EUROPEAN DATA PROTECTION SUPERVISOR

EDPS OPINION
ON THE STATUS OF PRIVATE SERVICE PROVIDERS VIS-À-VIS THE EUROPEAN INVESTMENT BANK
(Case 2021-0750)

1. INTRODUCTION

1. This Opinion regards the status of private service providers, and in particular external legal advisers, in relation to the processing of personal data that they carry out either in the context of providing their services to the European Investment Bank ('EIB') or in order to comply with separate legal obligations linked to such a provision of services. This Opinion is also relevant to other Union institutions and bodies ('EUIs').

2. The EDPS issues this Opinion in accordance with Article 58(3)(c) of Regulation (EU) 2018/1725 ('the Regulation').

2. BACKGROUND INFORMATION

3. The Data Protection Officer ('DPO') of the EIB has consulted the EDPS as to the status of private service providers, and in particular external legal advisers, in so far as they carry out processing of personal data either in the context of providing their services to the EIB or in order to comply with separate legal obligations linked to such a provision of services.

4. The EIB uses various external advisers for obtaining legal advice on core operational matters (such as lending agreements) or litigation matters. In this context, the EIB shares with external legal advisers personal data of various data subjects, both EIB staff and other individuals from whom the EIB has collected personal data in the course of its operations, e.g. consultants, beneficiaries, etc. The EIB also indicates that external advisers may be based both inside and outside the Union, and may or may not be subject to the GDPR.

5. More specifically, the EIB asks whether such service providers, as well as other private service providers that they procure services from (such as auditors, insurance providers or health-care professionals) should be considered processors, joint controllers with the EIB or separate controllers.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

6. In this regard, the EIB has taken the view that in particular legal advisers should be considered processors since the EIB determines the purpose (providing legal advice) and essential elements of the means of processing, such as the type of personal data to be processed, the retention period, limitations to transfers to certain territories etc. This is taken into account in the framework agreements that the EIB entered into with various external advisers. Those advisers as processors nevertheless maintain a significant degree of autonomy in providing their services, in particular in their field of expertise, and determine non-essential elements of the means of processing of the personal data. The EIB stresses that the advisers may make certain decisions as to the processing of the personal data, however in compliance with the relevant framework agreements and the instructions provided by the EIB. According to the EIB, such instructions do not compromise the advisers' independence in providing the requested legal advice.

7. However, the EIB indicates that certain external advisers are of the view that they should be considered either separate or joint controllers, since they supposedly determine the purpose and means of the processing and have a significant degree of independence and since regulated professions are subject to specific legal obligations.

8. As a specific example, the EIB refers to the provision of services by banks, both within and outside the European Economic Area ('EEA'), in the context of opening bank accounts by the EIB. In such situations, the relevant banks consider themselves to be controllers since the contractual relationship with the EIB as their client is based on their standard terms and conditions. In this instance, the EIB considers that separate controllership is acceptable.

9. In light of the above, the EIB questions how to qualify the relationship between the EIB and such service providers as regards the processing that goes beyond the mandate given by the EIB, for example to comply with their obligations under anti-money laundering or anti-terrorism laws. It also questions whether such qualification influences or compromises the allocation of roles of the processing carried out for the provision of the services requested by EIB. In particular, it highlights the question as to the proper allocation and documentation of roles (rights and obligations) between the EIB and the service providers, in both of the above situations.

3. LEGAL ANALYSIS AND RECOMMENDATIONS

3.1. Qualification of service providers

10. The qualification of a service provider engaged by an EUI, either as a (separate or joint) controller or a processor with regard to the processing that it carries out in relation to the provision of services, will depend on various factors. In this regard, it is important to note that in accordance with Article 4(7) of Regulation (EU) 2016/679 ('GDPR') as well as Article 3(8) of the Regulation[1], **controller** means the entity which, alone or jointly with others, **determines the purposes and means** of the processing of personal data. Unless controllership is determined by Union or Member State law, it stems from an analysis of the **factual elements** or circumstances of the case, in particular by

[1] Since this Opinion concerns private service providers who are in principle subject to GDPR, the definition as provided for in the GDPR is referred to. However, elements relevant in this regard also apply, *mutatis mutandis*, to controllers as defined in Article 3(8) of the Regulation.

establishing who has influence over the processing by virtue of an exercise of decision-making power[2].

