EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FOURTH SECTION

DECISION

Application no. 57294/16
Wilhelmus Paulus WILLEMS
against the Netherlands

The European Court of Human Rights (Fourth Section), sitting on 9 November 2021 as a Chamber composed of:

Yonko Grozev, *President,*
Tim Eicke,
Armen Harutyunyan,
Gabriele Kucsko-Stadlmayer,
Pere Pastor Vilanova,
Jolien Schukking,
Ana Maria Guerra Martins, *judges,*

and Andrea Tamietti, *Section Registrar,*

Having regard to the above application lodged on 27 September 2016,

Having deliberated, decides as follows:

THE FACTS

1. The applicant, Mr Wilhelmus Paulus Willems, is a Dutch national who was born in 1947 and lives in Wijnandsrade. He was represented before the Court by Mr T. Barkhuysen, a lawyer practising in Amsterdam.

A. The circumstances of the case

2. The facts of the case, as submitted by the applicant, may be summarised as follows.

3. The applicant applied to the mayor of Nuth for a new passport in June 2010. The mayor did not process the request because the applicant had refused to provide fingerprints that would be digitised and saved on a Radio Frequency Identification microchip ("RFID chip") in his passport and in a database. The applicant lodged an objection (*bezwaar*) against this decision,

arguing that creating and storing such biometric data constituted a serious breach of his physical integrity and his right to privacy.

4. On 22 July 2010 the objection was dismissed. It was pointed out that the storage of digitised fingerprints in the passport was required by Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, as amended by Regulation (EC) No. 444/2009 of the European Parliament and of the Council of 28 May 2009 (see paragraphs 10 and 16 below). The requirement had been incorporated in the Passport Act (*Paspoortwet*), which left no room for an exception in the case of the applicant. As to the storage in the database, the mayor referred to the Explanatory Memorandum to the recent amendments to the Passport Act (Parliamentary Documents, Lower House of Parliament, no. 31324, no. 3) where the legislator had explained that this interference with the right to private life was justified.

5. On 29 August 2011 the Maastricht Regional Court (*rechtbank*) rejected an appeal lodged by the applicant, which included a complaint under Article 8 of the Convention.

6. The applicant lodged a further appeal with the Administrative Jurisdiction Division of the Council of State (*Afdeling Bestuursrechtspraak van de Raad van State* – "the Administrative Jurisdiction Division"). He restated his objections against the taking and storage of his fingerprints, asserting, *inter alia*, that the Regional Court had wrongly held that the interference with his right to private life had been sufficiently foreseeable and proportionate. He also argued that the storage and use of biometric data was insufficiently protected against abuse and claimed that he suffered damages because he was unable to travel for business due to the lack of a valid passport. According to the applicant he should have been exempted of providing fingerprints as a conscientious objector, arguing that the text of the applicable legislation did not preclude such an explanation.

7. On 28 September 2012 the Administrative Jurisdiction Division referred the following questions to the Court of Justice of the European Union ("the CJEU") for a preliminary ruling:

> "1. Is Article 1(2), of Council Regulation (EC) 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, as amended by Regulation (EC) No. 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Regulation (EC) No. 2252/2004, valid in light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms?
>
> 2. If the answer to question 1 implies that Article 1(2) of Council Regulation (EC) 2252/2004 of 13 December 2004 on standards for the security features of and biometric data in passports and travel documents issued by Member States, as amended by Regulation (EC) No. 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Regulation (EC) No. 2252/2004 is valid, must

> Article 4(3) of Regulation 2252/2004, read in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, Article 8(2) of the European Convention on the Protection of Human Rights and Fundamental Freedoms and Article 7(f) of the Privacy Directive [95/46], read in conjunction with Article 6(1)(b) of that directive, be interpreted as meaning that, when the Member States give effect to Regulation No. 2252/2004, there should be a statutory guarantee that the biometric data collected and stored pursuant to that regulation may not be collected, processed and used for any purposes other than the issuing of the document concerned?"

In its reference, the Administrative Jurisdiction Division noted that the referred question in the pending case of *Michael Schwarz v Stadt Bochum* (C-291/12) concerned the same issue and requested the CJEU, so far as possible, to proceed with those cases simultaneously.

