Are personal data always personal? Case T-557/20 SRB v. EDPS or when the qualification of data depends on who holds them

Alexandre Lodie

Are personal data always personal? Case T-557/20 SRB v. EDPS or when the qualification of data depends on who holds them

European Law Blog, Blogpost 45/2023, 7 November 2023

By Alexandre Lodie

In case T-557/20 Single Resolution Board v. EDPS, the General Court had to settle an issue related to the extent of the definition of 'personal data' under Article 3 (1) of Regulation 2018/1725 (hereafter 'EUDPR'). This case takes place in the context of the adoption of a resolution scheme, involving the Single Resolution Board (SRB), in its capacity of Banking Union resolution authority, and a Spanish bank called Banco Popular. During the process of resolution, the SRB invited the shareholders to submit comments in order to assess whether they should be given compensation. To examine these comments, the SRB classified them and attributed them an alphanumeric code. Some comments were sent to an independent valuer, Deloitte, to help complete the assessment. Following these events, five shareholders filed a complaint before the European Data Protection Supervisor (EDPS) on the ground that they had not been informed of their personal data being transferred to a third-party. Without digging into too much detail, the EDPS agreed with the complainants that their personal data had been processed by Deloitte while they had not been informed of any transfer of their data by the SRB. SRB, for its part, claimed that data processed by Deloitte were not personal data. Basically, the General Court had to determine whether the comments held by Deloitte could be considered personal data.

To summarise the outcome of this case, the Court held that the transfer of comments which were attributed an alphanumeric code could not necessarily be considered as a transfer of personal data. Instead, it must be carefully assessed whether the data recipient is reasonably able to re-identify data subjects from the pseudonymised comments. The Court thus adopted a relative approach of what constitutes 'personal data' which, in our opinion, runs the risk of undermining the level of protection of personal data within the EU and the protection of personal data of EU citizens more globally.

This issue is particularly important since it does not only relate to the interpretation of the Regulation 2018/1725 but more generally to the way EU data protection law must be applied, including the General Data Protection Regulation ('GDPR'). As a matter of fact, the EUDPR expressly provides that these two regulations must be 'interpreted homogeneously' (Recital 5).

Pseudonymisation, anonymisation and the status of data as personal

Both the General Court and the EDPS base their reasoning on Article 3 (1) and Recital 16 of the EUDPR, which help understand the notion of personal data. Personal data are

information 'relating to an identified or identifiable natural person'. The key concept here is the identifiability criterion. Data do not need to relate directly to the individual to be considered personal. From this perspective data can also relate in an indirect manner to data subjects (see, for instance, Finck and Pallas). This is why the Court of Justice (ECJ) previously held in *Breyer* that '[t]he use by the EU legislature of the word 'indirectly' suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified' (para 41). In *Breyer*, the Court of Justice underlined that an IP address could be considered as personal data when combined with the additional information held by the internet service provider necessary to identify the data subject. The definition of personal data is thus inclusive since even IP addresses - which are allocated to machines, not to individuals - can be considered as personal data in some circumstances, as they can permit an indirect identification of data subjects, with additional information held by internet service providers.

To improve privacy and security, data controllers can, and are even invited to, implement data de-identification techniques designed to weaken the link between data subjects and their data. In other words, these techniques make the identifiability of data subjects harder. Typically, pseudonymisation and anonymisation are two de-identification techniques which are incidentally mentioned in Recital 16 of the Regulation. This provision emphasises that while anonymised data lie outside the scope of the Regulation, data which are merely pseudonymised remain personal data. This statement is quite logical because 'pseudonymisation is merely a method which can reduce the likelihood of identifiability of individuals' (See Spindler et Schmechel, here). Consequently, pseudonymised data remain personal data since the data subject is still identifiable through 'additional information' (Article 3 (6) of the EUDPR). On the other hand, anonymised data are no longer personal as the anonymisation process 'must be irreversible' (See the Opinion of the Working Party 29 on anonymisation here, p.5). Therefore, data subjects are not identifiable anymore once their data anonymised. If this distinction between anonymised and pseudonymised data is theoretically impeccable, it might raise some issues as regards the development of re-identification attacks carried out by malicious actors on said anonymised datasets. Still, this distinction remains relevant as it will determine the legal regime applicable to data.