11. In other words, the actual degree of influence of a party in determining both purposes and means may identify its role as a controller. However, this does not imply that a party has to equally determine both in order for it to be considered controller. While it must determine the purpose of the processing ('why'), it might only determine the essential elements of the means of processing ('how')[3]. The processor may therefore determine non-essential elements of the means without assuming controllership.

12. Essential elements of the means are closely linked to the purpose and the scope of the processing, such as the type of personal data processed, the categories of recipients and the categories of data subjects. On the other hand, non-essential elements of the means concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures[4].

a) Service provider as processor

13. The essence of the role of a **processor** lies in the processing of personal data on behalf of the controller[5]. This means that the processor is serving the controller's interests in carrying out a specific task and that it is thus following the instructions set out by the controller, at least with regard to the purpose and essential elements of the means of processing[6].

14. In this regard, the fact that the processor acts on behalf of the controller does not necessarily undermine its **independence** in carrying out specific tasks assigned to it. The processor may enjoy a considerable degree of autonomy in providing its services, also in terms of carrying out its core tasks. However, this is due to the controller choosing to give that operational independence to the processor. Indeed, the processor may advise or propose certain measures, in particular in its field of expertise, but it is up to the controller whether to accept such advice or proposal, after having been fully informed of the reasons for the measures, what the measures are and how they would be implemented[7].

15. The activities carried out by service providers engaged by an EUI may involve a data processing operation or a set of operations which have a single purpose, or a sequence of distinct (sets of) processing operations, each of them with its own purpose. In practice, this may mean that the control exercised by the EUI may extend to the entirety of processing at issue but may also be limited to a particular stage of the processing[8]. More specifically, the EUI will be considered as controller, and the service provider as processor, for processing operations for which the EUI determines both the purposes and (essential) means. This may mean that within the context of a specific service provided, the roles of controller and processor, respectively, might not be attributed to the same entities for all processing operations related to such a provision.

---

[2] EDPB Guidelines 07/2020 of 7 July 2021 on the concepts of controller and processor in the GDPR, para. 20.
[3] EDPS Guidelines of 7 November 2019 on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 9-10.
[4] EDPB Guidelines of 7 July 2021, para. 40.
[5] See Article 3(12) of the Regulation.
[6] EDPS Guidelines of 7 November 2019, p. 16.
[7] Ibid., p. 16-17.
[8] EDPB Guidelines of 7 July 2021, para. 42.

b) Service provider as separate controller

16. In particular, the service provider may be considered **separate controller** with regard to certain processing operations where it is subject to specific **legal requirements** in terms of processing personal data, for which the EUI does not determine the purposes nor the means. This may occur during[9] or after[10] the provision of the service, in principle with regard to processing operations that are not necessary in order to carry out such a provision but are, however, required by law, in particular as regards regulated professions (for example under anti-money laundering, anti-terrorism and other reporting obligations). In those cases, the personal data are the same but the purposes and means of the processing are different.

17. Furthermore, where service providers, and in particular external legal advisers, act with a significant **degree of independence** in their provision of services, they may, under certain circumstances, be considered as controllers for the processing operations carried out in the context of such a provision. This may be particularly true where the procurement of services does not specifically target the processing of personal data[11], however this circumstance cannot in itself lead to the conclusion that the service provider is to be considered controller[12]. The existence of such controllership by the service providers will largely depend on the **level of instructions** given by the EUI. Should the service provider be given sufficiently detailed instructions on the processing of personal data, entailing a sufficient degree of control by the EUI, it would nonetheless be considered processor[13].

18. Additionally, certain services providers, especially those that wield substantial contractual power over the EUI due to their market position[14], may conduct their business in accordance with standard **terms and conditions** that they have unilaterally drawn up, thereby leaving only limited choice to the EUI concerned. However, this alone is not a sufficient basis to conclude that such a service provider is to be considered controller[15]. Depending on the content of such terms and conditions, in particular as regards the processing of personal data, as well as any supplementary contractual arrangements that the EUI might be able to ensure, such a service provider may be processor or (separate or joint) controller.

c) Service provider as joint controller with the EUI

19. In this regard, it is in principle also necessary to assess whether processing operations having seemingly different purposes should be considered as one set of operations at a "macro-level", in fact pursuing a joint purpose using jointly defined means[16]. The latter could imply **joint controllership,** which requires an arrangement between the joint controllers determining in a transparent manner their respective responsibilities for

