EUROPEAN DATA PROTECTION SUPERVISOR

EDPS SUPERVISORY OPINION 1/2025

ON THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE (EESC) AND THE EUROPEAN COMMITTEE OF THE REGIONS (CoR) USE OF DATA SUBJECTS' CONSENT FOR PROCESSING HEALTH DATA BY USING A SOFTWARE CONNECTED WITH A NATIONAL HEALTHCARE SYSTEM

(Case 2024-0080)

Executive Summary

This Opinion addresses the request from the European Economic and Social Committee (EESC) and the European Committee of the Regions (CoR) regarding the use of data subjects' consent as a possible lawful ground for the processing of health data by their medical services using a software connected with the Belgian national healthcare system.

It focusses both on the transmission of health data from the EESC and CoR Medical Services to the Belgian healthcare system and the transmission of health data from the Belgian healthcare system to the EESC and CoR Medical Services.

This EDPS opinion addresses not only data subjects' consent, but also the lawfulness, controllership, necessity and proportionality of the processing operations under analysis.

In accordance with Article 58(3)(c) of the Regulation (EU) 2018/1725[1], the EDPS issues this Supervisory Opinion and makes a number of recommendations, in particular:

- include in the consent form all the elements referred to in Article 15 EUDPR;
- inform data subjects about the right to withdraw their consent at any time, and the corresponding procedure;
- clarify that the staff members can only provide consent in relation to their family members if they are their legal representatives;
- remove the possibility to consent to the retrieving, consulting and using of health data from the Belgian central digital medical file;
- determine whether an existing legal act in Union law provides a legal basis for retrieving, consulting, and using staff members' health data from the Belgian central digital medical file;
- carry out the DPIA for the processing operations that are likely to result in a high risk to the rights and freedoms of natural persons.

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

Table of Contents

1. INTRODUCTION

1. This Supervisory Opinion addresses the application of data subjects' consent as legal basis for the processing of health data by the European Economic and Social Committee (EESC) and the European Committee of the Regions (CoR) medical services in the context of the use of a medical software that allows connection to the online services offered by the Belgian National Healthcare System (Belgian NHS).

2. On 19 January 2024, the EESC and the CoR informed the EDPS about their intention to use a software connected with the Belgian NHS that would enable their Medical Advisors, upon the data subject's consent, to issue electronic prescriptions, consult and upload medical documents. The EESC and the CoR asked the EDPS' opinion on the consequences in case a data subject withdraws his or her consent to the retrieval of documents from the Belgian NHS.

3. The EDPS issues this Supervisory Opinion in accordance with Article 58(3)(c) of the Regulation (EU) 2018/1725[1] ('EUDPR').

2. FACTS

4. On 19 January 2024, the EESC and the CoR informed the EDPS of its intention to transition from a paper-based management system for medical files to an electronic one, to increase the effectiveness of the management of medical files and its security. To this end, both entities plan to use a software that enables integration with the online services provided by the Belgian NHS. In doing so, this new software would enable EESC and CoR medical advisers to issue electronic prescriptions, consult and upload medical documents from the Belgian central digital medical file in their local file[2]. According to the EESC and the CoR, this would be done in accordance with Article 36 of Belgian law of 22 April 2019[3] on the quality of healthcare practices.

[1] Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 on the protection of natural people with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ, L 295, 21.11.2018, pp. 39-98.

[2] Email from EES & CoR to the EDPS dated 19 January 2024.

[3] https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2019042220&table_name=loi#LNK0002.

5. In this regard, **the EESC and the CoR have requested the EDPS' opinion on the consequences of the data subjects' withdrawing their consent for retrieving documents** from the Belgian central digital medical file.

6. The EESC and the CoR have provided the EDPS with a consent form designed to obtain data subjects' informed consent, in addition to an informational document containing general information for the data subjects, the data protection notice, the record of processing activity, a data protection impact assessment (DPIA) and their joint controllership arrangement.[4]

7. In light of this information, the Shared Health Dossier is a set of documents that the relevant healthcare providers, in consultation with data subjects, agree to share electronically as they are deemed necessary and relevant for the improved management of the data subjects' health. The EESC and the CoR clarified that behind the Shared Health Dossier is the eHealth platform[5], a Belgian federal public institution.

8. The record of processing activity[6] establishes that the Medical Services of the EESC and the CoR **collect and process health data from their staff members**: laboratory analysis results, medical reports, and medical certificates. The Medical Services of the EESC and the CoR collect and process staff members' health data for the **purpose of providing them with health care services** in the framework of their preventive occupational[7] health policy (i.e., the performance of pre-recruitment medical examination or annual check-ups). The record of processing details fifteen different purposes, including pre-recruitment medical examinations, medical examinations and expert medical opinions, monitoring of absenteeism or the exchange of medical files with other institutions.

