

Application No. 37050/22
Foreningen imod Ulovlig Logning v. Denmark
Observations of the Government of Denmark

1. Introduction

1. By letter of 20 January 2023 the European Court of Human Rights (hereinafter ‘the Court’) notified the Government of Denmark (hereinafter ‘the Government’) of the above application (hereinafter ‘the application’) and invited the Government to notify the Court of its position regarding a friendly settlement of the case. By letter of 14 April 2023, the Government informed the Court that it did not consider the present case suitable for a friendly settlement.

2. By letter of 18 April 2023 the Court invited the Government to submit written observations on the admissibility and merits of the case with regard to whether the existing Danish rules and the Danish Supreme Court judgment of 30 March 2022 are contrary to Articles 8, 10 and 13 of the European Convention on Human Rights (hereinafter ‘the Convention’).

3. In essence, the Government submits, in the first place, that the application is inadmissible under Article 35(1) of the Convention and in the second place, that the applicant has failed to demonstrate any violation of Article 8, 10 or 13, whether due to the repealed Danish data retention rules or the existing Danish data retention rules.

4. The Government is at the disposal of the Court should these observations or the application in general give rise to any questions.

2. Facts of the case

2.1. The civil proceedings between Foreningen imod Ulovlig Logning and the Minister for Justice

5. On 1 June 2018, proceedings were instituted by Foreningen imod Ulovlig Logning (*the Association Against Illegal Surveillance*) (hereinafter ‘the applicant’) against the then Minister for Justice before the Copenhagen

City Court (*Københavns Byret*), which referred the matter to the Eastern High Court (*Østre Landsret*).

6. The applicant made two claims for a declaratory judgment. The applicant's first claim was that the Executive Order No. 988 of 28 September 2006 on the Retention and Storage of Traffic Data by Providers of Electronic Communications Networks and Services ('the Executive Order on Data Retention'), which applied previously, was invalid under EU law, and the second claim was that the Minister for Justice had not brought an end to the invalid state of the law created by the Executive Order on Data Retention as soon as possible as required by EU law. The applicant submitted that the claims were not ranked according to priority.

7. The Eastern High Court delivered a judgment in the matter on 29 June 2021. As regards the first claim, the Eastern High Court gave judgment in favour of the Minister for Justice based on the reasoning that the legal effect of an established conflict with EU law is not to render the Retention Order or any single provisions therein invalid. Instead, Danish courts must refrain from applying Danish rules to the extent that they are incompatible with directly effective provisions under EU law. The applicant's second claim was dismissed for lack of *locus standi*.

8. On 10 July 2021, the Association Against Illegal Surveillance appealed the High Court judgment of 29 June 2021 to the Supreme Court, which delivered a judgment in the matter on 30 March 2022. The Supreme Court upheld the High Court judgment in favour of the Minister for Justice based on the reasoning that, under Danish law, there was no basis for finding the Order on Data Retention – or any single provision therein – invalid to everyone, regardless of the specific circumstances, and the Supreme Court also gave judgment in favour of the defendant as regards the claim that the Danish data retention rules then in force were inapplicable under EU law. The Supreme Court dismissed the applicant's second claim that the Ministry of Justice had failed to bring an end to the invalid state of the law as soon as possible as

required under EU law. The Supreme Court found that the applicant had no *locus standi* in the determination of that claim.

3. Relevant domestic law and practice

3.1. Rules on the retention and storage of data

3.1.1. The rules previously in force

9. Section 786(4) of the Danish Administration of Justice Act (*retsplejeloven*) then in force had been inserted by section 2(3) of Act No. 378 of 6 June 2002. The provision had come into force on 15 September 2007.

10. Under section 786(4) of the Administration of Justice Act then in force, telecommunication network providers and telecommunication service providers were obliged to retain and store traffic data (data retention) for one year for use in criminal investigations and for the prosecution of criminal offences. The Minister for Justice was empowered to make detailed rules for the implementation of this provision following negotiation with the Minister for Industry, Business and Financial Affairs.

11. In pursuance of the authority conferred by section 786(4) of the Administration of Justice Act, detailed rules were laid down on the retention and storage of traffic data by service providers in the Executive Order on Data Retention. The Executive Order came into force on 15 September 2007 (*i.e.* at the same time as the commencement of section 786(4) of the Administration of Justice Act).

12. The Executive Order on Data Retention was amended by Executive Order No. 660 of 19 June 2014, which repealed the rules on the retention of session data (retention and storage of data on Internet connections and Internet traffic data). The statutory amendment was made following the judgment delivered by the European Court of Justice on 8 April 2014 in *Digital Rights Ireland Ltd.* (Joined Cases C-293/12 and C-594/12) as it was the assessment of the Ministry of Justice that the rules were not strictly necessary.

13. It was provided in section 1 of the Executive Order on Data Retention that providers of electronic communications networks and services for end users had to retain and store telecommunication traffic data generated or processed in their networks so that such data could be used in criminal investigations and for the prosecution of criminal offences. However, the contents of communications did not have to be retained and stored.

14. Under section 4 of the Executive Order on Data Retention, providers had to retain specific data on fixed-line and mobile telecommunications as well as on SMS, EMS and MMS messages. The data to be retained included data on calling and receiving numbers, the exact time of the start and end of telecommunications and, as far as mobile communications were concerned, the transmitter mast(s) that a mobile phone connected to at the start and end of the relevant communication and the exact geographic or physical location in the cell at the time of the communication as well as data on the use of anonymous telecom services (pre-paid calling cards). However, as already mentioned, the contents of communications did not have to be retained or stored.

15. Under section 5 of the Executive Order on Data Retention, providers had to retain specific data on users' Internet access. Under section 5(1) of the Executive Order on Data Retention, providers had to retain data on the exact time of the start and end of telecommunications and on the assigned user identities (IP addresses).

16. Under section 9 of the Executive Order on Data Retention, providers had to store data subject to the duty of retention for one year.

