T-384/20 OC v European Commission: The General Court Falls out of Line on Personal Data

By Tiago Cabral and Sophia Hassel

On 4 May 2022, the General Court shielded OLAF (European Anti-Fraud Office) from liability for the infringement of data protection rules, at the cost of departing from ECJ case law and widely accepted legal principles in EU data protection law. This decision was legally flawed (as we argue below) and indeed has already been appealed before the ECJ at the time of writing. Had the General Court arrived at the correct judgment – that is, that the press release by OLAF *did* contain personal data under Article 3(1) of Regulation 2018/1725 (on the processing of personal data by the Union institutions, bodies, offices, and agencies) – it would have been forced to answer also the question of damages and scope under the GDPR (General Data Protection Regulation). *OC v Commission,* therefore, missed its chance to be a landmark judgment. Currently, however, the judgment places the General Court on opposing paths with the ECJ, creating uncertainty, causing fragmentation in practice, and undermining the EU's efforts to harmonise data protection law.

1. The *OC v European Commission* case

The facts of *OC v European Commission* are as follows: an academic (the applicant) received EU funding for a research project and was discovered to have fraudulently claimed €245,525.43 in personal expenses. OLAF recommended that the European Research Council Executive Agency (ERCEA) take appropriate measures to recover the sums and initiate proceedings for fraud and use of forgery. Within a year, OLAF issued a press release on the matter labelled No. 13/2020.

In her action for damages against the EU (Articles 268 and 340 TFEU) before the General Court, the applicant argued – and the European Commission conceded this point (see para 56 of the judgment) – that a reader of the press release, using the data contained therein,

could identify several characteristics of the applicant, such as the fact that she was a Greek national woman, the amount of the funding, and the fact that her father worked at the same university.

In its ruling, the General Court, however, found that there was no personal data contained in the press release, because the applicant was not identified, and was not identifiable according to the means reasonably likely to be used. To determine whether the applicant was identifiable according to means reasonably likely to be used the General Court employed a test of the 'average reader' (*lecteur moyen* in the French version, para 76), which we argue is an overly restrictive approach to personal data. While this judgment is based on Regulation 2018/1725, it is also relevant from the standpoint of the GDPR, as the concept of personal data in both legal instruments are the same.

2. Legal Background

Article 3(1) Regulation 2018/1725 (and 4(1) of the GDPR) outlines the definition of personal data, which is (i) any information; (ii) relating to (iii) an identified or identifiable (iv) natural person (data subject). The applicability of the GDPR often turns on the question of 'identifiability.' This has been recognised by the European Data Protection Supervisor who stated that the 'essential criterion [for the definition of personal data] is the identifiability of the individual'.

Article 4 of the GDPR states that an identifiable natural person is 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.' Recitals 26 of the GDPR and 16 of Regulation 2018/1725 further clarify that '[t]o determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used'. This includes '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 ECJ tends to lean towards an expansive definition of personal data. In fact, it appears to expand the concept as necessary to ensure 'a high level of protection of the fundamental rights and freedoms of natural persons' without exceeding the limits required by legal certainty. This approach is seen in judgments such as *Breyer* (paras 31ff), *Scarlet Extended* (para 51), *Nowak* (paras 27ff) and very recently also in *Vyriausioji tarnybinės etikos komisija* (paras 117ff), in which the ECJ was addressing special category data but whose logic can be extended to personal data more generally. As an example, in *Breyer*, the ECJ decided that dynamic IP addresses should be considered personal data, even if the controller is unable to identify the data subject based on the IP address itself (paras 31ff).

Considering the ECJ's expansive interpretation of 'personal data', it is surprising that the General Court concluded that there was no personal data included in the press release in *OC v Commission*. Below, we will critique the argumentation of General Court for being

out of line with current ECJ case law and the regulatory guidance on the GDPR and Regulation 2018/1725. We believe these issues most likely also led the ongoing appeal the General Court's judgment (see C-479/22 P). Indeed, the appellant – OC – raises a similar point to our critique in her appeal, citing an ´incorrect interpretation of Article 3(1) Regulation 2018/1725' as her first ground.

3. *OC v. European Commission* was wrongly decided

There are two key problematic elements to the General Court's judgment that will be discussed in detail below: the newly created 'average or likely reader' test and the strict interpretation on the identifiability threshold of the data subject.

