Recommended Rectifications to EDPB Guidelines 03/2026: Persons Depicted in Scraped Images and the Biometric Status of Facial Images

Comments for the public consultation on web scraping in the context of generative AI

Emanuele Conti-Vecchi
Paris · 30 October 2026 · Submitted in a personal capacity, as a citizen of the Union

I ask the Board to clarify two issues in the final Guidelines. First, the general duties of controllers must protect identifiable persons depicted in images published by someone else. Second, a digital facial image is biometric data under Article 4(14), which names facial images itself; whether Article 9(1) applies turns on the purpose of uniquely identifying a natural person. The proposed amendments below concern paragraphs 29, 37–38, 64, 66(f), 66(h) and 67.

Consider a wedding photograph showing the uploader, a guest and a child. The uploader's publication decision does not establish the other persons' expectations. A request from the guest cannot depend on control of the uploader's account. Replacing the caption does not establish that identifying information has been removed from the photograph. Paragraph 12 already recognises that pictures can directly identify individuals. The following amendments give that recognition practical effect.

1 Apply the general controller duties to the persons depicted

In Russmedia, the Court explains that Article 5(2) places on the controller the burden of demonstrating compliance with each principle in Article 5(1). Articles 24 and 25 require preventive measures and effective safeguards at the design stage and during processing. Article 32 gives concrete expression to that responsibility through security appropriate to the risks. Article 26 governs the allocation of responsibilities where parties jointly determine the purposes and means. Responsibility must be assessed separately for each processing operation (C-492/23, paragraphs 60–63, 85–89, 109–118).

These duties govern personal data generally. The requirements of Article 9(1) and (2) are additional where special categories of data are involved. Applied here, a controller determining the purposes and means of scraping must design its collection, safeguards and rights procedures to address the persons whose data it processes, including people shown in material published by others. That duty does not depend on classifying every facial image as biometric data.

Restore the condition for limiting rights under Article 11

Paragraph 29 moves from processing that does not require identification to the non-application of Articles 15–20. It omits the further condition in Article 11(2): the controller must demonstrate that it is not in a position to identify the data subject. It also omits the obligation to inform the data subject where possible. Article 12(2) reinforces the requirement to demonstrate inability before refusing a rights request on this ground.

Not needing identification for the processing purpose does not establish inability to identify the requester. The Guidelines should preserve both conditions. This correction respects Article 11(1), including its protection against collecting additional identifying information solely to comply with the GDPR.

Replace paragraph 29

> Where the purposes for which personal data are processed do not or no longer require the controller to identify the data subject, Article 11(1) does not oblige the controller to maintain, acquire or process additional identifying information solely to comply with the GDPR. The restriction on the application of Articles 15–20 in Article 11(2) applies only where the controller can demonstrate that it is not in a position to identify the data subject. The controller must inform the data subject accordingly, if possible. The restriction does not apply where the data subject provides additional information enabling identification for the exercise of those rights.

Under Article 12(2), the controller must facilitate the exercise of rights. The absence of an account held by a person depicted in scraped material does not, by itself, demonstrate inability to identify that person. The controller must consider relevant information already available to it and additional information supplied by the requester.

Assess the expectations of the persons depicted

Paragraph 64 expressly refers to publication "by the data subject themselves". Examples 4 and 5 also concern a person uploading their own data. Those premises do not cover everyone shown in a photograph published by another person. The Board should add an example addressing that distinct case.

Add after paragraph 64

Where published material contains personal data concerning persons other than the publisher, the controller must assess the reasonable expectations of those affected persons. The publisher's account settings, publication decision and awareness of scraping must not automatically be attributed to them. An assessment by categories of persons in comparable circumstances must preserve material differences, including minority and the absence of any relationship with the source platform.

Add Example 5a after Example 5

A person publishes a wedding photograph on a freely accessible platform that informs its users about scraping for AI development. The photograph also depicts an identifiable guest and a child who have no account on the platform. The uploader's receipt of the notice does not establish that either depicted person received it. Publication by the uploader does not, by itself, establish that those persons reasonably expect the reuse of their images for AI development. The controller must assess their circumstances and the impact of the proposed processing, including the particular protection required for children.

Provide a rights route for depicted persons without an account

Paragraph 66(f) offers an optional list for objections supported by information identifying a person on the source website. The list of measures is non-exhaustive. The problem is therefore the absence of an example for a depicted person who has no account and may not know where the image was published. Article 12(2) supplies the obligation to facilitate rights. Article 12(6) permits necessary additional verification where reasonable doubts about identity arise.

Add to paragraph 66(f)

Rights mechanisms should accommodate persons depicted or described in material published by others. They must not require ownership or control of the publishing account. Controllers should explain what information can enable them to locate the relevant data and verify the requester. They should consider a copy of the image, a source reference or other relevant contextual information supplied by the person. A source URL should not be mandatory where other supplied information enables the controller to identify the data subject and locate the relevant data. Any additional verification must comply with Article 12(6). Where Article 11(2) is relied upon, the conditions explained in paragraph 29 apply.

Apply minimisation and safeguards to the image content

The need for images of faces does not, without further assessment, establish the necessity of retaining identifiable images of particular people. Paragraphs 35–38 already require minimisation. Paragraphs 51–52 address less intrusive alternatives. The Guidelines should apply those requirements expressly to facial images.

Paragraph 66(h) qualifies its placeholder example with "in some cases". The qualification should be made concrete for images. Removing a name or account label does not establish compliance with Article 4(5) while the remaining image itself still permits attribution to a specific data subject without the protected additional information.