3.1.2. Revisions to the Danish data retention rules

17. On 24 March 2021, *i.e.* following the judgment delivered by the European Court of Justice on 6 October 2020 in *La Quadrature du Net and Others* (Joined Cases C-511/18, C-512/12 and C-520/18), the Ministry of Justice submitted to the Danish Parliament a preliminary draft bill revising

the data retention rules. It had to be viewed in light of the assessment made by the Ministry of Justice that the clarity provided by *La Quadrature du Net and Others* as to the EU law requirements of national data retention rules called for a revision of the Danish data retention rules.

18. On 18 November 2021, the Ministry of Justice introduced the Bill Amending the Administration of Justice Act and the Act on Electronic Communications Networks and Services (Amending the rules on retention and storage of traffic data (data retention), etc.) to the Danish Parliament. The Bill was intended to bring the Danish rules in line with EU law. It was suggested in the Bill that the rules should come into force on 1 January 2022. However, the enactment of the Bill was rescheduled as the Legal Affairs Committee (*Retsudvalget*) of the Danish Parliament wanted more time to review and peruse the Bill.

19. On 3 March 2022, the Bill was enacted by the Danish Parliament as Amendment Act No. 291 of 8 March 2022 (the revised data retention rules). The Act came into force on 30 March 2022 (at the same time as the delivery of the Supreme Court judgment in the civil proceedings between the applicant and the Minister for Justice).

3.1.3. Applicable rules

20. By the enactment of Amendment Act No. 291 of 8 March 2022, a number of new provisions were inserted into the Administration of Justice Act on the retention and storage of traffic data by service providers ('data retention') under which it is possible to order service providers to retain and store traffic data. Accordingly, the Amendment Act introduced a two-dimension scheme for the retention of traffic data as the contents of communications are still not retained and stored.

21. *Firstly*, a scheme was set up in pursuance of sections 786b to 786d of the Administration of Justice Act under which service providers could be ordered to perform traffic data retention relating to specific persons and geographical locations in connection with efforts to combat *serious criminal offences*. The

powers conferred by section 786c(1)(i) of the Administration of Justice Act were utilised in part as on 28 June 2022, the National Commissioner of Police (*Rigspolitiet*) ordered service providers to perform a *targeted geographical retention* in areas with many reports of serious offences and areas which require special security considerations in pursuance of section 786c(2) of the Administration of Justice Act. On 29 March 2023, the National Commissioner of Police again ordered service providers to perform *targeted geographical retention*, which order replaced the order imposed by the National Commissioner of Police on 28 June 2022. The rules on *data retention targeted at specific persons* set out in sections 786b and 786d of the Administration of Justice Act are currently not utilised.

22. *Secondly*, a scheme was introduced in pursuance of section 786e of the Administration of Justice Act under which the Minister for Justice, following negotiation with the Minister for Industry, Business and Financial Affairs, may lay down rules by which service providers are ordered to perform *general and indiscriminate retention of traffic data* where, based on sufficiently concrete circumstances, there is reason to assume that Denmark faces a *serious threat to national security* that is deemed to be genuine and present or foreseeable. Rules on general and indiscriminate retention of traffic data can be laid down to apply for periods of one year at a time, see section 786e(2) of the Administration of Justice Act. Section 786e of the Administration of Justice Act was most recently utilised in Executive Order No. 337 of 28 March 2023 on General and Indiscriminate Retention of Traffic Data as from 30 March 2023 until 29 March 2024 and Storage until 29 March 2025 as it is the assessment of the Ministry of Justice that Denmark faces a serious threat to national security that is deemed to be genuine and present or foreseeable. The Ministry of Justice made its assessment based on contributions from the Director of Public Prosecutions (*Rigsadvokaten*), the Danish Security and Intelligence Service (*Politiets Efterretningstjeneste*), the Centre for Terror Analysis (*Center for Terroranalyse*), the Danish Defence Intelligence Service (*Forsvarets Efterretningstjeneste*) and the Centre for Cyber Security (*Center for Cybersikkerhed*). When making its assessment, the Ministry of Justice also took into account the contents of a number of publicly available analysis

documents from the Danish Security and Intelligence Service, the Centre for Terror Analysis, the Danish Defence Intelligence Service and the Centre for Cyber Security.

23. Subject to a substantial litigation risk, it was assumed in the *travaux préparatoires* of Amendment Act No. 291 of 8 March 2022 that in cases of *serious criminal offences*, it was a prerequisite that it was possible for the police and the prosecution service to be granted access to traffic data *generally and indiscriminately* retained and stored by service providers *in order to protect national security*, see section 786e of the Administration of Justice Act. However, the European Court of Justice said in its judgment of 5 April 2022 in *G.D. v. Commissioner of An Garda Síochána* (case C-140/20) that in cases concerning *serious criminal offences*, the police and the prosecution service could not be granted access to traffic data and location data generally and indiscriminately retained and stored by service providers in order to protect national security as otherwise presupposed. **Against that background, the Director of Public Prosecutions and the National Commissioner of Police instructed the police and the prosecution service on the date of the judgment, i.e. on 5 April 2022, that in cases concerning serious criminal offences, the police could not request a court to order service providers, in pursuance of the rules of the Administration of Justice Act, to disclose traffic data generally and indiscriminately retained in order to protect national security. Due to that judgment, it is necessary to amend the Administration of Justice Act.**

24. Under section 786f of the Administration of Justice Act, service providers are also obliged to make a general and indiscriminate retention of data on end users who connect to the Internet. Such data does not disclose the contents of end users' communications, nor the websites or other services that end users visit or use. It takes investigation proper to obtain such data. Executive Order No. 380 of 29 March 2022 on General and Indiscriminate Retention of Traffic Data on End Users' Connection to the Internet provides detailed rules on the duty of service providers to retain and store specific data. The Executive Order provides rules on the data that service providers have to retain and store, including data identifying the individual Internet end user

(i.e. the allocated IP address and source port number as well as the name and address of that subscriber). The police and the prosecution service can by court order file a claim for a discovery order under sections 804 and 804a of the Administration of Justice Act to obtain access to dynamic IP addresses if an ongoing investigation concerns an offence carrying a sentence of imprisonment for a term of three years or more (serious criminal offences), see para. 36 below.

3.2. Rules on access by the police to data retained and stored by telecommunication service providers

3.2.1. Introduction

25. Under Danish law, the police do not automatically have access to data retained and stored by telecommunication service providers.

