General Data Protection Regulation: GDPR

Spiecker gen. Döhmann / Papakonstantinou / Hornung / De Hert

2023
ISBN 978-3-406-74386-3
C.H.BECK

umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

of identification criteria regarding what was set in the DPD definition. Besides an 'identification number' the Comm proposed 'location data' and 'online identifier". The EP added 'name' to the list of criteria as well as "unique identifier" instead of 'online identifier'. These changes were adopted in the GDPR definition with the option of 'online identifier'. The Comm-P also added genetic identity as one of the domains where specific factors may be used to identify a person (→ Art. 4(13)). This change was also included in the GDPR. Overall, the changes proposed by the Comm and the EP broaden the scope of the concept thus amplifying the material scope of the GDPR.

7 The EP also put forth definitions of 'pseudonymous data' and 'encrypted data'. The former was almost completely adopted under the definition of 'pseudonymisation' (→ Art. 4(5)). This reference shows that although the European legislator considered pseudonymisation as a means to reduce the risks of data processing it nevertheless allowed for the possibility that such data can still be linked to a person and they must thus be considered as personal data. Other than this new reference to pseudonymisation, both recitals 26, in the DPD and the GDPR, are in line with each other. The latter definition of **encrypted data** was not included in the GDPR, even though encryption is mentioned in several places in the text. This poses a difficulty when considering if encrypted data are personal data under the GDPR in situations where controllers, processors and third parties in general do not hold the key to perform the decryption operations,[26] such as in messaging apps with end-to-end encryption. The EP also developed the identification criteria set out in recital 23 of the Comm-P. It added the direct or indirect singling out as one way to identify a person through data and it also added the demand to account for "all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development".[27] The first proposal had also been made by the Art. 29 WP[28] and it seems to be its influencing source. These proposals were included in recital 26 of the GDPR. The Comm's and the EP's concern regarding online identifiers on recital 24 of the proposal were combined in recital 30 of the GDPR.

III. The constituent elements of the concept of personal data

1. Information

8 The GDPR does not define the term 'information'. Furthermore, it states that personal data refers to 'any' information. As such, the CJEU has interpreted information in a broad implicit sense,[29] building from the work of the Art. 29 WP.[30] This means that anything that can be understood as information falls within the concept of personal data if the remaining constituent elements apply. What is to be understood as information remains for the interpreter to argue within the conventions of language,[31] but it must surely denote a relational property as foreseen in Art. 4 no. 1: information, though a thing in

[26] Noting this aspect, Karg, 'Art. 4(1)', in Simitis/Hornung/Spiecker gen. Döhmann, 284-285, mn. 11.

[27] EU Parliament Report on the on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals regarding the processing of personal data and on the free movement of such data.

[28] Cf. Art. 29 WP199, p. 5.

[29] CJEU C-434/16, 20.12.2017, *Nowak*, ECLI:EU:C:2017:994, para. 34.

[30] See Art. 29 WP136, pp. 6 et seq.

[31] Bygrave, 'Information Concepts in Law: Generic Dreams and Definitional Daylight', *Oxford Journal of Legal Studies*, Vol. 35, No. 1 (2015, pp. 91 et seq.; see also Karg, 'Art. 4(1)', in Simitis/Hornung/Spiecker gen. Döhmann, 287-288, mn. 26; Purtova, 'The law of everything', pp. 48 et seq.; Hallinan/Gellert, 'The Concept of 'Information', pp. 269-319.

itself[32], always comprises the relation between the availability of certain knowledge and one or more entities, be they persons, objects, states of affairs or something else (and even if inaccurately identified as shown below).[33] However, although information always relates to an entity, it is for the law to determine what are the relational criteria that can be used to consider that a piece of information relates to specific persons and should therefore be understood as personal data.

