Case C-61/22

Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice

Date lodged:

1 February 2022

Referring court:

Verwaltungsgericht Wiesbaden (Germany)

Date of the decision to refer:

13 January 2022

Applicant:

RL

Defendant:

Landeshauptstadt Wiesbaden

Subject matter of the main proceedings

Taking of fingerprints and storing them in identity cards – Article 3(5) of Regulation (EU) 2019/1157 – Validity – Procedure for adopting the regulation – Articles 7 and 8 of the Charter of Fundamental Rights of the European Union – Article 35(10) of the General Data Protection Regulation

Subject matter and legal basis of the request

Validity of Article 3(5) of Regulation (EU) 2019/1157; Article 267 TFEU

Question referred for a preliminary ruling

Does the obligation to take fingerprints and store them in identity cards in accordance with Article 3(5) of Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union

citizens and their family members exercising their right of free movement (OJ 2019 L 188, p. 67) infringe higher-ranking EU law, in particular

(a) Article 77(3) TFEU

(b) Articles 7 and 8 of the Charter

(c) Article 35(10) of the GDPR

and is it therefore invalid on one of those grounds?

Provisions of EU law relied on

Charter of Fundamental Rights of the European Union: Articles 7, 8 and 52;

Treaty on the Functioning of the European Union: Articles 21, 77 and 289;

Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement: recitals 2, 17, 18, 19, 21, 22, 40 and 41, and Articles 3 and 11;

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): Articles 9 and 35.

Provisions of national law relied on

Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Law on identity cards and electronic proof of identity; 'the PAuswG'): Paragraphs 5 and 9.

Succinct presentation of the facts and procedure in the main proceedings

1 The applicant seeks the issuance of an identity card without his fingerprints being taken. The defendant refuses to comply with that request, on the ground that Paragraph 5(9) of the PAuswG, which is based on Regulation (EU) 2019/1157, provides for the mandatory taking of two fingerprints.

2 Regulation (EU) 2019/1157 has applied since 2 August 2021. Article 3(5) of Regulation (EU) 2019/1157 provides that identity cards issued by Member States are to include a storage medium which is to contain a facial image of the holder of the card and two fingerprints in interoperable digital formats. German law also contains provisions on the inclusion of fingerprints in identity cards

(Paragraph 5(9) of the PAuswG), whereby, as shown by the explanatory memorandum to that law, the German legislature proceeded on the assumption that fingerprints were to be included in accordance with Article 3(5) of Regulation (EU) 2019/1157.

3 On 30 November 2021, the applicant applied for a new identity card – without fingerprints – because the chip in his old identity card was defective. The issuance of a new card was refused on the ground that the inclusion of fingerprints had been mandatory since 2 August 2021. Moreover, the applicant was not entitled to the issuance of a new identity document, since he was already in possession of a valid identity document. An identity card continues to be valid even with a defective chip.

4 The authority responsible for issuing identity cards under German law acts as a threat-prevention authority. Nevertheless, the issuance of identity cards and the related data processing is not in fact subject to Directive (EU) 2016/680, but rather the General Data Protection Regulation ('the GDPR'), as can be inferred from recital 40 of Regulation (EU) 2019/1157. Therefore, in the present case, the Oberbürgermeister (Mayor) is not acting in the field of EU law on the prevention of threats, which is to be interpreted autonomously. Under Article 1(1) and Article 2(1) of Directive (EU) 2016/680, the latter is applicable only where authorities act for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Those purposes do not cover the passport and identity card system.

Succinct presentation of the reasoning in the request for a preliminary ruling

5 A ruling on the question referred is necessary in order for judgment to be given. If Article 3(5) of Regulation (EU) 2019/1157 infringes higher-ranking EU law, the applicant is entitled to be issued an identity card without the inclusion of fingerprints (first sentence of Paragraph 9(1) of the PAuswG). The national regime in Paragraph 5(9) of the PAuswG would lose its basis, as it would infringe EU law.