9. In addition, the envisaged transmission of the staff members' personal data to the Belgian central digital medical file would involve the processing of the following **health data**: health summaries, exam results, list of medications taken,

[4] Email from EESC & CoR to the EDPS providing additional information 'DPIA Medispring V4 final, Management of medical files, Notice de protection des données dossier médical and Poster_SM_v3 ', dated 07 February 2024.
[5] https://www.ehealth.fgov.be/fr/a-propos-esante
[6] EESC record of processing on the management of medical files, available at https://www.eesc.europa.eu/sites/default/files/2024-08/RoPA%20E068_Management%20of%20medical%20files.pdf
[7] According to the World Health Organisation, "Occupational health is an area of work in public health to promote and maintain highest degree of physical, mental and social well-being of workers in all occupations. Its objectives are:
1. the maintenance and promotion of workers' health and working capacity;
2. the improvement of working conditions and the working environment to become conducive to safety and health;
3. the development of work organization and working cultures that should reflect essential value systems adopted by the undertaking concerned, and include effective managerial systems, personnel policy, principles for participation, and voluntary quality-related management practices to improve occupational safety and health.
See https://www.who.int/health-topics/occupational-health.

hospitalisation and consultation reports, possible pathologies and allergies, an inventory of medical care received and a list of vaccinations[8]. This health data would be transmitted to the Shared Health dossier for **health purposes** within the framework of ensuring continuity and quality of care. The aim is to provide the staff members with a better management of their health (i.e., make their health data accessible to the healthcare professionals, simplify the transmission of their medical history during their consultations or avoid unnecessary prescriptions).

10. Moreover, the potential retrieval, consultation and use of staff members' documents from the Belgian central digital medical file by the Medical Advisors of the EESC and the CoR would involve the processing of the aforementioned health data (i.e., exam results, list of medications taken, hospitalisation). The Medical Services of the EESC and the CoR would retrieve, consult and use such staff members' health data for the **purpose of providing them with better health care services**. The aim is to provide them with a better preventive or therapeutic medical advice, as part of their preventive occupational medicine policy.

11. Pursuant to the data protection notice, the Medical Services of the EESC and the CoR will also process personal data, where necessary, in relation to **family members**: surname, first name and address, in the context of the appointing authority's opinions concerning requests for special leave, family leave, part-time work, teleworking, authorisation to spend sick leave away from the place employment and other similar requests.

12. The EESC and the CoR informed the EDPS that they carried out a **DPIA on the specific Medispring software** and the controllers considered that the identified risks can be mitigated by reasonable means. Therefore, the EESC and the CoR considered that a prior consultation within the meaning of Article 40 EUDPR was not considered necessary.

3. LEGAL ANALYSIS AND RECOMMENDATIONS

13. According to Article 2(1) EUDPR, the EUDPR is applicable to the EESC and the CoR since they are Union institutions and bodies under Article 13 of the Treaty on European Union, and therefore two of the 'Union institutions and bodies' as defined in Article 3(10) EUDPR.

[8] Email from EESC & CoR to the EDPS providing additional information 'Poster_SM_v3 dated 07 February 2024.

14. According to Article 3(1) EUDPR, 'personal data' refers to any information relating to an identified or identifiable natural person.

15. The Medical Services of the EESC and the CoR collect and process information from the staff members (i.e., name, age, contact details, laboratory analysis results, medical reports, and medical certificates), which constitute **personal data** within the meaning of Article 3(1) EUDPR.

16. In accordance with Article 3(19) EUDPR, 'data concerning health' refers to personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about their health status. As such, some of the data listed above in paragraph 15 of this Opinion, constitute **data concerning health**, in accordance with Article 3(19) EUDPR.

17. In addition, the Medical Services of the EESC and the CoR intend to transmit and retrieve the following information of the staff members to/from the data subject Belgian central digital medical file: health summaries, exam results, list of medications taken, hospitalisation and consultation reports, possible pathologies, allergies, an inventory of medical care received and a list of vaccinations[9]. This information also constitutes personal data concerning health, within the meaning of Article 3(19) EUDPR, as it relates to the physical or mental health of a natural person and may reveal information about their health status.

18. According to Article 10(1) EUDPR, the processing of data concerning health is considered processing of **special categories of data** and is, therefore, subject to the provisions of that article.

19. Additionally, according to Article 3(3) EUDPR, 'processing' refers to any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, … storage, … retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available…'. The set of operations of collecting personal data in a medical file, transmitting the data to other entities, and the retrieval, consultation and using of similar health data kept by the Belgian NHS, constitutes **processing**, within the meaning of Article 3(3) EUDPR.

20. This opinion concerns the **personal data processing operations** performed by the EESC and the CoR with respect to:

[9] Email from EESC & CoR to the EDPS providing additional information 'Poster_SM_v3 dated 07 February 2024.

(i) the collection and transmission of their staff members' medical file to the online systems of the Belgian NHS, as well as

(ii) the retrieval, consultation and use of health data by the EESC and CoR from the medical file created by the Belgian NHS are conducted for purposes of preventive and curative medicine.

Given its relevance, the EDPS will address not only the specific question regarding the withdrawal of consent, as requested by the EESC and the CoR, but also the lawfulness, necessity and proportionality of the processing operations under review.

3.1. Collection and transmission of EESC and CoR staff members' medical file to the Belgian e-Health system

3.1.1. Purposes of the two data processing operations

21. As required by Article 4(1)(b) EUDPR, personal data must be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.

22. As indicated above (paragraph 8), the Medical Services of the EESC and the CoR collect information from staff members which involve the processing of health data for the purpose of providing them with health care services in the framework of their preventive occupational medicine policy (i.e., pre-recruitment medical examination or annual check-ups).

