MEMORANDUM FOR THE EDPB PUBLIC CONSULTATION

# Guidelines 02/2026 on Anonymisation — identifiers, registers, and section 2.4

Emanuele Conti-Vecchi · Paris · 30 October 2026

Submitted in a personal capacity, as a citizen of the Union; the views expressed are the author's own.

**Abstract.** This memorandum makes four points. Part I argues them; Part II sets the Guidelines' text against them, provision by provision, with proposed wording; Part III states what the memorandum does not ask and lists the changes.

**1. Relativity is right, but the Guidelines do not explain how it works.** Identifiers identify through registers that end in a face or a fingerprint, and only for those who hold or can reach them. A civil name with date and place of birth identifies in every hand, because the State has bound it to a face and the law opens the register; a Google account identifier identifies its holder for Google, and in Apple's hands, with nothing connecting it to a person, it is a string. Part I explains the chains; paragraph 23 should state, for each value it lists, which register binds it and for whom it identifies.

**2. The definition of identification departs from Opinion 4/2007 without saying so.** Identification is a sameness assessment: the finding that a natural person is the same across space, time and digital navigation. Its key component is distinction from all other persons within a group of persons; being treated differently, as a user or a non-user, is not identification. The Board should keep the definition of the Article 29 Working Party's Opinion or, at the least, require distinction from all other persons in the given context.

**3. The MAC address example of paragraph 25 is wrong.** Through registration alone, an object's identifier identifies its keeper in that capacity, and the person using the object only where the object is registered to that person and that person has exclusive access to it. A MAC address is not even a stable identifier of the device: many devices rotate it, and a controller may not notice that an address has changed or now denotes another device. Its allocation registers no owner or user, and a login identifies the user of an account, not of the machine. The example should be deleted unless the Board explains how "in turn" works: how an entity moves from an observed address to a device, and from the device to the natural person using it.

**4. Likelihood belongs to the means, never to identification.** Recital 26 asks whether a means of identification is reasonably likely to be used, not how likely identification is. Paragraph 8 asks the second question, and paragraphs 22, 35, 36 and 87 build on it: an error of law, since identification is unique and certain.

## I. The argument

### The question

The protection of personal data is a fundamental right, and it is a natural person's: Article 8 of the Charter and Article 16 TFEU give it to everyone in respect of data concerning him or her, beside the right to respect for private life in Article 7, and the Regulation opens with that statement (Recital 1). Article 4(1) GDPR fixes the reach of the right by reference to an identified or identifiable natural person, so that identification is where data acquire a person and the person acquires the right. The Guidelines rely, at footnote 13, on Opinion 4/2007 on the concept of personal data (WP 136), adopted on 20 June 2007 by the Article 29 Working Party, the Board's predecessor, under Directive 95/46/EC, whose definition of personal data the Regulation carries forward in Article 4(1). The Opinion defines identification as distinguishing a person, within a group of persons, from all other members of the group, and identifiability as the possibility of doing so, "the meaning of the suffix '-able'" (p. 12). Paragraph 25 of the Guidelines says that a MAC address "can identify the device and, in turn, the individual using the device"; Example 6 of the Guidelines says that a pseudonym derived from a browser fingerprint identifies the individual. Neither names a record connecting the object to a person. The question, for each value the Guidelines call an identifier, is what connects it to the natural person said to be identified, and which entity can use that connection.

## 1. Relativity, explained: what identifies a natural person, and for whom

The Board's relative approach is right: whether a person is identifiable depends on the means reasonably likely to be used by the entity concerned (Guidelines, sections 2.1 and 2.2; EDPS v SRB, C-413/23 P, paras 82–87). The Guidelines state it; they do not explain how it works. It works through chains: a record binds a value to a natural person, someone keeps that record, and only those who hold it or can reach it can follow the chain to the person. Three chains show the mechanism: the legal one, Google's and Apple's.

**The legal chain.** An identifier is a value bound to a natural person by a record. Two kinds of identifier reach the person differently. An intrinsic identifier originates in the body, a face or a fingerprint; it is bound to the person by origin, and it is the only kind that can be compared with the person present. Every other identifier is bound by a record, and reaches the person only through a chain of records that ends in an intrinsic one. The civil register is the model. The chain starts with the person present at enrolment. The authority establishes that the applicant exists in law, verifies that the photograph represents the person applying, and records the legal name, date and place of birth and document number against the photograph and, in the Union, two fingerprints (Regulation (EC) No 2252/2004, Article 1(2)). The sequence is the natural person, the photograph, the recorded particulars; in France the passport rules require the holder's particulars and photograph on the title and the register retains the civil particulars, the facial image and the title number (décret n° 2005-1726, Articles 1 and 6-1; décret n° 2016-1460, Article 2).

The State keeps the authoritative binding, and the person receives a copy of it: the passport or identity card, whose laminate and signed chip seal the particulars to the picture, and the picture to whoever presents it (Regulation 2252/2004, Annex, section 5). The passport is a certified copy of the register entry, and the copy gives the bond two independent sides. From the holder's side, the document proves sameness between the person carrying it and the person to whom the legal name is bound: a traveller at a border who wants to be identified presents the copy, the officer compares the face with the picture (Regulation 2252/2004, Article 4(3); ICAO Doc 9303, Part 9), and nothing is needed from the keeper. From the keeper's side, the register holds the same bond whether or not the holder wants it proved: a suspect who discards the document has not discarded the entry, and the authority that reaches the entry, by document number or through any record that leads to it, compares the person with the portrait on file and needs nothing from the holder. Each side can prove the bond without the other, and neither can repudiate it alone. This memorandum calls the keeper of that register a truth provider, because its record constitutes the identity in law; the vocabulary of chains and providers is the memorandum's own, and the instruments cited establish the links, not the terms. A name in a database is data purporting to refer to a person; the register is what makes the reference good.