6 Even if the applicant's old identity card continues to be valid despite the defective chip in accordance with Paragraph 28(3) of the PAuswG, the applicant must be issued with a new identity card after the expiry of the 10-year period of validity at the latest. Moreover, in accordance with Paragraph 6(2) of the PAuswG, the applicant may apply for a new identity card before the expiry of the validity of an identity card if a legitimate interest in the reissue is demonstrated. In the case of a defective chip, it is no longer possible to use the online ID function. The use of automated border control systems is also no longer possible. That limited possibility of use must be regarded as giving rise to a legitimate interest in the issuance of a new identity card.

7 The referring court has doubts as to whether Article 3(5) of Regulation (EU) 2019/1175 is compatible with EU law. Those doubts are based on the fact that Regulation (EU) 2019/1157 was adopted in the ordinary legislative procedure, on the compatibility of Article 3(5) of Regulation (EU) 2019/1157 with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter') and on the lack of a decision on the weighing of interests pursuant to Article 35(10) of the GDPR.

8 The referring court takes the view that Regulation (EU) 2019/1157 should have been adopted in accordance with the special legislative procedure under Article 77 TFEU.

9 The TFEU distinguishes between the ordinary legislative procedure and the special legislative procedures in Article 289. Regulation (EU) 2019/1157 was based on Article 21(2) TFEU and adopted in accordance with the ordinary legislative procedure. According to Article 21(2) TFEU, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may adopt provisions with a view to facilitating the exercise of the right to free movement, if action by the Union should prove necessary to attain this objective and the Treaties have not provided the necessary powers.

10 The first sentence of Article 77(3) TFEU contains a further rule regarding competence that relates, inter alia, to provisions concerning identity cards. According to that rule, the Council, acting in accordance with a special legislative procedure, may adopt provisions concerning passports, identity cards, residence permits or any other such document, if action by the Union should prove necessary to facilitate free movement, and if the Treaties have not provided the necessary powers. The Council is to act unanimously after consulting the European Parliament. That requirement of unanimity leaves the maximum possible degree of sovereignty to the Member States in this area.

11 Article 77 TFEU corresponds to the former Article 62 TEC (EC Treaty). At the time of its adoption, Regulation (EC) 2252/2004, Article 1(2) of which provides that fingerprints are to be stored in passports, was based by the legislature on Article 62 TEC. By judgment of 17 October 2013, *Schwarz* (C-291/12, EU:C:2013:670), the Court of Justice of the European Union ('the Court') held that Article 62(2)(a) TEC was an appropriate legal basis for adopting Regulation No 2252/2004 and, in particular, Article 1(2) thereof.

12 The competence under Article 77(3) TFEU takes precedence over Article 21(2) TFEU, since Article 77(3) TFEU, as a more specific provision in terms of content, imposes more stringent requirements on the legislative procedure, and Article 21(2) TFEU is relevant only if the Treaties have not provided other powers necessary to attain the objective of facilitating freedom of movement. Although Regulation (EU) 2019/1157 does not refer to the further development of the Schengen *acquis*, it intends, like Regulation (EC) 2252/2004, the approximation of security features and the integration of biometric identifiers as an important

step towards the use of new elements in the perspective of future developments at European level. As in the case of Regulation (EC) 2252/2004, those developments are intended to render the travel document more secure (*in casu*: identity cards instead of passports).

13 In the light of the foregoing, the referring court takes the view that the effective adoption of Regulation (EU) 2019/1157 – and thus also of Article 3(5) thereof – would have required the special legislative procedure pursuant to Article 77(3) TFEU.

14 In addition, there are doubts as to the compatibility of the taking and storing of fingerprints in identity cards with Articles 7 and 8 of the Charter.

15 According to Article 7 of the Charter, everyone has the right to respect for his or her private and family life, home and communications. Under Article 8 of the Charter, everyone has the right to the protection of personal data concerning him or her.