Average or Likely Reader

The General Court appears to accept that whether OLAF's press release contained personal data is tied not only to the 'means reasonably likely to be used' to identify the applicant but also by the 'average or likely reader' of said press release (para 76). The General Court goes on to disregard the actual identification of the applicant by a German journalist. It argues that this journalist could not be considered an average reader since he was a professional with wide qualifications and an insider's perspective due to his information network. Furthermore, the journalist appeared to be a daily reader of OLAF's publications, which the General Court considered to be unusual (para 80).

The concept of an 'average reader', whilst widely used in consumer law for example, has never been used before by the ECJ in data protection case law. Advocate General Szpunar did refer to the concept of average European consumer or internet user when analysing requirements for provision of information in *Planet49* (para 113). However, since this was not followed by the ECJ and the context is fairly different, it remains difficult to see why the General Court adopted this 'average reader' test in its judgment. The General Court's decision thereby effectively restricts application of the GDPR (and Regulation 2018/1725) to cases where someone can be identified by the average reader (as opposed to just being identifiable) and lowers the number of cases where this high level of protection will be enjoyed.

This directly contradicts the wide scope that the EU legislature intended to give to the concept of personal data (see Recital 26 and Article 4(1) of the GDPR and Recital 16 and Article 3(1) of Regulation 2018/1725). To understand how the ECJ adopts a widely different position we need to look no further than its recent judgment in *Vyriausioji tarnybinės etikos komisija* in which the ECJ argued that the objective of the EU's data protection legislation is to ensure (argued for the GDPR but also applicable for Regulation 2018/1725) 'a high level of protection of the fundamental rights and freedoms of natural persons, in particular of their private life, with respect to the processing of personal data concerning them' (paras 61 and 125), and opts for a wide interpretation of data protection concepts (in *Vyriausioji tarnybinės etikos komisija*, special category data and what could 'reveal' a person's sexual orientation) to protect this objective. With the ECJ favouring interpretations that protect fundamental rights and ensure the effectiveness of data

protection legislation, the use of this new and restrictive 'average reader' test of the General Court appears strange and out of line with the objective of EU data protection law.

However, above all, the General Court's interpretation is simply not desirable. One example where this would not be feasible is ID numbers. ID numbers without context will not make sense to an 'average person' but are nonetheless widely viewed as personal data. Under the interpretation of the General Court, if you were to publish someone's ID number on a social network, this would not be a disclosure of personal data as the average reader would likely be unable to identify the data subject. Additionally, following the General Court's interpretation, data breaches where millions of IP addresses and usernames (not real names) were to be released to the public would also not actually be data breaches, as the average person accessing the information probably would not able to identify anyone, even if a few more computer-savvy individuals can, sometimes with serious consequences (note that this contradicts the ECJ's judgment in *Breyer*, for example).

This interpretation also creates a strange scenario where a document (such as a press release), when drafted but before being made public, exists in a peculiar state where it both contains and does not contain personal data. Whether or not it contains personal data will depend on where it is released, on its average readership, if it is shared with a more knowledgeable readership in the future, etc. Additionally, by the General Court's logic in *OC v. European Commission*, one could argue that, if the same press release that was considered as not containing personal data were to be downloaded and sent directly to the same specialised German journalist, it would then contain personal data, because the likely and average reader of this direct communication would have the means to identify the data subject. The lack of legal certainty of such an approach is unacceptable.

Identifying a data subject

The General Court also appears to take a strict interpretation of what 'means are likely to be used to identify the data subject'. To decide whether the means can identify the data subject the General Court had to analyse 'all objective factors', such as costs, time, and technology (Recital 26 GDPR). The judgment concedes that by taking the information in the press release and searching ERCEA's website, it would be possible to isolate three funded projects and its data subjects (para 72). To do so, it would be necessary to comb manually through the descriptions of 70 projects in the ERCEA's website. Further use of a search engine would then allow the identification of the specific scientist. This procedure would certainly be (somewhat) time-consuming and bothersome, but far from impossible or even difficult. In fact, it would take no more than a couple of hours and require basic technical skills. Nonetheless, for the General Court, a couple of hours and basic technical skills are unlikely means to be used by someone trying to identify a data subject.

This is completely out of line with the ECJ's interpretation that, for data not to be considered personal, identification needs to be illegal or 'practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant' (see *Breyer* at para

46). By comparison, in *OC v Commission*, the risk of identification does not appear to be insignificant: the required manpower is one person, and, while time-consuming, the procedure would certainly not take a completely disproportionate amount of time.

4. What the General Court left unaddressed and the way forward for the ECJ

Since the General Court ruled that there was no breach, it did not go on to rule on damages. If the ECJ quashes the judgment, it will need to address the question of damages and clarify the scope of personal data.