**Trust providers, and three kinds of register.** Once a binding exists, another party can rely on it when it makes a record of its own. This memorandum calls such a party a trust provider: one whose recorded association others rely on under a contract or an institutional arrangement. A bank that opens a relationship on an identity document, an operator that registers a subscriber on one, an employer that issues a device to a named employee: each keeps a record bound to the civil particulars and, through them, to the portrait. Such records bind secondary identifiers, a tax number, a bank relationship, a SIM registration, to the person. Within the civil chain, every further identifier that reaches a person is added either by comparing the person with the picture on the document, or by relying on a record made by that comparison.

The relationship recorded determines whom the chain reaches. Object identifiers, a device address, a telephone number, a network address, refer to objects. They reach a person only through a keeper register, a record of who holds the object, and only if that keeper was enrolled somewhere; and even then they reach the keeper, not the person using the object, unless the keeper has exclusive access to it. Traffic law draws the same line, for the same reason: an act is attributed to the person who did it, not to the keeper of the object used. A camera's reading of a number plate reaches, through the vehicle register, the holder of the registration certificate, who in France answers for the fine but bears no criminal responsibility for it unless it is established that he was driving: the plate reaches the keeper, the face identifies the driver (Code de la route, Articles L121-1 and L121-3). Three kinds of register follow. An object register records that an object exists. A keeper register connects an object to a party in a stated role. A person register binds particulars to a bodily identifier. A chain of object identifiers, however long, ends at data unless one of its links reaches a person register.

**A chain without a civil name.** The civil chain is one way to establish a binding to a person; Opinion 4/2007 illustrates another. Asylum seekers "hiding their real names in a sheltering institution have been

given a code number for administrative purposes. That number will serve as an identifier, so that different pieces of information concerning the stay of the asylum seeker in the institution will be attached to it, and by means of a photograph or other biometric indicators, the code number will have a close and immediate connection to the physical person, thus allowing him to be distinguished from other asylum seekers and to have attributed to him different pieces of information, which will then refer to an 'identified' natural person" (Opinion 4/2007, Example 11, p. 14).

Four things are in the example. The legal name is withheld, so the civil register is out of reach. The institution builds an identity of its own, independent of the legal name, and builds it in the civil order: the natural person, a photograph or other biometric indicator, a code, and a register that binds the three. The code identifies "by means of" that register, not by itself; it is a unique identifier of a natural person precisely because the institution has registered the person, through the biometric, against the code. A code so bound identifies as firmly as a civil name does, and the chain has no name in it: code, photograph, person. And it identifies within the group of asylum seekers in the institution, a group of persons. The institution is the truth provider for its code: the code is an identifier of a person in the institution's hands only, and only because the binding of the code to the picture is entered in its register; anyone who binds anything further to that code relies on the truth the institution established, and is a trust provider in its system. For the institution, and for anyone who can reach that register, the code identifies a natural person; for anyone else the code is a number, unique, persistent, attached to information about a stay, and still a number. The Opinion gives the other side of the same rule in Example 13 (p. 16): serial numbers attributed at random to clinical cases travel to a pharmaceutical company without the patients' names, which stay with their doctors, and an authority "may consider that no means are present" in the company's processing that make identification reasonably likely. Same kind of value; opposite result; the variable is access to the register.

**Google's chain and Apple's.** Platforms run identification systems of their own, and they are built like the civil one. The chain starts with an e-mail address, which the platform that created it makes the account's name. To that root the platform binds, durably, further identifiers as they are supplied or observed: a telephone number, a recovery address, the locations connected from, the cookies set. Within the chain these are personal data, as the particulars are within the civil chain, and like a legal name they are not necessarily unique: one telephone number serves several accounts, one connection serves a household. The e-mail singles out the account within the platform's architecture, and the bindings reach the account. A device is bound to it by observation, not by enrolment: the platform logs which device signed in to which account and when. There is no register in which the hardware is bound to the account's holder through a bodily identifier, and no copy of such an entry in the holder's hands, as the passport is a copy of the civil entry; what the holder carries is a credential, a password or a key, which shows control of the account and nothing about who holds it. Anyone can use a given device with any digital identifier, and the holder can repudiate the binding by saying so: the platform's log proves that the device signed in, not who held it, where the civil bond can be repudiated by neither side. Nor is the relationship symmetrical. The platform can take both steps of an identification, singling out the account by its identifier and checking it against the bindings it recorded; the holder, who has no copy of the entry, can show control of the account by exercising the credential, and cannot prove the binding to anyone independently of the platform. In the civil chain the copy makes the holder a party to the bond, able to prove it alone; in a platform's chain every proof runs through the keeper. The account's main identifier can identify its holder, through what the platform recorded at enrolment or during later use; the machine does not thereby become an identifier of that holder, or of whoever operates it. The same machine is used logged off and with other accounts, and the platform's log ties it to an account only for the session it records. Google's chain, Apple's, Meta's and Microsoft's are each built this way, and each belongs to the platform that keeps it. Within the chain the identifiers reach the account and, where the platform has recorded a payment credential or a document, the holder of that credential or document; they identify a natural person for the platform and for whoever can reach the platform's register by contract or by legal channel. Outside every chain, they identify nothing. For a recipient outside the chain, the assessment must also include its own records and any usable matches to other chains. A cookie identifier that Google can link to an identifiable person is personal data for Google. Lack of access to Google's register does not establish anonymity if the recipient has another means reasonably likely to be used to make that connection; where no other usable connection is available, a Google account identifier such as "YUCPHCHF55FT8F8XF" is, in the hands of a controller outside Google's chain, a string. Apple keeps a chain of its own and is outside Google's: that identifier in Apple's hands is a string, whatever Apple's resources, unless Apple holds or can reach Google's register, receives the value with something its own records connect to a person, or is reasonably likely to pass it back into the chain, which is the paragraph 21 route by which it becomes personal data for

