Reports of Cases

JUDGMENT OF THE COURT (Grand Chamber)

21 March 2024*

(Reference for a preliminary ruling – Regulation (EU) 2019/1157 – Strengthening the security of identity cards of EU citizens – Validity – Legal basis – Article 21(2) TFEU – Article 77(3) TFEU – Regulation (EU) 2019/1157 – Article 3(5) – Obligation for Member States to include two fingerprints in interoperable digital formats in the storage medium of identity cards – Article 7 of the Charter of Fundamental Rights of the European Union – Respect for private and family life – Article 8 of the Charter of Fundamental Rights – Protection of personal data – Regulation (EU) 2016/679 – Article 35 – Obligation to carry out a data protection impact assessment – Maintaining the effects for a certain time of a regulation which has been declared invalid)

In Case C-61/22,

REQUEST for a preliminary ruling under Article 267 TFEU from the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), made by decision of 13 January 2022, received at the Court on 1 February 2022, in the proceedings

RL

v

Landeshauptstadt Wiesbaden,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Arabadjiev, A. Prechal, E. Regan (Rapporteur), T. von Danwitz, F. Biltgen and Z. Csehi, Presidents of Chambers, J.-C. Bonichot, S. Rodin, D. Gratsias, M.L. Arastey Sahún and M. Gavalec, Judges,

Advocate General: L. Medina,

Registrar: D. Dittert, Head of Unit,

having regard to the written procedure and further to the hearing on 14 March 2023,

after considering the observations submitted on behalf of:

– RL, by W. Achelpöhler, Rechtsanwalt,

* Language of the case: German.

– the German Government, by J. Möller and P.-L. Krüger, acting as Agents,

– the Belgian Government, by P. Cottin and A. Van Baelen, acting as Agents, and by P. Wytinck, advocaat,

– the Spanish Government, by L. Aguilera Ruiz, acting as Agent,

– the Polish Government, by B. Majczyna, acting as Agent,

– the European Parliament, by G.C. Bartram, P. López-Carceller and J. Rodrigues, acting as Agents,

– the Council of the European Union, by M. França and Z. Šustr, acting as Agents,

– the European Commission, by H. Kranenborg, E. Montaguti and I. Zaloguin, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 29 June 2023,

gives the following

Judgment

1 The request for a preliminary ruling concerns the validity 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) and, in particular, Article 3(5) thereof.

2 The request has been made in proceedings between RL and the Landeshauptstadt Wiesbaden (City of Wiesbaden, Land capital, Germany) ('the City of Wiesbaden') concerning the rejection by the latter of RL's application for an identity card which does not include RL's fingerprints.

I. Legal context

A. European Union law

1. Regulation 2019/1157

3 Recitals 1, 2, 4, 5, 17 to 21, 23, 26 to 29, 32, 33, 36, 40 to 42 and 46 of Regulation 2019/1157 are worded as follows:

'(1) The Treaty [on European Union (TEU)] resolved to facilitate the free movement of persons while ensuring the safety and security of the peoples of Europe, by establishing an area of freedom, security and justice, in accordance with the provisions of the TEU and of the [TFEU].

(2) Citizenship of the [European] Union confers on every citizen of the Union the right of free movement, subject to certain limitations and conditions. Directive 2004/38/EC of the European Parliament and of the Council [of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ 2004 L 158, p. 77)] gives effect to that right. Article 45 of the Charter of Fundamental Rights of the European Union (the Charter) also provides for freedom of movement and residence. Freedom of movement entails the right to exit and enter Member States with a valid identity card or passport.

…

(4) Directive [2004/38] provides that Member States may adopt the necessary measures to refuse, terminate or withdraw any right conferred by that Directive in the case of abuse of rights or fraud. Document forgery or false presentation of a material fact concerning the conditions attached to the right of residence have been identified as typical cases of fraud under that Directive.

(5) Considerable differences exist between the security levels of national identity cards issued by Member States and residence permits for Union nationals residing in another Member State and their family members. Those differences increase the risk of falsification and document fraud and also give rise to practical difficulties for citizens when they wish to exercise their right of free movement. Statistics from the European Document Fraud Risk Analysis Network show that incidents of fraudulent identity cards have increased over time.

…

(17) Security features are necessary to verify if a document is authentic and to establish the identity of a person. The establishment of minimum security standards and the integration of biometric data in identity cards and in residence cards of family members who are not nationals of a Member State are important steps in rendering their use in the Union more secure. The inclusion of such biometric identifiers should allow Union citizens to fully benefit from their rights of free movement.

