



HAL
open science

Case C-479/22 P, Case C-604/22 and the limitation of the relative approach of the definition of ‘personal data’ by the ECJ.

Alexandre Lodie

► To cite this version:

Alexandre Lodie. Case C-479/22 P, Case C-604/22 and the limitation of the relative approach of the definition of ‘personal data’ by the ECJ.. 2024. hal-04609263

HAL Id: hal-04609263

<https://hal.science/hal-04609263v1>

Submitted on 12 Jun 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Case C-479/22 P, Case C-604/22 and the limitation of the relative approach of the definition of ‘personal data’ by the ECJ.

By Alexandre Lodie

On 7 March 2024, the ECJ released two very important decisions on the extent of the definition of ‘personal data’ under EU data protection law in cases [C-479/22 P](#) and [C-604/22](#).

The latter case involves a Belgian non-profit organisation called IAB Europe which designed a tool, a framework called TCF, with the purpose of enabling website providers and data brokers to process personal data lawfully (see Paragraph 20).

The preferences that a user select via a consent management platform (CMP) are subsequently encoded in the TCF string which is a combination of letters and characters. The CMP places a cookie on the user’s device so that the cookie and the TCF string can be linked to the user’s IP address (see Paragraph 25). The Court was asked whether, in this context, a character string containing the preferences of a web user could be considered personal data in the hands of IAB Europe and whether IAB Europe could be regarded in this scenario as a (joint) controller.

The former case, which has already been discussed [here](#), deals with a Greek researcher that was under investigation by the European Anti-Fraud Office (OLAF) for allegations relating to potential financial misconduct following the attribution of fundings granted by European Research Council Executive Agency (ERCEA) to carry out a research project.

OLAF published a press release concerning the ongoing investigation and its results, which led to an identification of the researcher by journalists. The researcher thus seized the [General Court](#) arguing that OLAF infringed [Regulation 2018/1725](#), which is the regulation on the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (EUDPR), as well as her right to the presumption of innocence.

In this case – and without digging into too much detail – the [General Court](#) in case [T-384/20](#) basically held that the press release could not be seen as personal data since the German journalist who re-identified the researcher was an investigative journalist with particular knowledge in that matter and could not be seen as an “average reader” (“lecteur moyen” in French). The plaintiff appealed this decision, which gave rise to the decision of the ECJ in case [C-479/22 P](#)

In the next two sections we will discuss how these two judgments by the ECJ seem to limit the relative approach of what constitutes personal data as the Court adopts a definition of the notion of personal data which is more protective for data subjects. Eventually, in the last section it is argued that these decisions should not be overinterpreted since they limit the relative approach, without really ruling it off.

Case C-479/22 P and the limitation of the relative approach

As previously mentioned, the plaintiff [appealed](#) the General Court’s decision on the ground that the press release did constitute an information regarding an identifiable person and that the Court misinterpreted the notion of the “means reasonably likely to be used” to identify a person.

In substance the plaintiff challenged the fact that the Court held that the press release was not personal data.

This judgment from the General Court is in line with case [SRB v EDPS](#) discussed [here](#) (see also [Spajic](#)) where the General Court held that although when data could be considered as pseudonymised (and thus personal data according to the [EDPS](#)) one had to consider whether the recipient of that data could (reasonably and lawfully) get the additional information needed to re-identify them in order to qualify data as personal. In the negative, data could not be regarded as personal data and thus the right to information would not apply.

Both cases demonstrate a certain trend from the General Court toward a relative approach on what can be considered “personal data” and a weakening of data protection, as it narrowed the extent of the concept of personal data. According to this relative approach, data are not personal or non-personal by nature. Their legal qualification depends on the ability of the organisations who hold them to re-identify them. This approach had been outlined in ECJ’s famous [Breyer](#) case.