the transfer and for Apple. Membership in a chain is held in records, not bought with resources; paragraphs 26 and 29 measure how practicable a route is, and do not create one. The civil identifiers differ in kind. "Marco Rossi, born in Bologna on 4 May 1978" identifies the same person in Google's hands, in Apple's, and in the hands of a controller that belongs to no chain at all.

**For whom.** The existence of a binding and an entity's ability to use it are distinct questions. Each link is held by an identifiable entity. Whoever holds a link and has means reasonably likely to be used to reach the next one can follow the chain: through its own records, through a legal channel to another entity's (Guidelines, paragraph 29), or through an entitlement to require the information under a framework's rules (IAB Europe, C-604/22, paras 48–50). That is the test Recital 26 sets, and paragraph 28 of the Guidelines already describes it as a "chain" of means. It is the relative approach of sections 2.1 and 2.2, stated by its mechanism: access to a register that traces back to the natural person settles identifiability for a third party. The Court's position in EDPS v SRB is the same: pseudonymised data are not personal data "in all cases and for every person" (C-413/23 P, para 86), and they become personal for a recipient, and indirectly for the entity, where the entity puts them at the disposal of a person with means reasonably likely to be used (para 84). This memorandum accepts relativity in that form.

**For whom a civil identity identifies.** The answer is everyone, and the reason is not that every recipient has a route to the State's register. It is that the identification has already been performed. Paragraph 27 of the Guidelines states the consequence: "[i]f the individual to whom the information relates has already been identified, then the information is not anonymous." A face and a civil name with date and place of birth taken together are primary identifiers of the person the truth provider has bound; the person carries the copy into every relationship that asks for it, and the law opens the register to lawful inquiry. That is why the conclusion holds for every recipient and not only for those with a route to the register: those primary identifiers supply the identity particulars themselves. A passport or social security number is a unique indirect identifier for, and only for, those who can reach the register that binds it to the person. So many can that it is commonly treated as an identifier in every hand; access to the register is still what makes it one. Whether a name is unique is a separate question, settled by adding a date of birth or similar particulars "to prevent confusion between that person and possible namesakes" (Opinion, p. 13); a non-unique legal name is still an identifier and still personal data.

**The Guidelines' own examples sort by register.** Paragraph 23 lists "a name, IP address, social security number or e-mail address" as single pieces of unique data by which identification is done. A person register kept by the State: a civil name with date and place of birth supplies primary identity particulars; a social security number is a register key and identifies for, and only for, those who can reach the record linking it to the person. A keeper register kept by a private party: the IP address, which the provider's allocation records bind to the signatory of the internet access contract, so that it identifies that signatory, not any account reached through the connection, and, through those records alone, the user only where the signatory has exclusive access to it; it does so for those who hold the records or can obtain them by legal channels. An account register kept by a platform or an organisation: the e-mail address, which identifies a mailbox or an account, and a person only where the records bound to the account, or something like an employer's directory, bind it to one. For any value the Guidelines call an identifier, four questions therefore decide the matter: what the value distinguishes; what connects it to a natural person; which person that connection reaches; and who can use the connection.

## 2. Identification: an unexplained departure from Opinion 4/2007

The Guidelines cite the Opinion at footnote 13 and change its definition of identification without saying so (Part II, first row). The change reaches the core of every identity system. The civil register, a platform's account system and an institution's code all do one thing: they establish that a natural person is the same across space, time and digital navigation, that the traveller at the border is the person in the register, that the person a platform meets on one site and on another is the holder it enrolled. Identification is that sameness assessment, the finding that a record and a reference concern the same natural person, and its key component is distinction from all other persons: without it, a finding of sameness is a guess.

Opinion 4/2007 lists singling out among the means of identification and defines identification as distinction within a group of persons. It never says why singling out identifies. The reason is in its own examples: the person singled out can be checked against a reference that reaches the person, and is thereby identified. In Example 5 of the Guidelines the reference is the body in view; in the Opinion's Example 11 it is the photograph the institution holds against the code in its register; in the Opinion's

Example 10 it is the old newspapers in which the persons involved in a reported case can be looked up. Singling out a record is its first term, and the Guidelines have taken it for the whole.

The passage at page 14 of the Opinion, which says that web traffic tools identify "the behaviour of a machine and, behind the machine, that of its user", establishes the sameness of a machine across visits and reaches the user through a premise it states, that the computer is "the individual's contact point". The strongest reading against the memorandum is that the passage treats sustained recognition and profiling as identification without any civil identity. It does, for the individual whose contact point the machine is; it cannot be read as holding that an unregistered machine address identifies a given user where several people can use the machine, and it says nothing about which of them a profile concerns. Where a device has several users the Opinion attributes nothing to any of them; its Example 7 relates an office telephone's call log to the company, the employee and the cleaning staff, each through a stated link (p. 11). The sameness that fingerprinting and a hardware address establish, where neither changes nor rotates, is sameness of a configuration or a device. Whether the same person is behind it is the second term, and it has to be supplied.