26. The rules are laid down in Amendment Act No. 291 of 8 March 2022. The Amendment Act harmonised the conditions of access to retained and stored data, imposing identical conditions regardless of whether or not access would be obtained through the interception of communications.

3.2.2. The basic rules applicable to access by the police to data retained and stored by telecommunication service providers

27. The rules applicable to access by the police to retained and stored data are set out in Parts 71 and 74 of the Administration of Justice Act. Part 71 concerns, *inter alia*, the interception of communications (*indgreb i meddelelshemmeligheden*) and Part 74 concerns, *inter alia*, discovery orders (*edition*) in criminal cases.

28. Amendment Act No. 291 of 8 March 2022 created a general harmonisation of the conditions to be met to access data retained and stored by telecommunication service providers. Accordingly, regardless of whether access to data has to be requested under the rules on the interception of communications or under the rules on discovery, the condition that it must be a serious crime is the same. According to that condition, the police can only be granted access to retained and stored data if the investigation concerns a

criminal offence that carries a sentence of imprisonment for a term of three years or more, see section 781(1) and (3) and section 781a (interception of communications) as well as sections 804 and 804a (discovery) of the Administration of Justice Act. Furthermore, the investigation of certain other criminal offences may also justify the grant of access to retained and stored data. That may be the case if the criminal offences investigated concern the intrusion of privacy, for example the unlawful intrusion into another person's computer ('hacking').

29. Furthermore, it is a general condition in order for the police to be granted access to retained and stored data that a certain evidentiary threshold is met.

30. Moreover, for the police to be granted access to retained and stored data, it is a general condition that such access is of some importance to the investigation.

31. The general principle of proportionality also applies to all powers exercised by the police during criminal investigations, see section 782(1) and section 805(1) of the Administration of Justice Act. Accordingly, the police cannot be granted access to retained and stored data if it is a disproportionate measure in light of the purpose of the measure, the importance of the matter and the intrusion and inconvenience that the measure will cause to the person(s) affected.

32. Finally, the interest of the police in being granted access to retained and stored data must be balanced against the intrusion of privacy caused by the measure.

3.2.3. The role of the Danish courts

33. A court order is required before the police can intercept communications and request discovery, see section 783 of the Administration of Justice Act (interception of communications) and section 806 of the Administration of Justice Act (discovery). Before issuing an order, the court will consider whether the conditions specified above have been met.

34. However, the police may intercept communications and request discovery directly from the service providers without a court order if the purpose of the measure may otherwise be defeated, see sections 783(4) and 806(4) of the Administration of Justice Act. In such cases a subsequent court order can be requested.

35. An attorney-at-law must be assigned to represent the party(ies)/person(s) affected by the measures in court, see sections 784, 785 and 806(10) of the Administration of Justice Act. Furthermore, the persons concerned must subsequently be notified by the court of the measure, see sections 788 and 806(10) of the Administration of Justice Act. However, the court may decide that no notification will be given if such notification may be detrimental to the investigation.

3.2.4. Special rules on identity data (IP addresses)

36. According to section 804b of the Administration of Justice Act, the police may demand without a court order that telecommunication service providers disclose data identifying an end-user's access to an electronic communications network or service, for example data retained and stored under section 786f of the Administration of Justice Act. It is a requirement under section 804b that the IP address must be static. If a user has a dynamic IP address, it follows from sections 804 and 804a of the Administration of Justice Act that the rules on discovery must be applied and that, *inter alia*, a court order is required.

4. Admissibility

37. The Government has been asked to address the following questions in its observations:

'1. Can the applicant association claim to be the victim of a violation of Articles 8, 10 and 13 (see, *inter alia*, *Centrum för rättvisa v. Sweden*[GC],no. 35252/08, § 166-177, 25 May 2021)?

2. Was the Supreme Court judgment of 30 March 2022 in breach of Articles 8, 10 or 13 of the Convention (see, *inter alia*, *Big Brother Watch and Others v. the United Kingdom*[GC], nos. 58170/13, and *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, 11 January 2022)?'

4.1. Preliminary observations

38. As a preliminary observation, the Government does not contest that data related to the applicant's correspondence was and is still retained and stored in pursuance of the Danish data retention scheme. Furthermore, the Government does not contest that there is no doubt that the applicant also has the right to respect for its correspondence under Article 8 of the Convention, see, *inter alia*, para. 374 of *Ekimdzhiev and Others* (cited above).

39. However, the Government wants to observe that the domestic proceedings initiated by the applicant prior to the present case related to an *abstract* assessment of Danish law and *abstract claims* for a declaration. As elaborated further below, Danish procedural law does not provide for such assessment. The applicant could instead very easily have used the domestic remedies available to it for the specific retention of the applicant's data and have brought a tort action or similar proceedings.

40. Such remedy would be in accordance with the way that EU law and human rights obligations are enforced by the Danish courts in civil proceedings, *i.e.* that a plaintiff argues that the Danish authorities have acted contrary to applicable EU law or human rights obligations in a *specific* situation. If the courts find in favour of the plaintiff, the authorities will be ordered to refrain from applying the national rule that is found to be contrary to, for example, EU law or human rights obligations.

41. The underlying logic of this type of enforcement can be clearly illustrated by way of the following examples.

42. If proceedings concern, for example, taxation rules claimed to be contrary to EU law or human rights obligations, a plaintiff may claim before

the courts that the plaintiff be taxed so that the national authorities refrain from applying the national rule. On the other hand, if a plaintiff claims that the taxation legislation is generally inapplicable, such claim will not succeed.

43. If proceedings concern, for example, family reunification rules, a plaintiff may claim to have the right to family reunification because a national family reunification rule cannot be applied to the plaintiff because of the rule's non-conformity with EU law or human rights law. On the other hand, if a plaintiff claims that the national family reunification legislation is generally inapplicable, such claim will not succeed.

44. In the present case it is not contested that before Amendment Act No. 291 of 8 March 2022 came into force certain parts of the Danish data retention scheme were contrary to EU law and therefore had to be revised. However, the fact that certain parts of the Danish data retention scheme were contrary to EU law did not, as confirmed by the Supreme Court, mean that the rules were generally inapplicable, but rather that courts and authorities in concrete cases had to refrain from applying the national provisions that were found to be contrary to EU law.