Were the General Court to have decided that the press release included personal data, it would likely have found an infringement by OLAF due to the processing not respecting the: a) principles of minimisation, purpose limitation, and lawfulness, fairness and transparency; b) the need to have a proper legal basis for processing personal data; c) requirement to provide information to the data subject; d) the rules on compatible processing (para 31 of *OC v Commission*). The General Court would then have to assess the liability of OLAF under Article 65 of Regulation 2018/1725 (similar in function to Article 82 of the GDPR). Assessing this liability would have required examining among other things, damages, and causation.

Considering the facts of the case, it is quite possible that the applicant would not have been able to prove that she suffered material or non-material damage from the disclosure of her personal data and that this damage was caused directly by OLAF's press release. The German journalist, in particular, could have used other sources to identify her having an insider's perspective and a wide network of information (as stated by the General Court in para 77). Thus, the General Court would have to answer the question of whether an infringement of data protection law (in this case, the possible unlawful disclosure of personal data) by itself should be considered as having caused damage to the data subject, a matter which has caused great controversy under the GDPR (for example: [Knetsch, 2022](#), [O'Dell, 2017](#), [Alsenoy, 2017](#), and [Cordeiro, 2019](#)). In the context of the GDPR, this question has also been referred by a number of national courts to the ECJ in currently pending cases: for example, a preliminary reference by the [Austrian Supreme Court](#), – where AG Campos Sánchez-Bordona has opted for a fairly [restrictive interpretation](#) according to which a) a mere infringement of a GDPR provision is not in itself sufficient to merit compensation if that infringement is not accompanied by the relevant material or non-material damage and; b) the compensation provided by the GDPR does not cover mere upset which the person concerned may feel as a result of the infringement of provisions of the Regulation – and a reference by a [German court](#). In *OC v Commission*, the General Court regrettably missed the opportunity to be the first EU court to address this matter. If it had done so, this would have clearly been a landmark judgment and potentially paved the way also for the ECJ.

When viewed in the context of earlier ECJ decisions, the General Court's narrow interpretation of personal data in *OC v European Commission* appears incorrect. The pending appeal of *[OC v European Commission](#)* could compel the ECJ to build upon its previous interpretations of the concept of personal of data, particularly the concept of

'identifiability'. It will have to decide whether the new ideas introduced by the General Court are at all relevant and, thus, in any case, have to provide further clarification on the scope of application of the GDPR and Regulation 2018/1725. The issue is certainly significant also from a practical standpoint. In fact, AG Bobek already drew attention to it (suggesting that the GDPR could become the law of everything) in his Opinion on C-245/20 (para 58). By using the phrase 'the law of everything', Bobek implies that the ECJ's failure to clearly develop the GDPR's material scope has made the GDPR expansive to the point where compliance is impossible and widespread disregard of the GDPR is required.

The General Court fails to provide a real explanation for why it is making decisions that contradict current ECJ's case-law. As a result, it squandered an opportunity to raise its objection in line with Bobek's concerns about the societal and economic consequences of an overly broad interpretation of personal data, missing the chance to initiate a valid debate about personal data's 'unlimited' scope. In the appeal, we believe the ECJ should disregard the General Court's position (for the reasons established in our conclusion) and address, directly and clearly, the issue of damages, compensation, and scope of interpretation of the concept of personal data.

Conclusion

The case of *OC v. European Commission* has largely gone unnoticed, with little written about it, but the data protection issues it addresses (or should have addressed) are extremely pressing and relevant at this time. Enforcement of EU data protection law has increased (both by national supervisory authorities and through private enforcement), and new EU legislation continues to build on the framework established by the GDPR. Thus, sooner rather than later, questions on damages and scope will come up again. *OC v European Commission* currently places the ECJ and the General Court on opposing paths, creating uncertainty for both data controllers and data subjects.

The General Court's line of reasoning regarding the means likely to be used to identify a data subject and the newly created concept of average reader/user are extremely restrictive. To realise truly the possible effects of the General Court's decision on the protection on privacy and personal data protection in the EU, it is important to consider that if the ECJ were to uphold the General Court's judgment, it would significantly restrict the scope of application of Regulation 2018/1725 (and indirectly also of the GDPR). In fact, numerous situations in which we nowadays consider personal data to be processed and, thus, enjoy a higher level of protection, would fall outside the scope of protection. If the General Court's interpretation were to prevail, it would result in a much more restrictive data protection regime, limiting the protection afforded to data protection and privacy rights in the European Union, directly affecting Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and Article 16 TFEU.