**Neither uniqueness nor different treatment is identification.** The asylum seeker's code is unique and identifies only through the photograph; a MAC address may be locally unique, and there is no photograph. Paragraph 25 answers the question whether the value is unique and treats the answer as settling what the value identifies. Example 5 of the Guidelines, two paragraphs earlier, applies the Opinion's test correctly: a person seen on a street is distinguished from the other people there by attributes perceived together with the body. Paragraph 25 keeps the conclusion and drops the body. On the Opinion's definition, a comparison that leaves another person as a live candidate has identified no one; that is the point Part II takes against paragraph 87. The Guidelines add a second substitute, a distinction that makes different treatment possible, and different treatment is available at the level of a class: a site that serves one page to a returning browser and another to a new one treats whoever is behind it as a user or a non-user, and no person has been distinguished from all other persons. Example 6 of the Guidelines rests its conclusion on the same substitute: profiling across sites and the choice of adverts show that a browser configuration has been told apart from others, not which natural person used it. The definition to be respected is the Opinion's: distinguished, within a group of persons, from all the other persons, not treated as a user or a non-user. If the Board keeps "in a given context", it should at least write "from all other persons in that context", and drop treatment.

## 3. The MAC address example is wrong

Paragraph 25 says that a MAC address "can identify the device and, in turn, the individual using the device". As the paragraph presents it, nothing connects the address to a person. The only register behind a universally administered address, kept by the IEEE Registration Authority, records blocks of addresses and the organisations that received them, not devices and not persons; current iOS and Android devices present a different randomised address to each Wi-Fi network by default (RFC 9724, section 7); and a link-layer address is visible only on the local network. Through registration alone, an object's identifier identifies the person using the object only where the object is registered to that person and that person has exclusive access to it; paragraph 25 establishes neither. "In turn" asserts two links, from the address to a device and from the device to a person, and names a register for neither (Part II, third row). Because MAC addresses sit in every network a business runs, in every laptop, telephone, printer and dishwasher connected to it, the sentence as drafted would require every controller, including the small and medium-sized enterprises that make up 99% of businesses (European Commission, SME definition), to decide without criteria whether its network logs are personal data.

## 4. Likelihood: of the means, never of identification

Recital 26 asks whether a means of identification is reasonably likely to be used; it never asks how likely identification is. For the Court, a means is not reasonably likely to be used where "the risk of identification appears in reality to be insignificant", because identification is prohibited by law or practically impossible (EDPS v SRB, para 82). Paragraph 8 asks instead "how likely it is that the individual will be identified", and paragraphs 22, 35, 36 and 87 build on that question. That is an error of law. The test governs only identifiability, the second element of Article 4(1): a person is identifiable where a means of identification exists, its use is reasonably likely, and, if used, it would identify him uniquely and with certainty, distinguishing him from all other members of the group. Whether information relates to a person turns on content, purpose or effect (paragraph 16), not on likelihood.

# II. The text, provision by provision

*The table sets each provision against the argument in Part I. The first column quotes the Guidelines as adopted for public consultation on 7 July 2026. The second explains what is wrong with the text and quotes the sources on which the explanation rests. The third proposes replacement text: new or changed words are in bold italics, deleted words are struck through, and editorial instructions are in square brackets.*