45. Thus, if the Court were to declare the present application admissible, such finding would in reality impose an obligation on domestic courts to conduct an *abstract* assessment, even though no such obligation follows from Danish law or EU law. Furthermore, in the present case, the Court would find itself to be a first-instance court, because – due to the procedural choices, *i.e.* the nature of the claims, made by the applicant and the professional counsel representing the applicant before the Danish courts – the Danish courts have not yet examined the compatibility to the Convention of the Danish data retention scheme.

46. As a further preliminary observation, it is the view of the Government that the abstract nature of the applicant's domestic proceedings makes it essential to distinguish between the two legal contexts of the present case, *i.e.*

the situations *before* and *after* the enactment of Amendment Act No. 291 of 8 March 2022.

47. The legal context *after* the enactment of Amendment Act No. 291 of 8 March 2022 has not been examined by the domestic courts in any way.

48. As regards the situation *before* the enactment of Amendment Act No. 291 of 8 March 2022, the applicant brought civil proceedings at the Danish courts but the courts did not examine the substance of the case due to the abstract nature of the applicant's claims.

49. The Government therefore understands the Court's first question to refer to the *current* legal context, *i.e.* whether the applicant has been a victim of a violation of the Convention as a consequence of the rules following from Amendment Act No. 291 of 8 March 2022.

50. The Government further understands the Court's second question to refer to the *previous* legal context, *i.e.* whether the applicant has been a victim of a violation of the Convention as a consequence of the rules in force before the enactment of Amendment Act No. 291 of 8 March 2022.

4.2. Non-exhaustion of domestic remedies relating to the current legal context

51. Regardless of whether the Court may examine the legislation in question *in abstracto*, which the Court has accepted in the case of secret surveillance measures, and depart from the general approach of the Court to deny individuals such right to challenge a law *in abstracto*, see, *inter alia*, para. 169 of the judgment in *Roman Zakharov v. Russia* (application No. 47143/06) the Government would, in the first place, raise a plea of inadmissibility for non-exhaustion of domestic remedies relating to the part of the application that concerns the *current* legal context, *i.e.* the rules following from Amendment Act No. 291 of 8 March 2022.

52. Based on the following arguments, the Government submits that there are effective domestic remedies available to the applicant. Since the applicant

has not exhausted the domestic remedies relating to the current legal context, the Government submits that the application should be declared inadmissible under Article 35(1) of the Convention for non-exhaustion of domestic remedies.

53. The Government refers to the close affinities between Article 13 and Article 35(1) of the Convention, see, *inter alia*, para. 42 of the judgment in *Slimani v. France* (application No. 57671/00).

54. Article 35(1) of the Convention stipulates that the Court may only deal with the matter after all domestic remedies have been exhausted.

55. The Government observes that it follows from the case-law of the Court that when an applicant has access to a remedy under domestic law which is accessible, capable of providing redress in respect of the applicant's complaints, and offer reasonable prospects of success, the applicant is obliged to use it before applying to the Court, see, *inter alia*, para. 41 of the judgment in *Slimani v. France* (cited above).

56. The Government observes that it is a fundamental principle that states are dispensed from answering before an international body for their acts before they have had an opportunity to put matters right through their own legal system, and those who wish to invoke the supervisory jurisdiction of the Court as concerns complaints against a State are thus obliged to use first the remedies provided by the national legal system, see, *inter alia*, para. 70 of the judgment in *Vučković and Others. v. Serbia*, (applications Nos. 17153/11 and others). Therefore, the Convention machinery is first and foremost of a subsidiary nature.

57. As regards the present case, the Government submits that the applicant has used no domestic remedies before referring the matter to the Court as regards the Danish rules in force after the enactment of Amendment Act No. 291 of 8 March 2022. As will be elaborated further below, the applicant could

very easily have brought a tort action in the domestic courts, and such action would have offered the applicant reasonable chances of success.

58. The exhaustion of such remedies is a necessary step to be taken before the Court can decide a matter if respect for the principle of subsidiarity is to be maintained and in order to prevent the Court from *de facto* becoming a court of first instance.

4.3. Non-exhaustion of domestic remedies relating to the previous legal context

59. The Government submits that the domestic proceedings before the Eastern High Court and the Supreme Court do not mean that the applicant has exhausted domestic remedies relating to the *previous* legal context. **The Government further submits that the applicant chose to institute proceedings in a way that did not enable the courts to examine the substance of the matter even though the applicant could very easily have instituted proceedings, for example have brought a tort action, concerning data retention relating to the applicant's correspondence, and in that case the applicant would have had access to *feasible remedies with reasonable chances of success.*** In the second place, the Government therefore wants to raise a plea of inadmissibility for non-exhaustion of domestic remedies relating to the part of the application that concerns the *previous* legal context, *i.e.* the rules *before* the enactment of Amendment Act No. 291 of 8 March 2022.

60. The Government observes that the obligation to exhaust domestic remedies requires applicants to make normal use of remedies which are available and sufficient in respect of their Convention grievances, see, *inter alia*, para. 71 of the judgment in *Vučković and Others. v. Serbia*, (cited above).

61. It follows from the case-law of the Court that when an applicant is presented with a choice of different remedies, it is for the applicant to select which feasible legal remedy to pursue, see, *inter alia*, para. 23 of *Airey v. Ireland* (application No. 6289/73) and paras 110 and 111 of *O'Keeffe v. Ireland*, (application No. 35810/09). It is the Government's view that this

case-law cannot be applied to mean that an applicant can exhaust domestic remedies by filing claims **that according to national procedural law does not give the courts the possibility to try the substance of the matter.**

Choice of proceedings instituted by the applicant

62. Before the Danish courts, the applicant – who was represented before two Danish court instances **by a major Danish law firm** – made two claims for a declaration. In the first place, the applicant claimed that the Danish data retention rules according to EU-law were declared invalid and, in the second place, that the invalid state of the law according to EU law had not been brought to an end as soon as possible.