8. The CJEU did not; it issued a ruling in the *Schwarz*-case on 17 October 2013 (C-291/12, ECLI:EU:C:2013:670). The CJEU found that the taking and storing of fingerprints by the national authorities, as governed by Article 1(2) of Regulation No. 2252/2004, constituted an interference with the rights to respect for private life and the protection of personal data. However, that twofold interference was provided for by law and justified. In so far as relevant, the ruling reads:

> "... concerning the objective of general interest underlying that limitation, it can be seen that Article 1(2) of Regulation No. 2252/2004, when read in the light of recitals 2 and 3 of that regulation, has two specific aims: the first, to prevent the falsification of passports and the second, to prevent fraudulent use thereof, that is to say, use by persons other than their genuine holders.
>
> 37. Accordingly, Article 1(2) is designed, through pursuit of those aims, to prevent, *inter alia*, illegal entry into the European Union.
>
> 38. In those circumstances, it must be found that Article 1(2) of Regulation No 2252/2004 pursues an objective of general interest recognised by the Union.
>
> ...
>
> 40. Fourth, the Court must establish whether the limitations placed on those rights are proportionate to the aims pursued by Regulation No 2252/2004 and, by extension, to the objective of preventing illegal entry into the European Union. It must therefore be ascertained whether the measures implemented by that regulation are appropriate for attaining those aims and do not go beyond what is necessary to achieve them (see *Volker und Markus Schecke and Eifert*, paragraph 74).
>
> 41. As to whether Article 1(2) of Regulation No 2252/2004 is appropriate for attaining the aim of preventing the falsification of passports, it is common ground that the storage of fingerprints on a highly secure storage medium as provided for by that provision requires sophisticated technology. Therefore such storage is likely to reduce the risk of passports being falsified and to facilitate the work of the authorities responsible for checking the authenticity of passports at EU borders.
>
> 42. Mr Schwarz submits that the method of ascertaining identity using fingerprints is not appropriate for attaining the aim of preventing fraudulent use of passports, since there have been mistakes when implementing that method in practice; given that no two digital copies of a set of fingerprints are ever identical, systems using that method are not sufficiently accurate, resulting in not inconsiderable rates of unauthorised

persons being incorrectly accepted and of authorised persons being incorrectly rejected.

43. In that regard, however, it must be held that the fact that the method is not wholly reliable is not decisive. Although that method does not prevent all unauthorised persons from being accepted, it is enough that it significantly reduces the likelihood of such acceptance that would exist if that method were not used.

44. Although it is true that the use of fingerprints as a means of ascertaining identity may, on an exceptional basis, lead to authorised persons being rejected by mistake, the fact remains that a mismatch between the fingerprints of the holder of a passport and the data in that document does not mean that the person concerned will automatically be refused entry to the European Union, as is pointed out in the second subparagraph of Article 4(3) of Regulation No 2252/2004. A mismatch of that kind will simply draw the competent authorities' attention to the person concerned and will result in a more detailed check of that person in order definitively to establish his identity.

45. In the light of the foregoing, the taking and storing of fingerprints referred to in Article 1(2) of Regulation No 2252/2004 are appropriate for attaining the aims pursued by that regulation and, by extension, the objective of preventing illegal entry to the European Union.

46. Next, in assessing whether such processing is necessary, the legislature is obliged, *inter alia*, to examine whether it is possible to envisage measures which will interfere less with the rights recognised by Articles 7 and 8 of the Charter but will still contribute effectively to the objectives of the European Union rules in question (see, to that effect, *Volker und Markus Schecke and Eifert*, paragraph 86).

47. In that context, with regard to the aim of protecting against the fraudulent use of passports, it must in the first place be considered whether the threat posed by the measure of taking fingerprints does not go beyond what is necessary in order to achieve that aim.

48. In this respect, it is [to] be borne in mind, on the one hand, that that action involves no more than the taking of prints of two fingers, which can, moreover, generally be seen by others, so that this is not an operation of an intimate nature. Nor does it cause any particular physical or mental discomfort to the person affected any more than when that person's facial image is taken.