| Guidelines 02/2026 — text as adopted | Commentary: what is wrong, and the sources | Proposed text |
|---|---|---|
| EXECUTIVE SUMMARY · THIRD PARAGRAPH (P. 2); PARAGRAPH 19; PARAGRAPH 22, FIRST SENTENCE<br>Information can relate to a natural person by reason of its content, purpose or effect. The existence of such a link need not be readily apparent and may require some processing to establish. A natural person is "identified or identifiable" if they can be distinguished from others in a given context using means reasonably likely to be used and in a way that makes it possible to treat them differently. "Means" should be interpreted broadly and may include means that are only accessible through a third party. Whether they are reasonably likely to be used will depend on the relevant entity's perspective and should be assessed in light of all objective factors.<br>19. To identify a natural person means to distinguish them from others within a given context, consequently making it possible to treat them differently from those other people. This can be done using direct identifiers (such as a name, ID number or reference code), or one or more attributes which relate to that person.<br>22. Importantly, for information to be anonymous, the likelihood of the individual being successfully distinguished from others within the given context does not need to be zero; instead, that likelihood should be insignificant in reality. […] | **An unexplained departure, not a paraphrase.** Opinion 4/2007 defines identification by three features: "a natural person can be considered as 'identified' when, within a group of persons, he or she is 'distinguished' from all other members of the group. Accordingly, the natural person is 'identifiable' when, although the person has not been identified yet, it is possible to do it (that is the meaning of the suffix '-able')" (p. 12). The Guidelines cite the Opinion at footnote 13 and record one terminological difference there, "result" for "effect". They record none for the definition of identification, which is changed on three points; the change is repeated at paragraph 19 and becomes the operative threshold at paragraph 22.<br>**1. The reference class.** The Opinion distinguishes a person "within a group of persons"; the Guidelines, "in a given context". A group of persons is made of persons. A context need not be: a network, a dataset and a set of browser configurations are contexts, and within each a value can be perfectly distinguishing while no person has been distinguished from any other. The Opinion lets the group change size, never kind: a common family name fails "from the whole of a country's population" and succeeds "in a classroom" (p. 13).<br>**2. The quantifier.** The Opinion requires distinction "from all other members of the group"; the Guidelines, "from others". Without the universal the test admits a comparative reading, on which distinguishing device D from other devices would count as distinguishing "its user" from the users of other devices: a role, not a person, which several people may fill and one person may fill on several devices, so that no one is distinguished from all other persons. The universal also keeps likelihood where Recital 26 puts it, on the means: the question is whether means of identification are reasonably likely to be used (EDPS v SRB, paras 82–83), not how likely identification is. Identification is unique and certain. Paragraphs 22 and 87 make it a matter of degree, with a "likelihood" of being distinguished and a result held with "sufficiently high confidence"; a match that leaves other candidates open distinguishes from most, not from all.<br>**3. The criterion.** The Opinion defines identification by distinction alone. The Guidelines add that the distinction must make it possible "to treat them differently". The Opinion places treatment in the relating-to element and says so in its conclusions (p. 25); the Guidelines keep it there too, at paragraph 16(c). Paragraph 19 makes treatment a consequence of identification, the executive summary a condition, and Example 6 the proof. Different treatment is available at the level of a class, and that is where the criterion fails. A site that serves one page to a returning browser and another to a new | *[Executive summary, third paragraph:]*<br>Information can relate to a natural person by reason of its content, purpose or effect. The existence of such a link need not be readily apparent and may require some processing to establish. ~~A natural person is "identified or identifiable" if they can be distinguished from others in a given context using means reasonably likely to be used and in a way that makes it possible to treat them differently.~~ ***A natural person is "identified" when, within a group of persons, they are distinguished from all other members of that group, and "identifiable" when, although not yet identified, they can be identified using means reasonably likely to be used. Distinguishing a record, an account or a device from others does not by itself identify a natural person; where identification depends on such an intermediate identifier, the register that binds it to the person, and who keeps it, must be established.*** "Means" should be interpreted broadly and may include means that are only accessible through a third party. Whether they are reasonably likely to be used will depend on the relevant entity's perspective and should be assessed in light of all objective factors***, including which register binds an identifier to a natural person and who keeps it***.<br>*[Paragraph 19:]*<br>To identify a natural person means to distinguish them ~~from others within a given context, consequently making it possible to treat them differently from those other people~~***, within a group of persons, from all other members of that group***. This can be done using direct |

| Guidelines 02/2026 — text as adopted | Commentary: what is wrong, and the sources | Proposed text |
|---|---|---|
| | one, a network that admits a known device and refuses an unknown one, treats whoever is before it as a user or a non-user. A class has been sorted from the rest; no person has been distinguished from all other persons, and the treatment attaches to whoever presents the device. The definition to be respected is the Opinion's: distinguished, within a group of persons, from all the other persons, not treated as a user or a non-user.<br>**Example 5 applies the Opinion's test.** It carries forward the Opinion's own illustration of "the man wearing a black suit" (p. 13); its reference class is the people on a street; the combination identifies because only one individual there presents it. A group of persons and uniqueness, the two elements the summary drops, are the two elements Example 5 applies, and it reaches identification without mentioning treatment. It is the yardstick for paragraph 25.<br>**Example 6 shows the criterion at work.** Example 6 concludes that a pseudonym derived from browser fingerprints identifies the individual because the third party can "distinguish the individual and treat them differently from others". What such a value permits is profiling across sites and the choice of adverts, that is, treatment of a browser configuration; no person is distinguished from all other persons. The value is recomputed from a configuration, and recognising the same configuration does not show which natural person used it. Example 6 should state, for the websites and for the third party separately, the route by which each could reach a natural person, or withdraw the conclusion.<br>**The departure recurs wherever the definition is applied.** The executive summary's sentence on techniques ("distinguished and treated differently"), paragraph 54 ("from others in a given group"), paragraph 87 ("sufficiently high confidence … to be distinguished and treated differently"), paragraph 98 ("distinguished from others"), Example 24 ("to treat any respondent differently") and Example 6 ("distinguish the individual and treat them differently from others") are one definition applied at each point where the Guidelines decide whether a person has been identified, and they should be corrected together. | identifiers (such as a name~~, ID number or reference code~~ ***together with date and place of birth, or a face***), or one or more attributes which relate to that person. ***Identification is the finding that information and a natural person concern the same individual: a person is identified when a record or observation is matched to a reference that reaches that person, such as a register entry bound to a photograph, an identity document or published information. Singling out a record does not by itself identify the individual. The individual is "identifiable" when, although not yet identified, it is possible to identify them, the meaning of the suffix "-able" (Opinion 4/2007, p. 12), with means reasonably likely to be used (Recital 26). A pseudonym, account identifier or reference code identifies a natural person only through the register that binds it to that person, and only for an entity that holds that register or has means reasonably likely to be used to reach it, including through others (paragraphs 15, 20 and 21).***<br>*[Alternatively, if the Board keeps "in a given context": in the executive summary and in paragraph 19, for "from others" read "from all other persons", and delete the words on different treatment.]*<br>*[Paragraph 22, first sentence:]*<br>~~Importantly, for information to be anonymous, the likelihood of the individual being successfully distinguished from others within the given context does not need to be zero; instead, that likelihood should be insignificant in reality.~~ ***Information is anonymous if it does not relate to an identified or identifiable natural person. To assess identifiability, account must be taken of all means reasonably likely to be used by the controller or another person to identify the individual.***<br>*[Paragraph 87, second sentence:]*<br>~~This does not necessarily require perfect accuracy or~~ |

