

Patricia Sharp

Uniwersytet Zielonogórski

ORCID 0009-0007-9547-563X

20000967@stud.uz.zgora.pl

AI Advancements and GDPR Obligations Regarding the Content of Personal Data Processing Notices: Challenges for Public Administration in Poland

Keywords: personal data processing notice, GDPR transparency, artificial intelligence, public administration, automated decision-making

Summary. The integration of artificial intelligence systems into public administration in Poland raises significant compliance challenges under the EU General Data Protection Regulation (GDPR). This article examines the content requirements for personal data processing notices, the primary transparency instrument under GDPR Articles 13 and 14, as they apply to AI systems deployed by Polish public bodies. The article argues that AI systems create genuine and previously underappreciated challenges for fulfilling transparency obligations, particularly the requirement to provide “meaningful information about the logic involved” under Article 13(2)(f) of the GDPR. The analysis identifies three temporally and functionally distinct disclosure obligations arising from the intersection of GDPR, the EU AI Act, and Poland’s Administrative Procedure Code, and demonstrates that processing notices under GDPR Article 13 occupy an irreplaceable ex ante role that cannot be substituted by procedural transparency requirements.

Rozwój AI a obowiązki RODO w zakresie treści klauzul informacyjnych: wyzwania dla administracji publicznej w Polsce

Słowa kluczowe: klauzula informacyjna o przetwarzaniu danych osobowych, przejrzystość RODO, sztuczna inteligencja, administracja publiczna, zautomatyzowane podejmowanie decyzji

Streszczenie. Integracja systemów sztucznej inteligencji z administracją publiczną w Polsce generuje istotne wyzwania w zakresie zapewnienia zgodności z unijnym Ogólnym Rozporządzeniem o Ochronie Danych (RODO). Artykuł podejmuje analizę wymogów treściowych klauzul informacyjnych dotyczących przetwarzania danych osobowych, stanowiących podstawowy instrument realizacji zasady przejrzystości wynikającej z art. 13 i 14 RODO, w kontekście systemów AI wykorzystywanych przez polskie organy władzy publicznej. W artykule wykazano, że zastosowanie systemów sztucznej inteligencji prowadzi do powstania rzeczywistych oraz dotychczas niedostatecznie rozpoznanych trudności w zakresie realizacji obowiązków informacyjnych, w szczególności w odniesieniu do wymogu przekazania „istotnych informacji o zasadach podejmowania decyzji”, o którym mowa w art. 13 ust. 2 lit. f RODO. Analiza wskazuje, że specyfika systemów AI, w tym ich złożoność techniczna oraz ograniczona przejrzystość modeli decyzyjnych, utrudnia spełnienie standardu informacyjnego przewidzianego w przepisach o ochronie danych osobowych. W artykule zidentyfikowano trzy odrębne obowiązki ujawnieniowe wynikające z interakcji między RODO, unijnym Aktem w sprawie

sztucznej inteligencji (AI Act) oraz przepisami polskiego Kodeksu postępowania administracyjnego. Wykazano, że klauzule informacyjne sporządzane na podstawie art. 13 RODO pełnią autonomiczną i niezastępowalną funkcję *ex ante*, której nie mogą zastąpić późniejsze mechanizmy transparentności o charakterze proceduralnym.

Introduction

A personal data processing notice is a document or notification provided to a person whose personal data are being processed by a controller. The provision of such notices is mandated by the EU's General Data Protection Regulation (GDPR). The GDPR imposes an information obligation to provide the data subject with specified information concerning the processing of their data. This obligation, implemented through the provision of a data processing notice containing information relevant to the collection of personal data and their subsequent processing, constitutes one of the principal safeguards of an individual's informational self-determination and serves to enable the effective exercise of the rights conferred on the data subject in relation to the processing of personal data. Personal data processing notices are expected to be clear to understand for the recipient.

The drive for the integration of artificial intelligence (AI) systems into public administration in Poland has been gaining momentum, with official support from Polish public bodies. As stated in the Policy for the Development of Artificial Intelligence in Poland since 2020¹, AI and the public sector is one of the six main areas of interest. Actions are aimed at supporting the public sector in carrying out AI-related procurements, coordination enhancement, and the further development of programs such as GovTech Poland.

The Policy explicitly states:

AI-based solutions can improve the efficiency of central government and local government bodies. The constantly improving technical capabilities makes process automation a more and more attractive avenue pursued by public administration. Thanks to advances in artificial intelligence, processes that had to be done by numerous clerks just a couple of years ago can be partially automated these days.