49. It is true that those fingerprints are to be taken in addition to the facial image. However, the combination of two operations designed to identify persons may not *a priori* be regarded as giving rise in itself to a greater threat to the rights recognised by Articles 7 and 8 of the Charter than if each of those two operations were to be considered in isolation.

50. Thus, as regards the case in the main proceedings, nothing in the case file submitted to the Court permits a finding that the fact that fingerprints and a facial image are taken at the same time would, by reason of that fact alone, give rise to greater interference with those rights.

51. On the other hand, it should also be noted that the only real alternative to the taking of fingerprints raised in the course of the proceedings before the Court is an iris scan. Nothing in the case file submitted to the Court suggests that the latter procedure would interfere less with the rights recognised by Articles 7 and 8 of the Charter than the taking of fingerprints.

52. Furthermore, with regard to the effectiveness of those two methods, it is common ground that iris-recognition technology is not yet as advanced as

fingerprint-recognition technology. In addition, the procedure for iris recognition is currently significantly more expensive than the procedure for comparing fingerprints and is, for that reason, less suitable for general use.

53. In those circumstances, the Court has not been made aware of any measures which would be both sufficiently effective in helping to achieve the aim of protecting against the fraudulent use of passports and less of a threat to the rights recognised by Articles 7 and 8 of the Charter than the measures deriving from the method based on the use of fingerprints.

54. In the second place, in order for Article 1(2) of Regulation No 2252/2004 to be justified in the light of that aim, it is also crucial that the processing of any fingerprints taken pursuant to that provision should not go beyond what is necessary to achieve that aim.

55. In that regard, the legislature must ensure that there are specific guarantees that the processing of such data will be effectively protected from misuse and abuse (see, to that effect, European Court of Human Rights judgment, *S. and Marper*, § 103).

56. In that respect, it should be noted that Article 4(3) of Regulation No 2252/2004 explicitly states that fingerprints may be used only for verifying the authenticity of a passport and the identity of its holder.

57. In addition, that regulation ensures protection against the risk of data including fingerprints being read by unauthorised persons. In that regard, Article 1(2) of that regulation makes it clear that such data are to be kept in a highly secure storage medium in the passport of the person concerned.

58. However, the referring court is uncertain, in the light of its assessment, whether Article 1(2) of Regulation No 2252/2004 is proportionate in view of the risk that, once fingerprints have been taken pursuant to that provision, the – extremely high quality – data will be stored, perhaps centrally, and used for purposes other than those provided for by that regulation.

59. In that regard, it is true that fingerprints play a particular role in the field of identifying persons in general. Thus, the identification techniques of comparing fingerprints taken in a particular place with those stored in a database make it possible to establish whether a certain person is in that particular place, whether in the context of a criminal investigation or in order to monitor that person indirectly.

60. However, it should be borne in mind that Article 1(2) of Regulation No 2252/2004 does not provide for the storage of fingerprints except within the passport itself, which belongs to the holder alone.

61. The regulation not providing for any other form or method of storing those fingerprints, it cannot in and of itself, as is pointed out by recital 5 of Regulation No 444/2009, be interpreted as providing a legal basis for the centralised storage of data collected thereunder or for the use of such data for purposes other than that of preventing illegal entry into the European Union.

62. In those circumstances, the arguments put forward by the referring court concerning the risks linked to possible centralisation cannot, in any event, affect the validity of that regulation and would have, should the case arise, to be examined in the course of an action brought before the competent courts against legislation providing for a centralised fingerprint base.

63. In the light of the foregoing, it must be held that Article 1(2) of Regulation No 2252/2004 does not imply any processing of fingerprints that would go beyond

what is necessary in order to achieve the aim of protecting against the fraudulent use of passports.

64. It follows that the interference arising from Article 1(2) of Regulation No 2252/2004 is justified by its aim of protecting against the fraudulent use of passports.

65. In those circumstances, there is no longer any need to examine whether the measures put into effect by that regulation are necessary in view of its other aim (namely, preventing the falsification of passports)."