| Guidelines 02/2026 — text as adopted | Commentary: what is wrong, and the sources | Proposed text |
|---|---|---|
| | | ~~absolute certainty; rather, the result should be at least sufficiently close, and provide at least a sufficiently high confidence in the circumstances at hand, to allow the data subjects to be distinguished and treated differently.~~ ***Identification is unique and certain: the result must distinguish a data subject from all other members of the group of persons concerned. A result that leaves several candidates, or points to one only with some confidence, has not identified the individual; the additional means needed to distinguish the remaining candidates must be specified and assessed under paragraphs 26 to 29.***<br>*[Consequential: align the executive summary's sentence on techniques, paragraphs 54 and 98 and Examples 6 and 24 with the same definition; in Example 6, assess the websites and the third party separately and state each one's route to a natural person.]* |
| **Paragraph 23 (with paragraph 50 and Annex 1)**<br>In many cases, identification is done by reference to an identifier that is unique within a given context. In the simplest cases, this could, for example, be a single piece of unique data, such as a name, IP address, social security number or e-mail address. | **Four values, four registers.** A name and a social security number are bound to a natural person by a register the State keeps: the civil register, bound to a portrait through the identity document; the social security number, recorded against the particulars of birth that anchor it to the portrait, so that applying it to a person present runs back through a document that carries the picture. The primary identifiers are the face and the civil name with date and place of birth taken together. A social security number identifies for, and only for, a controller that can reach the record linking it to the person. An IP address is bound by a register the provider keeps: its allocation records link the address, for a period, to the signatory of the internet access contract. It identifies the signatory, and, through those records alone, the user only where the signatory has exclusive access to the connection. That is a fact of network architecture, not a rule of any one legal order, and a United States court of appeals, with the signatory already identified from the provider's records, stated it plainly: "Because multiple devices and individuals may be able to connect via an IP address, simply identifying the IP subscriber solves only part of the puzzle" (Cobbler Nevada, LLC v. Gonzales, 901 F.3d 1142, 1145 (9th Cir. 2018)). It identifies the signatory for those who hold the records or can obtain them by legal channels. An e-mail address is bound by an account register: it identifies a mailbox or an account, and a person only where the records bound to the account, an employer's directory or a comparable record bind it to one. "Unique within a given context" describes the value; it says nothing about the register, if any, behind it.<br>**The list is carried forward.** A near-identical list reappears at paragraph 50, and the first question of the Annex 1 flowchart treats data containing "e-mail, phone numbers, | In many cases, identification is done by reference to an identifier that is unique within a given context. In the simplest cases, this could, for example, be a single piece of unique data, such as a name, IP address, social security number or e-mail address. ***A unique value identifies what a register binds it to. A civil name with date and place of birth supplies primary identity particulars in every entity's hands. A passport or social security number is a register key and identifies for, and only for, an entity that can reach the record linking it to the person. An IP address identifies the signatory of the internet access contract recorded in the provider's allocation records, for an entity that holds those records or can obtain them through legal channels (paragraph 29); through those records alone, it identifies the person using the connection only where the signatory has exclusive access to it, and it does not identify an account reached through it. An e-mail address identifies a*** |

| Guidelines 02/2026 — text as adopted | Commentary: what is wrong, and the sources | Proposed text |
|---|---|---|
| | etc.” as obviously not anonymous. A telephone number denotes a subscription; whether it reaches a person depends on the operator’s register, or another record linking the number to a person, and on access to it. | ***mailbox or an account, and a person only where a register, such as the records bound to the account or an employer’s directory, binds it to one. Where no register binds the value to a natural person, the value identifies the object it denotes.*** *[Consequential: paragraph 50 and the first question of Annex 1 to be aligned.]* |
| **Example 5**<br>When looking at live CCTV of people on a street, many people are wearing black suits, and many people are walking dogs. Within the context of that street, “the person in a black suit” is not, therefore, unique and that description does not allow for the identification of a particular individual. The same is true of “the person with a dog”. However, only one individual on the street is both wearing a suit and walking a dog. Within the context of that street, the combination of those attributes is therefore unique to that individual and the description “the person in a black suit who is also walking a dog” allows for them to be identified.<br>**Paragraph 25**<br>Importantly, the identifiers or attributes do not necessarily have to be about the individual per se but can also be about other individuals, groups or objects which are otherwise linked to them. For example, a user’s device may have a hardware identifier – such as a MAC address – that can identify the device and, in turn, the individual using the device. Equally, a website may “fingerprint” its visitors based on their unique combination of web browser, operating system, screen resolution, time zone etc., and use this fingerprint to then identify them as they move from page to page and across different visits. | **The referent changes and the change is not marked.** Example 5 concerns properties of a person, perceived together with the person, on one street at one moment. Paragraph 25 concerns properties of a device. The bridge that Example 5 supplied by perception is not replaced; the words “otherwise linked” and “in turn” stand in its place.<br>**“Can identify” is not a rule.** The sentence says that a MAC address “can identify the device and, in turn, the individual using the device”. A controller cannot comply with a possibility. Guidance has to say whether the address identifies a natural person and in what circumstances; this sentence states neither.<br>**“In turn” compresses two inferences, and no register supports either.** First, an observed address may not denote one device across networks and time. By default, current iOS and Android devices present a different randomised address to each Wi-Fi network (Apple, “Use private Wi-Fi addresses on Apple devices”; Android Open Source Project, “Implement MAC randomization”; RFC 9724, section 7); and Apple warns that addresses can be copied, spoofed or changed. A link-layer address is visible only on the local network or within radio range of it, so the observer is a local operator, not the website of the following sentence. Second, a device does not denote a natural person. One machine and its address can be linked to several accounts. Those links alone establish neither that the accounts belong to the same natural person nor which natural person used the machine. The machine therefore cannot, on that basis alone, serve as a proxy for a particular natural person. Household, shared, borrowed and resold devices break the relation, and nothing in the address records that the user has changed. “The individual using the device” names a role; who fills it is a conclusion, not an identifier. The only register behind a universally administered address, the IEEE Registration Authority’s allocation of address blocks, records the issuer. There is no photograph.<br>**What a stated link looks like.** Opinion 4/2007 uses the same words for a garage’s service record, which carries a plate number and an engine number “which in turn can be linked to the owner”, and then makes the result depend on a connection the garage establishes “between the vehicle and the owner, for the purpose of billing”, after which the information “will ‘relate’ to the owner or to the driver” (Example 6, p. 10). Where one exists, an employer’s inventory of the devices it issues to named staff, or a registration of the device made against an identity document, is a link of that kind. The register identifies the person to whom the device is assigned. Through that assignment record alone, the address identifies that person as the user only where that person has exclusive | *[Example 5 unchanged. Add at the end:]*<br>***The description identifies the individual because the observer perceives the person and the attributes together, at the same place and time. Where an attribute belongs to an object, such as a device, the link between the object and the person must be established separately (paragraph 25).*** *[Paragraph 25:]*<br>Importantly, the identifiers or attributes do not necessarily have to be about the individual per se but can also be about other individuals, groups or objects which are otherwise linked to them. ***Identifying an object is not, however, the same as identifying a natural person. Where identifying a person depends on moving through one or more intermediate identifiers, objects, accounts or records, the assessment should name the register that binds each to the next, who keeps it, and the means the relevant entity could reasonably be expected to use to reach it. The existence of such a register should not be inferred from the uniqueness, persistence or correlation of the object identifier.*** ~~For example, a user’s device may have a hardware identifier – such as a MAC address – that can identify the device and, in turn, the individual using the device. Equally,~~ ***For example,*** a website may “fingerprint” its visitors based on their unique combination of web browser, operating system, screen resolution, time zone etc., and use this fingerprint to ~~then identify them as they move~~ |