An example of how Poland is advancing AI in public administration is the recent launching of models like PLLuM (Polish Large Language Model)² for automating tasks, citizen communication, and reducing bureaucracy. The first pilot

¹ Policy for the Development of Artificial Intelligence in Poland from 2020, Appendix to the Resolution No. 196 of the Council of Ministers of 28 December 2020 (item 23), available at: <https://www.gov.pl/attachment/928200fa-b1a6-4c0c-b3a8-d1fbf1e1175a> [accessed on: 09.02.2026].

² Ministerstwo Cyfryzacji, PLLuM — polski model językowy, jak działa i do czego może się przydać, available at: <https://www.gov.pl/web/cyfryzacja/pllum-polski-model-jezykowy-jak-dziala-i-do-czego-moze-sie-przydac> [accessed on: 09.02.2026].

project was carried out in the city of Częstochowa³, in southern Poland. Developed by Polish research institutions, working on behalf of the Ministry of Digital Affairs, it is capable of understanding Polish grammar, socio-cultural context, and official administrative language.

HIVE AI is a direct continuation of the *Polish Large Language Model (PLLuM)* project⁴. The PLLuM was a government-backed AI project started in 2023 with an aim to produce a language model that could more effectively process and produce texts in the Polish language. The follow-on initiative, HIVE AI aims to facilitate the integration of Polish language models into the mObywatel app (Poland's official digital ID and documentation phone app), develop a clerical assistant for the Polish Ministry of Digital Affairs, and conduct a pilot implementation of LLMs in a municipal or provincial office⁵.

Poland facilitates public access to government services through a project known as eGovernment, the HIVE AI project strongly aligns with its goals. An implement consulting group study commissioned by Google in partnership with SGH Warsaw School of Economics found that: "Generative AI has significant potential to enhance productivity in public administration, creating 7% more value in money, equivalent to an annual contribution of PLN 8 billion"⁶.

However, the rapid integration of artificial intelligence systems into public administration in Poland (as well as across the European Union) also represents a challenge to established data protection principles and to public bodies who must still comply with the GDPR.

This challenge is further strenuous in Poland by the absence of detailed supervisory authority guidance comparable to that available in some other EU Member States. While France's CNIL (the French national data protection enforcement agency) has published comprehensive, AI-specific guidance on processing notice content, Poland's President of the Personal Data Protection Office (PUODO) has

³ Ministerstwo Cyfryzacji, Polski model językowy PLLuM trafi do samorządów, available at: <https://www.gov.pl/web/cyfryzacja/polski-model-jezykowy-pllum-trafi-do-samorzadu> [accessed on: 09.02.2026].

⁴ National Information Processing Institute — National Research Institute (OPI PIB), HIVE AI: Development and pilot implementation of large language models in Polish public administration, available at: <https://opi.org.pl/en/project/hive-ai-rozwoj-i-pilotazowe-wdrozenie-duzych-modeli-jezykowych-w-polskiej-administracji-publicznej/> [accessed on: 09.02.2026].

⁵ NASK, *About HIVE AI Project*, available at: <https://www.nask.pl/en/institute-for-institutions/hive-ai/about-project> [accessed on: 09.02.2026].

⁶ Implement Consulting Group, *The AI opportunity for eGovernment in Poland* (2025), commissioned by Google in partnership with SGH Warsaw School of Economics, available at: <https://cms.implementconsultinggroup.com/media/uploads/articles/2025/The-AI-opportunity-for-eGovernment-in-Poland/2025-The-AI-opportunity-for-eGovernment-in-Poland-English.pdf> [accessed on: 09.02.2026].

not yet delivered equivalent resources, leaving public bodies deploying systems like PLLuM and HIVE AI without clear implementation standards.

It is obvious that the GDPR was designed for and adopted in an extensively different technological reality than today's world, in which there is an ever-increasing reliance on language models. It provides that the protection of natural persons in relation to the processing of personal data is a fundamental right, one that should not be diminished by the omnipresence of AI.

Any information referred to in Articles 13 and 14 of the GDPR and any communication under Articles 15 to 22 and 34 of the GDPR relating to personal data processing must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Public bodies using AI systems are therefore challenged with the task of providing a notice that contains "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing" (GDPR Article 13(2)(f)) about systems that are not fully understood even by their creators⁷.

Public bodies are also faced with dealing with a population with varying levels of digital literacy⁸, and the need to comply not only with GDPR but also the AI Act⁹ and Poland's Administrative Procedure Code (*Kodeks postępowania administracyjnego*), which imposes its own transparency and justification requirements.

In this context, the article provides an analysis that examines whether processing notices used by public administration are subject to change with a further emergence and use of AI.

The article further addresses the following interconnected questions:

- What specific content must processing notices contain when AI systems are used by Polish public administration?
- Why do modern AI systems create particular difficulties for meeting content requirements put in by the GDPR?
- What practical frameworks or solutions can enable Polish public bodies to achieve compliance?

