EUROPEAN DATA PROTECTION SUPERVISOR

EDPS OPINION ON THE PROCESSING OF CERTAIN DATA CONCERNING HEALTH DUE TO COVID-19 (Case 2021-0425)

1. INTRODUCTION

- This Opinion regards the processing of certain data concerning health by the European Investment Bank ('EIB') related to medical vulnerability to COVID-19.
- The EDPS issues this Opinion in accordance with Article 58(3)(c) of Regulation (EU) 2018/1725 ('the Regulation').

2. BACKGROUND INFORMATION

2.1. Facts

1. The College of Staff Representatives ('the College') of the EIB has brought to the attention of the EDPS several concerns regarding requests for data concerning health by the EIB's Occupational Health Service ('OHS') to establish medical vulnerability to COVID-19 of staff members and members of their household, as well as regarding the use of vulnerability status of staff members by persons outside the OHS.
2. According to the College, the EIB recommended, on 9 March 2020, that vulnerable persons and pregnant women stay at home due to the COVID-19 pandemic. Later, the possibility of teleworking was extended to staff who lived in the same household as a person (particularly) vulnerable to COVID-19. Procedurally, eligible staff were to write an email to their direct supervisors, informing them of their vulnerability status and their intention to telework, and to only contact the OHS in case of doubt.
3. Subsequently, this procedure was modified by requiring staff who wished to obtain vulnerability status to send their requests to the OHS. Those requests had to include

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

data concerning health to be reviewed by the Occupational Doctor or an external doctor contracted by the EIB, who would, based on those data, make a decision on the vulnerability status. This decision was notified to the relevant staff members by email which, in case of a positive decision, included a recommendation to telework until further notice and a request to forward the email to their direct manager. Certificates of vulnerability issued by other medical practitioners, either general physicians or specialists, were not accepted.

4. On 3 November 2020, the OHS, on request by the EIB administration and in agreement with the EIB Data Protection Officer ('DPO'), informed all vulnerable staff, by email, that access to the confirmation of vulnerability status could be granted to designated persons within DG Personnel, the hierarchy of the staff member and the Coordination of the staff member's Directorate. The OHS, however, noted that no medical data would be communicated outside the OHS. It also requested vulnerable staff who wished to continue teleworking when presence on site would become mandatory, to reply to the email acknowledging that they had read it. Furthermore, the OHS informed vulnerable staff that the confirmation of their vulnerability status would not be shared if they informed the OHS that they did not plan to continue teleworking 100 % when presence on site would become mandatory. Lastly, the OHS informed vulnerable staff that the data concerned would be shared if it did not hear back from them by the end of November 2020. On 10 December 2020, the OHS clarified in its email to relevant staff that the confirmation would be shared only in case their presence in the office became mandatory.

5. The EDPS informed the EIB DPO of the College's letter, providing the EIB with an opportunity to make comments. The EIB as the controller, in consultation with EIB DPO, acknowledged that the information whether an individual had been granted a status of medical vulnerability indeed constituted data concerning health, but that it contained no further medical information. The EIB further compared the confirmation of vulnerability status to a medical certificate the purpose of which is to justify absence from work due to sick leave, and confirmed that the purpose of sharing the confirmation to a limited number of persons outside the OHS was necessary to ensure appropriate health protection measures, including appropriate office space planning and allocation and building occupancy. Additionally, the controller indicated that those persons were subject to the EIB Code of Conduct ensuring that they respected the rules of secrecy relating to their duties, and that they had signed special confidentiality declarations subjecting them to an obligation of secrecy equivalent to professional secrecy. Lastly, it noted that the staff were also informed about the processing concerned via the EIB intranet and record of processing activities.