| Guidelines 02/2026 — text as adopted | Commentary: what is wrong, and the sources | Proposed text |
|---|---|---|
| | access to the device. Paragraph 25 names none.<br>**Read literally, the sentence reaches every network.** With the executive summary's definition, "in turn" makes every entity that assigns, filters or logs MAC addresses a controller of personal data, whether or not it holds any record about a person. The Court's case law points the other way: pseudonymised data are not personal data "in all cases and for every person" (EDPS v SRB, paras 86–87), and a VIN becomes personal only "as regards someone who reasonably has means" to link it to a person (Scania, C-319/22, para 46). On 16 October 2025 the Polish Supreme Administrative Court, a court of last instance, applied the same discipline to online identifiers: it held that neither an IP address nor a cookie identifier is personal data in every case, and that the supervisory authority had to establish, from the circumstances at the time of the visit and the objective factors Recital 26 names, that the website operator could identify the person (III OSK 2595/22); it did not hold that data about a device cannot be personal data, only that the classification must be demonstrated rather than presumed. On the literal reading a bare MAC address would be personal data unconditionally, while an account identifier is personal data only where a chain connects it to a person: the device would carry more than the account. Where a platform reads a hardware address from a device and records it against an account, an operation Article 5(3) of the ePrivacy Directive already governs, the link to a person comes from the account register, not from the address "in turn". The binding is itself questionable: the account is used with a credential from any device and does not need the device it is bound to, and recurrent use is not exclusive access. The platform thus attributes to the holder what others do on that device, as if a car's keeper were criminally responsible for offences others commit with it. No one is criminally responsible except for his own act (Code pénal, Article 121-1), and identification rests on the same personhood: Article 4(1) requires a particular individual, not his objects in others' hands, to be identified or capable of being identified. Paragraph 25 credits the address with what the binding does, leaves the binding unexamined, and burdens every local network operator instead. MAC addresses sit in every network a business runs, down to the printer and the dishwasher, and small and medium-sized enterprises, 99% of businesses, would have to decide without criteria whether those logs are personal data.<br>**The remedy.** Delete the example. An unregistered object identifier is not an identifier of a natural person. "In turn" should go unless the Board states how the link from the device to the person is made and who keeps the register that records it. If the Board keeps an example, it should say what the address identifies and for whom: a device, only if distinguishable for a given observer, network and period; a person, only where the entity holds or can reach a register linking the device to that person. Where a separate record, such as a camera image or an authenticated session, establishes who acted, that record identifies the person; the MAC address adds nothing to the identification. A rule so stated can be applied by a small business. "Can identify" cannot be applied at all. | ***recognise the same configuration*** from page to page and across different visits***; whether that configuration corresponds to a single natural person must be established, not assumed. The persistence of a device or browser identifier, or of a browser configuration, is something the user may lawfully change, by address randomisation, by clearing stored identifiers, by a private browsing mode or by an anonymising network; persistence is to be evaluated, not presumed.***<br>*[If the Board retains a hardware-identifier example, insert in place of the deleted sentence:]*<br>***For example, a user's device has a hardware identifier, such as a MAC address, which may distinguish the device for a given observer, network and period, subject to changes in or reuse of the address. It identifies a natural person only where the entity holds, or has means reasonably likely to be used to reach, a register linking the device to that person, such as an employer's inventory of devices issued to named employees or a registration of the device made against an identity document. The register identifies the person to whom the device is assigned. Through that assignment record alone, the address identifies that person as the user only where that person has exclusive access to the device. A login identifies the user of the account, not of the device.*** |