9. On 11 November 2013 the registrar of the CJEU sent the Administrative Jurisdiction Division a copy of the *Schwarz* judgment and enquired whether the request for a preliminary ruling in the applicant's case would be maintained. On 25 November 2013 the applicant wrote to the Administrative Jurisdiction Division asking it to maintain the request. On the same date, the mayor wrote to the Administrative Jurisdiction Division informing it to see no need to maintain the request for its preliminary ruling in the applicant's case. On 4 December 2013 the Administrative Jurisdiction Division informed the CJEU that it wished to maintain its request for a preliminary ruling. However, it withdrew its first question (see paragraph 7 above) from the order for reference, because the ruling in *Schwarz* had already answered it. A hearing was held before the CJEU on 6 November 2014 during which the applicant presented his case. On 11 November 2014, the applicant sent a letter to the Administrative Jurisdiction Division in which he complained about the withdrawal of the first question from the order for reference.

10. On 16 April 2015 the CJEU issued a ruling in the *Willems v Burgemeester van Nuth* case (joined cases C-446/12 to C449/12, ECLI:EU:C:2015:238) in which it noted that the first question in the applicant's case concerned the validity of Article 1(2) of Regulation No. 2252/2004, which corresponded to the question referred for a preliminary ruling which gave rise to the judgment in *Schwarz*, and that following that judgment the referring court withdrew that question. Answering the remaining question, it held that Article 4(3) of Regulation No. 2252/2004 did not require the member States to guarantee that biometric data collected and stored pursuant to that regulation would not be collected, processed and used for purposes other than the issue of the passport or travel document, since that was not a matter which fell within the scope of that regulation.

11. On 3 December 2015 a hearing before the Administrative Jurisdiction Division was held. The parties' representatives as well as experts on information security from both sides were heard.

12. On 25 May 2016 the Administrative Jurisdiction Division delivered its final judgment. In response to the applicant's complaint about the withdrawal of the first question from its order for reference, it held, after summarising the CJEU's findings in *Schwarz*:

> "7.6 There was no reason to maintain the question referred, because it can be established on the basis of the foregoing that in the *Schwarz* judgment the [CJEU] assessed the validity of the provisions submitted for interpretation in the light of Articles 7 and 8 of the Charter [of Fundamental Rights of the European Union]. It included the aspects that were mentioned in the Administrative Jurisdiction Division's order for reference.
>
> This is confirmed in the [CJEU's] judgment of 16 April 2015 in the joined cases *Willems and Others* ...
>
> The fact that the [CJEU] carried out its assessment on the basis of the arguments provided in *Schwarz*, and not on the basis of the arguments provided by [the applicant], is no reason to rule otherwise. It is important that all relevant aspects were assessed by the [CJEU] in the case of *Schwarz* and that it reached a firm conclusion on them. [The applicant's] arguments do not deviate on their main points from what had been adduced in the case of *Schwartz*, and his arguments did not cast the issue of the validity of the provisions of the Regulation submitted for referral in a different light to such an extent that it was justifiable to ask the [CJEU] for a renewed opinion on that issue."

13. The Administrative Jurisdiction Division further held that the relevant European Union ("EU") legislation left no room for the member States to use alternatives to the prescribed RFID chip (see paragraph 3 above). Nor did it provide for exceptions to the obligation to provide fingerprints other than those set out therein (specifically, children under the age of 12 and persons physically incapable of giving fingerprints). As to the latter point, it referred to Recital 4 in the preamble to Regulation No. 444/2009, which introduced exceptions to the obligation laid down in Regulation No. 2252/2004:

> "The harmonisation of exceptions to the general obligation to provide fingerprints is essential in order to maintain common security standards and with a view to simplifying border controls. Both for legal and security reasons it should not be left to national legislation to define the exceptions to the obligation to provide fingerprints in passports and travel documents issued by Member States."

In the light of the foregoing, the Administrative Jurisdiction Division rejected the applicant's argument that, interpreting the text of the applicable legislation broadly, his situation might be considered to fall within the category of exceptions.