Add after paragraph 38

For image datasets, the controller should assess whether the processing purpose requires retaining information that makes the depicted natural persons identifiable. Where Article 6(1)(f) is relied upon, the controller must assess whether an equally effective and less intrusive alternative can achieve that purpose. Relevant alternatives may include synthetic images, narrower collection criteria and effective transformations of identifying image content. Their suitability must be assessed for the specified purpose.

Unnecessary personal data must be excluded from collection. Where such data have nevertheless been collected, they must be removed without being used for training. The controller should document the assessment and the effectiveness of the measures adopted.

The assessment must cover children depicted in material published on general-purpose websites. Excluding websites mainly used by minors does not address every such image. The controller should use appropriate collection criteria, filters and review procedures to address those risks. The uploader's declared age does not establish the age of every person depicted.

Add to paragraph 66(h)

For images, replacement of accompanying names, account identifiers or captions does not by itself establish pseudonymisation under Article 4(5). The assessment must also address the identifying information in the image. Where the remaining image itself permits attribution to a specific data subject without the separately protected additional information, replacing its label does not meet that definition. The controller must assess the actual effect of the transformation rather than rely on the removal of the label.

2 A digital facial image is biometric data; Article 9(1) turns on purpose

Article 4(14) defines biometric data by reference to their technical production, their relationship to a natural person's characteristics and their capability to allow or confirm unique identification. Article 9(1) separately specifies the identification purpose that engages its prohibition. Neither provision states that a template must be created or retained, or that the comparison must be automated. A conclusion based only on the absence of those features leaves the statutory criteria unanswered.

The Belgian authority expressly distinguishes identifying capability from the purpose of the processing. It also recognises raw facial images and templates as different forms of biometric reference data (Recommendation 01/2021, version 1.1, II.2.1, p. 12, and II.2.3, p. 14). In Comdribus, the Court treats the collection of fingerprints and facial photographs for police identification as biometric processing under Directive 2016/680 (C-371/24, paragraph 37). Article 3(13) of that directive uses the same definition as Article 4(14) GDPR. The relevance here is the treatment of the source images under that definition.

Paragraph 74 of Guidelines 3/2019 states that processing raw data "must imply a measurement", and paragraph 90 describes face images as "raw data". Article 4(14) contains no express measurement requirement and includes facial images and dactyloscopic data as examples. Paragraph 82 also refers to the "raw form of biometric data". The label "raw" therefore does not itself resolve classification. The Board should explain the basis and meaning of its measurement requirement, without treating a numerical output or template as an additional statutory condition.

The conclusion follows from the text. Article 4(14) requires specific technical processing but prescribes no particular technical method or additional processing stage. The process relied upon here is digital capture. The resulting personal data must relate to the person's characteristics and allow or confirm unique identification. A digital facial image does both, and Article 4(14) names facial images among its own examples: it is biometric data. The grammar of the definition settles where that capability sits. "Relating to" and "allow or confirm" qualify the personal data, not the "specific technical processing": the English verb is plural ("allow", where the processing would take "allows"); the French text reads "données … relatives aux caractéristiques … qui permettent", the Italian "dati … relativi alle caratteristiche … che ne consentono", both agreeing with the data, not with "traitement" or "trattamento". The capability to identify is a property of the data; the processing need only produce them. Recital 51 confirms the test rather than displacing it: a photograph falls within the definition when processed through specific

technical means allowing unique identification, and digital capture is such a means. Whether the processing falls under Article 9(1) depends on its purpose, which the Guidelines must assess for each operation.

Add paragraph 67a after paragraph 67

> For facial-image processing, the controller must distinguish the definition in Article 4(14) from the purpose condition in Article 9(1). A digital facial image is biometric data within the meaning of Article 4(14): the Regulation names facial images among its examples, digital capture is the specific technical processing from which the image results, and it is the image, as personal data relating to the person's physical characteristics, that allows or confirms the person's unique identification. The same holds for representations derived from it, including those processed only transiently. Neither a numerical output nor a stored template is a condition of Article 4(14), and the absence of a created or retained template does not take a source image outside it.
>
> Where the data meet Article 4(14), the controller must assess whether their collection or subsequent processing pursues the purpose of uniquely identifying a natural person. This includes establishing that different images represent the same natural person. Comparison by a person rather than an automated system does not, by itself, remove that purpose. Where Article 9(1) applies, an applicable exception under Article 9(2) is required in addition to a lawful basis under Article 6. A general description of the project as AI development does not replace the assessment of the specific operations carried out.

The Board should accompany this addition with an example distinguishing the assessment of a captured facial image from the assessment of a template derived from it. That example should identify the relevant technical processing and explain the application of each condition in Article 4(14), before examining the purpose under Article 9(1).

Authorities

European Data Protection Board, Guidelines 03/2026 on web scraping in the context of generative AI, version 1.0, adopted 7 July 2026, paragraphs 12, 29, 35–38, 51–52, 55–56, 64 and 66–67. Official text

Regulation (EU) 2016/679, OJ L 119, 4 May 2016, pp 1–88, Articles 4(1), 4(5), 4(14), 5, 6, 9, 11, 12, 24–26 and 32, and recital 51. Official text

Court of Justice, Grand Chamber, 2 December 2025, Russmedia Digital and Inform Media Press, C-492/23, ECLI:EU:C:2025:935, paragraphs 60–63, 79–89 and 109–118. Judgment

Court of Justice, 19 March 2026, Comdribus, C-371/24, ECLI:EU:C:2026:219, paragraphs 5 and 37–38. Judgment

Autorité de protection des données, Recommendation 01/2021 on biometric data, version 1.1, 1 December 2021, II.2.1, p. 12, and II.2.3, p. 14. Official text

European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, version 2.1, 26 February 2020, paragraphs 74–76, 82 and 90. Official text