_swissprivacy.law

Clarification on the qualification of a processing, a processor, a controller and the associated responsibility

Hermine Lacour, le 18 juillet 2023

The preliminary ruling from May 4, 2023, is a welcome clarification of different articles of the GDPR, the European Court of Justice being given an opportunity to bring valuable information on the interpretation of the notions of processing, controller and processor, as well as the application of the mechanism of administrative fines provided by the art. 83.

Case C-683/21 – Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos vs Valstybinė duomenų apsaugos inspekcija, Request for a preliminary ruling, Opinion of the Advocate General Emiliou (May 4, 2023)

Introduction

The concrete application of the GDPR is still raising questions, and the case before the Regional Administrative Court of Vilnius, Lithuania (Vilniaus apygardos administracinis teismas, "Court"), is no exception. By requesting a preliminary ruling on different articles of the GDPR, the Court is giving the European Court of Justice an opportunity to bring more clarity on the interpretation of the notions of processing, controller and processor, as well as the application of certaine fines. As such, the opinion rendered by the advocate general Emiliou is a goldmine for any data protection professional

First, we need to explain the facts leading to this preliminary ruling, which takes us back to the first months of Covid in Europe. In 2020, the Lithuanian authorities, as in many other countries, decided to develop a mobile application to allow contact tracing. The facts take place within only two months.

The National Public Health Centre (Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos, "NVSC") is appointed by the Ministry of Health on March 24, 2020, to organise the development and acquisition of such an application, named "Karantinas". A private company, IT sprendimai sėkmeim ("ITSS"), is selected on March 27 2020, by the NVSC, which communicates the scope of the assignment. Only a confidentiality agreement is then drawn up, and no development contract is made.

Karantinas is released for Android on April 4 2020 and for iOS on April 6 2020 and from then remains available for download and use. The users can see both ITSS and the NVSC mentioned as controllers in the documentation of the application, despite the lack of contract and the absence of acquisition of the application.

By decision of April 10, 2020, the Ministry of Health instructed the NVSC to proceed with the acquisition of Karantinas. The procedure is initiated but failed, and by decision of May 15, 2020, the NVSC request ITSS to stop using or referring to the NVSC in the privacy policy available in the application.

This could have been the story of a failed collaboration if the State Data Protection Inspectorate ("Inspectorate") had not opened an investigation about Karantinas, against both the NVSC and ITSS, on May 18, 2020. This investigation led to the suspension of the application on May 26, 2020, and a decision on May 24, 2021, establishing the infringement of art. 5, 13, 24, 32 and 35 GDPR, and imposing an administrative fine against the NVSC and the ITSS as joint controllers.

The NVSC has challenged the decision before the Regional Administrative Court of Vilnius, which requested a preliminary ruling on different aspects of the GDPR :

- The first three questions concern the concept of controller as defined by 4 par. 7 GDPR, to determine if, respectively, the fact that a procurement procedure has not been concluded, the fact that the entity has not approved or acquired the rights on an application, and the fact that the entity has not performed the processing itself, are relevant for the qualification of controller.
- The fourth question is about the concept of controller and the concept of processing, as defined by 4 par 2 GDPR, and to know if the fact that a processing is limited to test operations has an impact or not on the qualification of a processing and incidentally on the qualification of a controller.
- The fifth question is to clarify the scope of the joint controllership, as per 4 par. 7 and 26 par. 1 GDPR, and to determine which kind of elements are required for such a qualification.
- Finally, the sixth question is important, and regards whether the element of fault is required or not for the application of the administrative fine as provided by 83 par. 1 GDPR, and if a local regulator is allowed to add this requirement or not in the law.

On May 4, 2023, the opinion of the advocate general is released, shedding light on these topics. More than detailing the six sub-questions raised, we noted two interesting principles

arising from these questions. These principles will be used to structure the present commentary : the analysis of the situation for the applicability of the GDPR must be factual (I), and an important clarification on the scope of the administrative fines as foreseen by art. 83 par. 1 GDPR (II).

1. The factual analysis as a requirement for the application of the GDPR

The answers to the fifth first questions clarify the method to qualify what is a controller (A) and a processing (B) according to the GDPR.

A. Qualification of a controller and joint controller

Through the facts presented above, we can see that if the NVSC had the impulsion of the project, and defined the main lines, no formal collaboration had been established, as no agreement had been signed between the parties. Furthermore, the application had never been acquired and the NVSC even expressly asked not to be mentioned anymore in the associated documentation, including the privacy policy.