[9] E.g. to comply with a requirement to organise and transmit certain personal data to designated public authorities.
[10] E.g. to comply with a requirement to retain or otherwise further process the personal data following the provision of the service.
[11] EDPB Guidelines of 7 July 2021, para 27, law firms example.
[12] EDPB Guidelines of 7 July 2021, para. 83.
[13] EDPB Guidelines of 7 July 2021, para. 40, accountants example.
[14] Such as banks, as also noted by the EIB.
[15] EDPB Guidelines of 7 July 2021, para. 110.
[16] EDPB Guidelines of 7 July 2021, para. 43.

compliance with their data protection obligations as well as their respective roles and relationships vis-à-vis the data subjects[17].

20. However, the EDPS encourages EUIs making use of services provided by private companies to make sure that such **companies only act as processors** for related processing operations. While EUIs are able to outsource services when carrying out the tasks assigned to them by law in the public interest, it would not be appropriate for a private party to exercise the kind of influence that would result in it being a joint controller[18]. This is especially the case when the processing of personal data lies at the core of the service contract (for example IT services in relation to personal data management). The EDPS welcomes the fact that the EIB has taken that into account in its framework agreements with service providers, such as external legal advisors.

d) Conclusion

21. The qualification of an EUI's service provider as separate controller, processor or joint controller should be the **result of careful consideration** by the EUI on the role it aims and has to play depending on the nature, scope, context and purposes of the processing. Moreover, the concepts of controller and processor are functional: they aim to **allocate responsibilities according to the actual roles of the parties**[19]. Therefore, the allocation of the roles of the parties in the contract should stem from a careful analysis of the factual circumstances of the envisaged processing. The formal/artificial designation, in a contract, of an actor either as controller or processor, whereas it does not match reality, would be inoperative.

3.2. Recommendations

22. In accordance with Article 29(1) of the Regulation, the controller is to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject. This obliges the controller to assess whether the guarantees offered by the processor are sufficient. In doing so, the controller may take into account whether the processor provides adequate documentation, information security policies, external audit reports, certifications, etc.[20]. Moreover, the controller should take into account the processor's expert knowledge, reliability and its resources[21]. In addition to that, the controller should carefully assess whether the service provider in question allows it to exercise a **sufficient degree of control**, taking into account the nature, scope, context and purposes of processing as well as the potential risks for data subjects[22]. A service provider may offer a predefined service as a processor as long as the EUI as the controller makes the final decision to actively approve the way the processing is carried out, at least concerning the essential elements of the means of processing[23].

[17] Article 28(1) and (2) of the Regulation; see also EDPB Guidelines of 7 July 2021, para. 46-72, and EDPS Guidelines of 7 November 2019, p. 22-31.
[18] EDPS Guidelines of 7 November 2019, p. 23.
[19] EDPB Guidelines of 7 July 2021, para. 12.
[20] Ibid. p. 18.
[21] Recital 51 of the Regulation; see also EDPB Guidelines of 7 July 2021, para. 94-99.
[22] EDPB Guidelines of 7 July 2021, para. 83.
[23] Ibid. para. 84.

Recommendation 1: With regard to the processing operations for which the EIB is to determine the purposes and essential elements of the means of processing, the EIB should consider not engaging a service provider which gives an indication before the conclusion of a service contract that it does not agree to being a processor, nor to complying with a processor's obligations under the Regulation. This may be particularly relevant where the processing in question is important for reasons of public interest underlying such processing[24].

23. As elaborated above[25], the service provider may be, under certain circumstances, nonetheless considered controller with regard to the processing operations carried out in the context of the provision of services, in particular where it has a significant degree of independence and has not received detailed instructions as to the processing of personal data. This may be particularly likely where the services are provided in accordance with standard terms and conditions drawn up unilaterally by the service provider.

Recommendation 2: In order for private service providers to only act as processors, the EIB should provide sufficiently detailed instructions as to the processing of personal data, in order to maintain its controllership, wherever this is feasible in view of the specific circumstances related to the services provided. In this regard, the EIB should make reasonable efforts to choose a service provider that will agree to carrying out the relevant processing operations in accordance with the EIB's instructions[26]. As elaborated above[27], in order for the EIB to maintain a sufficient degree of control over the processing, it would suffice that it actively approve the manner in which the processing of personal data is carried out, even if that is, to a greater or lesser extent, exhaustively proposed by the service provider.