23. In addition, as noted above (paragraph 9), the Medical Services of the EESC and the CoR intend to transmit staff members' health data to the Belgian central digital medical file for health purposes. In particular, to provide the staff members with a better management of their health within the framework of primary care (i.e., make their health data available to the healthcare professionals; simplify the transmission of their medical history during their consultations; or avoid unnecessary prescriptions).

24. The EDPS notes that **the collection of staff members' health data by the Medical Services of the EESC and the CoR and its potential transmission to the Belgian central digital medical system pursue different purposes**. Indeed, the purpose of providing health care services to fulfil occupational medicine obligations differs from the health-related objectives pursued in the context of primary care. The first regards the employees' aptitude to work and the need for adjustments at their work place as an obligation under the Staff Regulation and the

CEOS[10], as mentioned above. By contrast, the second concerns '... a model of care that supports first-contact, accessible, continuous, comprehensive and coordinated person-focused care. It aims to optimize population health and reduce disparities across the population by ensuring that subgroups have equal access to services'[11]. Consequently, the first requires access to specific health-related personal data necessary for providing occupational medicine services as described in the record of processing. This is a relevant factor with implications not only for defining the purposes, but also for assessing the necessity and proportionality assessment (Article 9(2) EUDPR), which will be analysed in section 3.1.4 of this opinion.

25. Furthermore, occupational medicine requires personal data to be segregated in a way that the employer only has access to the medical doctor's assessment "apt/inapt/apt with reserve", ensuring professional medical secrecy. This requires the involvement of medical professionals, who will be responsible for safeguarding and storing the staff members' medical file.

3.1.2. Lawfulness of the collection of EESC and CoR staff members' medical files.

26. Article 5(1)(b) EUDPR provides that processing shall be lawful if the processing is necessary for compliance with a legal obligation to which the controller is subject.

27. According to Article 10(1) EUDPR, the processing of special categories of data, such as data concerning health, is prohibited, unless one of the conditions mentioned in Article 10(2) EUDPR is applicable.

28. According to Article 10(2)(b) EUDPR, the processing of special categories of personal data shall be lawful if it is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

29. Additionally, according to Article 10(2)(h) EUDPR, the processing of special categories of personal data shall be considered lawful if it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on

[10] See Art. 28e), Art. 33, Art. 59§6 Staff Regulation and Art. 12§2 , Art.13 ,Art. 16, Art. 32, Art. 82§3, Art. 83 Art. 91 CEOS.
[11] See World Health Organisation, https://www.who.int/teams/integrated-health-services/clinical-services-and-systems/primary-care.
See Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), 2007.

the basis of Union law or pursuant to contract with a health professional and subject to the conditions and safeguards.

30. The EESC and the CoR processing operations requiring health data have the purpose of carrying out obligations and exercising rights in the field of employment and for the assessment of the employees' working capacity (i.e., pre-recruitment medical examination, annual medical visits, management of work related illnesses, invalidity procedures, etc.), which are lawful under Article 5(1)(b) and Articles 10 (2)(b) and (h) EUDPR. In this respect, **the processing of personal data described above is necessary for the compliance with a legal obligation** of the EESC and the CoR under the Staff Regulations[12] and the Regulation laying down provisions for implementing the third subparagraph of Article 28a(2) and the third subparagraph of Article 96(2) of the Conditions of Employment of Other Servants of the European Communities (CEOS)[13].

3.1.3. Lawfulness of the envisaged transmission of EESC and CoR staff members' medical files to the Belgian e-Health system

31. As noted above (paragraph 24), the purpose of the envisaged transmission of the staff members' health data differ from the original purpose for which the health data were collected by the Medical Services of the EESC and the CoR.

3.1.3.1. Compatibility of purposes (Article 6 EUDPR) - Further processing

32. According to Article 6 EUDPR, where processing for a purpose other than that for which the personal data were collected is not based on the data subject's consent or on Union law, and constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 25(1), the controller shall ascertain whether the processing for the new purpose is compatible with the original purpose for which the personal data were initially collected.

33. In order to determine whether the purpose of the envisaged transmission of staff members' health data is compatible with the original purpose for which the health data were initially collected by the Medical Services of the EESC and the CoR, it is necessary to consider, inter alia, the elements outlined in Article 6 EUDPR.

[12] Consolidated text: Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community, OJ P 045 14.6.1962, p. 1385

[13] Règlement (CE) n o 780/2009 de la Commission du 27 août 2009 fixant les dispositions d'exécution de l'article 28 bis , paragraphe 2, troisième alinéa, et de l'article 96, paragraphe 2, troisième alinéa, du régime applicable aux autres agents des Communautés européennes (RAA), JO L 226 du 28.8.2009, p. 3-7.

34. Regarding the **link between the purposes** (Article 6(a) EUDPR), the EDPS observes that the purpose of the envisaged transmission (i.e., better management of health in the framework of primary care) cannot be implied in the initial purpose for the collection of the personal data (i.e., provision of health care services in the framework of preventive or occupational medicine).

35. In relation to the **context in which the health data were collected** (Article 6(b) EUDPR), the EDPS notes that the context in which the staff members' health data was initially collected (i.e., employment relationship) differs from the context in which the EESC and the CoR intend to further process the data (i.e., primary care).