16 Already in the judgment of 17 October 2013, *Schwarz* (C-291/12, EU:C:2013:670, paragraphs 27 and 30), the Court, referring to the judgment of the ECtHR of 4 December 2008, *S. and Marper v. the United Kingdom* (Reports of judgments and decisions 2008-V, p. 213, §§ 68 and 84), stated that the taking of fingerprints and storing of them in passports by the national authorities which is governed by Article 1(2) of Regulation No 2252/2004 constitutes a threat to the rights to respect for private life and the protection of personal data. Fingerprints constitute personal data, as they objectively contain unique information about individuals which allows those individuals to be identified with precision. The same fundamental rights are also affected in the taking and storage of fingerprints for identity cards.

17 The referring court has doubts as to whether the taking of fingerprints, and thus an interference with Articles 7 and 8 of the Charter, in particular with regard to Article 52 and Article 8(2) of the Charter, is also justified in the case of identity cards. Article 8(2) of the Charter provides that personal data cannot be processed except on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

18 In the present case, the referring court takes the view that persons applying for identity cards have not consented to having their fingerprints taken – as held by the Court in relation to passports. However, Article 3(5) of Regulation (EU) 2019/1157 establishes the taking of fingerprints as a legal rule for all identity cards.

19 According to the first sentence of Paragraph 1(1) of the PAuswG, all Germans are obliged to possess a valid identity card as soon as they reach the age of 16 and are subject to the general obligation to register or, without being subject to it, are predominantly resident in Germany. Therefore, the mandatory taking of fingerprints is prescribed for the issuance of that document. As there is an

obligation to possess an identity card, persons applying for identity cards cannot be deemed to have consented to such data processing (see also CJEU, judgment of 17 October 2013, *Schwarz*, C-291/12, EU:C:2013:670, paragraph 31).

20 Therefore, a ***legitimate*** legal basis is required, in accordance with Article 52(1) of the Charter.

21 It is true that the inclusion of fingerprints in identity cards is provided for by law in Article 3(5) of Regulation (EU) 2019/1157. This also corresponds, at least in part, to the objectives of general interest recognised by the Union, as expressed in recitals 1, 2, 4, 18 and 46.

22 Within the European Union, identity cards can be used in the context of border crossing. In addition, States that are not part of the European Union also allow entry by means of identity cards, such as, in particular, Switzerland, Iceland, Norway, Albania and Montenegro. Against that background, identity cards are at least also used as travel documents, with the result that the regime also serves the purpose of preventing illegal entry from those countries. This would constitute an objective of general interest recognised by the Union (CJEU, judgment of 17 October 2013, *Schwarz*, C-291/12, EU:C:2013:670, paragraph 38). However, identity cards are precisely not intended primarily to serve as travel documents in the Schengen area, like passports. In that respect, the recitals of Regulation (EU) 2019/1157 rightly do not refer to the Schengen area, as an area of freedom, unlike those in Regulation 2252/2004.

23 Nor does Regulation (EU) 2019/1157 regulate the use of the stored biometric data in that sense, in so far as Article 11(6) of Regulation (EU) 2019/1157 states that the stored biometric data may be used for the purpose of verifying authenticity or the identity of the holder. Consequently, Regulation (EU) 2019/1157 leaves open the question as to how freedom of movement is to be facilitated. In that respect, the objective of preventing illegal entry cannot be equated with the facilitation of freedom of movement.

24 However, even if the regime were to pursue an objective of general interest, there are doubts as to whether Article 3(5) of Regulation (EU) 2019/1157 is proportionate. This would be the case only if the limitations placed on those rights under the Charter are proportionate to the aims pursued by Regulation (EU) 2019/1157 and, by extension, to the objective of preventing illegal entry into the European Union and of enabling the reliable identification of the identity card holder. To that end, the measures implemented by that regulation must be appropriate for attaining those aims and must not go beyond what is necessary to achieve them (CJEU, judgment of 17 October 2013, *Schwarz*, C-291/12, EU:C:2013:670, paragraphs 38 and 40).

