EFTA Court

1 rue du Fort Thüngen

L-1499 Luxembourg

Vaduz, 14 July 2025

To the President and Members of the EFTA Court

Written Observations

submitted, pursuant to Article 20 of the Statute and Article 97 of the Rules of Procedure of the EFTA Court, by the

Government of the Principality of Liechtenstein

represented by Dr. Andrea Entner-Koch, Director of the EEA Coordination Unit (*Leiterin der Stabsstelle EWR der Regierung des Fürstentums Liechtenstein*) and Dr. Claudia Bösch, Deputy Director of the EEA Coordination Unit *(Stellvertretende Leiterin der Stabsstelle EWR der Regierung des Fürstentums Liechtenstein)*, acting as agents of the Government of the Principality of Liechtenstein,

in Case E-5/25

Rainer Silbernagl v Universität Liechtenstein (University of Liechtenstein)

in which the Princely Supreme Court (*Fürstlicher Oberster Gerichtshof*; hereinafter referred to as '*Princely Supreme Court'*) has requested the EFTA Court to give an advisory opinion pursuant to Article 34 of the Agreement between the EFTA States on the Establishment of a Surveillance Authority and a Court of Justice.

The Government of the Principality of Liechtenstein (hereinafter referred to as '*Liechtenstein Government*') has the honour to submit the following observations:

I. Questions referred to the EFTA Court

The Princely Supreme Court has stayed its proceedings in order to refer the following questions to the EFTA Court:

1. Must the second sentence of Article 38(3) of the GDPR be interpreted as meaning that it precludes a national provision such as, in the present case, Article 7(4) of the Data Protection Act, according to which a data protection officer employed by a public body may only be dismissed by the public body with just cause, in particular, where circumstances exist in the presence of which continuation of the employment relationship can, on good faith grounds, no longer be reasonably expected, even if the data protection officer precisely does not perform his function or does not perform it correctly?

2. Must the second sentence of Article 38(3) of the GDPR as worded in German be interpreted as meaning that the term '*dismissed*' (in German '*abberufen*') includes also an (ordinary) termination of the employment contract by the employer of the data protection officer if, as a result, the employment contract basis and thus the factual possibility of exercising the activity of data protection officer ceases to exist?

3. Does the protective purpose of the second sentence of Article 38(3) of the GDPR, that is to say, safeguarding the functional independence of the data protection officer, require an interpretation of this provision and corresponding national rules serving the same protective purpose, such as Article 7(3) and (4) of the Data Protection Act, to mean that a dismissal which is effected contrary to these rules entails that the

dismissal is void and that the employment relationship between the employer and data protection officer as such remains intact?

II. Factual background of the case

1. As regards the facts of the case at hand, the Liechtenstein Government would like to refer to the summary of the facts provided by the Princely Supreme Court in its request for an advisory opinion.

III. Legal framework

2. As regards the legal framework applicable to the case at hand, the Liechtenstein Government would like to refer to the summary of the legal framework relevant to answer the questions referred for a preliminary ruling as laid down by the Princely Supreme Court in its request for an advisory opinion.

3. In its following written observations, the Liechtenstein Government will refer to the following legal framework:

EU and EEA Law

4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as '*Data Protection Directive'*)[1] was a landmark piece of European Union legislation. It laid the foundation for modern data protection law in Europe.

5. The Data Protection Directive was incorporated into the EEA Agreement by Joint Committee Decision No. 83/1999,[2] which entered into force on 1 July 2000.

6. The application of the Data Protection Directive was extended to the EU institutions and bodies themselves by Article 286 of the Treaty establishing the European

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 298, 23.11.2000, p. 41.

Community (hereinafter referred to as '*EC Treaty*').[3]

7. Article 100a of the EC Treaty[4] served as a legal basis for the Data Protection Directive. Article 100a, which was renumbered and replaced by Article 114 of the Treaty on the Functioning of the European Union (hereinafter referred to as the '*TFEU*')[5] with the Treaty of Lisbon in 2009[6], empowered the EU legislator to adopt measures for harmonizing laws necessary for the establishment and functioning of the internal market.