63. As regards the first claim, the Supreme Court found that no such abstract and general claim could be assessed under Danish law. As regards the second claim, the Supreme Court found that the applicant had no *locus standi*, again because of the abstract nature of the claim that had no impact on the legal situation of the applicant.

64. The matter was therefore not tried in substance before the domestic courts because the applicant had made claims that could not be tried in abstract under Danish procedural law.

65. It is a fundamental principle of Danish civil procedural law that the parties to a dispute must present the facts of and arguments in a case. This is a feature of the adversarial procedure according to which the parties to a dispute have the primary responsibility for finding and presenting evidence. The principle is set out in section 338 of the Administration of Justice Act, which states that courts cannot award a party more than claimed by the party and that courts can only take into consideration what the parties have presented before the court. **Courts cannot, by their own accord, gather information about the matter nor take into consideration claims not introduced by the parties themselves.** Accordingly, courts may only give judgment to the basis provided by the parties. This principle expresses respect for the fact that

a civil case pertains to the circumstances of the parties to the case and as such, the parties should be in full command of their own affairs.

66. The adversarial procedure forces the parties to present their claims and the basis of the claims that the parties can ask a court to adjudicate on. As stated above, the parties cannot demand a court to take more into consideration than what has been presented. Additionally, the adversarial procedure is also an element of the principle of enforceability.

67. If a party to a case fails to present its claims and facts in a manner that makes it possible for the court to decide the matter, the court may dismiss the case or rule in favour of the other party. As such, if a claim is too abstract or does not concern a party itself, the court cannot make a decision, and the case will be dismissed, or judgment will be given in favour of the other party.

68. Judges have the possibility to guide parties in order to help them clarify their claims and arguments if those presented by the parties are unclear or incomplete. This possibility is set out in section 339 of the Administration of Justice Act, which says that a judge may ask questions to help clarify claims. Section 339 is optional, and judges should avoid using the possibility if the party in question is represented by a counsel, as was the case with the applicant. Even when a judge seeks to clarify a claim or an argument, the fundamental principle of the adversarial procedure must be upheld. It is paramount that the questions asked by a judge do not jeopardise the impartiality of the judge.

69. When applied to the present case, it is relevant to reiterate that a party's legal interest in a case must not be purely academic or hypothetical. A claim that the authorities must recognise a certain general interpretation of a legal provision does not constitute a matter of current interest, see, *inter alia*, the Supreme Court judgment published in the Weekly Law Reports for 2010 under **U2010.2109 H**, in which the Supreme Court dismissed a case brought against the Ministry of Culture concerning the general interpretation of a provision of the Copyright Act and not a concrete legal dispute.

70. Since the applicant's proceedings before the domestic courts concerned a matter of general interpretation, *i.e.* the claim that the Danish data retention rules should be declared invalid under EU law, and not a concrete legal dispute, the outcome of the proceedings was attributable to the procedural choices made by the applicant.

71. The applicant was not faced with any obstacles preventing it from instituting civil proceedings with claims of a less abstract nature. If such proceedings had been instituted, it would have added essential elements that could have been taken into account by the domestic courts, see, *inter alia*, para. 69-73 of the Court's decision in *Köhler v. Germany* (application No. 3443/18)

72. In light of the above principles of Danish procedural law and the abstract nature of the applicant's claims before the Danish courts, the Government is of the view that the applicant's procedural choices were the reason why the case was not tried in substance. When domestic law provides a remedy with reasonable chances of success, as demonstrated below, the applicant is required to exhaust such remedy before the matter can potentially be brought before the Court, see *a contrario, inter alia*, part I.B.1 of the decision in *Bosphorus Hava Yollari Turizm ve Ticaret AS v. Ireland* (application No 45036/98) and the decision in *Hilal v. the United Kingdom* (application No. 45276/99).

73. Before the Danish courts, the applicant took the path of an abstract assessment of Danish legislation instead of instituting civil proceedings, for example with a claim for compensation, which could have been symbolic of nature, on the ground that data relating to the applicant association or its members had been retained and stored according to Danish legislation. **If such a case had been brought to court, the courts would be obliged to determine whether the Danish data retention rules were compatible with EU law.**

74. Were the Court to declare the present application admissible, it would therefore entail a *de facto* rejection of the basic Danish procedural rules applicable to civil proceedings.

Remedies available under Danish law

75. The Supreme Court's judgment in favour of the Minister for Justice was based, *inter alia*, on the grounds that the claims submitted by the applicant were that abstract in nature that they could not be assessed. In its reasoning, the Supreme Court addressed the circumstance that the applicant's claim could have been subject to assessment if it had concerned a concrete legal dispute.

76. As the subject matter of the case brought before the domestic courts related to the claim that Danish law was not in conformity with obligations under EU law, the Danish case law provides examples demonstrating that civil tort proceedings with such claims offer real prospects of success. In the Supreme Court judgment published in the Weekly Law Reports for 2017 under U2017.1243 H, the Supreme Court found that the Ministry of Employment was liable to pay compensation to the plaintiff for its failure to revise a statute (the Holiday Act) to make it accord with EU law (Directive 2003/88/EC concerning certain aspects of the organisation of working time) in a timely manner. Another example is the Eastern High Court judgment of 19 May 2022 (case BS-25897/2019-OLR) in which the Eastern High Court found that Danish law was not in compliance with EU law (Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society) and that the Ministry of Culture was liable to pay compensation to the plaintiff.

77. Danish case law provides further examples concerning the rules on discovery, where it was found that those rules could not be applied in relation to concrete data retained and stored by telecommunication service providers. In the High Court judgment published in the Weekly Law Reports for 2019 under U2019.2019Ø, the Eastern High Court found that according to, *inter*

alia, EU law, service providers could not be required to provide concrete data stored in pursuance of data retention obligations for the use in civil proceedings concerning specific copyrights infringements. **The High Court's judgment was therefore an effective remedy in the concrete case.**

78. The examples mentioned above clearly demonstrate that the applicant had feasible remedies available and still has. The exhaustion of such remedies is a necessary step to be taken before the Court can decide a matter if respect for the principle of subsidiarity is to be maintained and in order to prevent the Court from *de facto* becoming a court of first instance.