As regards the SRB vs EDPS case, one of the arguments put forward by the EDPS was precisely that alphanumeric codes provided by the SRB to the comments made by the shareholders involved were indirectly related to the shareholders as data subjects. From this background, and according to the EDPS, the Court should have concluded that the comments transferred to Deloitte were pseudonymised and thus, personal data. This view seems to be in line with Recital 16 of the Regulation which expressly provides that pseudonymised data are personal data. However, the Court did not endorse the EDPS's view, as it retained a relative approach of what is personal data.

The relative approach to the concept of personal data

There is an ongoing debate among academics (see for instance F. Zuiderveen Borgesius, pp. 264-265) to determine whether the qualification of data as personal must follow a relative approach or an objective approach. According to the former view (see Finck and Pallas, p. 19), the nature of data as personal depends on the means reasonably likely to be carried out by the data holder to re-identify data, while, according to the latter view, the nature of data is dependent on the capacity to re-identify data, which must be assessed in an abstract manner, considering the inner robustness of the de-identification method used, and the abstract possibility of anyone to re-identify data. It is in this context that the SRB v. EDPS Judgment must be read.

As mentioned previously, the General Court rejected the arguments made by the EDPS. The Court specifically determined that the EDPS failed to assess whether Deloitte, as data recipient, had any reasonable means – legal means - to get the additional information held by SRB (the decoding database) to re-identify data subjects from the data received. Consequently, in the Court's view, the EDPS could not conclude that Deloitte processed personal data since the qualification of data as personal should have been made *in concreto* and not *in abstracto*. More specifically the Court stated that 'the EDPS merely examined whether it was possible to re-identify the authors of the comments from the SRB's perspective and not from Deloitte's' (para 103). Put differently, it cannot be asserted that data are pseudonymised or anonymised in an abstract fashion. Quite the opposite, the General Court asserted that the EDPS should have assessed whether, in this specific case, the data recipient, *i.e* Deloitte, had means reasonably likely to be carried out to re-identify data irrespective of whether data could be considered as 'pseudonymised' by nature.

This *dictum* builds upon the ECJ's previous ruling in the abovementioned *Breyer* case. Indeed, the Court concluded that the German institutions, as website publishers processed personal data (IP addresses) because there were, under German law, legal procedures enabling website publishers to ask identifying information to internet service providers (see also the note of F. Zuiderveen Borgesius on this case) in case of cybersecurity incidents. These legal channels thus constitute a means which was reasonably likely to be used by the website publishers to identify data subjects. This is why, in this context, website publishers were considered as processing personal data when processing IP addresses.

Here, the General Court uses a similar reasoning. It considers that Deloitte must be in position to receive the additional information – as the website publisher in *Breyer* – to be considered as processing personal data. The means likely to be used must be assessed as regards the efforts in terms of costs and time needed by the potential re-identifier to re-identify data (as underlined by Recital 16, DPAs and academics). From this perspective it

sounds logical to acknowledge that the Court endorses a relative approach of what is personal data.

However, on the other side of the coin, Recital 16 provides that the means reasonably likely to be used are those which can be carried out 'either by the controller or **by another person**' (emphasis added). From that perspective, the Court's reasoning is much more questionable. As a matter of fact, if we put the emphasis on this part of Recital 16, the logical outcome would be that, when at least one person is able to bridge the gap between the pseudonymised data and data subjects, the said data cannot be regarded as non-personal.