25 In that respect, the referring court takes the view that it must be taken into account that identity cards cannot be equated with passports in fact and in law, but, rather, there are clear differences with regard to the use of those documents.

Nevertheless, Article 3(5) of Regulation (EU) 2019/1157 treats the two documents equally with regard to fingerprints.

26 It is true that identity cards can also be used as travel documents – as already explained above. Nevertheless, identity cards and passports differ in both legal and practical respects. Even if identity cards are also used as travel documents in the context of freedom of movement, there are no routine checks, at least when travelling between EU Member States. Moreover, for most Union citizens, the primary function of the national identity card is unlikely to be linked to freedom of movement. This is because identity cards have uses that go beyond freedom of movement. For example, identity cards are used in everyday life for interactions with national administrative authorities or with private third parties, such as banks or airlines. Union citizens wanting to exercise their freedom of movement can already do so using their passport (see also, to that effect: Opinion of the European Data Protection Supervisor (EDPS) on the planned introduction of the storage of fingerprints in identity cards of 10 August 2018).

27 In addition, there is an obligation to possess an identity card in Germany (first sentence of Paragraph 1(1) of the PAuswG). By contrast to passports, citizens cannot make their own decision as to whether or not to apply for an identity card. The EDPS also considers that the taking and storage of fingerprints would have a wide-ranging impact on up to 370 million Union citizens, potentially subjecting 85% of the EU population to a mandatory fingerprinting requirement. This wide scope, combined with the very sensitive data processed (facial images in combination with fingerprints) calls for close scrutiny according to a strict necessity test. The referring court concurs with the consideration of the EDPS that, given the differences between identity cards and passports, the introduction of security features that may be considered appropriate for passports to identity cards cannot be done automatically, but requires reflection and a thorough analysis. This did not take place in this case.

28 The referring court takes the view that, in combination with the broad possibilities of use described above and the large number of Union citizens affected, there is a much greater intensity of interference in comparison with passports, which, in return, also requires stronger justification.

29 In the context of the interpretation of Articles 7 and 8 of the Charter, account must also be taken of the principles of the GDPR, as follow from recitals 1 and 2 thereof.

30 Dactyloscopic data constitute special types of personal data according to Article 9(1) of the GDPR, namely biometric data. Such data are defined in point 14 of Article 4 of the GDPR as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. In accordance with Article 9(1) of the GDPR, the processing of such biometric

data is in principle prohibited and is permitted only in narrowly defined exceptional cases.

31 In so far as fingerprints are to be included in identity cards in order to reinforce security against forgery, the EDPS Opinion on the planned introduction of the storage of fingerprints in identity cards states that it has been reported that only 38 870 fraudulent identity cards have been detected in the years 2013-2017 and that the use of fraudulent identity cards has been decreasing for years.

32 It is not sufficiently clear from the outset whether the inclusion of fingerprints is in fact capable of reinforcing security against forgery. A match between biometric data stored in the chip of the identity card and the fingerprints of the holder of the identity card merely confirms that the document belongs to the document holder. That match does not as such constitute proof of identity unless the identity card itself has been proved to be authentic. It is true that it is acknowledged that the use of biometric data reduces the likelihood of a document being successfully forged, with the result that the inclusion of fingerprints may at least partially serve to achieve the purpose.

33 However, it appears to be highly questionable whether that possibility is able to justify the far-reaching interference, especially given that identity cards with a defective chip also continue to be valid under German law, contrary to Regulation (EU) 2019/1157. In that regard, the Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) states that ‘an identity card with a non-functional chip remains valid, even if the integrated chip is manifestly defective. Its security as an identity document is afforded by the physical security features’. However, if security is provided solely by the physical security features (in particular microprints, UV overprints, etc.), the question as to the necessity of including fingerprints arises all the more clearly.