36. Concerning the **nature of the personal data** (Article 6(c) EUDPR), the EDPS observes that the nature of personal data is the same in both cases. The data processed initially by the Medical Services of the EESSC and the CoR and the data intended to be further processed, both relate to the processing of data concerning health, which fall under special categories of personal data under Article 10(1) EUDPR.

37. In relation to the possible **consequences of the intended further processing** for data subjects (Article 6(d) EUDPR), the EDPS notes that the consequences of the intended further processing (i.e., personalised healthcare to patients) are different from the consequences of the collection of staff members' health data by the Medical Services of the EESC and the CoR (i.e., successful pre-recruitment medical examination).

38. Regarding the existence of **appropriate safeguards** (Article 6(e) EUDPR), the EDPS notes that the potential health data transmitted would be encrypted (at the level of the authorised user) and it would not be possible to gain access to it without the decryption key belonging only to the authorised persons of the EESC and the CoR[14].

39. In light of the above, the EDPS noted that **it is not possible to ascertain whether the purpose of the envisaged transmission of health data is compatible with the purpose for which the personal data were initially collected** by the Medical Services of the EESC and the CoR, due the limitations outlined in Articles 6(a), (b) and (d) EUDPR. Consequently, **a separate legal basis,** distinct from one that allowed the initial collection of the personal data **is required for further processing** of the data and for proceeding with the envisaged transmission of the staff members' health data to the Belgian central digital medical file.

[14] Email from EESC & CoR to the EDPS providing additional information 'Data Protection Notice' dated 07 February 2024.

40. In the present case, the EESC and CoR intend to proceed with the transmission and further processing of the personal data initially collected by their Medical Services to the online systems provided by the Belgian NHS, based on the data subjects' consent under Article 5(1)(d) EUDPR.

3.1.3.2. Lawfulness based on explicit consent (Articles 3(15), 5(1)(d) and 10(2)(a) EUDPR)

41. Article 5(1)(d) EUDPR provides that the processing shall be lawful if the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

42. According to Article 3(15) EUDPR, 'consent' of the data subject refers to any freely given, specific, informed and unambiguous indication of the data subject's wishes, by which they, through a statement or a clear affirmative action, express agreement to the processing of personal data related to them.

43. In addition, according to Article 10(2)(a) EUDPR, the prohibition of processing special categories of data shall not apply if the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

44. The EDPS observes that the transmission of the personal data to the Belgian NHS, collected based on the provisions of the Staff Regulations, can be lawful if the EESC and CoR rely on the data subjects' consent as the legal basis, provided that all the requirements for valid consent under Articles 3(15) and 5(1)(d) and 10(2)(a) EUDPR are met.

45. On the criteria of consent being **freely given**, the EDPS takes note that the consent under analysis requested by the EESC and the CoR is not tied to any condition. Even though it is the employer (the EESC and the CoR) requesting the consent to transmit their staff's health data to the Belgian NHS, there is no imbalance of power in this request for consent, given that the data subjects will not experience any adverse effects regardless of their decision to provide consent or not. As a result, this situation is one of the few where consent can be freely requested within the work context. Consequently, consent is deemed to be freely given by data subjects, in accordance with Article 3(15) EUDPR.

46. Regarding the element of being **specific**, the requirement for specific consent, in conjunction with the principle of purpose limitation under Article 4(1)(b) serves as a safeguard against the gradual expansion or ambiguity of the purposes for which data is processed, after a data subject has consented to the initial collection of data. Obtaining specific consent necessitates that the purpose of the processing is clearly defined, providing sufficient detail about the various processing operations, and ensuring a clear distinction between information related to the processing

operations for which consent is sought and other matters. The consent form presented by the EESC and CoR includes a specific section related to the transmission of health data to healthcare providers and the inscription in the reference eHealth Belgium register via the Health Network of Brussels (*Réseau Santé Bruxellois)*[15].

47. The EDPS notes that the consent form distinguishes clearly the processing operation under analysis. Consequently, the EDPS considers that the consent is specific, and in accordance with Article 3(15) EUDPR.

48. Regarding the element of being **informed**, consent needs to include a minimum of information that is crucial for the data subject to make an informed choice.

49. Article 15 EUDPR outlines the information that the controller shall provide to the data subject at the time when personal data is collected, specifically when the data is obtained directly from the data subject.

50. The EDPS notes that the information included in the explanation note, the data protection notice and the consent form provided by the EESC and the CoR do **not include all the elements mentioned in Article 15 EUDPR regarding the transmission of health data collected under the Staff Regulation and CEOS.** In particular, the following items are not specified:

    (i) the identity of the controller and its contact details (Article 15(1)(a) EUDPR), are not provided, as joint controllership is neither reflected in the data protection notice nor in the consent form;

    (ii) the purposes and legal basis for all the processing operations(Article 15(1)(c) EUDPR); and,

    (iii) the right to withdraw consent at any time without affecting the lawfulness of the processing based on the consent before its withdrawal (Article 15(2)(c) EUDPR).