2.2. Queries by the EIB College

6. In view of the facts presented above, the College is enquiring whether it is within the purview of the OHS to request medical data to form an opinion on the medical status of:

   A. staff members, instead of relying on the vulnerability certificates that private doctors can issue on the basis of the overall medical condition of the staff members, and, if yes, whether:

   i) there are any specific requirements for the processing of those medical data;

ii) it is relevant for the OHS to keep those medical data or whether they should be deleted once the vulnerability status has been decided;

B. members of the household of the staff members.

Furthermore, the College is enquiring the following:

C. May the vulnerability certificate be shared with persons outside the OHS?

D. Until what time is it relevant for the EIB to keep the data pertaining to the vulnerability status?

E. May a "list" of vulnerable staff, providing an identification by name, be produced, stored and shared outside the OHS?

F. May a non-reply to an email be considered as tacit consent or approval by staff for sharing their health data outside the OHS?

G. Is it legitimate for the administration to "force" vulnerable staff to return to the premises if they do not give consent to their vulnerability status being shared outside the OHS?

3. LEGAL ANALYSIS AND RECOMMENDATIONS

3.1. Processing of certain data concerning health by the OHS

(*Questions A, B and D of the College*)

7. The OHS has requested EIB staff members wishing to obtain vulnerability status to provide either their own data concerning health or those of their family members, as applicable, in order for it to establish medical vulnerability in relation to COVID-19. Staff members with such a vulnerability status would in turn obtain the possibility of working remotely 100 % when physical presence is mandatory[1] and would in fact be recommended to work remotely.

8. Since such data fall under special categories of personal data in accordance with Article 10(1) of the Regulation, their processing requires valid **grounds for lawfulness** both under Article 5(1) and Article 10(2) of the Regulation. In this regard, the EDPS considers that Article 10(2)(h) as well as Article 10(2)(i) of the Regulation may serve as relevant grounds for lawfulness since the processing is intended to protect the health and safety of staff. The Health, Wellbeing and Safety Policy of the EIB Group[2] could be deemed to satisfy the requirement under those provisions that the basis of the processing must be laid down in Union law. That Policy provides, inter alia, that the "*EIB Group aims to protect health and wellbeing as well as safety by committing to align with the Council Directive 89/391/EEC*[3] *as well as relevant health and safety legislation*"[4].

---

1 In view of the epidemiological situation.

2 Adopted by the EIB Management Committee on 24 October 2019. It should be noted that the EIB and its staff are not subject to the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union and that the EIB adopts rules applying to its staff in accordance with Protocol (No 5) on the Statute of the European Investment bank and with its Rules of Procedure.

3 Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work.

4 This provision is similar to Article 1e(2) of the Staff Regulations of Officials of the European Union ('EU Staff Regulations') which provides that officials in active employment are to be accorded working conditions complying with appropriate health and safety standards at least equivalent to the minimum requirements applicable under measures adopted in these areas pursuant to the Treaties.

Recommendation 1: The EDPS recommends that the Policy be supplemented by an EIB executive decision providing for suitable and specific measures to safeguard the rights and freedoms of data subjects, as required by Article 10(2)(h) and (i) and Article 10(3) of the Regulation. In particular, the EIB should ensure that data concerning health are processed solely by staff bound by professional (medical) secrecy, unless there is a valid legal basis for processing by other designated staff members, duly taking into account the principles of necessity and proportionality (more on that in section 3.2 of this Opinion).

9. In accordance with Article 4(1)(c) of the Regulation, personal data are to be adequate, relevant and limited to what is **necessary** in relation to the purposes for which they are processed[5]. That provision requires, in this specific case, that the OHS does not collect or otherwise process personal data that are not necessary to determine whether staff member or members of their household are particularly vulnerable with regard to COVID-19, i.e. whether they should be granted vulnerability status. Similarly to medical services of other EU institutions and bodies ('EUIs'), the OHS has established and made available to staff a list of medical conditions that signify a higher level of vulnerability with regard to COVID-19. In order for the OHS to determine whether staff members or members of their household indeed fall within such categories, it should be able to require (only) information that would allow it to make such a determination. Since criteria used by a private doctor for establishing vulnerability might differ from those laid down by the OHS, it may indeed be necessary for the OHS not to rely solely on an unsubstantiated[6] indication from such a doctor that a person is to be considered vulnerable, also to prevent possible unequal treatment of staff members.