Advocating for this view underlines the importance of the qualification of personal data as such and not necessarily the contextual elements related to the data processing, and it was basically what the EDPS did by stating in its pleadings that '[p]seudonymisation does not lead to anonymisation. The Applicant confuses pseudonymisation and anonymisation and blurs completely the distinction intended by the EU legislator' (p.4). In other words, pseudonymised data are those which can be re-identified with the help of additional information while anonymised data lead to irreversible de-identification, as defended by the Working Party 29 (pp.5-6). Interestingly, the EDPS claims that this opinion is also derived from the *Breyer* Judgement, which suggests that the *Breyer* case can be used to advocate both the relative and the objective approach of personal data. Eventually, it is worth mentioning that the EDPS, in collaboration with the Spanish DPA released guidelines on anonymisation where it claimed that 'the use of 'additional information' can lead to the identification of the individuals, which is why pseudonymous personal data is still personal data'.

The consequences of adopting a relative approach

It is argued here that the definition of personal data as retained by the General Court in the SRB v. EDPS Judgment is likely to undermine the level of protection of personal data in the EU. If one were to follow the General Court's approach, the same dataset could be regarded as personal for one party (the one who holds the 'additional information') and non-personal for another (the data recipient who does not hold the information necessary to re-identify data subjects). This situation is a source of legal uncertainty. Indeed, since data protection regulations, such as the GDPR or the EUDPR only regulate the processing of personal data, it would mean that, in our scenario, one party will have to apply data protection law whereas the other will not have to (if data are said to be non-personal in the hands of this latter party). This could pose a significant issue with regard to data transfer to third countries. One could argue that since pseudonymised datasets are considered non-personal, at least in the hands of a data recipient who is reasonably unlikely to re-identify them, the latter will be free to transfer them to a third country. This means that EU

data protection law will no longer be applicable, hence increasing the risk of a loss of control over the data of European citizens.

Furthermore, that approach blurs the line between personal and non-personal data, which is likely to make the identification of the right set of rules applicable even harder. This issue is getting increasingly complex due to the multiplication of regulations within the EU which call into question the 'personal/non-personal' data dichotomy (see Lazarotto and Malgieri). The Data Governance Act ('DGA'), for instance, seems to embrace, to a certain extent, the uncertainty related to the exact delineation between personal and non-personal data. It creates a kind of hybrid category of 'highly sensitive' non-personal data (see Recital 24 and Article 5 (13) of the DGA). The transfer of these data to third countries will be limited when it 'may lead to the risk of re-identification of non-personal, anonymised data' (Article 5 (13) of the DGA). Therefore, it can be deduced from this provision that the distinction between personal and non-personal data is not clear-cut. It shows that the irreversible nature of anonymisation may be questioned and that some data initially considered non-personal can, in fact, be re-identified, consequently regaining their status as personal data.

Overall, it appears that recent cases decided by the General Court, as discussed here for instance, tend to restrain the definition of personal data in EU law. Indeed, in case T-384/20, the Court held that even though a person had been re-identified by journalists due to information published in a press release, this information could not be considered as personal data since an 'average reader' would not have reasonably been able to re-identify data. What is worth underlining in this case, beyond the specific and concrete facts, is that the Court settled this issue as if the personal knowledge of a third party could not be taken into account in the balance to qualify data as personal.

As a conclusion, it is getting increasingly difficult to understand what the notion of personal data precisely covers. In the SRB vs EDPS case, the Court suggests that even pseudonymised data can be considered as non-personal when the person who holds the data cannot reasonably re-identify them. This decision is part of a broader trend which tends to restrict the definition of personal data and thus the overall level protection of personal data of European citizens.

To conclude, it is worth noting that the Judgment has been appealed by the EDPS, in particular on the ground that the General Court did not 'give consideration to the notion of pseudonymisation'. The issue of the definition of personal data is therefore far from being definitively settled…

This work has been supported by the ANR 22-PECY-0002 IPOP (Interdisciplinary Project on Privacy) project of the Cybersecurity PEPR and by Inria action-exploratoire DATA4US.