51. Therefore, the EDPS considers the current consent form incomplete and emphasises the necessity for the entities acting as controllers to be clearly identified. The EDPS further requires that **all elements specified in Article 15 EUDPR be included in the consent form and that comprehensive information regarding the processing operation be provided in writing simultaneously, to ensure that consent is informed, in accordance with Articles 3(15) and 15 EUDPR (Recommendation 1).**

[15] The documents were provided in French and the translation was made by the case officer.

52. Regarding the element of consent being **unambiguous**, data subject must express their wishes either through an explicit statement or by taking a clear, affirmative action. The EDPS notes that the consent form provided by the EESC and Cor includes a specific section for consenting to the transmission of health data, where staff members can indicate their consent by signing and dating the form. Therefore, the consent is considered unambiguous in accordance with Article 3(15) EUDPR.

53. Regarding the criteria of consent being **explicit**, data subjects must give their consent by statement or a clear affirmative action. In the present case, the EDPS observes that the EESC and the CoR offer data subjects the possibility to express in writing their consent for the transmission of their health data. And the EESC and the CoR would make sure that the written statement is signed by their staff members. Therefore, the consent is considered explicit under Articles 3(15) and 10(1)(a) EUDPR.

54. In light of the above, **the EDPS notes that the transmission and further processing of the staff members' personal data to the Belgian NHS, collected on the basis of the Staff Regulation provisions, can be lawful if the EESC and CoR use the data subjects' consent as the legal basis under Articles 3(15) and 5(1)(d) and 10(2)(a) EUDPR, provided that the criterion of being informed is met.**

55. As previously mentioned by the EDPS in its Guidelines concerning the processing of health data in the workplace[16], further processing of health data collected on the basis of the EU Staff Regulations provisions can only be considered as lawful provided that it is based on an informed and freely given consent of the data subject (Article 5(1)(d) EUDPR).

3.1.3.3. Additional conditions under Article 7 EUDPR for a valid consent

56. Article 7 EUDPR introduces three additional conditions for a valid consent.

57. Firstly, the **controller must be able to demonstrate that informed and explicit consent** has been obtained (Article 7(1) EUDPR). The EDPS highlights that according to the accountability principle (Article 4(2) EUDPR), the controller is responsible for demonstrating compliance with data protection rules and principles, including the obligation to demonstrate that data subjects have provided consent for the processing of their personal data (Article 7(1) EUDPR). In that regard, the EESC and CoR must document the information process enabling data subjects to have a full and clear comprehension of the processing operations entailed in their

[16] See EDPS Guidelines concerning the processing of health data in the workplace by Community institutions and bodies, 2009, p. 5.

consent. The EDPS notes that the consent form, which will be retained by the Medical Services of the EESC and CoR will suffice to demonstrate the compliance with this legal provision.

58. Secondly, consent given in the context of a written declaration shall be presented in an **intelligible and accessible form using clear and plain language** (Article 7(2) EUDPR). As noted above (see paragraph 50), the EDPS observes that some relevant information is not available to data subjects at the time of providing consent, and that there is not a clear explanation of the terms and conditions of the processing activities that the consent would allow, which makes it unintelligible for data subjects to provide their consent.

59. Thirdly, **data subjects must be able to withdraw their consent at any time, and it shall be as easy to withdraw as to give consent** (Article 7(3) EUDPR). In practice, if data subjects withdraw their consent for the EESC and CoR to disclose their health data with the Belgian NHS, the EESC and Cor will have to stop the transmission of that information, since they would no longer have a lawful ground for such processing operation under Article 5 EUDPR. In the present case, the EDPS notes that if the annual medical appointment occurs once a year and if it is not feasible to book an appointment or reach the medical service at any time to withdraw the consent, then the data subjects would not be able to withdraw their consent at any time and as easily as they have given it, in line with Article 7(3) EUDPR.

60. In addition, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The controllers shall inform the staff members about this consequence prior to giving consent, in accordance with Article 7(3) EUDPR. The EDPS observes that the procedure for withdrawing consent is not explicitly outlined in any documentation provided to the EDPS, nor is there information regarding the lawfulness of consent prior to its withdrawal. Since the staff members are not informed about the lawfulness of consent before its withdrawal, the EDPS finds that the consent does not fulfil the requirements outlined in Article 7(3) EUDPR. Therefore, the **EDPS deems necessary that the EESC and the CoR inform data subjects about the right to withdraw their consent at any time, the procedure for exercising that right, along with the provision of necessary information regarding the lawfulness of the processing between the time consent is given and their withdrawal** (which is not clearly outlined) **(Recommendation 2).**

3.1.3.4. Limitations of consent for processing health data of family members of EESC and CoR staff members

61. As noted above (paragraph 11), the EESC and the CoR indicated that they may process personal data in relation to **family members**: surname, first name and address. In particular, the EESC and the CoR explained that they may process any data of a medical or social nature relating to the staff member or members of his family, as deemed relevant by the medical service, in order to provide health care services within the context of preventive occupational medicine.

62. According to Article 5(1)(d) EUDPR, the processing shall be lawful if the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

63. In addition, Article 7(1) EUDPR provides that where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

64. Consent as a legal basis under Articles 5(1)(d) and 7(1) EUDPR is only valid for the processing operations regarding the data subjects' own personal data. Hence, staff members will not be able to provide consent regarding their family members, unless they are their legal representatives (e.g. regarding personal data on their children under 18 years old) or their proxy.