10. With regard to the processing of personal data of **members of the household** of staff members, the EDPS notes that staff members are to provide such data only if they wish to benefit from the possibility of working remotely 100 % (when physical presence is mandatory) due to the increased vulnerability of such members of their household. It appears that the EIB has offered this possibility, at least in part to the advantage of such vulnerable members of their household, in order to eliminate the risk of their infection with COVID-19 that would arise from staff members' physical presence in the office. In this regard, the EDPS notes that also family leave as a special right[7] is granted to staff members only after the EUI has established serious illness or disability of a family member[8], requiring the provision of his or her data concerning health that the EUI's medical staff consider necessary.

11. As regards the **retention** of such personal data, the EDPS recalls that, in accordance with Article 4(1)(e), personal data are to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed[9]. This applies also for the processing under section 3.2 of this Opinion. The

[5] *See* EDPS Necessity Toolkit and EDPS Proportionality Guidelines.
[6] Without specifying, at least in a concise manner, the underlying diagnosis for such an assessment.
[7] Primarily to the advantage of the staff member, however, undoubtedly also to the advantage of the family member concerned.
[8] Article 5.1.4.5 of EIB Staff Rules (similar to Article 42b of the EU Staff Regulations).
[9] For further guidance in this regard, see EDPS Guidelines concerning the processing of health data in the workplace by Union institutions and bodies, p. 11-12.

EDPS takes note in this regard that the EIB indicated[10] that the data concerned would be deleted at the end of the COVID-19 pandemic[11].

Recommendation 2: The EDPS recommends that the EIB review the retention period regularly, taking into account the dynamic evolution of the epidemiological situation and its scientific understanding.

3.2. Processing of certain data concerning health outside the OHS

(*Questions C, E, F and G of the College*)

12. According to the EIB[12], the confirmation of vulnerability status granted by the OHS can be shared with, and therefore processed by, designated persons within DG Personnel[13], the hierarchy of the staff member[14] and the Coordination of the staff member's Directorate[15]. As further elaborated by the EIB[16], such personal data are to be shared with those persons only if presence in the office of the staff members concerned is mandatory[17].

13. As indicated by the EIB[18], confirmation of vulnerability status does not contain any personal data regarding the underlying medical condition giving rise to such a status, nor information that would allow discernment whether the staff members were granted vulnerability status due to their own medical condition or that of a member of their household.

14. In this regard, it should be borne in mind that in order for information to be considered **personal data** it suffices that it relates to an identifiable natural person[19]. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly[20]. Indeed, it may be reasonably likely for persons processing the confirmation of vulnerability status outside the OHS to possess or obtain additional information[21] that would allow them to determine whether the data regarding vulnerability relates to the staff member or to a

---

[10] In a letter of 13 November 2020 by EIB Secretary-General and Director-General of DG Personnel to EIB College.

[11] See in that regard the EDPB-EDPS Joint opinion on the digital green certificate, para. 28, 29 and 54.

[12] Email of 3 November 2020 from OHS to relevant staff.

[13] "*... so that they can provide aggregated data for the global situation at the Bank and ensure the appropriate administrative follow up at Bank level, while protecting the health of the Bank's vulnerable staff in accordance with the safety measures drawn by the EIB*".

[14] "*... so that they can organise their teams efficiently taking into consideration staff members' presence at the premises as well as certain staff members' unavailability to be physically present due to their vulnerable status. In addition, managers need to be in a position to manage their staff's deliverables efficiently by assigning tasks that cannot be performed remotely to staff members who are not considered vulnerable*".

[15] "*... so that they can make the necessary office space adjustments in order to comply with the decisions regarding presence at the premises*".

[16] Email of 10 December 2020 from OHS to relevant staff.