8. With Article 16 TFEU, the Treaty of Lisbon further introduced the constitutional basis for the EU's modern data protection framework.[7]

9. On the basis of Article 16 TFEU, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (*General Data Protection Regulation*; hereinafter referred to as '*GDPR*') was adopted.[8]

10. The GDPR was incorporated into the EEA Agreement by Joint Committee 154/2018,[9] which entered into force on 20 July 2018.

National Law

11. The Liechtenstein Data Protection Act of 4 October 2018 entered into force on 1 January 2019.[10] Relevant for the case at hand is Article 7 paragraphs 3 and 4 of the Data Protection Act.

12. Article 7 paragraph 4 of the Data Protection Act refers to Article 24 of the Law of 24

---

3 OJ C 325, 24.12.2002, p. 33.
4 OJ L 169, 29.6.1987, p. 1.
5 OJ C 202, 7.6.2016, p. 1.
6 OJ C 306, 17.12.2007, p. 1.
7 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016E016.
8 OJ L 119, 4.5.2016, p. 1.
9 OJ L 183, 19.7.2018, p. 23.
10 LR 235.1. See also the English version of the Data Protection Act.

April 2008 on the State Employees (*Staatspersonalgesetz*; hereinafter referred to as '*State Employees Act*').[11]

13. Moreover, the following written observations will refer to the Liechtenstein Civil Code of 1 June 1811 (*Allgemeines Bürgerliches Gesetzbuch*; hereinafter referred to as '*Liechtenstein Civil Code*').[12]

IV. Preliminary remarks

The GDPR and its overall objective

14. Data protection was one of the areas which was not as well-known as today in Liechtenstein before its accession to the EEA.

15. Equally, in the EU, the necessity for data protection developed gradually.

16. In the early to mid-1990s, the need for a harmonised measure to ensure the well-functioning of the internal market for data protection occurred.

17. However, until Article 16 TFEU was established with the Treaty of Lisbon, the EU legislator had no specific legal basis for the harmonization of data protection law.

18. In the absence of such a specific legal basis in EU primary law, the European legislator had to base its first Data Protection Directive on Article 100a TFEU, the general legal basis for harmonizing internal market laws.

19. With the well-functioning of the internal market, not only the economic and social integration increased, but also cross-border flows of personal data. In that sense, Member States and their authorities are being called upon by Union – and EEA law – to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

---

11 LR Nr. 174.11.
12 LR Nr. 210.0.

20. Consequently, the Member States considered it necessary to establish a standalone provision in EU primary law referring explicitly to data protection.

21. Accordingly, with the Treaty of Lisbon, Article 16 TFEU was introduced as the first specific article in EU primary law dealing with data protection.

22. Article 16 TFEU grants every individual the right to the protection of their personal data and empowers the EU legislator to adopt laws governing data processing by both the EU institutions, and the Member States when acting within the scope of EU law.

23. On the basis of Article 16 TFEU, the GDPR was adopted. Article 16 TFEU is the sole legal basis of the GDPR.

24. The overall objective of the GDPR is the protection of personal data of individuals as regards the processing of their personal data and the free movement of personal data.

25. This is also extensively described in the numerous recitals of the GDPR, and very clearly stated in Article 1 paragraph 1 GDPR:

    '*This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data*.'

26. Further, Article 1 paragraph 2 GDPR states that '*this Regulation protects fundamental rights and that freedoms of natural persons and in particular their right to the protection of personal data'*.

27. The nearly 100 articles of the GDPR are dedicated to achieving this overall objective: the protection of natural persons' personal data.

Data protection officer – Legal basis and objectives

28. The vast majority of the articles of the GDPR set up the rules for the controller and the

processor of personal data of individuals. [13]

29. Only three Articles of the GDPR, concretely Articles 37, 38 and 39 GDPR, deal with the Data Protection Officer.

30. Article 37 GDPR governs the designation of a data protection officer and sets out when and by whom a data protection officer must be appointed. In particular, Article 37 states the obligation of the controller and the processor of personal data to designate a data protection officer in specific cases.

31. Pursuant to Article 37 GDPR, the obliged organisations are

- public authorities or bodies, irrespective of what data is being processed,
- if the core activities of the controller and processor consist of processing operations, which require regular and systemic monitoring of data subjects on a large scale, or
- if the core activities of the controller and processor consist of processing on a large-scale special category of data or personal data relating to criminal convictions and offences.[14]

32. Article 38 GDPR governs the position of the data protection officer, whereas Article 39 defines the responsibilities and tasks of a data protection officer.

