d_equalTreat	Process all equally	0/1	—	—
Q7e_advocateLaw	Advocate legislative change	0/1	—	—
Q7f_noAction	No action necessary	0/1	—	—
Q8_verifyID	Allow identity verification?	1 Always · 2 Only if misuse · 3 Never · 4 Unsure	—	Policy stance
Q9_distinguish	Treat AI vs. human requests differently?	1 Stricter for AI · 2 Treat equally · 3 Unsure	—	Policy stance
Q10_comment	Other comments	Free text	—	Open question

This table lists each survey item with its short question wording, the corresponding variable name, response formats or value ranges, any recoding or derived variables, and a brief description of each variable's purpose.

Appendix G: Table II: Sample Description

Variable	Category	n	%
Status	Student	15	37%
	Working professional	24	60%
	Admin / IT staff	0	0%
	Academic staff	0	0%
	Other	1	3%
Age group	< 20 yrs	2	5%
	20–29 yrs	24	60%
	30–39 yrs	9	23%
	40–49 yrs	2	5%
	50 + yrs	3	8%

This table displays the frequency (n) and percentage (%) of participants across status categories (Student; Working professional; Admin/IT staff; Academic staff; Other) and age groups (< 20 yrs; 20–29 yrs; 30–39 yrs; 40–49 yrs; 50+ yrs) for the total sample (n = 40).

Appendix H: Table III: Survey Flow

Metric	Value
Invitations sent	N/A (Used groups and lists with thousands of members)
Surveys started	40
Surveys finished	40
Response rate	N/A (Invitation number N/A)

This table summarizes key survey metrics: number of surveys started (n = 40), number of surveys completed (n = 40), and notes on invitations sent and response rate where exact denominators were unavailable.

Appendix I: Table IV: Full Questionnaire

Demographics

1. *Which of the following best describes your current status?*
   □ Student □ Working professional □ Administrative/IT staff □ Academic staff □ Other

2. *What is your age group?*
   □ Under 20 □ 20–29 □ 30–39 □ 40–49 □ 50 or older

Knowledge & attitudes

3. *Were you aware that, in the EU, environmental information can be requested anonymously?*
   □ Yes □ No
4. *Do you think it is generally acceptable to allow anonymous information requests?*
   □ Yes □ No □ Unsure

Risk perception

5. *How high do you perceive the risk for an institution receiving many anonymous information requests?*
   1 □ 2 □ 3 □ 4 □ 5 □
6. *How high do you perceive the risk from AI-generated mass information requests?*
   1 □ 2 □ 3 □ 4 □ 5 □

Institutional response

7. *Imagine Nova SBE receives 1,000 anonymous or AI-generated information requests per week. How should it respond?* (select all that apply)
   □ Introduce technical protections (CAPTCHAs, request limits)
   □ Only respond to verified identity requests
   □ Limit the number of requests per sender
   □ Process all requests equally, regardless of sender identity
   □ Advocate for legislative changes
   □ No action necessary

Identification requirements

8. *Should institutions be allowed to require identity verification (e.g., name) before processing information requests?*
   □ Yes, always □ Only in case of suspected misuse □ No, never □ Unsure
9. *Should there be a distinction between human-generated and AI-generated requests?*
   □ Yes, AI-generated requests should be treated more strictly
   □ No, all requests should be treated equally
   □ Unsure

Open comment

10. *Do you have any other comments or concerns about anonymous or AI-generated information requests?*
    _____

This table presents each questionnaire item in the order administered, along with the corresponding response formats or option lists.