# AI Transparency for PII Principal

Privacy risks to PII principal increase when generative AI is used due to its capability to automatically process information in relation to the LLM. As a result, generative AI it is able to profile PII automatically, at scale, providing comprehensive profiling and surveillance capacities, in accordance with the data sources, which include sources of data not available in the physical context.

Transparency for PII principal must signal if the authoritative source of LLM data and its providences. If it is bound to the physical context and purpose of use, the PII principal, then the AI application, has a dramatically reduces risk. If source of the LLM data, and associated PII is not bound to purpose of use and the PII principals physical scope of disclosure, this risk is mitigated with proportionate and reciprocal for PII principal transparency to be effective.

Transparency of generative AI application for PII Principal not only requires complying with current compulsory security and privacy notice obligations for the collection and processing of PIl, generative AI introduces new transparency modalities, which are required,

* 1. traceability,
  2. explainability,
  3. interpretability,[[1]](#footnote-1)

The use of standard record format, for notice of ai, in addition to commonly used ‘AI model cards’ and ‘AI Datasheet, specified in conjunction with ISO/IEC 27560 consent record information structure and standard data privacy vocabulary, proportionately reduce the cognitive transparency risks of using AI for PII principals.

Notice, notification, or disclosure obligations should be provided prior to processing PII o mitigate, security and privacy risks in the use of AI by the PII principal, a record of this notice, and a receipt provided for the data input should be consider best practice to achieve these new requirements.

It must be clear to the PII principal, that PII Controllers, are accountable for the use of AI applications and should not rely on a privacy policy for transparency, as this is not proportionate, be clear about scope of disclosure and evidence a record of consent for a secondary purpose of use.

Security and privacy risks can be systematically addressed with a notice record, generated when AI transparency notice was presented. Liability of generative AI risks can be further mitigated by transferring some of the liability for the AI application by providing the PII principal with a notice and consent receipt. Providing the ability for the PII principal to exercise right and manage risk autonomously, decentralising data governance, through standard records for traceability, AI assisted explainability, and interpretability, in accordance with the purpose of PII processing, and its context of use, which naturally regulate data governance..

1. Lorenz, P., K. Perset and J. Berryhill (2023), “Initial policy considerations for generative artificial intelligence”, in OECD Artificial Intelligence Papers, OECD Publishing, Paris,<https://www.oecd-ilibrary.org/science-and-technology/initial-policy-considerations-for-> generative-artificial-intelligence\_fae2d1e6-en (accessed on 5 June 2024). [↑](#footnote-ref-1)