9 The Art. 29 WP recognises the relational property of information as an autonomous constitutive element ("relating to")[34] of the definition of personal data and provides for a categorisation of **criteria of connection between information and natural persons: i) content, ii) purpose or iii) result**. Information relates to a natural person from the perspective of **content** when such information is about a natural person in a common sense, in as much as it provides knowledge of traits of a certain person.[35] Regarding the **purpose** criterion, information relates to a natural person when it may be used, according to context, to evaluate, ground decisions or influence the "status or behaviour of an individual".[36] Finally, information may relate to a natural person concerning a **result** criterion when, although not about traits of a natural person or aimed at conforming behaviour, nonetheless affects the legal positions of a person, such as rights, liberties or interests.[37] For example, when data about cars allow for the monitoring of their drivers or data about products tag to clients.[38] The criteria through which information may relate to natural persons show that the crucial common element is the potential or existent effect of information on the legal sphere of a natural person, which also calls on the importance of **context-dependant analysis**.[39]

10 Regarding the nature of the information, a distinction between **objective and subjective information** is usually made,[40] both being admitted by the GDPR. This means that for the purpose of the concept of personal data, information is considered not only when an objective appraisal of knowledge is possible (physical traces for instance) but also when such knowledge relies on a subjective appreciation.[41] This means that the information may be false, inaccurate or dependant on third party judgments (such as the opinion of a friend or the evaluation of a service provider) and can still be considered information under the GDPR.[42] Indeed, **evaluative information** comprises an important part of personal data.[43] There must always be a connection between the

[32] See, Buckland, 'Information as thing', *Journal of the American Society for Information Science*, 42, 5 (1991), pp. 351-360.

[33] See also the concept of information as "semantic information", Hallinan/Gellert, 'The Concept of 'Information'', pp. 282-284.

[34] See Art. 29 WP136, p. 9.

[35] Ibid, p. 10.

[36] Ibid.

[37] Ibid, pp. 10-11.

[38] See on this, in the context of RFID technology, Art. 29 WP105.

[39] See Purtova, 'From knowing by name to targeting: the meaning of identification under the GDPR', *IDPL*, Vol. 12, No. 3 (2022), pp. 163-183.

[40] See Art. 29 WP 136, p. 6; CJEU C-434/16, 20.12.2017, *Nowak*, ECLI:EU:C:2017:994, para. 34.

[41] See Art. 29 WP 136, p. 6; see also Finck/Pallas, 'They who must not be identified', pp. 11-12.

[42] See however CJEU Joined Cases C-141/12 and C-372/12, 17.07.2014, *YS*, EU:C:2014:2081, para. 44 to para. 48. In this judgement, the CJEU found that, although information contained in an asylum request application was personal data, the assessment done by public officials was not, due to the understanding that such assessment did not contain information relating to the applicant but related to asylum law in as much as it would apply to any other applicant in similar circumstances. For this reason, the Court differentiates this situation which refers to access to administrative documents from a case of protection of personal data. This distinguishes the present case from the *Nowak* decision, as the CJEU recognises (see C-434/16, 20.12.2017, *Nowak*, ECLI:EU:C:2017:994, para. 56).

[43] See Karg, 'Art. 4(1)', in Simitis/Hornung/Spiecker gen. Döhmann, 288, mn. 29.

availability of certain knowledge and an entity, even if that connection is merely stated but not proved.

The GDPR does not limit the notion of Information to **types of content** within the spectrum of private/public sphere of information (although this spectrum is relevant within the GDPR, after certain knowledge has been qualified as information). This is in line with the distinction made in the EU CFR between the right of respect for private and family life in Art. 7 and the right to the protection of personal data in Art. 8.[44] Information, in the broad sense adopted by the GDPR, confirms itself as a nexus between any knowledge and an entity identified by such knowledge: a certain (natural) person as we shall see *infra* concerning the second constituent element of the concept of personal data. This makes it clear that information, in the sense of the GDPR, comprises not only intimate and private information but also information related to public dimensions of a person, be it in a family, professional,[45] leisurely or other capacity. Public information,[46] even if divulged by the data subjects (for instance, in social networks), and whatever the context of relevance,[47] is to be considered as information under the GDPR, unless exceptions to the material scope apply (→ Art. 2 para. 2 lit. c mn. 54). This is confirmed by the identifiers used as examples in Art. 4 no. 1. **11**