14. Addressing the complaints relating to security of the RFID chip, the Administrative Jurisdiction Division held that the Netherlands had opted for the highest possible level of technical security measures, and that the chip would be sealed after the personal data had been stored. In that respect it referred to the drafting history of the relevant provisions of the Passport Act, from which it appeared that this process had been tested and it had been proven that no information could be altered subsequently. Furthermore, the RFID chip contained guarantees to verify the authenticity of the information on it and to protect against abuses, such as the copying, falsifying and unauthorised reading or monitoring of the information on the chip. An expert on information security who had accompanied the

representatives of the mayor at the hearing before the Administrative Jurisdiction Division had explained that, according to the state of scientific knowledge at that time, the data security of the chip was sound and there were no known methods to evade the security measures. Each piece of equipment used by authorised persons to read information on the chip was certified in respect of security standards and encrypted with a constantly changing, unique code. The Administrative Jurisdiction Division held that the applicant had failed to disprove that the authorities had opted for the highest level of security measures available. As to the exchange with other countries of the encryption codes necessary to read the information on RFID chips, it pointed to the common certification scheme devised by the European Commission, which contained guarantees against abuse. In addition, under the rules in force at the time, the competent minister could revoke the authorisation to read the data on Dutch passports if a member State did not conform to the prescribed standards or if the data were to be used for other aims than border control. There was no obligation to share encryption codes with countries outside the EU. Regarding the company responsible for the manufacturing of passports in the Netherlands, which was part of a group of companies that also had offices in the United States, the Administrative Jurisdiction Division noted that the responsible minister had concluded an agreement with that company to make sure that adequate measures were taken to prevent any data from falling into the hands of the Government of the United States by means of the Patriot Act and to provide data security during the manufacturing process. In conclusion, the Administrative Jurisdiction Division considered that although not every data security risk could be eliminated, the applicant had not substantiated any risks disproportionate to the legitimate aims for which the processing of biometric data in the passports is prescribed by Regulation No. 2252/2004.

15. As for the applicant's objections related to the storage of his biometric data in a database, the Administrative Jurisdiction Division observed that at the relevant time the applicable legislation provided for the possibility of storage of digitised fingerprints in a database, that it however transpired from a letter by the Minister of the Interior and Kingdom Relations of 26 April 2011 (Parliamentary Documents, Lower House of Parliament, no. 25 764, no. 46) that the legislator had refrained from its intention to set up such a database, and that in the meanwhile the applicable legislation had been amended in the sense that it now only allowed fingerprints to be taken for storage on the RFID chip in the passport. The biometric data provided for passport production would thus not be used for purposes other than the obligations arising from Regulation No. 2252/2004. The Administrative Jurisdiction Division further noted that, when he had applied for a new passport, the applicant had also been requested to provide fingerprints for the storage in the database. It considered that, as conceded by the competent minister, it had not been technically possible at that time

to guarantee secured storage of the fingerprints in the database, and concluded that this resulted in an unjustified interference with the applicant's rights protected by Article 8 of the Convention. The Administrative Jurisdiction Division quashed both the Regional Court's judgment and the mayor's decision as they had failed to recognise this aspect. Nevertheless, the Administrative Jurisdiction Division held that the legal effects of the mayor's decision were to remain intact, as the applicant had refused to provide fingerprints altogether, including fingerprints used for the storage of the RFID chip in his passport.

B. Relevant domestic and EU law

16. An overview of the relevant EU and domestic law has been set out in paragraphs 3-15 of the CJEU's judgment of 16 April 2015 (ECLI:EU:C:2015:238 – see paragraph 10 above).

17. As regards the scope of Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter"), the Explanations relating to the Charter (2007/C 303/02) contain the following guidance for the interpretation of Article 7:

> **Explanation on Article 7 – Respect for private and family life**
>
> "The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the ECHR. ...
>
> In accordance with Article 52(3), the meaning and scope of this right are the same as those of the corresponding article of the ECHR. Consequently, the limitations which may legitimately be imposed on this right are the same as those allowed by Article 8 of the ECHR: ..."