65. The EDPS notes that EESC and the CoR do not include any reference to the processing of data in relation to family members in data subjects' informed consent. Therefore, consent for such processing operation is not valid, according to Articles 5(1)(d), 7(1) EUDPR. Consequently, **the EDPS deems necessary that the EESC and CoR either include a specific consent for the processing of the staff member's family health data and clarify that the staff members can only provide consent in relation to their family members if they are their legal representatives, in compliance with data protection rules[17] (Articles 5(1)(d) and 7 EUDPR), or do not perform such processing operation in view of the lack of legal basis under Article 5 EUDPR (Recommendation 3)**.

[17] The EDPS reminds that EESC and CoR would need to justify under the accountability principle (Article 4(2) EUDPR that contacting the doctors the EESC and the CoR staff family members is adequate, relevant and limited to what is necessary for the occupational medicine, in accordance with Article 4(1)(c) EUDPR.

3.1.4. Additional conditions for the transmission of personal data to recipients that are not EU institutions (Article 9 EUDPR) - Necessity and proportionality

66. In accordance with **Article 9 EUDPR**, the transmission of personal data from Union institutions to recipients established in the Union but which are not Union institutions shall only occur under certain **conditions**. To fulfil those conditions those recipients need to establish that the **data are either necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the recipient (Article 9(1)(a) EUDPR)**, **or necessary to have the data transmitted for a specific purpose in the public interest and the controller, where there is any reason to assume that the data subjects' legitimate interests might be prejudiced, establishes that it is proportionate to transmit the personal data for that specific purpose** after having demonstrably weighed the various competing interests **(Article 9(1)(b) EUDPR)**.

67. In the present case, the EESC and the CoR are going to transmit data to the online systems of the Belgian NHS, a recipient in the EU, which is not an EU institution.

68. For the transmission to be lawful, it must satisfy one of the criteria outlined in Article 9(1) EUDPR. In the present case, the Belgian NHS (the recipient) has to establish that the data are necessary for the performance of a task carried out in the exercise of its official authority. Since there are no data subjects' legitimate interests that might be prejudiced by the transmission of health data from the EESC and CoR to the Belgian NHS, Article 9(1)(b) EUDPR is not applicable. Furthermore, in accordance with Article 9(2) EUDPR, the EESC and the CoR shall provide evidence that the transmission of personal data is both necessary and proportionate to the intended purposes.

69. According to the general information provided by the EESC and the CoR, the purpose of transmitting health data collected under occupational medicine obligations to the Belgian NHS is to provide a more holistic healthcare to the patients in Belgium and to avoid the duplication of medical exams. Those goals are aligned with the purpose of the processing operations held by the Belgian NHS and are also in the interest of the data subject.

70. In regard to necessity, the more complete the healthcare file is, the more comprehensive the healthcare provided to the data subject will be. The health data collected under the Staff Regulation seems necessary to achieve the aim of providing a holistic healthcare to data subjects.

71. Furthermore, necessity and proportionality, even though strictly linked to each other (both conditions must be fulfilled), entail two different tests.

72. Regarding the proportionality of the transmission of personal data (Article 4(1)(c) EUDPR), the EDPS finds that the purpose of providing holistic healthcare to data subjects is legitimate, and that the transmission of health data from the occupational services of EESC and CoR to the Belgian NHS is adequate, relevant and necessary for achieving that purpose.

73. Consequently, the EDPS considers that the transmission of health data from the EESC and CoR occupational medicine file to the Belgian NHS is necessary for and proportionate to the purposes of the transmission, meeting the requirements of Article 9(1)(a) and 9(2) EUDPR.

3.2. Retrieval, Consultation and Utilisation of health data from the Belgian central digital medical file by the Medical Advisers of the EESC and the CoR

74. Following their consultation, the EESC and the CoR communicated their intention to proceed with the retrieval, consultation and use of health data from the Belgian central digital medical file by their Medical Advisors.

75. As noted above (paragraph 10), the retrieval, consultation and use of health data by the Medical Advisors of the EESC and the CoR from the Belgian central digital medical file would involve the processing of data concerning health in line with Article 3(19) EUDPR, which is considered processing of special categories of personal data (Article 10 EUDPR).

3.2.1. Purposes of the three data processing operations

76. As required by Article 4(1)(b) EUDPR, personal data must be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.

77. The Medical Services of the EESC and the CoR intend to carry out the three processing operations (i.e., the retrieval, consultation and use health data from the Belgian central digital medical file) for the same purpose of providing the staff members with better health care services. In particular, to provide them with a better preventive or therapeutic medical advice, in the context of their preventive or occupational medicine obligations.

78. The Belgian central digital medical file from which the Medical Services of the EESC and the CoR intend to retrieve, consult and use their staff member's health data is created by the Belgian NHS for health purposes, in the framework of preventive and curative medicine.

79. As mentioned above under section 3.1.1, **the purpose of providing health care services to fulfil occupational medicine obligations is different from the health purposes in the context of primary care.** The aim of occupational medicine is linked to a legal obligation to ensure the employees' fitness to work, as well as to promote and maintain the highest degree of physical, mental and social well-being of workers. In contrast, primary care and curative medicine is meant to provide personalised healthcare to patients, either by promoting certain practices to prevent certain diseases or by providing treatment to address the patients' needs.