# III. Conclusion

## What the memorandum does not ask

It does not ask the Board to abandon the relative approach of sections 2.1 and 2.2; it supports it, and offers the chains of Part I as its clearer frame. It does not ask the Board to treat any dataset as anonymous, or to narrow the concept of personal data as the Court has defined it. It does not dispute that an online identifier may form part of an indirect identification chain: Recital 30 says so, and Scania and IAB Europe each show how such a chain is completed, through a register someone keeps. Where the memorandum asks for less, it asks that the register be named rather than assumed. Where it asks for more, at paragraph 23, it asks that a civil identity be treated as what it is: a reference to a person the State has already identified.

## Summary of proposed changes

1. **Relativity: paragraph 23, with paragraph 50 and Annex 1:** state, for each listed value, which register binds it to a natural person, who keeps that register, and for whom the value therefore identifies: a civil name with date and place of birth for every entity; a social security number for, and only for, those who can reach the record linking it to the person; an IP address for those who hold or can obtain the provider's records, and, through those records alone, the person using the connection only where the signatory has exclusive access to it; an e-mail address only where a register binds it to a person.
2. **Identification: executive summary, paragraphs 19, 22 and 87, and wherever the definition recurs (paragraphs 54 and 98, Examples 6 and 24):** restore the Opinion's definition, distinction within a group of persons from all other members of the group, or at the least require distinction from all other persons in the given context; remove different treatment from the definition; state the sameness test expressly; apply the reasonable-likelihood assessment to the use of identification means; at paragraph 87, specify the additional means needed to distinguish the remaining candidates and assess whether those means are reasonably likely to be used.
3. **The MAC address: paragraph 25:** delete the MAC address example; "in turn" goes unless the Board states how the link from device to person is made and who keeps the register. A retained example should state that the address may distinguish a device for a given observer, network and period; that identifying the user through registration alone requires registration to that person and that person's exclusive access to the device; that the persistence of device and browser identifiers and configurations is under the user's lawful control and is to be evaluated, not presumed; and that a sign-in identifies the user of an account, not of the device on which it is used.
4. **Likelihood: paragraphs 8, 22, 35, 36 and 87:** attach likelihood only to the use of means of identification, never to identification itself; in paragraph 8, replace "how likely it is that the individual will be identified" with whether means of identification are reasonably likely to be used, and apply the same test wherever paragraphs 22, 35 and 36 speak of a likelihood of identification or re-identification; identification is unique and certain, and a person is identifiable only where a means exists whose use is reasonably likely and which, if used, would identify him with certainty.

## The right the definition serves

Everyone has the right to the protection of personal data concerning him or her (Charter, Article 8(1)). The right is a natural person's, and it attaches to data at the point where the data reach that person; the definition of identification is therefore the boundary of the right, and the corrections asked for here guard it from both sides. A test that counts a comparison from most, treatment as a user or a non-user, or an unregistered object identifier, as identification spreads the right over data that reach no one, and the supervision it draws is spent on network logs rather than on the registers where persons are bound. A test that stops at the entity's own perspective where the State has already identified the person withholds the right where it is owed. Keeping Opinion 4/2007's definition, and naming the register, keeps the right where the Charter places it: with the natural person.

## Authorities cited

**Court of Justice of the European Union**

Gesamtverband Autoteile-Handel v Scania, C-319/22, 9 November 2023, para 46.
IAB Europe, C-604/22, 7 March 2024, paras 48–50.
EDPS v SRB, C-413/23 P, 4 September 2025, paras 82–87.

**Other courts**

Naczelny Sąd Administracyjny (Poland), 16 October 2025, III OSK 2595/22.
United States Court of Appeals for the Ninth Circuit, Cobbler Nevada, LLC v. Gonzales, 901 F.3d 1142 (2018).

**Article 29 Working Party and European Data Protection Board**

Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007, pp. 10–16 and 25.
EDPB, Guidelines 02/2026 on Anonymisation, version 1.0 adopted for public consultation, 7 July 2026.

**Legislation**

Charter of Fundamental Rights of the European Union, Articles 7 and 8; Treaty on the Functioning of the European Union, Article 16.
Regulation (EU) 2016/679, Article 4(1); Recitals 1, 26 and 30.
Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents, Articles 1(2) and 4(3) and Annex, section 5.
France: décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports, Articles 1 and 6-1; décret n° 2016-1460 du 28 octobre 2016 (titres électroniques sécurisés), Article 2; Code de la route, Articles L121-1 and L121-3.
Directive 95/46/EC, Article 2(a); Directive 2002/58/EC, Article 5(3).

**Technical sources**

Apple, “Use private Wi-Fi addresses on Apple devices” and “Recommended settings for Wi-Fi routers and access points”, support articles 102509 and 102766; Android Open Source Project, “Implement MAC randomization”.
IEEE Registration Authority, MAC Address Block Large (MA-L) assignments.
IETF, RFC 9724, State of Affairs for Randomized and Changing MAC Addresses, March 2025, section 7.
ICAO, Doc 9303, Machine Readable Travel Documents, Part 9: Deployment of Biometric Identification and Electronic Storage of Data in MRTDs, eighth edition.
European Commission, “SME definition”.