

DIGITAL OMNIBUS: CLOSING THE FRAUD PREVENTION GAP IN THE GDPR

ODDA supports the retention of Amendment 1043, introducing Article 9(2)(lb) GDPR, in the ITRE/LIBE compromise text, to the Digital Omnibus Regulation (2025/0360(COD))

The Online Dating and Discovery Association (ODDA), the trade association recognised as the voice of the online dating and social discovery sector, **supports AM 1043, which would introduce a new Article 9(2)(lb) GDPR legal basis covering the prevention of fraud, identity misuse, account takeover and abuse:**

In Article 9, paragraph 2, the following point is added:

'(lb) processing is necessary and proportionate for the prevention of fraud, the detection and prevention of abuse, bot and spam activity, identity misuse, account takeover or payment fraud, or for ensuring the security of accounts, payments and transactions, provided that the processing is subject to appropriate safeguards for the rights and freedoms of the data subject.'

Online fraud is a serious and growing problem across the EU, and the use of generative AI to create synthetic profiles and identities means the problem will get materially worse. **The risk is particularly acute on services that enable sustained interaction between people who may not previously have met.** Such accounts can facilitate romance fraud, financial scams, impersonation, sextortion and predatory conduct, with consequences that can include significant financial loss and lasting psychological harm.

The EU Agency for Fundamental Rights (FRA), in its 2026 EU-wide Eurobarometer survey of over 26,000 respondents across all Member States, found that **1 in 4 people in the EU has fallen victim to online fraud in their lifetime**. Among fraud types, **impersonation scams rank as the second most common**, affecting between 22–25% of fraud victims. Romance fraud, in which a fraudster establishes a false emotional relationship with a victim to extract money, represents one of the most harmful and fastest-growing fraud typologies. **Europol has identified romance fraud as a priority crime area**, and EU law enforcement operations demonstrate the scale of organised criminal networks operating in this space.

Combating this type of fraud effectively requires platforms to process personal data that can fall within the scope of Article 9 GDPR. Current derogations do not clearly cover the account integrity or proof of humanity use cases this requires. **AM 1043 closes that gap in a proportionate manner and does so at a moment when it is directly relevant to the EU's own forthcoming Action Plan on Fighting Online Fraud.**

CONTACT

Denisa Avram
Head of Public Policy, Europe
Match Group, board member of ODDA
denisa.avram@eu.match.com
TR: 5557202103388-25

Simon Newman
Chief Executive Officer
ODDA
simon@theodda.org
TR: 1201005102552-49

BRIEFING NOTE ON AMENDMENT 1043, ITRE/LIBE DRAFT REPORT

What the Omnibus says

Under **Article 9 of the GDPR**, the processing of special categories of personal data, including biometric data, is prohibited unless a specific exemption applies. The Digital Omnibus introduces a limited exception for biometric checks, provided that the biometric data or verification means remain under the sole control of the data subject.

EU Commission Proposal

(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.

What the ITRE/LIBE compromise text says

In the ITRE/LIBE compromise text, Amendment 1043 introduces a new Article 9(2)(lb) GDPR ground covering the prevention of fraud, identity misuse, account takeover and abuse, subject to necessity, proportionality and appropriate safeguards for the rights and freedoms of the data subject.

AM 1043

In Article 9, paragraph 2, the following point is added:

'(lb) processing is necessary and proportionate for the prevention of fraud, the detection and prevention of abuse, bot and spam activity, identity misuse, account takeover or payment fraud, or for ensuring the security of accounts, payments and transactions, provided that the processing is subject to appropriate safeguards for the rights and freedoms of the data subject.'

Justification

Amendment 1043 provides greater legal clarity for the proportionate use of biometric data for fraud prevention, identity misuse and account security. This clarity matters especially for online-to-offline platforms where two strangers agree to meet in person. On dating platforms, a compromised or misrepresented identity is not only a data protection risk, it is a physical safety or financial risk. This amendment helps clarify the interplay between data protection rules and safety considerations and gives platforms greater legal certainty to build and operate the safety tools that make that trust possible.

Platforms have developed a range of safety features to verify identity, protect account integrity, prevent access by previously banned users, and prevent accounts from being shared, sold, stolen or otherwise misused: photo and liveness verification to confirm the person behind a profile matches the person a user is corresponding with; checks against records of previously removed accounts to stop banned users, including those removed for harassment, impersonation or

predatory behaviour, from simply signing up again under a new identity; and ongoing monitoring to catch account takeover, bot-driven scam activity, and coordinated abuse networks that specifically target dating platform users for financial fraud.

In this context, sole control sounds like a fair principle, but it works against the purpose it's meant to serve. Checks exist for cases where the person can't be trusted to confirm themselves, such as an account that's been taken over, or someone previously banned trying to come back under a new identity. In both cases, the check only works if it doesn't depend on that person's control or cooperation. A rule requiring the user to stay in control ends up excluding exactly the situations it should be catching.

We believe that privacy and safety are not conflicting objectives. When properly balanced, they reinforce user trust and trust is the product on a platform where users are asked to meet strangers in person. Proportionate frameworks should allow platforms to perform targeted checks where necessary for fraud prevention, ban evasion and account security, while ensuring that biometric processing follows a privacy-by-design approach and remains targeted, purpose-limited and subject to strong safeguards, including data minimisation, retention limitations and access controls.

The Digital Omnibus and Amendment 1043 therefore provide an important opportunity to clarify the framework and enable the necessary, proportionate and privacy-preserving use of technology to protect European users, including, and especially, in the moments before an online connection becomes an offline meeting.