IAPP **AI Governance Global Europe 2026**

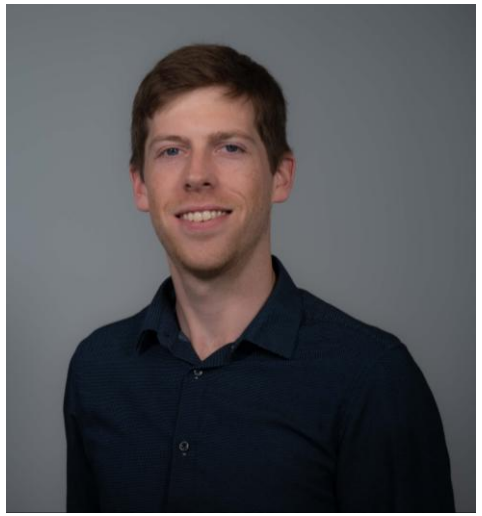
Training 1-2 June
Workshop 2 June
Conference 3-4 June
DUBLIN

#IAPPAIGG26

Pseudonymity and AI: The New Frontier of Responsible Data

Bridging the gap between strict privacy laws and the ambition of AI development.

WELCOME AND INTRODUCTIONS



Graham Doyle

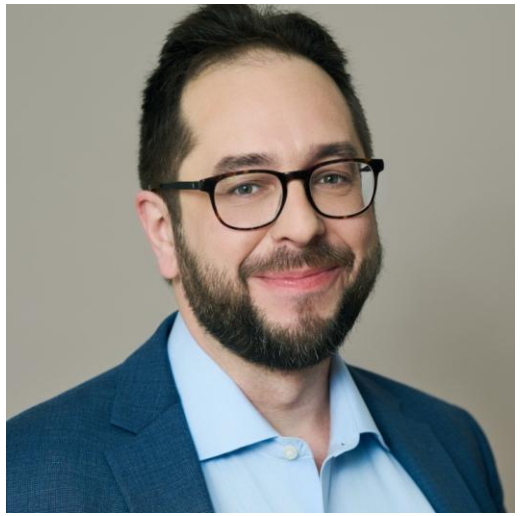
Assistant Commissioner

Irish Data Protection Commission

Monisha Varadan

Senior Privacy Engineer, DPO Office

Google



Claude-Etienne Armingaud, CIPP/E

Partner - Technology & Intellectual Property

Latournerie Wolfrom & Associés

Jiri Balek, AIGP, CIPP/E, CIPM, FIP

Data Privacy and Ethics Manager

Celonis

AGENDA OUTLINE

I. Session Outline
II. Welcome and Introductions
III. Summary: The Legislative Pivot
IV. The Relative-Anonymity Angle 1/2
V. The Relative-Anonymity Angle 2/2
VI. Friction & Real-World Cases
VII. Managing the Data Lifecycle
VIII. The Personalization Dilemma
IX. 2026 Strategy: The "Reasonably Likely" Bar

Summary: The Legislative Pivot

Regulatory Reversal: EU Council has deleted the proposed "Relative" definition of personal data from the Digital Omnibus.

Technical Imperative: In the absence of legal relief, should Privacy Enhancing Technologies (PETs) be now a strong compliance solution?

AI Model Risk: Pseudonymization without advanced safeguards remains risk under absolute identifiability standards.

The Relative-Anonymity Angle 1/2

GDPR BASELINE DEFINITIONS

- **Pseudonymised Data (Art. 4(5)):** Data that cannot be attributed to a specific person without auxiliary information.

  > **The Catch:** The "master key" must be kept separate under strict technical safeguards. It remains fully regulated as personal data.

- **Anonymised Data (Recital 26):** Data permanently and irreversibly unidentifiable by any reasonably likely means.

  > **The Benefit:** GDPR stops applying entirely; data is unlocked for scaling.

The Relative-Anonymity Angle 2/2

ABSOLUTE VS. RELATIVE SHIFT (EDPS V. SRB)

- **The Core Shift:** Absolute theory argued if *anyone* held the key, it was personal for *everyone*. The relative paradigm judges status purely by recipient perspective.
- **C-413/23 P Rule:** Pseudonymised data transferred to a recipient is legal "anonymous" data if they lack realistic, lawful means to reverse-engineer identity.

- **Red Lines (Anonymity Fails):** If the recipient has legal powers to request the key, discloses pseudonyms to keyholders, or passes records to a third party who can match identities.

Friction & Real-World Cases

THE LEGISLATIVE TUG-OF-WAR

EU Digital Omnibus: Proposed to formally write the "relative approach" into the statutory definition of personal data to unlock AI model training opportunities.