(18) The storage of a facial image and two fingerprints (“biometric data”) on identity and residence cards, as already provided for in respect of biometric passports and residence permits for third-country nationals, represents an appropriate combination of reliable identification and authentication with a reduced risk of fraud, for the purpose of strengthening the security of identity and residence cards.

(19) As a general practice, Member States should, for the verification of the authenticity of the document and the identity of the holder, primarily verify the facial image and, where necessary to confirm without doubt the authenticity of the document and the identity of the holder, Member States should also verify the fingerprints.

(20) Members States should ensure that, in cases where a verification of biometric data does not confirm the authenticity of the document or the identity of its holder, a compulsory manual check is carried out by qualified staff.

(21) This Regulation does not provide a legal basis for setting up or maintaining databases at national level for the storage of biometric data in Member States, which is a matter of national law that needs to comply with Union law regarding data protection. Moreover, this Regulation does not provide a legal basis for setting up or maintaining a centralised database at Union level.

…

(23) The specifications of ICAO [International Civil Aviation Organization] Document 9303 which ensure global interoperability including in relation to machine readability and use of visual inspection should be taken into account for the purpose of this Regulation.

…

(26) Member States should ensure that appropriate and effective procedures for the collection of biometric identifiers are in place and that such procedures comply with the rights and principles set out in the Charter, the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe[, signed in Rome on 4 November 1950] and the United Nations Convention on the Rights of the Child[, adopted by the United Nations General Assembly on 20 November 1989 (*United Nations Treaty Series*, Vol. 1577, p. 3), and which entered into force on 2 September 1990]. Member States should ensure that the best interest of the child is a primary consideration throughout the collection procedure. To that end, qualified staff should receive appropriate training on child-friendly practices for the collecting of biometric identifiers.

(27) Where difficulties are encountered in the collection of biometric identifiers, Member States should ensure that appropriate procedures are in place to respect the dignity of the person concerned. Therefore, specific considerations relating to gender, and to the specific needs of children and of vulnerable persons should be taken into account.

(28) The introduction of minimum security and format standards for identity cards should allow Member States to rely on the authenticity of those documents when Union citizens exercise their right of free movement. The introduction of reinforced security standards should provide sufficient guarantees to public authorities and private entities to enable them to rely on the authenticity of identity cards when used by Union citizens for identification purposes.

(29) A distinguishing sign in the form of the two-letter country code of the Member State issuing the document, printed in negative in a blue rectangle and encircled by 12 yellow stars, facilitates the visual inspection of the document, in particular when the holder is exercising the right of free movement.

…

(32) Member States should take all necessary steps to ensure that biometric data correctly identify the person to whom an identity card is issued. To this end, Member States could consider collecting biometric identifiers, particularly the facial image, by means of live enrolment by the national authorities issuing identity cards.

(33) Member States should exchange with each other such information as is necessary to access, authenticate and verify the information contained on the secure storage medium. The formats used for the secure storage medium should be interoperable, including in respect of automated border crossing points.

…

(36) Residence documents issued to citizens of the Union should include specific information to ensure that they are identified as such in all Member States. This should facilitate the recognition of the Union citizen's use of the right of free movement and of the rights inherent to this use, but harmonisation should not go beyond what is appropriate to address the weaknesses of current documents. Member States are free to select the format in which these documents are issued and could issue them in a format complying with the specifications of ICAO Document 9303.

…

(40) 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) (OJ 2016 L 119, p. 1) ("the GDPR")] applies with regard to the personal data to be processed in the context of the application of this Regulation. It is necessary to further specify safeguards applicable to the processed personal data and in particular to sensitive data such as biometric identifiers. Data subjects should be made aware of the existence in their documents of the storage medium containing their biometric data including its accessibility in contactless form as well as of all instances where the data contained in their identity cards and residence documents are used. In any case, data subjects should have access to personal data processed in their identity cards and residence documents and should have the right to have them rectified by way of issuance of a new document where such data is erroneous or incomplete. The storage medium should be highly secure and effectively protect personal data stored on it from unauthorised access.

(41) Member States should be responsible for the proper processing of biometric data, from collection to integration of the data on the highly secure storage medium, in accordance with [the GDPR].

(42) Member States should exercise particular caution when cooperating with an external service provider. Such cooperation should not exclude any liability of the Member States arising under Union or national law for breaches of obligations with regard to personal data.