34 The EDPS also stressed that security printing techniques, such as the use of holograms or watermarks, have a much lower intensity of interference. It stated that such techniques do not involve the processing of personal data but may allow forgery to be prevented and the authenticity of a document to be verified.

35 In that context, one of the most important principles of European data protection law must also be observed: the principle of data minimisation. According to that principle, the collection and use of personal data must be proportionate and necessary and limited to what is necessary for the purposes for which they are processed.

36 In the event that it is necessary to take fingerprints, the question also arises as to why it is necessary to take the entire print. It is true that this facilitates interoperability among the various types of fingerprint recognition systems. Those systems can be divided into three sub-categories. First, there are systems that store and compare complete images of fingerprints. Other systems use what are referred to as minutiae. These describe a subset of the characteristics extracted from

fingerprint images. The third category are systems that work with individual patterns extracted from fingerprint images. In the event that only minutiae were stored, a Member State working with a system that uses an image of the entire fingerprint would not be able to use them. Storing the entire fingerprint facilitates interoperability, but increases the amount of personal data stored and thus the risk of identity theft in the event of a data leak.

37 The RFID chips used in identity cards can potentially also be read by unauthorised scanners. This is because they are activated via a radio field and subsequently transmit data in encrypted form. Thus, the security of the procedure ultimately depends on the quality of the transmission and encryption technology. It is precisely the use of the entire fingerprint that has the effect of increasing risk in this context.

38 In that regard, it must also be noted that fingerprints are biometric data. The legislature has shown, inter alia by introducing Article 9 of the GDPR, that such data are subject to special protection.

39 Even Regulation (EU) 2019/1157 dispenses with the fingerprint 'security feature' for children under the age of 12 years and completely exempts children under the age of 6 years from the requirement to give fingerprints (Article 3(7) of Regulation (EU) 2019/1157). Much more importantly, however, persons in respect of whom fingerprinting is physically impossible are exempt from the requirement to give fingerprints. What purpose that security feature is then supposed to serve is not regulated and is simply left open in Regulation (EU) 2019/1157.

40 The EDPS also stresses in its opinion that Article 35(10) of the GDPR applies to the collection and processing of fingerprints. In accordance with Article 35(1) of the GDPR, a data protection impact assessment must be carried out prior to processing which is likely to result in a high risk to the rights and freedoms of natural persons. That data protection impact assessment should contain, in particular, an assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address the risks, including safeguards and security measures.

41 Since the legal basis is in EU law, to which the controller is subject, and since that legislation regulates the specific processing operation, the general impact assessment must be carried out in the context of the adoption of that legal basis (Article 35(10) of the GDPR). Such an impact assessment should therefore have been carried out when Regulation (EU) 2019/1157 was adopted. As is apparent from the recitals, this did not take place.

42 The referring court, like the EDPS in its opinion, takes the view that the impact assessment would not support the mandatory inclusion of both a facial image and (two) fingerprints in identity cards. Already during the legislative procedure, the EDPS recommended that the necessity and proportionality of the processing of

biometric data (facial image in combination with fingerprints) be reassessed against that background.

43 In recital 40 of the GDPR, the legislature addresses that issue in relation to the GDPR only in very general terms. They amount to nothing more than vague statements, such as, for example, the statement that Union citizens should be made aware of the storage medium and that it is necessary to further specify safeguards applicable to the processed personal data and in particular to sensitive data such as biometric identifiers. The storage medium should be highly secure and effectively protect personal data stored on it from unauthorised access. It remains unclear what is meant by 'highly secure' and what form the safeguards and security measures are to take. In particular, a balancing of the risks of data leaks from chips and the encroachment on Articles 7 and 8 of the Charter is not apparent.

44 The question therefore arises as to whether it is possible for failure to carry out a mandatory risk impact assessment not to affect the effectiveness of a rule or whether, on the contrary, where the legislature is under a mandatory obligation to carry out a risk impact assessment, failure to do so must lead to the invalidity of the rule. Otherwise, the legislature would be rewarded for its wrongdoing.