Regulatory Pushback: EDPB and EDPS heavily fought back, stripping the definition and warning that tracking longitudinal records without names still "singles out" individuals.

ENTERPRISE ACTION ITEMS

Don't Wait for Statute: Legislative revisions are stalled. Compliance teams must instead track EDPB regulatory guidance to map how strictly EDPS v. SRB case law applies in day-to-day enforcement.

€5.0M

CNIL FINE AGAINST IQVIA (MAY 2026)

- CNIL dismissed relative-anonymity arguments, ruling patient medical records as pseudonymous, not anonymous.
- High risk identified because unique identifiers allowed tracking longitudinal patient healthcare journeys.
- Combining deep clinical datasets with external, public tables allowed easy re-identification of patients.

Managing the Data Lifecycle

Pseudonymization requires continuous management

INGESTION

Initial masking and metadata tagging.

TRAINING

Apply PETs.

UTILITY REVIEW

Lifecycle hooks trigger re-review.

DELETION

Ensuring purge across all model weights.

The Personalization Dilemma

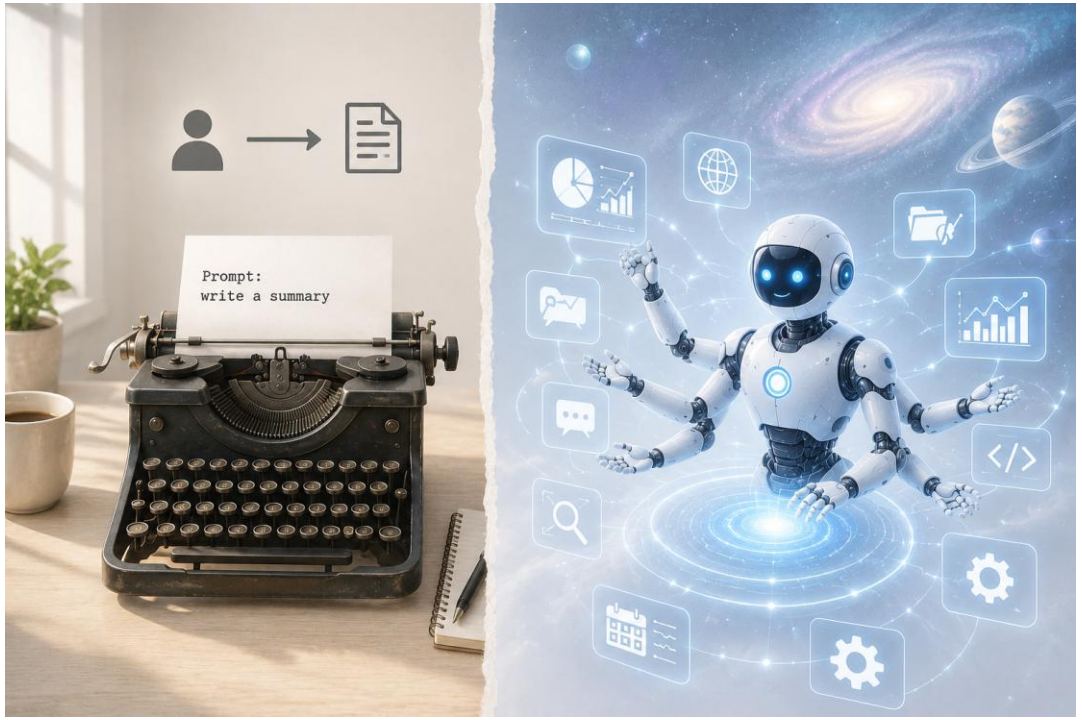
Massive Data vs. Agentic AI

Traditional AI:

- Thrives on large, generalized, and aggregated datasets. Easier to apply standard PETs.

Agentic AI:

- Requires hyper-personalized context (calendars, emails, habits) to execute autonomous tasks. Balancing privacy in these contexts is a major engineering hurdle.



2026 Strategy: The "Reasonably Likely" Bar

Since the legal definition remains broad, technical implementation must focus on the **Cost of Re-identification**.

Where is the line for PETs making identification "not reasonably likely" by:

- Prohibitive computational expense.
- Practical impossibility for data recipients.
- Robustness against future inference attacks.

RESOURCE LIST

I. EDPB Guidelines on Pseudonymization HERE.

II. OECD, Sharing trustworthy AI models with privacy-enhancing technologies, available HERE.

III. ICS, AI and PETS, available HERE.

IV. The Royal Society, Privacy Enhancing Technologies, available HERE.

V. ICO, Draft – Privacy Enhancing Technologies, available HERE.

VI. Google Privacy Framework – Our Approach to Protecting AI Training Data HERE.

VII. Visuals generated by Google Gemini and OpenAI ChatGPT.

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP AIGG Europe 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!