This article is based on doctrinal legal analysis, technical assessment, and policy evaluation. The analysis was performed in the followings stages: textual interpreta-

⁷ T. Constantino, "AI's Biggest Secret — Creators Don't Understand It", *Forbes*, 8 May 2025, available at: <https://www.forbes.com/sites/torconstantino/2025/05/08/ais-biggest-secret---creators-dont-understand-it-experts-split/> [accessed on: 09.02.2026].

⁸ 44% of citizens hold at least basic digital skills. European Commission, Digital Skills & Jobs Platform, *Poland digital skills map*, available at: <https://digital-skills-jobs.europa.eu/en/european-interactive-map/poland> [accessed on: 09.02.2026].

⁹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), OJ L 2024/1689, 12.7.2024, entered into force 1 August 2024.

tion of the GDPR and AI Act provisions, Court of Justice of the European Union (CJEU) case law, European Data Protection Board guidelines, and the Polish Personal Data Protection Office guidance documents.

The analysis concentrates on public administration in Poland. The paper does not address private sector applications of AI, except where they provide comparative insights. The legal analysis within focuses on data protection, AI regulation, and administrative procedure; it does not extensively address related areas such as substantive administrative law.

This paper specifically addresses the content requirements of processing notices under GDPR Articles 13 and 14 as they apply to AI systems, with particular emphasis on the enhanced obligations for automated decision-making and profiling under Article 13(2)(f).

The research also incorporates a comparative analysis of transparency approaches in the EU and examination of enforcement actions by data protection authorities to understand how content requirements are interpreted in practice.

1. Legal Framework for Processing Notice Content

The GDPR establishes transparency as a fundamental principle of data protection. Article 5(1)(a) requires that personal data be “processed lawfully, fairly and in a transparent manner in relation to the data subject”. This principle is not merely aspirational; it creates enforceable obligations implemented through specific requirements in Articles 12–14.

The transparency principle serves multiple functions: it enables data subjects to understand and verify the lawfulness of processing. Article 12(1) GDPR establishes how transparency obligations must be fulfilled, requiring that information be provided in a manner that is “concise, transparent, intelligible and easily accessible”. The information must use “clear and plain language”, which rules out purely technical descriptions accessible only to specialists, and must be provided “in writing, or by other means, including, where appropriate, by electronic means”.

Article 12(1) does not specify a maximum length for processing notices, recognizing that the amount of information needed depends on the complexity of the processing. However, the requirement for conciseness means controllers cannot simply provide exhaustive technical documentation and claim compliance. The Article 29 Working Party (now the European Data Protection Board) has endorsed a “layered approach” where brief, essential information is provided at the point of

data collection, with more detailed information available through links or separate documents¹⁰.

Articles 13 and 14 specify what information must be provided to data subjects, with Article 13 applying when data is collected directly from the individual and Article 14 applying when data is obtained from other sources. Both articles require disclosure of: the identity and contact details of the controller; the contact details of the data protection officer (where applicable); the purposes of processing; the legal basis for processing; the categories of personal data concerned (Article 14 only); the recipients or categories of recipients; information about international transfers if applicable; the retention period or criteria for determining it; the existence of data subject rights; the right to lodge a complaint with the supervisory authority; and where data provision is a statutory or contractual requirement, whether the individual is obliged to provide it and the consequences of failing to do so.

2. Understanding the Phrase “At Least in Those Cases”

Article 13(2)(f) requires controllers to provide data subjects with information about:

the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, **at least in those cases**, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject”.

Article 14(2)(g) contains identical language for situations where data is not obtained directly from the data subject.

In the GDPR, the phrase **at least in those cases** appears primarily in the context of transparency requirements regarding automated decision-making and profiling (Articles 13, 14, and 15) and has been subject to debate.

A narrow reading would limit the enhanced disclosure obligation to situations covered by Article 22, that is solely automated decisions that produce legal effects or similarly significantly affect the data subject.

A broader reading would extend it to all automated decision-making and profiling, regardless of whether Article 22 applies.

The Article 29 Working Party adopted the broad interpretation in its Guidelines on Automated Individual Decision-Making and Profiling, stating that: “informa-

¹⁰ “In the digital context, in light of the volume of information which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency. WP29 recommends in particular that layered privacy statements/ notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen, in order to avoid information fatigue”. Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, WP260 rev.01, adopted 29 November 2017, last revised 11 April 2018, p. 19.

tion must be provided whenever there is automated decision-making (including profiling)¹¹, not only when Article 22 applies.

The CJEU's February 2025 ruling in Case C-203/22¹² also provides support for the broad interpretation. While the case concerned Article 22 rights specifically, the Court emphasized that the GDPR's transparency requirements exist to enable data subjects to "exercise their rights effectively"¹³.