79. On the basis on the above observations, the Government therefore wants to raise a plea on inadmissibility for non-exhaustion of domestic remedies under Article 35(1) of the Convention.

5. Merits

80. Should the Court find that domestic remedies have been exhausted, the Government submits that the application should be declared inadmissible as manifestly ill-founded in its entirety within the meaning of Article 35(3)(a). Should the Court find the application admissible, the Government submits that neither the Supreme Court judgment of 30 March 2022 nor the current Danish legislation is in breach of Article 8, 10 or 13 of the Convention.

81. Given that the Supreme Court judgment did not include an assessment of the substance of the alleged violation – because the applicant had submitted claims, which did not provide for such an assessment even though it would have been possible to have had an assessment of the substance if the applicant and his professional counsel had submitted adequate claims, see paras 4.1-4.3 – the Government contends that the judgment cannot in itself constitute a breach of the Convention.

82. The Government therefore understand the Court's questions to concern, *in abstracto*, whether the Danish data retention rules constitute a breach of the Convention.

83. The Government wants to reiterate that such an assessment would be detrimental to the competence of the domestic courts as the issue has not yet been determined by the Danish courts since domestic remedies have not been exhausted, see paras 4.1-4.3.

84. Should the Court anyway undertake an *in abstracto* assessment, the Government observes that such an assessment would necessarily have to concern the *current* data retention scheme.

85. The Government observes that the Court found in para. 150 of its judgment in *Centrum för rättvisa v. Sweden* (cited above) that '*it cannot be the Court's task, when reviewing the relevant law in abstracto, as in the present case, to examine compatibility with the Convention before and after every single legislative amendment*'.

86. In *Centrum för rättvisa v. Sweden* (cited above), the Court examined the national legislation as it stood at the time of the examination.

87. Even though the merits should be examined on the basis of the current legislation, the Government observes that the previous Danish data retention rules were also in compliance with the Convention. The rules were revised following judgments delivered by the European Court of Justice that limited the grounds on which data could be retained, stored and accessed. The Government submits that this does not automatically mean that the Danish data retention rules were in breach of the relevant provisions of the Convention as interpreted by the Court, given that it has been established that the Court and the European Court of Justice have diverging views on the legal requirements of national data retention schemes. However, for the sake of completeness, the Government will include in its observations concerning the *grounds on which retained data can be accessed by the authorities* comments on the scheme repealed, given that the repealed scheme corresponds in essence to the current scheme on the other points.

a. Article 8 of the Convention

88. As mentioned above under para. 38, the Government does not contest that data related to the applicant's correspondence was and still is retained and stored in pursuance of the Danish data retention scheme. Furthermore, the Government does not contest that there is no doubt that the applicant also has a right to respect for its correspondence under Article 8 of the Convention, see, *inter alia*, para. 374 of the judgment in *Ekimdzhiev and Others* (cited above).

89. It follows from the case-law of the Court that any interference with an individual's Article 8 rights can only be justified under Article 8(2) if it is in accordance with the law, pursues one or more of the legitimate aims to which that provision refers and is necessary in a democratic society in order to achieve any such aim, see, *inter alia*, para. 332 of the judgment in *Big Brother Watch and Others v. the United Kingdom* (cited above).

90. The Government submits that the Danish data retention rules and the rules on the authorities' subsequent access pursue one or more of the legitimate aims set out in Article 8(2) of the Convention as they are intended to protect national security and public safety and to **prevent serious crimes**.

91. Regarding the final criteria for a justification of an interference under Article 8(2), *i.e.* that the interference is limited to what is necessary in a democratic society in order to achieve those aims, it appears from the case-law of the Court that in relation to the retention and storage of communication data, the lawfulness of the interference is closely related to the 'necessity', and it is therefore appropriate for the Court to address the conditions jointly, see para. 334 of the judgment in *Big Brother Watch and Others* (cited above) and para. 395 of the judgment in *Ekimdzhiev and Others*, (cited above).

92. **Furthermore, it follows from the case-law of the Court that the same safeguards concerning secret surveillance measures apply, *mutatis mutandis*, to the general retention of communication data by telecommunication service**

providers and to the authorities' access to the data in individual cases, see para. 395 of the judgment in *Ekimdzhiev and Others* (cited above).

93. According to paras 395-421 of the judgment in *Ekimdzhiev and Others* (cited above), these minimum conditions are: (1) Accessibility of the law, (2) protection of retained data by telecommunication service providers, (3) grounds on which retained data can be accessed by the authorities, (4) procedure for obtaining access, (5) amount of time for which the authorities may store and use accessed data not subsequently used in criminal proceedings, (6) procedures for storing, accessing, examining, using, communicating and destroying data accessed by the authorities, (7) oversight arrangements, (8) notification and (9) remedies.

(1) Accessibility of the law

94. The Government submits that all Danish statutory provisions **governing the retention of communication data** and the subsequent access by the authorities have been promulgated and are thus accessible to the public, see sections 780ff of the Administration of Justice Act and the relevant implementing measures.

(2) Protection of retained data by telecommunication service providers

95. The Danish rules clearly state that service providers can only store data for one year for the purpose of investigation and prosecution of criminal offences.

96. Furthermore, Danish legislation, *i.e.* section 3 of the Personal Data Security Order (Executive Order No. 1882 of 4 December 2020 (*persondatasikkerhedsbekendtgørelsen*)) requires service providers to continuously take appropriate technical and organisational measures in order to manage data security risks when providing services. Service providers must ensure, through these measures, a level of security that is proportionate to the risks in view of the current state of the technology and the costs associated with the implementation of the measures.

97. These rules require that the measures must at least (1) ensure that personal data can be accessed only by authorised persons and only for lawful purposes, (2) protect the personal data stored or transmitted against accidental or unlawful destruction, accidental loss or changes and unauthorised or illegal storage, processing, access or disclosure and (3) implement a personal data security policy applicable to the provision of services.

98. Service providers are thus required to store and process retained communication data in line with the rules governing the protection of personal data. According to the data protection rules, service providers must also implement various appropriate technical and organisational safeguards to ensure that personal data are not abused and that the data are destroyed when the statutory period for the retention of the data expires.