[17] Either because they perform business critical tasks or because presence at the premises has become mandatory again for all EIB staff members.

[18] Email of 8 September 2021 from EIB DPO to EDPS.

[19] Article 3(1) of the Regulation.

[20] Recital 16 of the Regulation.

[21] For example whether a staff member is using an asthma inhaler or whether the personal file of the staff member, which some DG Personnel staff members have access to, indicates that he/she receives a special allowance due to disability of a member of his/her household.

member of their household. Therefore, confirmation of vulnerability status constitutes personal data.

15. In addition, even though the confirmation of vulnerability status does not contain any information regarding the underlying medical condition, such a status is **data concerning health** as defined in Article 3(19) of the Regulation, taking into account the wide interpretation that is to be used with regard to this special category of personal data[22]. In this regard, the EDPS welcomes the fact that in the confirmation it is not specified whose medical condition gave rise to the vulnerability status, as a measure implemented pursuant to Article 4(1)(c) (data minimisation) and Article 27 (data protection by design and by default) of the Regulation.

16. On the other hand, the EDPS notes that the EIB in several of its communications to staff[23] indicated that no medical data would be communicated outside the OHS, effectively taking the view that the confirmation of vulnerability status did not constitute data concerning health. The EIB has since acknowledged[24] that the confirmation indeed constitutes such personal data.

Recommendation 3: The EDPS recommends that the EIB ensure that personal data are processed **fairly and in a transparent manner** in relation to the data subjects, in accordance with Article 4(1)(a) of the Regulation[25]. This provision requires that controllers avoid providing data subjects with inaccurate statements as regards the processing of their personal data, such as the one at hand[26].

17. The processing of the confirmation of vulnerability status outside OHS therefore requires valid **grounds for lawfulness** both under Article 5(1) and Article 10(2) of the Regulation. Similarly to what has been elaborated in section 3.1 of this Opinion, the EDPS considers that Article 10(2)(h) and Article 10(2)(i) of the Regulation may serve as relevant grounds since the purpose of the processing is to carry out activities intended to protect the health and safety of staff, including appropriate office space planning and allocation and building occupancy.

Recommendation 4: The EDPS recommends that any such processing be carried out only on the basis of Union law which applies to EIB, such as the Health, Wellbeing and Safety Policy of the EIB Group, supplemented by an EIB executive decision providing for suitable and specific measures to safeguard the rights and freedoms of data subjects, as required by Article 10(2)(h) and (i) and Article 10(3) of the Regulation.

---

[22] See recital 35 of Regulation (EU) 2016/679 (GDPR) in connection with recital 5 of Regulation (EU) 2018/1725, and EDPB Guidelines on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, p. 5.

[23] Emails of 3 November 2020 and 10 December from OHS to relevant staff, letter of 13 November 2020 by EIB Secretary-General and Director-General of DG Personnel to EIB College, and information notice on EIB's Intranet (as provided by EIB DPO in his email of 8 September 2021 to EDPS).

[24] Email of 8 September 2021 from EIB DPO to EDPS.

[25] See also Article 29 Working party Guidelines on transparency under Regulation 2016/679 and EDPS Guidance paper on transparency rights and obligations.

[26] It is true that the more detailed data concerning health giving rise to the confirmation of vulnerability status are not being shared outside the OHS, however the indication that no medical data (data concerning health) will be shared outside the OHS is inaccurate and misleading.

Recommendation 5: The EDPS recommends that the EIB provide the data subjects with all relevant information in accordance with Article 15 of the Regulation, including the **grounds for lawfulness** of the processing, both under Article 5 and, where applicable, Article 10 of the Regulation[27].

18. Additionally, the EDPS would like to stress that **consent**[28] cannot be considered appropriate grounds for lawfulness in this instance. First, consent to the processing of data concerning health must be explicit[29] and could not be implied from a non-reply to an email. Second, even if explicit, in order for consent to be freely given, as required under Article 3(15) of the Regulation[30], it would have to imply a real choice and control for data subjects[31]. Since the possibility for staff members to telework 100 % when their presence in the office is mandatory would cease in case they decided not to give or to withdraw their consent, the latter would not imply a choice without prejudice and would therefore not be freely given, as it is usually not in an employment context.