For Polish public administration, this means processing notices must contain the enhanced information whenever AI systems are used in decision-making, even if human oversight means Article 22 does not technically apply.

3. Specific Challenges for AI Systems

Article 13(2)(f) provides for the disclosure of the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The phrase "meaningful information" is a significant challenge for AI systems. The term in question is not used anywhere else in the GDPR. Recital 71 GDPR also provides only minimal guidelines that the right to information should not "adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software". However, Recital 71 also emphasizes that this limitation should not "result in the data subject being refused all information".

The phrase "at least in those cases, meaningful information about the logic involved", referring to "automated decision-making, including profiling", may, on the one hand, support the view that the information obligation encompasses both the "meaningful principles" of automated decision-making based on profiling and the "meaningful principles" of profiling itself, even where it does not lead to automated decision-making.

¹¹ Article 12, recital 58, Articles 13 and 14, and Article 22(1) of the GDPR. In this regard, please also see the European Data Protection Board, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251 rev.01, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 [accessed on: 09.02.2026], p. 17.

¹² Court of Justice of the European Union, judgment of 27 February 2025, Case C-203/22, EU:C:2025:117, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0203> [accessed: on 09.02.2026].

¹³ "In particular, in the specific context of the adoption of a decision based solely on automated processing, the main purpose of the data subject's right to obtain the information provided for in Article 15(1)(h) of the GDPR is to enable him or her effectively to exercise the rights conferred on him or her by Article 22(3) of that regulation, namely the right to express his or her point of view on that decision and to contest it", *Ibid.*, 45–50 (right to explanation under Art. 15(1)(h) GDPR).

On the other hand, Recital 73 GDPR provides that Union or Member State law may introduce restrictions on certain rights and obligations, including those relating to decisions based on profiling, where this is necessary and proportionate in a democratic society to safeguard public security, including the protection of human life, especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In this respect, the EU legislator refers not to profiling as such, but to decisions based on profiling.

Accordingly, it should be concluded that the object of protection envisaged by the EU legislator in the GDPR is not profiling per se but profiling that results in a decision-making process. Otherwise, profiling constitutes merely one method of processing personal data. A similar conclusion follows from Recital 24 of the GDPR, which addresses profiling while again emphasizing that it concerns profiling “in order to take decisions concerning the data subject or for analyzing or predicting personal preferences, behaviors and attitudes.” Importantly, the information provided on this basis should include the specific procedures and rules applied to the automated use of personal data relating to the individual concerned in order to produce a particular outcome (as held by the Court of Justice of the European Union in its judgment of 27 February 2025, C-203/22, EU:C:2025:117), rather than generic descriptions¹⁴. The Court in Case C-203/22 stated:

Those requirements cannot be satisfied either by the mere communication of a complex mathematical formula, such as an algorithm, or by the detailed description of all the steps in automated decision-making, since none of those would constitute a sufficiently concise and intelligible explanation.

Currently, the notion of the “meaningful principles” of automated decision-making based on profiling and of profiling itself is interpreted in light of the purpose of the information obligation. That purpose is to ensure transparency with regard to all circumstances surrounding profiling (see X. Konarski)¹⁵. From this perspective, informing the data subject about the specific computer program used for profiling

¹⁴ “Thus, the ‘meaningful information about the logic involved’ in automated decision-making, within the meaning of Article 15(1)(h) of the GDPR, must describe the procedure and principles actually applied in such a way that the data subject can understand which of his or her personal data have been used in what way in the automated decision-making at issue, with the complexity of the operations to be carried out in the context of automated decision-making not being capable of relieving the controller of the duty to provide an explanation” *Ibid.*, para. 62 (specific procedures, not algorithms).

¹⁵ P. Barta, M. Kawecki, P. Litwiński [in:] P. Litwiński (ed.), *Ustawa o ochronie danych osobowych. Komentarz* [in:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, edn. 2, Warszawa 2025, art. 13, Legalis.

does not appear to be of material relevance. Rather, the information should be structured so as to explain how profiling operates and to indicate its consequences for the data subject, thereby enabling the individual to challenge an automated decision (see W. Chomiczewski)¹⁶.

These traditional views made considerable sense for conventional profiling systems. If a controller uses a standard database query or statistical regression implemented in common software, the choice of software is largely irrelevant—the same logic could be implemented in different programs with identical results. An insured person who knows that their retirement benefit is calculated according to a statutory formula does not gain meaningful additional information from knowing whether the calculation is performed in Excel, within the pension office's internal system, or in any other software.

However, AI systems challenge this distinction between program and logic. For AI systems, the specific program often is the logic in a way that was not true for traditional profiling. The difference in explainability is inherent to the model architecture; it is not just about implementation details.