33. It is worth emphasizing that the GDPR offers the obliged organisations <u>two options</u>:

The data protection officer can

---

[13] The terms 'controller' and 'processor' are defined in Article 4 paragraphs 7 and 8 of the GDPR: 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; whereas 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

[14] Article 29 Data Protection Working Party, adopted 13 December 2016, last revised and adopted on 5 April 2017, p. 20 (https://ec.europa.eu/newsroom/just/document.cfm?doc_id=44100).

a) either be a staff member or

b) a person fulfilling this task by a services contract.

34. This distinction is decisive in two ways:

First, the European legislator was confident that both ways, either a data protection officer as a staff member or a person fulfilling this task by a services contract are able to secure the overall objective of the GDPR, namely the protection of the personal data of individuals.

Second, the GDPR itself leaves it up to the controller and the processor to choose what fits best for the concrete organisation.

35. Pursuant to Article 38 paragraph 6 GDPR, the data protection officer may fulfil other tasks and duties. However, the controller or processor must ensure that any such tasks and duties do not result in a conflict of interests.

36. It results from this that in case the data protection officer is a staff member, they may hold other roles in the organisation, but the controller or processor must always ensure that these additional duties do not compromise the data protection officer's independence or create a conflict of interests.

37. In case the controller or processor fails to appoint a data protection officer where required, or in case the controller or processor does not take all necessary measures to avoid a conflict of interests according to Article 38 paragraph 6 GDPR, the independent Data Supervisory Authority[15] may initiate an investigation for non-compliance. Such an infringement may result in administrative fines pursuant to Article 83 GDPR or penalties under Article 84 GDPR.

38. All these arguments combined together obviously demonstrate the clear intention of the European legislator to ensure the protection of the personal data of individuals to

[15] See Articles 51 et seq. GDPR.

the largest extent possible, while at the same time respecting the scope of its legislative competences and the Member States' competences in contract and labour law.[16]

39. It follows that the European Legislator had no intention to impose any kind of harmonisation in employment law with the GDPR, in order to respect the limits of its legislative power conferred to by Article 16 TFEU.[17]

Tasks of a data protection officer

40. In order to be able to answer the Princely Supreme Court's questions, the Liechtenstein Government considers it necessary to first of all carefully scrutinize the tasks assigned to the data protection officer by the GDPR:

41. The tasks of the data protection officer are defined in in Article 39 GDPR and can be summarized as follows:

    - involvement in all issues related to personal data in an advisory capacity,
    - but never with a decision-making competence.

42. The GDPR states that the data protection officer has to be a) informed, b) involved and c) has to render advice. According to Article 38 paragraph 3, the data protection officer must be able to perform their tasks with a sufficient degree of autonomy within the organisation and without any conflict of interests.

43. It results explicitly from the GDPR that it is always the controller or processor who is responsible for compliance with data protection law and it is always the controller or processor themselves who must be able to demonstrate compliance with data protection law.[18]

---

[16] European Court of Justice C-534/20, *Leistritz AG*, recital 32.

[17] Opinion of Advocate General Richard de la Tour in C-534/20 delivered on 27 January 2022, recital 60.

[18] See Articles 24 and 28 GDPR and further https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A, p. 15.

44. The GDPR only provides for a special level of protection for the data protection officer when performing their tasks under Article 39 GDPR:

    The Data Protection Officer '*shall not be dismissed or penalised by the controller or the processor for performing his tasks*'.[19]

45. In any other case, meaning all cases in which the data protection officer is not dismissed or penalised by the controller or the processor for performing their tasks as a data protection officer, the GDPR does not provide for special level of protection for the data protection officer.

46. It is thus evident that that the special level of protection granted to the data protection officer by the European legislator is limited strictly to the fulfilment of their designated tasks and does not extend beyond those tasks.

47. Consequently, Article 38 paragraph 3 GDPR allows for a termination of the data protection officer's contract for all reasons which do not relate to the fulfilment of their tasks as a data protection officer, provided that it complies with the applicable national labour or contract law.[20]

Legal Analysis

48. First of all, the Liechtenstein Government would like emphasize that the overall objective of the GDPR, namely the protection of personal data of individuals as regards the processing of their personal data and the free movement of personal data, must be borne in mind when answering the questions referred to the EFTA Court by the Princely Supreme Court.