…

(46) Since the objectives of this Regulation, namely to enhance security and to facilitate the exercise of the rights of free movement by Union citizens and their family members cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 [TEU]. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.'

4 Article 1 of Regulation 2019/1157, which is entitled ‘Subject matter’, provides:

‘This Regulation strengthens the security standards applicable to identity cards issued by Member States to their nationals and to residence documents issued by Member States to Union citizens and their family members when exercising their right to free movement.’

5 Article 2 of that regulation, which is entitled ‘Scope’, provides:

‘This Regulation applies to:

(a) identity cards issued by Member States to their own nationals as referred to in Article 4(3) of Directive [2004/38];

This Regulation shall not apply to identification documents issued on a provisional basis with a period of validity of less than six months.

(b) registration certificates issued in accordance with Article 8 of Directive [2004/38] to Union citizens residing for more than three months in a host Member State and documents certifying permanent residence issued in accordance with Article 19 of Directive [2004/38] to Union citizens upon application;

(c) residence cards issued in accordance with Article 10 of Directive [2004/38] to family members of Union citizens who are not nationals of a Member State and permanent residence cards issued in accordance with Article 20 of Directive [2004/38] to family members of Union citizens who are not nationals of a Member State.’

6 Article 3 of that regulation, which is entitled ‘Security standards/format/specifications’, provides, in paragraphs 5 to 7 and 10 thereof:

‘5. Identity cards shall include a highly secure storage medium which shall contain a facial image of the holder of the card and two fingerprints in interoperable digital formats. For the capture of biometric identifiers, Member States shall apply the technical specifications established by Commission Implementing Decision C(2018) 7767 [of 30 November 2018 laying down the technical specifications of the uniform format for residence permits for third country nationals and repealing Decision C(2002) 3069].

6. The storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data. The data stored shall be accessible in contactless form and secured as provided for in Implementing Decision C(2018) 7767. Member States shall exchange the information necessary to authenticate the storage medium and to access and verify the biometric data referred to in paragraph 5.

7. Children under the age of 12 years may be exempt from the requirement to give fingerprints.

Children under the age of 6 years shall be exempt from the requirement to give fingerprints.

Persons in respect of whom fingerprinting is physically impossible shall be exempt from the requirement to give fingerprints.

…

10. Where Member States store data for electronic services such as e-government and e-business in the identity cards, such national data shall be physically or logically separated from the biometric data referred to in paragraph 5.'

7 Article 5 of that regulation, which is entitled 'Phasing out' provides as follows:

'1. Identity cards which do not meet the requirements set out in Article 3 shall cease to be valid at their expiry or by 3 August 2031, whichever is earlier.

2. By way of derogation from paragraph 1:

(a) Identity cards which … do not include a functional MRZ, as defined in paragraph 3, shall cease to be valid at their expiry or by 3 August 2026, whichever is earlier.

…

3. For the purpose of paragraph 2, a functional MRZ shall mean:

(a) a machine-readable zone compliant with part 3 of ICAO document 9303; or

(b) any other machine-readable zone for which the issuing Member State notifies the rules required for reading and displaying the information contained therein, unless a Member State notifies the [European] Commission, by 2 August 2021, of its lack of capacity to read and display this information.

…'

8 The first paragraph of Article 6 of Regulation 2019/1157, which is entitled 'Minimum information to be indicated', provides as follows:

'Residence documents when issued by Member States to Union citizens, shall indicate at a minimum the following:

…

(f) the information to be included on registration certificates and documents certifying permanent residence, issued in accordance with Articles 8 and 19 of Directive [2004/38], respectively;

…'

9 Article 10 of Regulation 2019/1157, which is entitled 'Collection of biometric identifiers', provides:

'1. The biometric identifiers shall be collected solely by qualified and duly authorised staff designated by the authorities responsible for issuing identity cards or residence cards, for the purpose of being integrated into the highly secure storage medium provided for in Article 3(5) for identity cards and in Article 7(1) for residence cards. By way of derogation from the first sentence, fingerprints shall be collected solely by qualified and duly authorised staff of such authorities, except in the case of applications submitted to the diplomatic and consular authorities of the Member State.

With a view to ensuring the consistency of biometric identifiers with the identity of the applicant, the applicant shall appear in person at least once during the issuance process for each application.