3.2.2. Lawfulness

80. According to Article 4(1)(a) EUDPR, personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

81. In this case, the EESC and the CoR have informed the EDPS about their intention to rely on **data subjects' consent (Article 5(1)(d) EUDPR) as the legal basis** for the three processing operations: the retrieving, consulting and using health data from the Belgian central digital medical file.

82. The requirements already mentioned in the section 3.1.3.2 of the Opinion for a valid consent according to Articles 3(15), 5(1)(d) and 10(2)(a) EUDPR, are applicable to these processing operations. Put differently, for consent to be valid it has to be freely given, specific, informed and unambiguous. Moreover, the controller must be able to demonstrate consent (Article 7(1) EUDPR); consent given in the context of a written declaration must be clearly distinguishable from other matters and must be presented in an intelligible and accessible form using clear and plain language (Article 7(2) EUDPR); and data subjects must be able to withdraw their consent as easily as they have given it and at any time (Article 7(3) EUDPR).

83. The EDPS notes that in the scenario analysed in section 3.1.3.2 of this opinion, data subjects have the conditions to freely provide their consent for the transmission of their health data held by their employer's occupational health service to the data subjects' general practitioner and other healthcare providers. However, the same cannot be said for the retrieving, consulting and using health data from the Belgian healthcare services to the Medical Advisers of the EESC and CoR.

84. Given the employment context and the potential negative consequences, consent is unlikely to be a lawful ground for these processing operations. For example, the negative discrimination of an individual not being renewed his work contract due to the information provided by Belgian healthcare professionals in the data subject's general medical file (i.e., when an employee is followed by a psychiatrist and consequently considered not fit to work). In this scenario, there is an imbalance of power in the consent request, since data subjects might suffer negative consequences if they choose not to give consent[18]. Considering the dependency that stems from the employer/employee relationship, it is unlikely that data subjects can deny their consent to retrieving, consulting and using their health data without experiencing the fear or real risk of detrimental effects following their refusal. Consequently, **consent is not freely given by data subjects and it cannot be a lawful ground for these processing operations under Article 5(1)(d) EUDPR.**

85. In the absence of any lawful ground under Article 5 EUDPR, the EESC and the CoR cannot perform any of the three envisaged processing operations (i.e., retrieving, consulting and using of the health data). In this regard, Article 7(2) *in fine* EUDPR establishes that any declaration that constitutes an infringement of the EUDPR is not binding to the parties. This is of particular relevance in this case, as there is no applicable legal ground. Therefore, **the EDPS deems necessary that the EESC and CoR revise their consent form and remove the possibility to consent to the retrieving, consulting and using of health data from the Belgian central digital medical file by their Medical Advisers (Recommendation 4).**

86. Regarding the processing of personal data deemed necessary for fulfilling a legal obligation and/or for performing a task carried out in the public interest or in the exercise of official authority entrusted to the controller, a legal basis must be established under Union law[19]. Such a legal basis must be clear and precise and its application must be foreseeable to persons subject to it[20]. For example, this could be internal rules of general application intended to produce legal effects vis-à-vis data subjects. They should be adopted at the highest level of management of the Union institutions and bodies, within their competencies and in matters relating to their operation. Therefore the EDPS recommends that the EESC and the CoR **determine whether an existing legal act in Union law provides a legal basis for retrieving, consulting, and using staff members' health data from the Belgian central digital medical file for the provision of healthcare services in the context of preventive occupational medicine. In the absence of such**

[18] See European Data Protection Board's Guidelines 05/2020 on consent under Regulation 2016/679, p.9.
[19] Article 5(2) EUDPR;
[20] See also Recital 41 GDPR and Recital 23 EUDPR. These provisions complement the requirements of Article 7 and 8 of the Charter, as interpreted by the CJEU, according to which any interference must be provided for by law which is clear, precise and foreseeable. See for more details, EDPS, Guidance for co-legislators on key elements of legislative proposals, https://www.edps.europa.eu/system/files/2024-01/2023-0025_edps_guidance_for_co-legislators_en.pdf

an act, the EDPS recommends studying the creation of a legal framework to establish a clear and lawful basis for the envisaged activities (Recommendation 5).

3.2.3. Necessity and proportionality (Article 4(1)(c) EUDPR)

87. Even if there existed a lawful ground under Article 5 EUDPR for each of the three processing operations under analysis, the compliance with the remaining EUDPR data protection rules and principles would still be necessary.

88. According to Article 4(1)(c) EUDPR, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

89. In order to avoid the duplication of medical exams, the results of the exams requested by the occupational health services can be transmitted to the general practitioner and other medical service providers if the data subject consents in transmitting such data, as long as all the criteria described in section 3.1.3.2 of this opinion are checked. At the same time, if the health practitioner has requested exams that are necessary for occupational health, the data subject can provide the results to the occupational health doctor in a printed or digital copy.

90. In light of the above, the retrieving, consulting and using of health data from the Belgian central digital medical file by the Medical Advisers of the EESC and the CoR does not pass the necessity test foreseen in Article 4(1)(c) EUDPR.