In Case C-479/22 P the ECJ had thus to determine whether, the General Court’s judgment was accurate in considering that a press release containing information relating to potential fraud committed by a researcher was not personal data, even though the said researcher was subsequently re-identified by journalists. From a broader perspective, one of the main challenges of the decision was to consider whether the ECJ would uphold the reasoning of the General Court with regard to the relative approach of the definition of the notion of personal data.

Actually, the ECJ adopted a much more ‘protective’ stance than that of the General Court. Indeed, it recalled that, for data to be considered personal data, it is not necessary that people be identified directly from the information contained in the press release. Quite the opposite, additional information must be taken into account as well (see Paragraph 53).

From this background, the ECJ concluded that *“it is inherent in the ‘indirect identification’ of a person that additional information must be combined with the data at issue for the purposes of identifying the person concerned. It also follows that the fact that that additional information comes from a person or source other than that of the controller of the data in question in no way rules out the identifiable nature of a person”* (Paragraph 55, emphasis added).

This assertion is paramount to understand how the Court limits the scope of the relative approach. Here, the Court considers that no matter who holds the additional information necessary to re-identify a data subject, as far as such information exists, data must be considered as personal.

This is why, in the same line of thought, the Court also underlines that *“Regulation 2018/1725 does not lay down any conditions as regards the persons capable of identifying the person to whom an item of information is linked, since recital 16 of that regulation refers not only to the controller but also to ‘another person’”* (Paragraph 56).

This marks a huge difference vis-à-vis the dictum of the General Court, not only in this case, but also in the SRB v. EDPS case where the Court held that the assessment of the possibility to

re-identify data had to be carried out from the data recipient's perspective and not in an abstract and absolute fashion.

In the present case, the logic of the Court is essentially that despite the investigative journalists having personal (and particular) knowledge that an "average reader" does not have, data must still be considered personal since the means deployed to re-identify the researcher were not unreasonably likely to be used.

This decision must be read in relation with another decision released the very same day by the ECJ, in the case relating to IAB Europe.

Case C-604/22: Toward a more objective approach of the notion of personal data?

This case mainly deals with the issue of whether IAB Europe – in that it provides its members with a framework enabling them to comply with the GDPR – could be considered a (joint) controller. However, before considering this issue, the Court had to decide whether the TCF String, as a combination of letters and characters, could be considered personal data. To do so, the Court had to assess whether the combination of the TCF String with additional data such as IP address could make re-identification possible.

It is worth underlining here that IAB Europe does not have these pieces of information and thus cannot directly combine these data. On this issue, the Court stated that *"[i]n so far as associating a string composed of a combination of letters and characters, such as the TC String, with additional data, inter alia with the IP address of a user's device or with other identifiers, allows that user to be identified, it must be considered that the TC String contains information concerning an identifiable user and therefore constitutes personal data [...] That interpretation cannot be called into question by the mere fact that IAB Europe cannot itself combine the TC String with the IP address of a user's device and does not have the possibility of directly accessing the data processed by its members in the context of the TCF"* (See paragraphs 45 and 46).

Interestingly, the Court concludes that, although IAB Europe is not in a position to combine the TC String with the IP address and do not have access to data processed by its members, TCF strings still contain personal data and must be treated as such. The Court seems to qualify TCF String as personal data *per se*, without further consideration as to whether IAB Europe is, in practice, able to re-identify data.

In other words, it may be argued that the Court adopts a more objective view on what constitutes personal data. It must be recalled that in *Breyer*, the Court stated that it was the ability for an entity to get access to the additional information necessary to the re-identification of data subjects that determined whether said entity processed personal data. Here, conversely, the Court tends to consider that even in the situation where IAB Europe cannot directly access data nor combine them, data remain personal.

Despite this distancing of the ECJ from the General court, the scope and interest of these two decisions should not be overestimated, as it is discussed in the next section.

Why is the relative approach still relevant?