The format of information also does not define it under the GDPR although the GDPR does mention certain types of formats such as "biological samples" (Art. 4 no. 13), "facial images and dactyloscopic data" (Art. 4 no. 14) or "electronic means" (for instance Art. 15 para. 3). All these formats may be sources of information and provided that the remaining conceptual constituents verify may allow for the acknowledgement of personal data. The key feature is that the processing of information may be done through such formats. The CJEU has considered as personal data information in several different formats – physically or electronically written text,[48] Internet traffic data,[49] IP numbers[50] or cookies,[51] graphic representations, such as fingerprints,[52] and video **12**

[44] Art. 29 WP 136, p. 7.

[45] The CJEU supports this interpretation, building on the interpretation of Art. 8 ECHR and the abovementioned distinction between Art. 7 and Art. 8 of the EU CFR, see Joined Cases C-465/00, C-138/01 and C-139/01, 20.05.2003, *Österreichischer Rundfunk*, ECLI:EU:C:2003:294, para. 73; C-73/07, 16.12.2008, *Satakunnan Markkinapörssi and Satamedia*, 16.12.2008, ECLI:EU:C:2008:727, para. 65; C-342/12, 30.05.2013, *Worten*, ECLI:EU:C:2013:355, para. 46; C-683/13, 19.6.2014, *Pharmacontinente – Saúde e Higiene*, ECLI:EU:C:2014:2028, para. 13; See also the reference made in Art. 9 para. 2 lit. b which presupposes personal data relating to information processed in the context of an employment relationship.

[46] See CJEU C-73/07, 16.12.2008, *Satakunnan Markkinapörssi and Satamedia*, ECLI:EU:C:2008:727, para. 38 to para. 49.

[47] Indeed, it can regard information concerning people passing through common parts of a residential building, see CJEU C-708/18, 11.12.2019, *Asociatia de Proprietari*, ECLI:EU:C:2019:1064; or even someone passing through a specific point on a street, see CJEU C-212/13, 11.12.2014, *Rynes*, ECLI:EU:C:2014:2428.

[48] CJEU Joined Cases C-465/00, C-138/01 and C-139/0, 20.05.2003, *Österreichischer Rundfunk*, ECLI:EU:C:2003:294; Case C-101/01, 06.11.2003, *Lindqvist,* ECLI:EU:C:2003:596; C-524/06, 1, 6.12.2008, *Huber*, ECLI:EU:C:2008:724; C-73/07, 16.12.2008, *Satakunnan Markkinapörssi and Satamedia*, ECLI:EU:C:2008:727; C-553/07, 07.05.2009, *Rijkeboer*, ECLI:EU:C:2009:293; C-28/08, 29.06.2010, *Bavarian Lager*, ECLI:EU:C:2010:378; Joined Cases C-92/09 and C-93/09, 09.11.2010, *Volker und Markus Schecke GbR and Eifert*, ECLI:EU:C:2010:662; C-131/12, 13.05.2014, *Google Spain and Google*, ECLI:EU:C:2014:317; C-342-12, 30.05.2013, *Worten*, ECLI:EU:C:2013:355 C-683/13, 19.06.2014, *Pharmacontinente – Saúde e Higiene*, ECLI:EU:C:2014:2028; C-230/14, 01.10.2015, *Weltimmo*, ECLI:EU:C:2015:639; C-40/17, 29.07.2019, Fashion ID, ECLI:EU:C:2019:629.

[49] CJUE C-119/12, 22.11.2012, *Probst*, ECLI:EU:C:2012:748; Joined Cases C-293/12 and C-594/12, 08.04.2014, *Digital Rights Ireland*, ECLI:EU:C:2014:238.