19. As indicated above, personal data are to be adequate, relevant and limited to what is **necessary** in relation to the purposes for which they are processed. The confirmation of vulnerability status indeed constitutes data concerning health, however, the EDPS notes that those data are much narrower in scope than the personal data processed by OHS in this context. They contain solely information on whether a staff member is to be considered (particularly) vulnerable to COVID-19, without indicating whether the vulnerability stems from the medical condition of the staff member or a member of his/her household. Furthermore, such data will be shared, and further processed, outside the OHS only where presence in the office of the staff members concerned is mandatory, for the purposes of ensuring the possibility for vulnerable staff to telework 100 %, without compromising business continuity and the exercise of EIB's core activities. When determining whether presence in the office is mandatory, the EIB should take into account the existing epidemiological situation and guidance from national authorities. Lastly, the EDPS takes note[32] that the designated staff members processing the personal data concerned are subject to the EIB Code of Conduct that ensures that they respect the rules of secrecy relating to their duties, and that they have signed special confidentiality declarations subjecting them to an obligation of secrecy equivalent to professional secrecy, as required by Article 10(2)(i) and (3) of the Regulation.

20. In view of the above, the EDPS does not consider the processing of the personal data in question by designated staff members to be disproportionate to the purposes that it pursues. Similarly, the EDPS has already taken the view that data concerning health

---

[27] Please note that a recital of the Regulation (as indicated in the EIB Record of processing of personal data regarding the coronavirus crisis emergency measures) cannot serve as a legal basis for processing of personal data.

[28] Articles 5(1)(d) and 10(2)(a) of the Regulation.

[29] Article 10(2)(a) of the Regulation.

[30] Under Article 3(15) of the Regulation, consent means 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. In addition, as regards the processing of special categories of data, consent should be 'explicit' (Article 10(2)(a) of the Regulation).

[31] See EDPB Guidelines on consent under Regulation 2016/679, p. 7-13.

[32] Email of 8 September 2021 from EIB DPO to EDPS.

may be processed by non-medical staff in order to implement general health and safety measures, in so far as they are limited to necessary data only[33].

Recommendation 6: The EDPS recommends that the EIB implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks to the rights of data subjects, in accordance with Article 33 of the Regulation, in particular to prevent any unauthorised disclosure of the personal data concerned.

3.3. General remarks

Recommendation 7: The EDPS recommends that the EIB consider the need to carry out a **data protection impact assessment** ('DPIA') in accordance with Article 39 of the Regulation, if it has not carried one out yet[34], in order to ascertain risks and mitigating measures at all stages of the processing[35].

Recommendation 8: The EDPS also recommends that the EIB apply the principle of **data protection by design and by default** in accordance with Article 27 of the Regulation, ensuring that only the minimum amount of data necessary is processed and that privacy-friendly technologies are used.

4. CONCLUSION

21. The EDPS makes several recommendations to the EIB to ensure compliance of the processing with the Regulation, in particular as regards the review of the retention period, respect for the principles of lawfulness, fairness and transparency, security of processing, provision of relevant information where personal data are collected from the data subject and consideration of the need to carry out a DPIA.

22. 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 17 February 2022

(e-signed)

Thomas ZERDICK, LL.M.
Head of Unit "Supervision and Enforcement"

[33] EDPS Orientations on manual contact tracing by EU institutions in the context of the Covid-19 crisis, p. 8.
[34] In the EIB Record of processing of personal data regarding the coronavirus crisis emergency measures, it is indicated that the processing operation concerned is subject to a DPIA under Article 39 of the Regulation.
[35] See EDPS Decision on DPIA lists issued under Article 39(4) and (5) of Regulation (EU) 2018/1725.