99. Furthermore, according to section 7 of the Danish Telecommunications Act (*lov om elektroniske kommunikationsnet og tjenester*) telecommunication service providers, including their employees as well as former employees, are bound by a duty of confidentiality corresponding to what applies to public servants in general, see para. 126 below.

(3) Grounds on which retained data can be accessed by the authorities

100. The Government submits that Danish legislation stipulates in an exhaustive manner the grounds on which the authorities may seek access to retained communication data.

101. In short, the general data retention scheme relates to the protection of *national security*, as defined, *inter alia*, with reference to specific crimes forming the grounds on which data can be accessed. The targeted data retention scheme relates to the prevention of *serious crimes*, as defined, *inter alia*, with reference to the maximum length of the sentence for such crimes, which is the grounds on which data can be accessed.

102. The circumstances under which the police can access data are specified in sections 781, 781a, 804, 804a and 804b of the Administration of Justice Act. Those circumstances relate to the seriousness of the crime committed. It follows from those rules when interpreted consistently with EU law that data can be accessed only on the same grounds as those on which the data were retained, for example for reasons of national security if the data were stored for reasons of national security, or for the purpose of combatting serious criminal offences if the data were retained and stored in pursuance of an order on targeted geographical retention of data, for example in areas which require special security considerations.

103. The Government is of the view that the Danish legislation relevant to this case clearly defines the limited grounds on which retained data can be accessed by the relevant authorities.

The repealed Danish data retention rules

104. Before the enactment of Amendment Act No. 291 of 8 March 2022, it followed from Danish legislation that data could be retained and stored for the purpose of the investigation of crimes.

105. The police basically had two different sets of rules governing their access to data retained and stored by telecommunication service providers.

106. The rules on discovery were the default rules when the police wanted to request someone to disclose evidence for the purpose of criminal investigations, including data retained and stored by telecommunication service providers. As regards telecommunication service providers, the rules on discovery were, in practice, applied in order to have providers disclose the identity of the persons to whom a particular IP address had been allocated at a given time as well as lists of the mobile phones which had connected to a certain transmission mast (antenna data (*masteoplysninger*)) at a given time. However, the rules on discovery did not apply if the police wanted to request the disclosure of a message or the like that had been communicated or if the police wanted the disclosure of a list of the telephones or the like that had

been connected to each other, see section 801(3) of the Administration of Justice Act. In the above cases, access to the relevant data followed the rules on the interception of communications.

107. The reason for the distinction between whether or not the disclosure related to intercepted communications is that under Danish law, the interception of communications was considered a more severe intrusion in the right to privacy than disclosure in general. The interception of communications involves a breach of the duty of confidentiality by which telecommunication service providers were and are bound. It was a general condition to be allowed to intercept communications that the criminal offence investigated carried a sentence of imprisonment for a term of six years or more. That was different from the rules on discovery, which, at the time, stipulated no specific conditions concerning the seriousness of the criminal offence investigated to justify a discovery order. In principle, any investigable criminal offence could justify a discovery order.

108. Before Amendment Act No. 291 of 8 March 2022 came into force, the above distinction had the implication that in case the police wanted telecommunication service providers to disclose data, for instance, concerning the phone numbers that had been in contact with one or more specific phone numbers, the police would have to follow the strict rules of Part 71 concerning the interception of communications. However, if the police wanted telecommunication service providers to disclose data on the mobile phones that had connected to a certain transmission mast (antenna data (*masteoplysninger*)), they could rely on the ordinary rules on discovery in Part 74, since the disclosure of that data did not entail the interception of communications.

109. Both sets of rules required the police to obtain a court order before they could request access to retained and stored data. However, in case of urgency, the police could demand access without a court order. In that case, a subsequent court order could (or in case of the interception of

communications *had to*) be requested by the police or the person involved, see para. 118 below.

110. Before Amendment Act No. 291 of 8 March 2022 came into force, the police could, without a court order, order that telecommunication service providers disclosed data which identify an end-user access to an electronic communications networks or services (static IP addresses), see para. 36 above.

111. The Government submits that the repealed Danish data retention scheme provided sufficiently clearly defined and limited purposes for accessing data, and that the repealed Danish data retention rules were **therefore also in accordance with the Convention in this regard.**

(4) Procedure for obtaining access

– Standard procedure

112. **The Government submits that access to retained communication data is granted only when it is genuinely necessary and proportionate in each case.**

113. The Danish legislation **concerning the retention of communication data** and the authorities' subsequent access to such data provides clearly defined safeguards intended **to ensure that retained communication data are accessed only by the relevant authorities and only when it is justified.**

114. **Only the police can access data.** This right of access is governed by Part 71 and 74 of the Administration of Justice Act. Most importantly, it follows from section 783 and 806 of the Administration of Justice Act that access requires a court order.

115. Furthermore, sections 782 and 805 of the Administration of Justice Act clearly provides that no access will be granted if it is deemed disproportionate.

116. As regards the interception of communications (*indgreb i meddelelseshemmeligheden*), it follows from section 783(1) of the

Administration of Justice Act that a court order must specify the telephone numbers, locations, addresses or posting to which the intervention relates. Furthermore, the order must specify the time period that the intervention can be carried out, which period cannot exceed four weeks unless extended by a court order, see section 783(3) of the Administration of Justice Act.

117. Additionally, in pursuance of sections 784, 785 and 806(10) of the Administration of Justice Act, counsel is assigned to **represent the person whose data are the subject matter of the request for access before the court** issues a court order, and the counsel must be allowed the opportunity of making representations to the court, see section 784. The assigned counsel must be notified of all court hearings in the case and is entitled to attend such hearing and to **familiarise himself/herself with the material** presented by the police, see section 785(1).

– *Urgent procedure*

118. According to sections 783(4) and 806(4) of the Administration of Justice Act, the police may access retained communication data without obtaining a court order in advance in case the purpose of the interception of communication data would otherwise be defeated if the police would have to wait for a court order to be granted. **A subsequent court order can be requested. In the case of an interception of communications a subsequent court order is required.**

– *Access to IP addresses*

119. The above standard procedure applies to dynamic IP-addresses, see section 804a of the Administration of Justice Act. As regards static IP addresses, data can be disclosed without a court order, see section 804b of the Administration of Justice Act, see also para. 36 above.