[50] CJEU C-582/14, 19.10.2016, *Breyer*, ECLI:EU:C:2016:779; see also Moiny, 'Are Internet protocol addresses personal data? The fight against online copyright infringement', *Computer law & security review*, 27 (2011), pp. 348-361.

footage.[53] Any format of access to knowledge regarding a certain natural person may provide information within the concept of personal data of the GDPR.[54]

2. Natural person

13 As was mentioned at the beginning of the previous point, given the adopted concept, information necessarily relates to an entity, which means that the segment "relating to" in Art. 4 no. 1 is not an autonomous constituent element but a connecting term from the 'information' element to the 'natural person' element.[55] For information to become personal data Art. 4 no. 1 deems it necessary for any information to relate to "an identified or identifiable natural person". 'Natural person' is thus the next constituent element of the concept of personal data in the GDPR as it narrows the information that is to be considered.

14 The first important distinction to be made, and called upon by the definition, is between natural and legal persons. The GDPR excludes the protection of data pertaining **to legal persons,**[56] whatever form they may take in any Member State. The legislator establishes a direct connection with the fundamental rights recognised to natural persons, including the right to the protection of personal data, in the EU CFR.[57] The latter also protects legal persons[58] but the GDPR legislator chose to limit the concept of personal data in line with a teleological nexus between the human dignity principle (Art. 1 EU CFR) and natural persons but also in accordance with the mandate of Art. 16 para. 2 of the TFEU.[59] Under the DPD, the CJEU had determined that "legal persons can claim the protection of Articles 7 and 8 of the Charter […] in so far as the official title of the legal person identifies one or more natural persons".[60] This has changed under the GDPR. However, it seems to be the case that whenever information concerning members of bodies or statutory positions of legal persons refers to identifiable natural persons such information should be considered as personal data.[61] Thus, following recital 14 of the GDPR although legal persons cannot claim the protection of the GDPR[62] even for personal data which concern them, natural persons whose personal data are used by legal persons can claim protection of the GDPR if such personal data are processed in a context relating to these natural persons, on grounds of "content", "purpose" or "result".[63]

15 Once established that only natural persons matter for the purposes of the definition of personal data, the limits of such personality must still be ascertained. One must look at the beginning and the end of natural personality. The **relevant end of the natural person** regarding the concept of personal data in the GDPR results clearly from recital 27 where it is stated that the GDPR "does not apply to the personal data of deceased

---

[51] CJEU C-210/16, 05.062018, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388.
[52] CJEU C-291/12, 17.10.2013, *Schwarz*, ECLI:EU:C:2013:670.
[53] CJEU C-212/13, 11.12.2014, *Rynes*, ECLI:EU:C:2014:2428; C-345/17, 14.02.2019, *Buivids*, ECLI:EU:C:2019:122; C-708/18, 11.12.2019, *Asociatia de Proprietari*, ECLI:EU:C:2019:1064.
[54] See Art. 29 WP 136, p. 7.
[55] In a different sense see, Art. 29 WP 136, p. 6.
[56] See also recital 14.
[57] See recital 1.
[58] See Bygrave/Tosoni, 'Art. 4(1)', in Kuner/Bygrave/Docksey, p. 111, fn. 41.
[59] See recital 12.
[60] CJEU Joined Cases C-92/09 and 93/09, 9.11.2010, *Volker und Markus Schecke and Eifert*, ECLI:EU:C:2010:662, para. 53; see also Art. 29 WP 136, p. 23.
[61] See Art. 29 WP136, pp. 23 and 24.
[62] See CJEU C-620/19, 10.12.2020, *Land Nordrhein-Westfalen*, ECLI:EU:C:2020:1011, para. 46 and 47.
[63] See Art. 29 WP 136, pp. 23 and 24.

persons". Member States may, however, "provide for rules regarding the processing of personal data"[64] of such persons.