In this connection, the CJEU held the following in *J. McB. v. L.E.* (5 October 2010, C-400/10, ECLI:EU:C:2010:582):

> "53. ... Under Article 7 of the Charter, '[e]veryone has the right to respect for his or her private and family life, home and communications'. The wording of Article 8(1) of the ECHR is identical to that of the said Article 7, except that it uses the expression 'correspondence' instead of 'communications'. That being so, it is clear that the said Article 7 contains rights corresponding to those guaranteed by Article 8(1) of the ECHR. Article 7 of the Charter must therefore be given the same meaning and the same scope as Article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human Rights (see, by analogy, Case C-450/06 Varec [2008] ECR I-581, paragraph 48)."

C. Relevant Council of Europe instruments

18. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 has been ratified by all 47 Council of Europe member States and entered into force in respect of the Netherlands on 1 December 1993. The relevant

provisions of that Convention have been set out in *Breyer v. Germany* (no. 50001/12, § 57, 30 January 2020).

COMPLAINTS

19. The applicant complained that the obligation to provide fingerprints when applying for a passport and the subsequent storage of the fingerprints on an RFID chip in the passport, violated the right to respect for his private life guaranteed by Article 8 of the Convention and the right to freedom of movement as set out in Article 2 of Protocol No. 4 to the Convention.

20. Relying on Article 6 of the Convention and on Article 13 read together with Article 8, the applicant further complained that the Administrative Jurisdiction Division had wrongly withdrawn a question from its request to the CJEU for a preliminary ruling (see paragraph 9 above) and that he had been unable to challenge that decision. He also complained, with reference to the same provisions, that the Administrative Jurisdiction Division had ignored the submissions on the security of the RFID chip made by the expert who had appeared at his request at the hearing on 3 December 2015 (see paragraph 11 above), because no reference to them was made in the final judgment.

THE LAW

A. Complaint under Article 8 of the Convention

21. The applicant alleged a breach of Article 8, which, in so far as relevant, provides as follows:

> "1. Everyone has the right to respect for his private ... life, ...
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

22. The applicant submitted that the obligation under the Passport Act to have fingerprints taken when applying for a passport, as well as the storage of such prints on an RFID chip whose encryption codes could be shared with non-European countries, constituted an unjustified interference with the right to respect for his private life. He argued that there was no legitimate aim for that interference, as identity fraud with the previous type of passport ("lookalike fraud") had not been a serious problem. He also argued that the interference had not served a legitimate aim in his particular case. Fingerprints were still not being used for border controls, and it was unclear how fraud could not be combatted while making an exception for

conscientious objectors like him. The applicant further argued that the measure was not "necessary in a democratic society", since it had not been proven necessary for the prevention of fraud that fingerprints should be taken, stored on an RFID chip and shared with European and possibly non-European authorities. Safer alternatives to the RFID chip, such as a chip with a personalised code, had not been given sufficient, if any, consideration. In addition, the company that had been chosen to manufacture passports in the Netherlands had given rise to risks of abuse, because the data could be claimed by the Government of the United States under that country's Patriot Act. Relying on *S. and Marper v. the United Kingdom* ([GC], nos. 30562/04 and 30566/04, ECHR 2008), the applicant argued that the Netherlands had not lived up to its obligation to provide for sufficient guarantees against the risk of abuse and arbitrariness. Lastly, by not allowing for exceptions to the requirement at issue, insufficient consideration had been given to persons who, like the applicant, objected in principle to the taking and retention of fingerprints, or to particular personal circumstances, such as those of persons whose work required them to travel to undemocratic and corrupt countries, as was the case for the applicant.

23. The Court observes at the outset that the domestic authorities did not dispute in the present case that the taking and retention of fingerprints amounted to an interference with the right to respect for the applicant's private life within the meaning of Article 8 § 1 of the Convention. The Court does not see any reasons to hold otherwise. In turn, the applicant has not complained before this Court that the interference was not "in accordance with the law". The dispute, in so far as it concerns the complaint under Article 8, is therefore limited to two questions: (a) whether the interference pursued one or more legitimate aims, and (b) whether the interference was "necessary in a democratic society" in order to achieve the aim or aims concerned.