Though the answer of the advocate general is clear : the absence of a contract or formalization is not an obstacle at the qualification of a controller. What matters according to the GDPR and the guidelines of the European Data Protection Board (EDPB) on the question are the reality of the facts : if an entity has had an effective role in the definition of the purposes and the means of the processing, this person should be qualified as a controller and bear the associated responsibilities. The advocate general refers the case back to the Court to assess the facts in order to deduce the appropriate qualification. We personally share the view of the advocate general, and, in our opinion, any other direction would have led to disastrous practical consequences. If a controller could escape the qualification by not contracting or terminating an agreement, the entire ecosystem would have been at risk, with actors disappearing to elude their responsibility.

The same logic applies to the concept of joint controller, though the current opinion does clarify an additional element. To be considered joint controllers, two entities must both have this effective role in the definition of the means and purposes and exercise these roles "jointly". Based on the abovementioned guidelines 07/2020, the opinion states, "*such joint participation can exist in different forms. It can result from a common decision taken by two or more entities or it can merely result from converging decisions of those entities. Where the latter is the case, it only matters that the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on*

the determination of the purposes and means of the processing – meaning, in essence, that the processing would not be possible without the participation of both parties".

In practice, we can imagine that the interpretation of "jointly" may raise difficulties, as this opinion would go in the direction of an effective joint control, in a rather restrictive interpretation. The opinion does quote the pre-GDPR decision Fashion ID GmbH of July 29, 2019, concerning the insertion of the Facebook module on a website. In this decision, the ECJ had qualified the insertion and the associated transfer of data as a joint controllership, without assessing if the user of the widget had any actual power on the determination of the means and purposes relating to Facebook's activities, aside from the provision of personal data. Considering the imbalance between the actors in this configuration, we wonder if this activity would still be qualified as a joint controllership, or a controller-to-controller transfer, due to the independence of the two processing activities, and the absence of influence of each controller on the processing of the other. Future decisions will surely bring new elements on this open reflection.

In any case, this factual interpretation is not limited to the qualification of the parties and also applies to the processing *per se*.

B. The irrelevance of the purpose for the qualification of a processing

In the elements presented to the court, the NVSC contests the qualification of processing, and the qualification of controller, arguing that the operations were for test purposes. This raises the question of the relevance of the purpose to qualify a processing : does a processing need to be public, turned toward the outside to be qualified as such ? From a certain perspective, the question may be raised : in a test environment, the risks for privacy should be mitigated, as the accesses from third parties should be more limited, the data is not refreshed, and the operations do not reflect any reality.

The opinion quotes the definition of a processing according to the GDPR : "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means […]". The advocate general emphasizes that the word "any" leads to only one interpretation, which is that all operations on personal data should be considered, regardless of the factual purpose. Though an important clarification is made, relating to the scope of such processing, the testing activities and the "live" operations constitute two different processing, with different scopes, recipients, purposes and so on. As such, the factual purpose of the processing does not matter for the qualification, but might be relevant for the constitution of the records of processing activities , as provided by art. 30 GDPR.

In our opinion, this interpretation makes absolute sense in view of the practice. Indeed, testing activities will rarely be performed in a purely internal infrastructure, and different actors and recipients will be involved. Furthermore, this extraneity leads to potential risks, and even if the data are not related to any reality, mixing real data to fake data might create an even bigger risks for the privacy of related individuals. We cannot emphasize enough the need to create proper test datasets, that can be based on real data, but properly anonymised. We remind here that anonymization for such a purpose is a processing activity, which can be justified by the legitimate interest of the controller. Though, this operation may not be solely decided and conducted by a processor.

Further in this opinion, the importance of the analysis of the facts for the proper enforcement of the GDPR is not limited to qualification, but also for the application of the administrative fines under the GDPR.

II. The clarified scope of the administrative fines as per art. 83 par. 1

The advocate general interprets the sixth question of the court as dual, first to determine if an element of fault is necessary to impose such a fine (A), and second if a controller may be sanctioned even if the infringement was technically committed by its processor (B).