As far as the beginning of personality is considered the GDPR is mute, making no consideration regarding another important legal distinction between **unborn life** (*nascituri*) and already-born persons.[65] Such silence must then be interpreted, especially as it contrasts with the above-mentioned recital 27 insomuch as the GDPR does not take a similar stance regarding the delimitation of the beginning of natural personality. On the one hand, this contrast seems to support the view that the legislator could have used some criteria to assure such delimitation and chose not to. On the other hand, although natural personality is acquired by birth, information regarding conceived human life may become information related to "an identified or identifiable natural person" and thus call for protection even before the birth of such a person as a condition to guarantee the freedoms and rights of the new natural person.[66] This is especially clear in the case of genetic data.[67] It would defeat the purpose of the GDPR of protecting the personal data of natural persons from the moment of their birth if some data that would qualify as personal data after birth could already be collected before birth without the application of the GDPR. This is especially illustrated by the references in Art. 4 no. 1 to such personality specific factors as "physical, physiological, genetic [and] mental" factors. Thus, the GDPR must apply to unborn natural persons whenever all the remaining constituent elements apply.[68] **16**

3. Identification

Once "any information" relates to "natural persons" within the framework analysed above, the concept of personal data begins to assume its complete definition under the GDPR. But the way in which "any information" can relate to "natural persons" still allows for a great margin of uncertainty. Thus, the legislator uses a third and final constituent element: identification. The GDPR defines personal data as information relating to natural persons if and only if such information relates to "an identified or identifiable" natural person. This means that the GDPR does not apply to non-personal data both in the sense of data that do not pertain to any person but also in the sense of data that pertain to someone but do not and cannot identify a specific individual and thus according to Art. 4 no. 1 do not relate to a natural person. **17**

The legislator does not define "identified natural person" although it does explain on Art. 4 no. 1 what an "identifiable person" is. By doing so the legal interpreter can also understand what is meant by "identified natural person". The CJEU has treated this constituent element of the concept of personal data through a two-step approach, where first it is to be determined if certain information identifies a natural person and, second, in case it does not, it must be determined if such information may allow for the identification of the natural person indirectly when combined with ulterior data (as, for example, an IP address from a client held by an online store combined with the Internet Service Provider client's data).[69] **18**

[64] Recital 27.

[65] Under the DPD, the Art. 29 WP started from a position of considering that personal data was in principle referring to living individuals. But the Art. 29 WP admitted that in this regard the DPD left a margin of discretion to the legislation of Member States within the purpose of the data protection rules of the DPD, see Art. 29 WP 136, pp. 22 and 23.

[66] See Karg, 'Art. 4(1)', in Simitis/Hornung/Spiecker gen. Döhmann, p. 291, mn. 41.

[67] See Pormeister/Drozdzowski, 'Protecting the Genetic Data of Unborn Children: A Critical Analysis', *EDPLR*, Vol. 4, No. 1 (2018), pp. 53 et seq.

[68] Ibid, pp. 61 et seq.

19 The concept of 'identification' used by the GDPR is thus a referencing concept that allows for **a natural personal person to be singled** out[70] among all admissible others[71]. This means that identification stands on selected information that has the capacity to distinguish and individualise natural persons, be it one single piece of information (e.g., the name)[72] or a combination of several pieces of information (e.g., address and age).[73] This also means that only through identification does the information completely and fully relate to a natural person in the sense of personal data as defined by the GDPR.

20 The relevant information for **the identification process is context dependent**, meaning that the same identifier may be able to perform its task under certain conditions but may also be insufficient in other contexts.[74] The most common identifier – the name – may be enough on most situations but it is not mandatory for identification.[75] This is why Art. 4 no. 1 mentions than an identifier may work directly or indirectly depending on the identifier itself and other contextual factors. For example, in a certain group of natural persons the year of birth may be sufficient to identify one natural person when such natural person is the only one born on a different year, but in other situations where multiple individuals all share the same year of birth such information would not be a complete identifier. For instance, in a small village of only a few hundred persons publishing data referring to Covid-19 and stating only age may be sufficient to identify some of the persons.