91. Regarding proportionality (Article 4(1)(c) EUDPR), while it is legitimate that the preventive/curative medicine is as holistic as possible, the same cannot be said regarding occupational medicine. Even though the shared medical file does not contain all the information that the individual healthcare providers have on the data subject, but only health data that they find relevant to other healthcare providers, it may contain significantly more information than is necessary for the purposes of healthcare services within the context of occupational medicine. Moreover, the data subject might not be in full control of the data transmitted therein. Even if all health professionals have to justify their access to that data, the justification provided might not be plausible. For example, if the occupational health doctor would like to check the entire medical history of an employee.

92. Hence, the EDPS notes that the proportionality test foreseen in the data minimisation principle (Article 4(1)(c) EUDPR) is not met, since the data processed is not limited to what is strictly necessary.

3.3. DPIA as an accountability tool - Article 4(2) and Article 39 EUDPR

93. The accountability principle (Article 4(2) EUDPR) requires that the controllers are responsible for, and be able to demonstrate compliance with the data protection principles listed in Article 4(1) EUDPR.

94. Moreover, under Article 26 EUDPR, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the EUDPR. Concretely, the controller shall '*take into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. Those measures shall be reviewed and updated where necessary*'.

95. The EDPS observes that the DPIA is one of the accountability tools in the EUDPR.

96. Under Article 39 EUDPR, the DPIA should be conducted on the specific processing operations that are likely to result in a high risk to the rights and freedoms of natural persons.

97. In addition, according to Article 39(7)(b) EUDPR, the DPIA shall contain an assessment of the necessity and proportionality of the processing operations in relation to the purposes.

98. In the present case, the EESC and the CoR carried out the DPIA solely on the electronic medical file Medispring, and they made a necessity and proportionality assessment only for the switch to the electronic medical file[21].

99. However, the EDPS notes that **the EESC and the CoR have not conducted the DPIA on the comprehensive processing operations** that are likely to result in a high risk to the rights and freedoms of natural persons (i.e., regarding the transmission of health data to the Belgian healthcare platform), in line with Article 39 EUDPR. In particular, the DPIA does not include a detailed assessment on the risks associated to the transmission of the data concerning health to the online systems of the Belgian NHS, the use of consent as a legal basis for such access, the possible impacts on individual rights, including discrimination, as well as the compatibility of purposes of the different processing activities.

100. In light of the above, **the EDPS deems necessary that the EESC and the CoR carry out a DPIA for the processing operations that are likely to result in a high risk to the rights and freedoms of natural persons (i.e., regarding**

[21] Email from EESC & CoR to the EDPS providing additional information 'DPIA Medispring V4 final' dated 07 February 2024.

the transmission of health data from the Medical Advisers of the EESC and the CoR to the Belgian NHS), and include an assessment of the necessity and proportionality of the processing operations in relation to the purposes, in accordance with Article 39 EUDPR (Recommendation 6).

4. CONCLUSION

In this Opinion, the EDPS has made the following findings:

- The consent form intended to be presented by the EESC and the CoR to data subjects regarding the data processing operation for the transmission of personal data does not meet all the requirements established under Articles 3(15) and Article 7 EUDPR.

- Consent cannot be used as the lawful ground for any of the three processing operations of retrieving, consulting and using health data from the Belgian NHS to the occupational file of the EESC and the CoR staff members.

- The EESC and the CoR have not conducted the DPIA on the comprehensive processing operations that are likely to result in a high risk to the rights and freedoms of natural persons, in line with Article 39 EUDPR.

As indicated above, in order to ensure compliance of the processing with the EUDPR, the EDPS **deems it necessary** that the EESC and the CoR:

- **Recommendation 1 - include in the consent form all the elements referred to in Article 15 EUDPR and in writing simultaneously, to ensure that the consent is fully informed;**

- **Recommendation 2 - inform data subjects about the right to withdraw their consent at any time, the procedure to exercise that right and information about the lawfulness of the processing between the moment of the consent and their withdrawal;**

- **Recommendation 3 - either include a specific consent for the processing of the staff member's family health data and clarify that the staff members can only provide consent in relation to their family members if they are their legal representatives, in compliance with data protection rules (Articles**

5(1)(d) and 7 EUDPR), or the processing operation should not be carried out due to the absence of a legal basis under Article 5 EUDPR;

- **Recommendation 4 - remove the possibility to consent to the retrieving, consulting and using of health data from the Belgian central digital medical file by the EESC and the CoR Medical Advisers;**

- **Recommendation 5 - determine whether an existing legal act in Union law provides a legal basis for retrieving, consulting, and using staff members' health data from the Belgian central digital medical file for the provision of healthcare services in the context of preventive occupational medicine. In the absence of such an act, study the creation of a legal framework to establish a clear and lawful basis for these activities.**

- **Recommendation 6 - carry out the DPIA for the processing operations that are likely to result in a high risk to the rights and freedoms of natural persons (i.e., regarding the transmission of health data from the Medical Advisers of the EESC and the CoR to the Belgian NHS), and include an assessment of the necessity and proportionality of the processing operations in relation to the purposes, in accordance with Article 39 EUDPR.**

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

Done at Brussels on 21 February 2025.

Wojciech Rafał WIEWIÓROWSKI
(e-signed)