In case C-479/22 P, it is undisputable that the ECJ has done a path towards a more protective view on what constitutes personal data. As mentioned previously, it held that no matter who gets the additional information needed to re-identify data subjects, data should be considered as personal as long as this information exists.

However, this dictum must not be overstated because it is very context-dependent. Indeed in the core of its argumentation the Court provides that “*as is apparent from paragraph 66 of the judgment under appeal, the description on the ERCEA website of the 70 or so projects funded by that agency, the host institutions of which were located in Greece, contained several key factors enabling internet users to find the information sought, such as the name of the project manager or the name of the host institution or even the amount of funding*” (Paragraph 62). The Court subsequently held that, with regard to this information, which was publicly available, browsing the description of these 70 projects did not involve a “disproportionate” effort (Paragraph 63).

In other words, the Court still stands for the relative approach, and it only states that re-identification through basic browsing is an example of a reasonable means likely to be used to re-identify data. It cannot be deduced from this decision where the bar between reasonable and unreasonable means should be set. Reasoning in an abstract fashion, one would ask whether the solution would have been the same if the projects described were several thousands. Once again, it shows that the Court’s reasoning still relies on the additional information available, who holds them and who may have access to them. Here, as the area of research was pretty narrow (only 70 projects) and given that any web user could have access to the information needed and browse to cross-check information, the Court logically concludes that re-identification does not involve disproportionate effort. Therefore, it should not be interpreted as a reversal of the Court’s doctrine.

Furthermore, in case C-604/22, involving IAB Europe, the Court used the same reasoning it had in *Breyer*. However, as it has been mentioned previously, it seemed to open the door to a more “objective“ approach on personal data. This “protective” approach materialises by considering that no matter who holds additional data, if data are re-identifiable through the use of additional information, data must be considered personal data.

Once again, this conclusion should be regarded with caution. Indeed, the Court argues that “*it is apparent from the documents before the Court, and in particular from the decision of 2 February 2022, that the members of IAB Europe are required to provide that organisation, at its request, with all the information allowing it to identify the users whose data are the subject of a TC String*” (Paragraph 48). The fact that IAB Europe can require additional information from its members seems to be the decisive factor to consider data processed by IAB Europe as personal data. The Court concludes from this background that “[*i*]t therefore appears, subject to the verifications which are for the referring court to carry out in that regard, that IAB Europe has, [...] reasonable means allowing it to identify a particular natural person from a TC String” (Paragraph 49).

This judgement is thus perfectly in line with *Breyer*. In *Breyer* the Court considered that there were, under German law, legal channels enabling a webservice provider to get additional data from internet service providers to re-identify data subjects whose IP addresses belong to. Here, IAB Europe can require additional information from its members so that the access to additional information is reasonably likely. It results that these data are personal in the hands of IAB Europe since the organisation can re-identify them using reasonable efforts.

In both cases, the judgments seem to be data subject-friendly at first glance, and they actually are, since the outcome is that data controllers process personal data and are thus subject to the GDPR. However, it is argued here that these two judgments do not question the definition of personal data nor the relative approach adopted by both the General Court and the ECJ. This relative approach may lead to great legal uncertainty since the concept of personal data does not rely on objective bases but, rather, on the capacity of third parties to re-identify data. Such assessment must be carried out on a case-by-case basis, which can potentially lead to different solutions despite similar facts.

Conclusion

Although the ECJ seems to adopt a more protective view than that of the General Court, it does not fundamentally rule out the relative approach on personal data, which can be problematic, in particular in the case of international transfer of data (see for instance what data protection authorities stated with regard to the use of [Google Analytics](#) prior the adoption of the [DPF](#)) or processing of sensitive data, such as [health data](#).

These cases are part of a broader debate on the extent of the definition of the concept of personal data. The forthcoming ECJ's judgment following [the appeal lodged by the EDPS](#) in the SRB v. EDPS case will be without any doubt a milestone to better understand the scope of data protection law within the EU.