1. Legitimate aim

24. It follows from the judgments of the Administrative Jurisdiction Division and the CJEU that the interference was, *inter alia*, intended to combat identity fraud and falsification and/or the fraudulent use of passports (see paragraphs 8 and 12 above). The Court has no doubt that such an interference in principle pursues a legitimate aim within the meaning of the second paragraph of Article 8 of the Convention, namely the prevention of crime. Furthermore, the Court reiterates that compliance with EU law by a Contracting Party constitutes a legitimate general-interest objective of considerable weight (see, among other authorities, *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland* [GC], no. 45036/98, §§ 150-51, ECHR 2005-VI (hereinafter "*Bosphorus*"), and *O'Sullivan McCarthy Mussel Development Ltd v. Ireland*, no. 44460/16, § 109, 7 June 2018). The

relevant EU law aims to secure common technical standards for documents required for crossing external borders and to simplify controls.

25. In so far as the applicant has argued that the interference did not pursue a legitimate aim because it had not been established that passport fraud was a serious problem and that "lookalike fraud" was very rare (see paragraph 22 above), the Court notes that in any event, it follows from the foregoing that the interference in issue serves more aims than the combat of fraud alone. Therefore, the Court does not need to consider this argument.

2. Necessary in a democratic society

(a) The presumption of equivalent protection

26. As the Court has previously held, the Convention does not prohibit Contracting Parties from transferring sovereign power to an international organisation such as the European Union. State action taken in compliance with such legal obligations is justified as long as the relevant organisation is considered to protect fundamental rights, as regards both the substantive guarantees offered and the mechanisms controlling their observance, in a manner which may be considered at least equivalent to that for which the Convention provides. By "equivalent" the Court means "comparable"; any requirement that the organisation's protection be "identical" could run counter to the interest of international cooperation pursued (see *Bosphorus*, cited above, §§ 152-55).

27. As regards the protection of fundamental rights afforded by the European Union, the Court has recognised that this is in principle equivalent to that of the Convention system (ibid., §§ 159-65).

28. According to the Court's established case-law, the application of the presumption of equivalent protection is subject to two conditions. The first is that the impugned interference must have been a matter of strict international legal obligation for the respondent State, to the exclusion of any margin of manoeuvre on the part of the domestic authorities. The second condition is the deployment of the full potential of the supervisory mechanism provided for by EU law (see, for instance, *Avotiņš v. Latvia* [GC], no. 17502/07, § 105, 23 May 2016).

29. The presumption of Convention conformity can be rebutted if, in the circumstances of a particular case, it is considered that the protection of Convention rights was manifestly deficient (see *Bosphorus*, cited above, §§ 152-58; *M.S.S. v. Belgium and Greece* [GC], no. 30696/09, §§ 338-40, ECHR 2011; *Michaud v. France*, no. 12323/11, § 103, ECHR 2012; and *Bivolaru and Moldovan v. France*, nos. 40324/16 and 12623/17, § 101, 25 March 2021).

(b) The application of the presumption of equivalent protection in the present case

(i) Margin of manoeuvre

30. The Court observes that, in the Administrative Jurisdiction Division's ruling in the applicant's case, it was pointed out that under EU law, the Dutch authorities were unable to provide for exceptions to the obligation to include fingerprints other than those already specified, or use storage methods other than the RFID chip. It also held that the absence of other exceptions to the obligation to provide fingerprints was necessary to serve the aims of the relevant EU legislation (see paragraph 13 above).

31. Having regard to the treatment of EU Regulations in its case-law (see, *inter alia*, *Avotiņš*, § 106, cited above), and in the absence of any arguments to the contrary raised by the applicant, the Court sees no reason to depart from the Administrative Jurisdiction Division's conclusion that the impugned interference was a matter of strict international legal obligation for the respondent State, to the exclusion of any margin of manoeuvre.

(ii) Supervisory mechanism

32. The applicant could and did avail himself of the possibility of bringing the alleged violation before the domestic courts. In those proceedings, the Administrative Jurisdiction Division requested a preliminary ruling from the CJEU on the alleged violation of rights under, *inter alia*, Article 7 of the Charter of the Fundamental Rights of the European Union (see paragraph 7 above). The meaning and scope of the rights under that provision are the same as those of the rights under Article 8 § 1 of the Convention (see paragraph 17 above).