21 A **directly identified natural person** according to the GDPR is a natural person regarding whom a certain piece of information allows for immediate individualisation.[76] When referring to **indirectly identified natural persons** recourse to the combination of several pieces of information is necessary to achieve a "unique combination".[77] If such combination is done over time, the person is only considered to be identified when the resulting combination singles out the person. Until that moment the collected data are either non personal data or they must be considered as personal data of an identifiable individual if the data necessary to identify the person are **deemed to be available though not yet processed.**[78] The distinction between indirectly identified personal data and identifiable personal data thus raises some challenges.[79]

22 Information concerning an identified natural person presents a straightforward case: the information relates to an already identified person. It is thus unequivocally personal data. On the other hand, information concerning an 'identifiable natural person' not only presupposes that the information still needs to link to a certain natural person, but it raises the question of knowing how the identification can be done.

---

[69] See CJEU C-582/14, 19.10.2016, *Breyer*, ECLI:EU:C:2016:779, paras. 38 and 39.

[70] See recital 26.

[71] For the implications of this broad understanding see Davis, 'Facial Detection', p. 369 et seq.

[72] Art. 29 WP 136, p. 13.

[73] In this sense, CJEU C-582/14, 19.10.2016, *Breyer*, ECLI:EU:C:2016:779, para. 41.

[74] See recital 26.

[75] See CJEU, C-101/01, 6.11.2003, *Lindqvist*, ECLI:EU:C:2003:596, para. 27; See Borgesius, 'Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation', *Computer law & security review*, 32 (2016), pp. 268-269.

[76] This is also the case when the information is gathered in the presence of a natural person (so-called handshake identification) for then all the gathered information is directly referenced to the persons for duration of their presence (although it may cease to be personal data after the person leaves the place where the information was collected if such information cannot be linked to the person by any other identifier information), see Karg, 'Art. 4(1)', in Simitis/Hornung/Spiecker gen. Döhmann, p. 293, mn. 55.

[77] See Art. 29 WP 136, p. 13.

[78] Ibid.

[79] See Oostveen, 'Identifiability and the applicability of data protection to big data', *IDPL*, Vol. 6, No 4 (2016), pp. 299-309.

Identifiability is a possibility and information gathered on such possibility may only become personal data if a connection to a specific individual can be made under **certain conditions**. To this end, the legislator explains in Art. 4 no. 1 what must be understood as **an identifiable person**: "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". In these cases, the information collected, if the other constituent elements apply, is known to relate to a natural person but further steps will need to refer such information to a specific person. The legislator states several identifiers, i.e., referencing criteria (name, identification number, location data, online identifier) as well as factors specific to the identity of a single person which may also be used as identifiers (physical, physiological, genetic, mental, economic, cultural or social). The GDPR explicitly accepts any referencing criteria that allow information to relate to a natural person. The identification of a natural person may be done using a combination of different sets of identifiers and, while some identifiers allow for a more immediate and direct identification, in their absence a natural person may still be identified through an adequate set of identifiers.[80] The legal concept of personal data comprises all these possibilities of identification.[81] **23**

Recital 26 provides for some guidance on how to determine the limits of identifiability and thus the limits of the concept of personal data. It begins by stating that "[t]o determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used" and further determines that "[t]o ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". The most important aspect deriving from these excerpts concerning the limits of identifiability is the kind of judgment that it entails. For any given case, all the elements that can influence the identifiability of a person through the processing of information must be taken into consideration by the interpreter.[82] This judgment turns on the **means available to the entity or entities conducting processing operations**, such as financial, technical and human resources, but also on the **context of such operations**, such as the legal framework and the resources available to third parties that might contribute to identify a natural person. The goal is to reduce risk to a minimum or to eliminate it for a given moment,[83] using a risk management approach[84] under a principle of reasonableness.[85] This leads to an important discussion on the very notion of identifiability and the limits of anonymisation after the CJEU's *Breyer* judgement.[86] This means that identification operates in an instant, that may or may not proceed over time: as soon as an identifier singles out or allows to single out a person, be it for a short period of time or a long one, we are in the presence of personal data and as such the GDPR applies. As Purtova has correctly argued, in *Breyer,* where the CJEU dealt with dynamic IP addresses (which change **24**