---

[19] '*This requirement strengthens the autonomy of data protection officers and helps ensure that they act independently and enjoy sufficient protection in performing their data protection tasks*' (https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A, p. 15).

[20] https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A, p.15, 16: '*As a normal management rule and as it would be the case for any other employee or contractor under, and subject to, applicable national contract or labour and criminal law, a data protection officer could still be dismissed legitimately for reasons other than for performing his or her tasks as a data protection officer*'.

49. Further, the Liechtenstein Government notes that a clear distinction has to be made between

    a) a dismissal of a data protection officer (in German '*Abberufung*') in their function as a data protection officer and

    b) an ordinary termination of an employment contract of the data protection officer, which inherently entails the termination of their function as a data protection officer.

50. Whereas the first question of the Princely Supreme Court concerns the dismissal of a data protection officer for just cause, the second and the third question of the Princely Supreme Court concern the ordinary termination of the employment contract of a data protection officer.

Question 1 – Dismissal of a data protection officer

51. With its first question, the Princely Supreme Court seeks to know whether Article 38 paragraph 3 GDPR precludes a national provision, according to which

    - a data protection officer employed by a public body may only be dismissed for just cause,

    - even if the data protection officer precisely does not perform their function at all or does not perform it correctly.

52. As has been explained in detail above, the GDPR protects a data protection officer solely against a dismissal related to the performance of their data protection duties. The national law of the EEA States may, however, provide further safeguards for dismissal in line with the applicable national labour or contract law.

53. Such safeguards do not contradict the GDPR as long as they do not dismiss or penalise the data protection officer for performing their tasks under Article 39 GDPR (Article 38 paragraph 3 GDPR).

54. An interpretation of the GDPR that would protect the data protection officer even when they do not perform their function at all or if they do not perform their function correctly, would clearly contradict the overall objective of the GDPR, namely the protection of personal data of individuals.[21]

55. The second sentence of Article 38 paragraph 3 of the GDPR does hence not require such an interpretation.

56. Rather, the second sentence of Article 38 paragraph 3 of the GDPR must be interpreted as meaning that it precludes an interpretation of a national provision, according to which a data protection officer employed by a public body may only be dismissed by the public body with just cause, even if the data protection officer precisely does not perform his function or does not perform it correctly.

Question 2 – ordinary termination of an employment contract

57. With its second question the Princely Supreme Court asks whether the second sentence of Article 38 paragraph 3 GDPR as worded in German must be interpreted as meaning that the term '*dismissed*' (in German '*abberufen*') includes also an ordinary termination of the employment contract of the data protection officer if, as a result, the employment contract basis and thus the factual possibility of exercising the activity of a data protection officer ceases to exist.

58. With regard to the second question, the Liechtenstein Government refers to its considerations in recitals 51 and 52. The GDPR clearly distinguishes between a dismissal of the data protection officer according to Article 38 paragraph 3 GDPR and an ordinary termination of the employment contract, which has to be assessed under national labour or contract law.

---

[21] See the European Court of Justice C-534/20, *Leistritz AG*, recital 35: '*In particular, as the Advocate General observed in points 50 and 51 of his Opinion, such increased protection cannot undermine the achievement of the objectives of the GDPR. That would be the case if it prevented any termination of the employment contract, by a controller or by a processor, of a data protection officer who no longer possesses the professional qualities required to perform his or her tasks or who does not fulfil those tasks in accordance with the provisions of the GDPR*'.

59. It results from the wording of Article 38 paragraph 3 GDPR that said provision does not contradict a termination of the employment contract of a data protection officer for all reasons which do not relate to the performance of their tasks under Article 39 GDPR. Nonetheless, such a termination must comply with the applicable national labour or contract law. [22]

60. Thus, the admissibility of an ordinary termination of an employment contract with regular notice must not be assessed under the GDPR, including the second sentence of Article 38 paragraph 3 GDPR. Rather, it must be assessed under national labour or contract law.

61. In Liechtenstein, such an ordinary termination of an employment contract is subject to the provisions of the Liechtenstein Civil Code.