For traditional profiling using explicit rules (“if income < threshold AND age > 65, then...”), the logic is transparent regardless of the software implementing it. For AI systems that learn from data, the specific model embeds assumptions and patterns from its training data that may not be visible from general descriptions¹⁷. Differences are embedded in specific programs and fundamentally affect their behavior¹⁸. A data subject cannot meaningfully challenge a decision without understanding which model was used and how it was trained.

The EU AI Act creates a regulatory framework where the specific AI system's classification determines legal obligations:

- High-risk systems have extensive requirements (conformity assessment, registration, human oversight);
- Non-high-risk (minimal) systems have minimal requirements;
- General-purpose AI systems have different obligations.

A data subject cannot verify whether appropriate safeguards apply without knowing which specific AI system was used. If a public body claims to use a high-risk system subject to rigorous oversight, but actually uses a simpler non-regulated tool, this is material information that affects rights and remedies.

¹⁶ *Ibid.*

¹⁷ J. Burrell “How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms” (September 15, 2015). Available at: SSRN: <https://ssrn.com/abstract=2660674> or <http://dx.doi.org/10.2139/ssrn.2660674>, DOI: 10.1177/2053951715622512 [accessed on: 09.02.2026].

¹⁸ M.H. Jarrahi, V. Glaser, “Not All AI Systems Are Created Equal: A Typology of AI Systems’ Performance and Affordance”, *Proceedings of HICSS 2025*, DOI: 10.24251/HICSS.2025.655.

The EU AI Act, which entered into force on August 1, 2024, creates a risk-based regulatory framework for AI systems. Annex III of the Act lists “high-risk AI systems”, many of which are commonly deployed in public administration. These include AI systems used for: evaluating eligibility for public assistance benefits and services; assessing the creditworthiness of natural persons or establishing their credit score (when used by public authorities); dispatching or establishing priority in emergency services; evaluating students’ performance in educational institutions; and making decisions in relation to migration, asylum, and border control management.

The classification of an AI system as “high-risk” triggers extensive regulatory obligations, including transparency requirements that affect processing notice content. Importantly, the AI Act’s definition of “deployer” (Article 3(4)) encompasses public authorities that use AI systems for administrative purposes even when they did not develop the system themselves. This means Polish public bodies using commercial or centrally developed AI systems are “deployers” that are subject to AI Act obligations.

Article 13 of the AI Act requires providers of high-risk AI systems to provide deployers with instructions for use that include: the identity and contact details of the provider; the characteristics, capabilities, and limitations of the AI system’s performance; the level of accuracy, robustness, and cybersecurity of the system; known or foreseeable circumstances in which the system may not perform as intended; specifications for input data quality and formatting; the expected lifetime of the system and necessary maintenance; and descriptions of the human oversight measures built into the system.

For processing notice content, this creates an indirect but important obligation. Public bodies – as deployers cannot provide meaningful information about the logic involved in automated processing if they lack detailed information about how the AI system functions.

Article 13 of the AI Act ensures that deployers receive this information from providers, which they can then include in appropriate disclosure for data subjects. However, the information providers supply to deployers is typically technical and detailed, precisely the kind of information that C-203/22 ruled cannot simply be passed on to data subjects. Deployers must therefore engage in a translation exercise, converting provider documentation into explanations accessible to ordinary citizens.

Poland’s Administrative Procedure Code (KPA) further creates transparency and justification requirements that, while related to GDPR processing notice obligations, serve fundamentally different functions – a distinction that becomes more significant when AI systems are deployed.

The processing notice under GDPR Art. 13 operates independently of and prior to administrative proceedings. Its primary function is not procedural transparency (enabling participation in a specific case) but enabling data subjects to understand how their personal data will be processed and to exercise their data protection rights before processing begins or while it is ongoing¹⁹. This distinction was preserved when Poland adapted the KPA to GDPR. Art. 2a KPA, which addresses the procedural modalities of providing GDPR Art. 13 information within administrative contexts—when, how, and in what form the notice must be given—but does not alter the substantive content requirements of Art. 13, which derive directly from the GDPR itself²⁰.

Polish legal commentary recognizes that the information obligation under Art. 2a KPA is distinct from regulated procedural obligations because it protects a different interest: personal data rights rather than procedural participation rights²¹. The notice serves data subjects regardless of whether they become parties to administrative proceedings, and it must be provided at the point of data collection, not merely when a decision is rendered.