[80] See CJEU, C-101/01, 6.11.2003, *Lindqvist*, ECLI:EU:C:2003:596, para. 27.
[81] See Art. 29 WP 136, p. 14.
[82] See Art. 29 WP 136, p. 15.
[83] On the framework of this risk analysis resulting from the GDPR, the Art. 29 WP and the national authorities, see Finck/Pallas, 'They who must not be identified', p. 15.
[84] See, Finck/Pallas, 'They who must not be identified', pp. 34 et seq.
[85] See Oostveen, 'Identifiability', p. 306.
[86] See, for context on this discussion, Groos/van Veen, 'Anonymised Data and the Rule of Law', *EDPLR*, 4 (2020), pp. 499 et seq.; see also Urgessa, 'The Protective Capacity', p. 521 et seq.

with each Internet connection) there was, indeed, contrary to what the CJEU found, an identified individual, albeit during the duration of each specific connection[87].

25 Since identification or identifiability is the connection or possible connection between information and a specific individual, avatars pose particular problems. Avatars, which are usually representations of persons on virtual environments, may give rise to data being classified as personal, when information relating to an avatar can be referred to the individual which the avatar represents[88]. For instance, the information regarding the avatar used on an online gaming platform chat room or in the metaverse will be personal data if such information can be referred to the person represented by the avatar, singling out such person. There should be, however, caution in establishing such link as avatars can also be used by "bots", computer programs that work automatically and interact with people. In these cases, it is evident that no personal data is involved.

26 Big Data, referring to the use of tools that analyse and establish connections between bulks of information, poses a great challenge to the category of "identifiable data" as it raises the question of the possibility of anonymisation[89] and points to a scenario where all information relating to a natural person could in time become personal data[90].

27 Processed personal data may cease to be so. The Art. 29 WP has given opinion that the only way to safely determine a limit to identifiability is **complete and irreversible anonymisation**, which is presented as a standard for anonymisation techniques.[91] Thus, the Art. 29 WP considers, following its own position on the concept of personal data[92] that "[a]n effective anonymisation solution prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset. Therefore, generally speaking, removing directly identifying elements in itself is not enough to ensure that identification of the data subject is no longer possible. It will often be necessary to take additional measures to prevent identification, once again depending on the context and purposes of the processing for which the anonymised data are intended".[93]

28 The CJEU has considered, in *Breyer*, that the means available to controllers and processors should be taken into account in conjunction with the **resources held by third parties.**[94] That is, even if a controller or a processor do not have the means to identify a person through data, given certain circumstances such data may still be considered personal if identification can be achieved through the intervention of a third party.[95] The CJEU, however, draws some limits to this approach on identifiability, using two tests,[96] namely "the identification of the data subject was [1] prohibited by law or [2] practically impossible on account of the fact that it requires a disproportionate

---

[87] Purtova, 'From knowing by name to targeting', p. 180.

[88] Ibid, p. 179.

[89] Ibid; see also Papakonstantinou/de Hert, 'Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an interim period of no regulation at all)', *computer law & security review* 36 (2020), p. 9.

[90] Ibid, pp. 306 et seq.

[91] See Art. 29 WP 216, pp. 6-7 "– Anonymisation can be a result of processing personal data with the aim of irreversibly preventing identification of the data subject; – Several anonymisation techniques may be envisaged, there is no prescriptive standard in EU legislation".

[92] See Art. 29 WP 136, p. 21.

[93] See Art. 29 WP 216:9; see also, for a critique of the Art. 29 WP position, El Emam/Álvarez, 'A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques', *IDPL*, Vol. 5, No. 1 (2015), pp. 73 et seq.; Finck/Pallas, 'They who must not be identified', p. 15, particularly on the possible confusion between anonymisation and pseudonymisation.

[94] CJEU C-582/14, 19.10.2016, *Breyer*, ECLI:EU:C:2016:779, para. 44.

[95] CJEU C-582/14, 19.10.2016, *Breyer*, ECLI:EU:C:2016:779, para. 48.

[96] See Groos/van Veen, 'Anonymised Data', p. 502.