62. It follows that any employment contract is subject to national civil law principles and where such an employment contract ceases to exist, a person cannot act as a Data Protection Officer anymore.

63. Hence, in such a case, there is no need for a separate dismissal ('*Abberufung*').

64. Therefore, the answer to the second Question by the Princely Supreme Court is that an (ordinary) termination of the employment contract of a data protection officer does not necessitate a separate dismissal ('*Abberufung*'). Rather, the termination of the data protection officer's employment contract inherently results in their dismissal from the role of data protection officer.

Question 3 – consequences of an unjustified dismissal

65. With its third question, the Princely Supreme Court asks whether the protective purpose of the second sentence of Article 38 paragraph 3 of the GDPR, requires an interpretation of this provision and corresponding national rules to mean that a

[22] https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A, p. 15 and 16.

dismissal which is contrary to these rules entails that the dismissal is void and that the employment relationship between the employer and the data protection officer as such remains intact.

66. The second sentence of Article 38 (3) GDPR reads as follows:

'He or she (= the data protection officer) shall not be dismissed or penalised by the controller or processor for performing his tasks.'

67. In Liechtenstein Law, said provision is mirrored in Article 7 paragraph 3 Data Protection Act, stipulating that a data protection officer enjoys a higher level of protection as far as they perform their tasks in relation to the protection of personal data of individuals.

68. It clearly results from the wording of Article 38 paragraph 3 GDPR that said provision solely aims at protecting the data protection officer when performing their tasks as a data protection officer.

69. In all cases where the data protection officer is misusing their tasks as a data protection officer, their dismissal as a data protection officer is possible according to Article 7 paragraph 3 Data Protection Act, which refers to Article 24 of the State Employees Act.

70. Pursuant to Article 24 of the State Employees Act, a termination of a contract is permitted for just cause, meaning that an important reason ('*wichtiger Grund*') has to exist, which would make a continuation of the contract unacceptable.

71. It follows from this that the decisive element for an application of Article 7 paragraphs 3 and 4 Data Protection Act in combination with Article 24 State Employees Act is the termination of a contract of a data protection officer for an important reason.

72. All other cases of an ordinary termination, where an important reason does not exist, and with regular notice, are not subject to the GDPR, but they must be assessed under national labour or contract law.

73. In case an employment contract ceases to exist, a person has no contractual basis to act as a data protection officer anymore, meaning that a separate dismissal ('*Abberufung*') in addition to the termination of the employment contract is not necessary.

74. The absence of such a separate dismissal ('*Abberufung*') does hence not result in a situation in which the employment relationship between the employer and the data protection officer as such remains intact.

75. Therefore, Question 3 of the Princely Supreme Court has to be answered in the negative.

V. Conclusions

Following the observations above, the Liechtenstein Government considers that the questions referred to the EFTA Court for an advisory opinion should be answered as follows:

1. The second sentence of Article 38(3) GDPR must be interpreted as meaning that it precludes an interpretation of a national provision such as, in the present case, Article 7(4) of the Data Protection Act, according to which a data protection officer employed by a public body may only be dismissed by the public body with just cause, in particular, where circumstances exist in the presence of which continuation of the employment relationship can, on good faith grounds, no longer be reasonably expected, even if the data protection officer precisely does not perform his function or does not perform it correctly.
2. The second sentence of Article 38(3) of the GDPR as worded in German must be interpreted as meaning that the term '*dismissed*' (in German '*abberufen*') includes also an (ordinary) termination of the employment contract by the employer of the data protection officer if, as a result, the employment contract basis and thus the factual possibility of exercising the activity of data protection officer ceases to exist.

3. The protective purpose of the second sentence of Article 38(3) of the GDPR, that is to say, safeguarding the functional independence of the data protection officer, does not require an interpretation of this provision and corresponding national rules serving the same protective purpose, such as Article 7(3) and (4) of the Data Protection Act, to mean that a dismissal which is effected contrary to these rules entails that the dismissal is void and that the employment relationship between the employer and data protection officer as such remains intact.

On behalf of the Liechtenstein Government

Dr. Andrea Entner-Koch
Director
EEA Coordination Unit

Dr. Claudia Bösch
Deputy Director
EEA Coordination Unit