2. Member States shall ensure that appropriate and effective procedures for the collection of biometric identifiers are in place and that those procedures comply with the rights and principles set out in the Charter, the Convention for the Protection of Human Rights and Fundamental Freedoms and the United Nations Convention on the Rights of the Child.

Where difficulties are encountered in the collection of biometric identifiers, Member States shall ensure that appropriate procedures are in place to respect the dignity of the person concerned.

3. Other than where required for the purpose of processing in accordance with Union and national law, biometric identifiers stored for the purpose of personalisation of identity cards or residence documents shall be kept in a highly secure manner and only until the date of collection of the document and, in any case, no longer than 90 days from the date of issue. After this period, these biometric identifiers shall be immediately erased or destroyed.'

10 Article 11 of that regulation, which is entitled 'Protection of personal data and liability', provides in paragraphs 4 and 6 thereof as follows:

'4. Cooperation with external service providers shall not exclude any liability on the part of a Member State which may arise under Union or national law in respect of breaches of obligations with regard to personal data.

…

6. Biometric data stored in the storage medium of identity cards and residence documents shall only be used in accordance with Union and national law, by the duly authorised staff of competent national authorities and Union agencies, for the purpose of verifying:

(a) the authenticity of the identity card or residence document;

(b) the identity of the holder by means of directly available comparable features where the identity card or residence document is required to be produced by law.'

11 Paragraphs 1 and 2 of Article 14 of that regulation, which is entitled 'Additional technical specifications', provide as follows:

'1. In order to ensure, where appropriate, that identity cards and residence documents referred to in points (a) and (c) of Article 2 comply with future minimum security standards, the Commission shall establish, by means of implementing acts, additional technical specifications, relating to the following:

(a) additional security features and requirements, including enhanced anti-forgery, counterfeiting and falsification standards;

(b) technical specifications for the storage medium of the biometric features referred to in Article 3(5) and their security, including prevention of unauthorised access and facilitation of validation;

(c) requirements for quality and common technical standards for the facial image and the fingerprints.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 15(2).

2. In accordance with the procedure referred to in Article 15(2), it may be decided that the specifications referred to in this Article are to be secret and are not to be published. …'

2. The GDPR

12 Recital 51 of the GDPR states:

'Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. … The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition [on] processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his [or her] explicit consent or in respect of specific needs …'

13 Article 4 of that regulation, which is entitled 'Definitions', is worded as follows:

'For the purposes of this Regulation:

…

(2) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

…

(7) "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

…’

14 Paragraph 1 of Article 9 of the GDPR, which is entitled ‘Processing of special categories of personal data’, provides as follows:

‘Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.’

15 Paragraphs 1, 3 and 10 of Article 35 of that regulation, which is entitled ‘Data protection impact assessment’, provides as follows:

‘1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

…

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

…

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.’

3. Regulation (EU) 2016/399

16 Article 8 of Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ 2016 L 77, p. 1), as amended by Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 (OJ 2017 L 74, p. 1), provides, in paragraphs 1 and 2 thereof:

‘1. Cross-border movement at external borders shall be subject to checks by border guards. Checks shall be carried out in accordance with this chapter.

…

2. On entry and on exit, persons enjoying the right of free movement under Union law shall be subject to the following checks:

(a) verification of the identity and the nationality of the person and of the authenticity and validity of the travel document for crossing the border, including by consulting the relevant databases …

(b) verification that a person enjoying the right of free movement under Union law is not considered to be a threat to public policy, internal security, public health or the international relations of any of the Member States, …

Where there are doubts as to the authenticity of the travel document or the identity of its holder, at least one of the biometric identifiers integrated into the passports and travel documents issued in accordance with [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 (OJ 2004 L 385, p. 1)] shall be verified. Where possible, such verification shall also be carried out in relation to travel documents not covered by that Regulation.

…’

4. Directive 2004/38

17 Paragraphs 1 and 3 of Article 4 of Directive 2004/38, which is entitled ‘Right of exit’, provides as follows:

‘1. Without prejudice to the provisions on travel documents applicable to national border controls, all Union citizens with a valid identity card or passport and their family members who are not nationals of a Member State and who hold a valid passport shall have the right to leave the territory of a Member State to travel to another Member State.

…

3. Member States shall, acting in accordance with their laws, issue to their own nationals, and renew, an identity card or passport stating their nationality.’