Recommendation 3: In principle, joint controllership with private service providers should be avoided. The EIB should, in so far as possible, rather aim at determining the purposes and the essential elements of the means of processing concerned, thus keeping control over the processing. Where that is not feasible and joint controllership cannot be avoided, the EIB should ensure full compliance with Article 28 of the Regulation, taking due account of the nature of the personal data concerned and the risks to the rights and freedoms of the data subjects in the determination of the respective responsibilities of the joint controllers.

24. Furthermore, as provided for in Article 29(3) of the Regulation, the controller should ensure, by way of a **contract or another legal act** under Union or Member State law that is binding on the processor with regard to the controller, that the service provider in its role as processor receives sufficiently detailed instructions as regards the means of the processing as well as all other elements that must be set out therein on the basis of that Article[28].

Recommendation 4: When acting as the controller, the EIB should ensure that the contract or another legal act under Article 29(3) of the Regulation takes into account the

[24] In particular, this may be the case where processing is based on Article 5(1)(a) of the Regulation.
[25] See paragraphs 17 and 18 of this Opinion.
[26] The EDPS acknowledges that with regard to certain services and areas of expertise that may not be feasible.
[27] See paragraphs 14 and 21 of this Opinion.
[28] See also EDPB Guidelines of 7 July 2021, para. 100-145. The EIB may consider it necessary, on a case by case basis, to determine in greater detail, in a contract or another legal act, also the non-essential elements of the means of processing, thereby providing the processor with a more comprehensive set of instructions.

specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject[29].

25. Making sure that a contract or another legal act contains all the relevant provisions is important not only to ensure compliance with the Regulation but also to clearly delineate, prior to any processing, the responsibilities of the EUI and the service providers, including their respective roles of controller and processor. In this regard, the EDPS takes note of the concerns presented by the EIB with regard to the amount of control that it may have over the personal data concerned. In its capacity as controller, the EIB ensures such control mainly by way of a contract or another legal act as elaborated above. Nonetheless, the contract should not be a mere formal allocation of roles: the EIB should keep an actual sufficient degree of control on the processing, otherwise the relationship could be requalified as a separate controllership.

26. In any case, for processing operations that may be carried out by service providers in order to comply with their legal obligations and for which the EIB does not determine the purposes and means, the EIB cannot be considered controller. In relation to such processing operations, the EIB is therefore not bound by obligations incumbent on controllers in accordance with the Regulation, including to ensure the insertion of required provisions in a contract or another legal act.

Recommendation 5: The EIB should nonetheless consider referring in the contract with the service provider any specific obligations[30], which the service provider is subject to and which are known prior to entering into a contractual relationship. The purpose of such a reference would not be to establish the EIB's controllership as regards the processing operations stemming from such obligations but rather to obtain greater clarity and certainty as to the processing of personal data.

27. Furthermore, should a processor act beyond its mandate by infringing the contract or another legal act or making decisions about the purpose and the essential elements of the means of processing, it may qualify as a controller[31]. This would depend, inter alia, on the scope of the deviation, for example when such behaviour serves to ensure compliance with data protection principles[32].

28. Additionally, the EIB indicates that its external advisers and other service providers may be based both inside or outside the Union/EEA.

Recommendation 6: The EIB should ensure compliance with Chapter V of the Regulation as regards any **transfers** of personal data to third countries (outside the EEA) or international organisations. In particular, the EIB should ensure that the contract or another legal act binding on the processor specifies the requirements for such transfers in accordance with the Regulation, also in view of any supplementary measures that may be required in order to ensure an essentially equivalent level of protection[33].

[29] Recital 51 of the Regulation; see also EDPB Guidelines of 7 July 2021, para. 113.
[30] As referred to in paragraph 26 of this Opinion.
[31] See also Article 29(10) of the Regulation.
[32] EDPS Guidelines of 7 November 2019, p. 17.
[33] See also EDPB Recommendations 01/2020 of 18 June 2021 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0.

4. CONCLUSION

29. The EDPS has made several recommendations to ensure compliance of the processing with the Regulation, in particular as regards the obligations provided for in Articles 28 and 29 and Chapter V of the Regulation.

30. In light of the accountability principle, the EDPS expects the EIB to implement the above recommendations accordingly and has decided to **close the case**.

Done at Brussels on 6 April 2022

[e-signed]

Thomas ZERDICK, LL.M.