For AI systems, this temporal and functional separation has critical implications. A processing notice may be the primary—or only—mechanism through which data subjects learn that AI is being used and how it functions:

- Not all data subjects become parties to proceedings. A person whose data is processed for profiling or risk assessment may never receive an individual administrative decision triggering KPA Art. 107 justification requirements. Art. 13 GDPR information is supposed to enable [data subjects] to make informed decisions about the processing of their data, making the processing notice the primary transparency mechanism for those who never enter formal proceedings;
- The notice enables ex ante exercise of rights that cannot be exercised ex post. Data subjects who understand from the processing notice that AI profiling will occur can exercise rights such as objection (GDPR Art. 21) (in the case of a public authority, this may only concern processing based on Article 6(1)(e) GDPR)²² before the AI processes their data. Once a decision is made, these preventive rights are moot; only reactive rights (appeal, complaint) remain;

¹⁹ B. Adamiak [in:] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, edn. 19, Warszawa 2024, art. 2a, Legalis.

²⁰ *Ibid.*

²¹ P. Litwiński [in:] P. Litwiński (ed.), *Kodeks postępowania administracyjnego. Komentarz* [in:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, edn. 2, Warszawa 2025, art. 2a, Legalis.

²² P. Gołaszewski, K. Wąsowski [in:] R. Hauser, M. Wierzbowski (eds.), *Kodeks postępowania administracyjnego. Komentarz*, edn. 8, Warszawa 2023, art. 2a, Legalis.

- The notice reaches broader audiences than individual justifications. A processing notice published on an agency website or provided at first contact informs all potential data subjects about AI use. Individual decision justifications under KPA Art. 107 inform only those who receive adverse decisions—a much narrower group. The notice thus serves a systemic transparency function distinct from case-specific justification;
- The notice must explain AI logic while it remains abstract. At the point of data collection (when Art. 13 applies), the public body must explain how the AI system functions in general, not merely how it processed a specific person's data. This is actually more demanding than *ex post* justification because it requires explaining the system's methodology without reference to concrete facts.

The KPA's procedural transparency requirements (Arts. 10, 107) complement but do not substitute for processing notices. Article 10's right to express views on evidence presupposes that the party already knows. Article 107's justification is to explain how the AI analyzed the specific party's data but cannot inform those never subject to individual decisions. The processing notice thus occupies a distinct and irreplaceable position in the transparency framework.

This functional independence becomes even more significant when considering the additional requirements resulting from the AI Act.

Article 13 of the AI Act requires providers to furnish deployers (which public bodies would be considered to be) with detailed documentation about high-risk AI systems. Article 86 of the AI Act grants data subjects a right to obtain explanations of individual decisions.

These requirements create three temporally and functionally distinct disclosure moments:

1. *Ex ante* general disclosure (GDPR Art. 13 processing notice): Before/at data collection, explaining the AI system in abstract;
2. During-proceeding disclosure (KPA Art. 10): During the administrative process, enabling party participation;
3. *Ex post* individual disclosure (KPA Art. 107 + AI Act Art. 86): After decision, explaining how AI processed specific data.

Each serves a distinct purpose; none can substitute for the others. The processing notice's role is therefore not diminished but rather elevated in the context of AI: it becomes the foundational disclosure upon which subsequent procedural transparency depends.

The intersection creates potentially reinforcing obligations: GDPR Art. 13(2)(f) requires *ex ante* disclosure of AI logic in processing notices, while KPA Art. 107 requires *ex post* justification of how AI contributed to the specific decision, and

Art. 10 may require interim disclosure enabling party participation. Together, these create a higher transparency standard than either regime alone would impose.

The challenge of explaining “the logic involved” is compounded when AI systems are trained on large, diverse datasets. Data protection authorities have begun providing practical guidance on how controllers can satisfy Article 13(2)(f) disclosure requirements without overwhelming data subjects with unusable detail.

The French data protection authority *Commission Nationale de l’Informatique et des Libertés* (CNIL) has issued specific guidance addressing this challenge in the context of AI systems. The CNIL recognizes that different levels of specificity are appropriate depending on the nature and scale of data sources²³:

This guidance is directly relevant to Polish public bodies deploying AI systems like PLLuM or HIVE AI. These large language models are trained on an extensive sample of Polish-language that may include personal data from diverse online sources.

The CNIL has issued specific guidance addressing how to inform data subjects about AI training data sources²⁴. The CNIL distinguishes between two scenarios:

Individual information (when controllers can identify and contact data subjects): Controllers must provide all Article 13/14 GDPR information, including identity and contact details, purpose and legal basis, recipients, retention period, and data subject rights. For indirect collection, controllers must additionally specify categories of personal data and “a precise indication of the source(s) of the data (including whether or not they are publicly available sources)”²⁵.