A. The requirement of an element of fault

The opinion reminds the context around the "new" fine mechanism. Before the GDPR, sanctions were left to the discretion of Member States. The new regulation harmonises and defines through its art. 83 the conditions for the imposition of administrative fines. This article defines the principle, a fine if the regulation is infringed, and the conditions of imposition, including the elements to be taken into account by the local authority to determine its amount (cf. www.swissprivacy.law/162). In this context the question of the fault is raised.

The advocate general examines all the possible aspects, but concludes with two important elements : the fault is required, and this requirement is not left to the discretion of the national regulators. The opinion states that such a mechanism could be considered of criminal nature, considering its dissuasive purpose, and, as such, falls in the scope of the art. 49 of the Charter of Fundamental Rights of the European Union ("Charter"). Then, based on this Charter as well as the jurisprudence of the European Court of Human Rights, the element of fault appears as a requirement to impose such a fine. Despite the underlying logic, this interpretation could have been quite puzzling if the advocate general had not clarified the degree of fault necessary.

If a fault is necessary to impose a fine, the opinion states that the requirement is a fault or a negligence of such a low degree of severity that the cases where the fault would not be present seem rather virtual. Literature, as quoted in the decision, had already taken position in this direction, considering a failure to take action already constitutes not only negligence but gross negligence. Then, this will be on the local authority for data protection and the courts to qualify the fault according to the facts in order to impose an administrative fine for infringement of the GDPR.

Based on our experience, considering the number of points of control and the possibilities for a controller to impose technical and contractual measures to ensure the security of a processing and the compliance with the GDPR, we agree that such threshold must be low, but that a threshold must exist. For example, a case of extreme social engineering, violence and physical coercion, where all the best measures would not have prevented much, it would seem unfair to impose a fine for a factual breach. Then, on the contrary, a higher threshold to qualify the negligence could lead to elude the responsibility of the controller for the actions of its processor, which is also a point of clarification in this opinion.

B. The possible fine of the controller for the actions of its processor

In the case, the NVSC could have argued that only ITSS technically processed the data, and that NVSC did not take part in the actual processing. On this point, the opinion states that a controller does not need to process any data to be qualified as a controller, as long as this entity has an actual control on the definition of the purposes and means on processing.

The advocate general clearly states that, as long as the processor is acting within the mandate given by the controller, and according to the lawful instructions given by the controller, the responsibility is ultimately on the controller. On the contrary, if the processor is exceeding the scope of its mandate, then it should be considered as the controller for these activities, and the original controller could not be sanctioned by a fine as pursuing the art. 83 GDPR. It is up to the local authority for data protection as well as the courts to qualify the facts and determine if the processor acted within its mandate or beyond.

This part of the opinion appears more confusing to us. From the one hand, if we consider that these administrative fines are of a criminal nature, only the one who has committed a fault may be sanctioned because of it, and then the processor who went rogue is not under the responsibility of the controller. Nevertheless, from the other hand, the controller has the power to instruct as well as to audit the processor, as provided by art. 28 par. 3 let. h GDPR. A processor exceeding its mandate could then constitute a negligence of the controller, not

paying sufficient attention to its processor according to the above development.

Combining this consideration and the factual interpretation for the enforcement of the GDPR, we see two cases in practices.

In the first, the controller has the main economical power and the processor is dependent from the controller, e.g. a small company acting according to the instructions of a multinational. Here the controller has the means to ensure the processor will only operate according to its mandate, and the processor cannot afford any liability due to a careless activity.

A second scenario, where the processor has the economic advantage over its controller, e.g., a giant IT versus a small company acting as controller, is not as straightforward. Indeed, if the controller has legal possibilities to ensure the processor is not overstepping, this economic imbalance may lead to restricting the rights of the controller by imposing certain clauses in a contract. A glance at the contracts of different IT giants is insightful in this regard : the controller has to contractually limit certain rights, such as limiting the additional instructions or abandon the right to proceed with on-site audits, or the processor allows itself to process data for its own legitimate interests regardless of the instructions of the controller.

To us, the advocate general does cover these two cases with the present opinion. The detailed analysis of the facts would both avoid that any party would elude its responsibility thanks to a canny contractual structure, and the situation where a party could be fined due to an economic impossibility to enforce its rights.

This opinion is insightful at many regards and brings clarification around critical notions of the GDPR, and we have no doubt that the associated decision will be of a strong value.

Proposition de citation : Hermine LACOUR, Clarification on the qualification of a processing, a processor, a controller and the associated responsibility, 18 juillet 2023 *in* www.swissprivacy.law/240

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.