33. The applicant argued that in its *Schwarz* judgment (see paragraph 8 above) the CJEU had not ruled on his arguments, although its conclusion in that judgment had been applied in his case. For that reason, the supervisory mechanism had not been deployed to its full potential.

34. The Court has held that the condition of full deployment of the supervisory mechanism should be applied without excessive formalism and taking into account the specific features of the supervisory mechanism in question. In doing so, it does not require the domestic court to request a ruling from the CJEU in all cases without exception, including those cases where no genuine and serious issue arises with regard to the protection of fundamental rights by EU law, or those in which the CJEU has already stated precisely how the applicable provisions of EU law should be interpreted in a manner compatible with fundamental rights (see *Avotiņš*, cited above, § 109, and *Bivolaru and Moldovan*, cited above, § 99). Considering the CJEU's ruling in *Schwarz* and the Administrative Jurisdiction Division's reasoning for withdrawing the first question from its order for reference (see paragraphs 8, 9 and 12 above), the Court sees no

reason to reach a different conclusion from the one it reached in *Bosphorus* and *Avotiņš* (both cited above), namely that the presumption of equivalent protection is applicable in this case.

(iii) Manifest deficiencies

35. The applicant argued that the protection of his Convention rights had been manifestly deficient. He pointed to the fact that the CJEU did not join his case with that of *Schwarz*, and to the Administrative Jurisdiction's Division's partial withdrawal of its order for reference in response to the *Schwarz* ruling.

36. The Court considers that, in so far as the applicant had adduced other arguments in his further appeal than those which the CJEU had assessed in *Schwarz*, his arguments were nonetheless examined by the Administrative Jurisdiction Division and dismissed on the basis of elaborate reasoning in the latter's final judgment (see paragraphs 12-15 above). In the light of these considerations, the Court cannot find that the applicant has shown that the protection afforded to him was "manifestly deficient". As a consequence, the presumption of Convention conformity has not been rebutted in the present case (see the case-law quoted in paragraph 29 above).

(c) Conclusion

37. It follows that this complaint must be rejected as manifestly ill-founded, pursuant to Article 35 §§ 3 (a) and 4 of the Convention.

B. Other alleged violations

38. The Court has found above that the applicant's complaint under Article 8 is manifestly ill-founded (see paragraph 37 above). For the same reasons, the Court sees no reason to hold that the applicant's freedom of movement was unduly restricted.

39. Therefore, this complaint must be rejected as manifestly ill-founded, pursuant to Article 35 §§ 3 (a) and 4 of the Convention.

40. In the light of the Court's conclusion on the applicant's complaint under Article 8 (see paragraph 37 above) and the particular circumstances of the case, the Court does not discern an arguable claim for the applicant's complaint under Article 13 in conjunction with Article 8 (see *Boyle and Rice v. the United Kingdom*, 27 April 1988, § 54, Series A no. 131).

41. As to the applicant's complaints under Article 6, the Court reiterates that the right to a passport is not a civil right for the purposes of Article 6 of the Convention (see *Peltonen v. Finland,* no. 19583/92, Commission decision of 20 February 1995; *Karassev and family v. Finland*, no. 31414/96, Commission decision of 14 April 1998; *Šoć v. Croatia* (dec.),

no. 47863/99, 29 June 2000; *Sergey Smirnov v. Russia* (dec.), no. 14085/04, 6 July 2006; *Lolova and Popova v. Bulgaria* (dec.), no. 68053/10, § 57, 20 January 2015; and, more recently, *Alpeyeva and Dzhalagoniya v. Russia*, nos. 7549/09 and 33330/11, § 129, 12 June 2018). It follows that these complaints are incompatible *ratione materiae* with the provisions of the Convention within the meaning of Article 35 § 3 (a), and that they must be rejected in accordance with Article 35 § 4.

For these reasons, the Court, unanimously,

Declares the application inadmissible.

Done in English and notified in writing on 2 December 2021.

{signature_p_2}

Andrea Tamietti
Registrar

Yonko Grozev
President