120.

(5) Amount of time for which the authorities may store and use accessed data not subsequently used in criminal proceedings

121. The Government submits that it follows from sections 786b(5), 786c(3), 786d(3) and 786e(3) of the Administration of Justice Act that service providers have to store retained communication data for one year.

122. According to section 791(1) of the Administration of Justice Act, accessed communication data, *i.e.* data accessed following the rules on the interception of communications, must be destroyed if no charges are preferred or charges are dropped in the criminal case for which access was granted. If the accessed data are nevertheless of importance to the investigation, the police can upon court approval choose to keep the relevant data. It follows from section 791(4) that data turning out to be of no significance to the investigation must be destroyed.

123. If data have been obtained under sections 804a and 804b of the Administration of Justice Act, such data are governed by the rules of the Law Enforcement Act (Act No. 410 of 27 April 2017 (*retshåndhævelsesloven*)), implementing EU directive No. 2016/680 (the law enforcement directive) and the filing manual (*arkivhåndbogen*).

124. The Government further refers to the Notice of the Director of Public Prosecutions dated 28 February 2022 on the erasure of telecom data (appended as Exhibit 10).

125. The Government therefore submits that there are clear time limits for the destruction of data accessed by the authorities in the course of criminal proceedings.

(6) Procedures for storing, accessing, examining, using, communicating and destroying data accessed by the authorities

126. Communication data to which the police have obtained access are treated under the Danish data protection rules, which follow, *inter alia*, from the GDPR, Directive (EU) 2016/680, the Danish Data Protection Act (Act No.

502 of 23 May 2018 (*Databeskyttelsesloven*)) and the Law Enforcement Act. It follows from section 4(6) of the Law Enforcement Act that personal data must not be stored in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the data is processed. When administering this rule, the competent authority must balance the interests of the data subject against the interest of the authority in keeping the data, for example for the purpose of continued investigation.

127. Those data protection rules also apply to the retention of data, the consequence being that authorities can only process, collect and use personal data when necessary and proportionate in order to carry out their tasks. According to the data protection rules, the authorities must also implement appropriate technical and organisational measures to ensure that data are not abused, see the Notice of the Director of Public Prosecutions dated 28 February 2022 on the erasure of telecom data (appended as Exhibit 10).

128. Furthermore, data provided by telecommunication service providers to the police are subject to the general duty of confidentiality incumbent on public servants, see in particular section 27 of the Danish Public Administration Act (*forvaltningsloven*) and section 152 of the Danish Criminal Code (*straffeloven*).

129. The Government therefore submits that the procedure to be followed for examining, using and storing data obtained was clearly defined in Danish legislation and the implementing rules, and that the procedure provided the necessary safeguards.

(7) Oversight arrangements

130. It follows from the Danish Telecommunications Act (Consolidation Act No. 955 of 17 June 2022 (*teleloven*)) that the Danish Business Authority (*Erhvervsstyrelsen*) monitors that service providers comply with the rules for the processing of telecommunication data and personal data, see section 20(2) of the Telecommunications Act and sections 12 and 13 of the Personal Data

Security Order. It follows from section 27 of the Data Protection Act that the Danish Data Protection Authority (*Datatilsynet*) monitors the compliance with the rules on personal data security, including the GDPR.

131. Both the Danish Business Authority and the Danish Data Protection Authority may ask service providers to provide them with data relevant to their mandate, see section 12(2) of the Personal Data Security Order and section 29 of the Data Protection Act.

132. Under section 12, cf. section 3, of the Personal Data Security Order, the Danish Business Authority may furthermore review the technical and organisational measures taken by service providers to store retained communication data. The Authority may also give binding instructions to service providers and sanction them in case of non-compliance.

133. According to section 786i(3) of the Administration of Justice Act, service providers must inform the police of personal data breaches, see Article 4(12) of the GDPR. Such breaches may trigger a duty of notification of the relevant individuals, see Article 34 of the GDPR.

134. Service providers are also obligated to notify the Danish Business Authority of personal data breaches, see section 8 of the Telecommunications Act and section 5 of the Personal Data Security Order.

135. The nature of the monitoring of service providers' processing of communication data and of the powers of the supervisory authorities can therefore be derived directly from national legislation.

(8) Notification

136. When an interference with the secrecy of correspondence is ended, the relevant person must be notified of the interference, see sections 788 and 806(10) of the Administration of Justice Act. Such notification may be postponed if notification would be detrimental to the investigation or to the investigation in another case pending. In those circumstances, the assigned

counsel is notified and has the opportunity to make a submission, see sections 788(4) and 806(10).

(9) Remedies

137. Regarding the existence of effective remedies, the Government refers to its observations in paras 4.1.-4.3.

b. Article 10 of the Convention

138. The Government is of the view that the application should be examined solely under Article 8 of the Convention, see para. 361 of the judgment in *Ekimdzhiev and Others v. Bulgaria* (cited above).

c. Article 13 of the Convention

139. The Government is of the view that the application should be examined solely under Article 8 of the Convention, see para. 361 of the judgment in *Ekimdzhiev and Others v. Bulgaria* (cited above).

140. In any case, the Government submits that effective remedies were available to the applicant, and that the applicant failed to exhaust those remedies, see para. 4.1.-4.3. above.

6. Conclusion

141. In the first place, the Government submits that the application is inadmissible under Article 35(1) of the Convention for non-exhaustion of domestic remedies.


142. In the second place, the Government submits that the application should be declared inadmissible as manifestly ill-founded in its entirety within the meaning of Article 35(3)(a) of the Convention.

143. Should the Court find the application admissible, the Government submits that neither the Supreme Court judgment of 30 March 2022 nor the relevant Danish legislation is in breach of Articles 8, 10 or 13 of the Convention.

Copenhagen, 11 July 2023



Mrs Vibeke Pasternak Jørgensen
Agent of the Government of Denmark



Mrs Nina Holst-Christensen
**Co-Agent of the Government
of Denmark**