General information notice (when individual contact is impossible or disproportionate): Controllers must publish an information notice (*e.g.*, on a website) that includes as much information as would be provided individually, plus a statement that the controller cannot identify individuals to respond to right requests.²⁶

Within these frameworks, different levels of specificity apply based on data sources:

- **Limited sources:** Precise information required, including dataset names and hyperlinks. Example: “This training data comes from a publicly accessible dataset (hyperlink) containing 70,000 images...published on [social network] between 2020 and 2021²⁷”;

²³ CNIL (*Commission nationale de l’informatique et des libertés*), *AI system development: CNIL’s recommendations to comply with the GDPR*, 5 January 2026, available at: <https://www.cnil.fr/en/ai-system-development-cnils-recommendations-to-comply-gdpr> [accessed on: 09.02.2026].

²⁴ CNIL, *Informing data subjects*, available at: <https://www.cnil.fr/en/informing-data-subjects> [accessed on: 09.02.2026].

²⁵ *Ibid.*

²⁶ *Ibid.*

²⁷ *Ibid.*

- **Numerous sources:** “Overall information, such as source categories, or even the names of a few main or typical sources, is generally sufficient” Example: “The data was collected by scraping websites specialized in the field studied...”²⁸;
- **General-purpose AI models:** Article 53 AI Act requires “a sufficiently detailed summary” listing main datasets and explaining other data sources used²⁹.

The CNIL guidance thus operationalizes the principle established in C-203/22: explanations must enable data subjects to “understand the envisaged method and the main characteristics of the processing”¹ without requiring disclosure of every technical detail.

For AI training data, this means explaining *what kinds* of data sources were used, *what types* of personal data they contained, and *how* data subjects can learn more or exercise their rights—not exhaustively cataloguing every data point.

Conclusion

This paper has examined the content requirements for personal data processing notices when AI systems are deployed in Polish public administration, analyzing the intersection of GDPR transparency obligations, AI Act requirements, and Polish legal frameworks.

First, the existing legal framework creates extensive and specific content obligations. GDPR Articles 13 and 14 require baseline disclosures applicable to all processing, while Article 13(2)(f) mandates enhanced content when automated decision-making or profiling occurs: meaningful information about the logic involved, the significance of the processing, and the envisaged consequences. The EU AI Act adds further obligations, particularly Article 86’s right to explanation of individual decisions and Article 13’s requirement that providers furnish deployers with detailed system information. Polish law, including the Administrative Procedure Code, creates additional transparency expectations rooted in administrative law principles.

Second, modern AI systems create genuine technical challenges for meeting these content requirements. While simple, interpretable models can be explained straightforwardly, many AI systems that deliver superior accuracy rely on complex architectures that resist transparent explanation. The accuracy-interpretability trade-off means that choosing models that are easy to explain may sacrifice performance, potentially providing inferior service to citizens. This creates a fundamental tension: the law requires explanation of “the logic involved” but for some AI sys-

²⁸ *Ibid.*

²⁹ *Ibid.*

tems, the true logic cannot be explained in terms comprehensible to non-specialists without oversimplification that borders on misrepresentation.

Third, Polish public administration faces distinctive implementation challenges. These include resource constraints that limit investment in sophisticated AI systems with built-in interpretability; legacy IT infrastructure that may not integrate well with modern transparency tools; diverse populations with varying levels of digital literacy, requiring multiple explanation formats and languages; and coordination challenges among multiple supervisory authorities (PUODO for data protection, the proposed AI Commission, and sectoral regulators). The intersection of GDPR, AI Act, and KPA requirements creates particular complexity: processing notices must satisfy data protection law while also fulfilling administrative law expectations for justification and transparency.

PUODO should develop detailed guidance specifically addressing processing notice content for AI systems. This guidance should include: concrete examples of adequate and inadequate disclosures for common AI use cases in public administration; templates that public bodies can adapt to their specific circumstances; clear articulation of when simplified explanations are acceptable and when more detailed technical information must be provided; guidance on the layered transparency approach, including what must be in each layer; and clarification of how PUODO will assess compliance given the technical limitations of certain AI systems.

Public bodies need training in both data protection law and AI technology, enabling data protection officers and technical staff to collaborate effectively in drafting processing notices that are legally compliant and technically accurate.

The deployment of PLLuM and HIVE AI demonstrates commitment to AI-enabled public administration. Equally, detailed commitment to transparency is now required. Processing notices that adequately explain these systems—their training data sources, processing logic, and envisaged consequences—will determine whether Poland's AI transformation enhances or undermines citizens' trust in public institutions.

Empirical examination of processing notices issued by Polish public bodies deploying AI systems represents a promising avenue for future research. Such analysis could assess whether notices provide meaningful information about AI logic, how technical complexity is translated for ordinary citizens, and whether layered transparency approaches are effectively implemented. Comparative analysis across different public bodies and AI system types would reveal emerging best practices and common compliance challenges.

References

EU Legislation and Official Documents

- Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, WP260 rev.01, adopted 29 November 2017, last revised 11 April 2018
- European Data Protection Board, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251 rev.01.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), OJ L 2024/1689, 12.7.2024.

Polish Legislation and Official Documents

- Act of 14 June 1960 – Code of Administrative Procedure (KPA), consolidated text, Journal of Laws 2024, item 572.
- Policy for the Development of Artificial Intelligence in Poland from 2020, Appendix to the Resolution No. 196 of the Council of Ministers of 28 December 2020 (item 23), available at: <https://www.gov.pl/attachment/928200fa-b1a6-4c0c-b3a8-d1fbf1e1175a> [accessed on: 09.02.2026].

Polish and European Government and Institutional Sources

- Ministerstwo Cyfryzacji, *PLLuM — polski model językowy, jak działa i do czego może się przydać*, available at: <https://www.gov.pl/web/cyfryzacja/pllum-polski-model-jezykowy-jak-dziala-i-do-czego-moze-sie-przydac> [accessed on 09.02.2026].
- Ministerstwo Cyfryzacji, *Polski model językowy PLLuM trafi do samorządów* (pilot w Częstochowie), available at: <https://www.gov.pl/web/cyfryzacja/polski-model-jezykowy-pllum-trafi-do-samorzadu> [accessed: 9 February 2026].
- National Information Processing Institute - National Research Institute (OPI PIB), *HIVE AI: Development and pilot implementation of large language models in Polish public administration*, available at: <https://opi.org.pl/en/project/hive-ai-rozwoj-i-pilotazowe-wdrozenie-duzych-modeli-jezykowych-w-polskiej-administracji-publicznej/> [accessed on: 09.02.2026].
- NASK, *About HIVE AI Project*, available at: <https://www.nask.pl/en/institute-for-institutions/hive-ai/about-project> [accessed on: 09.02.2026].
- Implement Consulting Group, *The AI opportunity for eGovernment in Poland* (2025), commissioned by Google in partnership with SGH Warsaw School of Economics, available at: <https://cms.implementconsultinggroup.com/media/uploads/articles/2025/The-AI-opportunity-for-eGovernment-in-Poland/2025-The-AI-opportunity-for-eGovernment-in-Poland-English.pdf> [accessed on: 09.02.2026].
- European Commission, Digital Skills & Jobs Platform, *Poland digital skills map*, available at: <https://digital-skills-jobs.europa.eu/en/european-interactive-map/poland> [accessed on: 09.02.2026].

Case Law

- Court of Justice of the European Union, judgment of 27 February 2025, Case C-203/22, EU:C:2025:117, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0203> [accessed on: 09.02.2026].

Literature

- Adamiak B., [in:] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, edn. 19, Warszawa 2024, art. 2a, Legalis.
- Barta P., Kawecki M., Litwiński P., [in:] P. Litwiński (ed.), *Ustawa o ochronie danych osobowych. Komentarz* [in:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, edn. 2, Warszawa 2025, art. 13, Legalis.
- Burrell J., “How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms” (September 15, 2015). Available at SSRN: <https://ssrn.com/abstract=2660674> or <http://dx.doi.org/10.2139/ssrn.2660674>, DOI: 10.1177/2053951715622512, [accessed on: 09.02.2026].
- Constantino T., “AI’s Biggest Secret — Creators Don’t Understand It”, *Forbes*, 8 May 2025, available at: <https://www.forbes.com/sites/torconstantino/2025/05/08/ais-biggest-secret-creators-dont-understand-it-experts-split/> [accessed on: 09.02.2026].
- Gołaszewski P., Wąsowski K., [in:] R. Hauser, M. Wierzbowski (eds.), *Kodeks postępowania administracyjnego. Komentarz*, edn. 8, Warszawa 2023, art. 2a, Legalis.
- Jarrah, M.H., Glaser V., “Not All AI Systems Are Created Equal: A Typology of AI Systems’ Performance and Affordance”, *Proceedings of HICSS 2025*, DOI: 10.24251/HICSS.2025.655.
- Litwiński, P., [in:] P. Litwiński (ed.), *Kodeks postępowania administracyjnego. Komentarz* [in:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, edn. 2, Warszawa 2025, art. 2a, Legalis.

Regulatory Guidance

- Commission nationale de l’informatique et des libertés, AI system development: CNIL’s recommendations to comply with the GDPR*, 5 January 2026, available at: <https://www.cnil.fr/en/ai-system-development-cnils-recommendations-to-comply-gdpr> [accessed on: 09.02.2026].
- Commission nationale de l’informatique et des libertés, Informing data subjects*, available at: <https://www.cnil.fr/en/informing-data-subjects> [accessed on: 9 09.02.2026].