18 Paragraph 1 of Article 5 of that directive, which is entitled 'Right of entry', provides as follows:

'Without prejudice to the provisions on travel documents applicable to national border controls, Member States shall grant Union citizens leave to enter their territory with a valid identity card or passport and shall grant family members who are not nationals of a Member State leave to enter their territory with a valid passport.

No entry visa or equivalent formality may be imposed on Union citizens.'

19 Article 6 of that directive, which is entitled 'Right of residence for up to three months', provides as follows:

'1. Union citizens shall have the right of residence on the territory of another Member State for a period of up to three months without any conditions or any formalities other than the requirement to hold a valid identity card or passport.

2. The provisions of paragraph 1 shall also apply to family members in possession of a valid passport who are not nationals of a Member State, accompanying or joining the Union citizen.'

20 Paragraphs 1 and 3 of Article 8 of Directive 2004/38, which is entitled 'Administrative formalities for Union citizens', provide as follows:

'1. Without prejudice to Article 5(5), for periods of residence longer than three months, the host Member State may require Union citizens to register with the relevant authorities.

…

3. For the registration certificate to be issued, Member States may only require that

– Union citizens to whom point (a) of Article 7(1) applies present a valid identity card or passport, a confirmation of engagement from the employer or a certificate of employment, or proof that they are self-employed persons;

– Union citizens to whom point (b) of Article 7(1) applies present a valid identity card or passport and provide proof that they satisfy the conditions laid down therein;

– Union citizens to whom point (c) of Article 7(1) applies present a valid identity card or passport, provide proof of enrolment at an accredited establishment and of comprehensive sickness insurance cover and the declaration or equivalent means referred to in point (c) of Article 7(1). Member States may not require this declaration to refer to any specific amount of resources.'

5. The Interinstitutional Agreement

21 Points 12 to 14 of the Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016 (OJ 2016 L 123, p. 1) ('the Interinstitutional Agreement') is worded as follows:

'12. …

Impact assessments are a tool to help the three Institutions reach well-informed decisions and not a substitute for political decisions within the democratic decision-making process. …

Impact assessments should cover the existence, scale and consequences of a problem and the question whether or not Union action is needed. They should map out alternative solutions and, where possible, potential short and long-term costs and benefits, assessing the economic, environmental and social impacts in an integrated and balanced way and using both qualitative and quantitative analyses. The principles of subsidiarity and proportionality should be fully respected, as should fundamental rights. … Impact assessments should be based on accurate, objective and complete information and should be proportionate as regards their scope and focus.

13. The Commission will carry out impact assessments of its legislative … initiatives … which are expected to have significant economic, environmental or social impacts. The initiatives included in the Commission Work Programme or in the joint declaration will, as a general rule, be accompanied by an impact assessment.

… The final results of the impact assessments will be made available to the European Parliament, the Council [of the European Union] and national Parliaments, and will be made public along with the opinion(s) of the Regulatory Scrutiny Board at the time of adoption of the Commission initiative.

14. The … Parliament and the Council, upon considering Commission legislative proposals, will take full account of the Commission's impact assessments. To that end, impact assessments shall be presented in such a way as to facilitate the consideration by the … Parliament and the Council of the choices made by the Commission.'

B. German law

22 Paragraph 5 of the Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Law on identity cards and electronic proof of identity) of 18 June 2009 (BGBl. I, p. 1346), in the version applicable to the facts in the main proceedings ('the PAuswG'), entitled 'Model identity card; stored data', provides at subparagraph 9 thereof as follows:

'The two fingerprints of the [identity card] applicant to be stored on the electronic storage medium pursuant to Regulation [2019/1157] shall be stored on the storage and electronic processing medium of the identity card in the form of the flat print of the left index and right index fingers. If an index finger is missing, if the quality of the fingerprint is insufficient or if the fingertip is injured, the flat of either the thumb, the middle finger or the ring finger shall be stored as a substitute. Fingerprints shall not be stored if the taking of fingerprints is impossible for medical reasons which are not of a temporary nature.'

23 Paragraph 6 of the PAuswG, provides in subparagraphs 1 and 2 thereof as follows:

'(1) Identity cards shall be issued for a validity period of 10 years.

(2) Before the validity of an identity card expires, a new identity card may be applied for if it can be shown that there is a legitimate interest in issuing a new card.'

24 Paragraph 9 of the PAuswG, which is entitled 'Issuing the card', states in the first sentence of subparagraph 1 thereof as follows:

'Identity cards and provisional identity cards shall be issued on application to Germans within the meaning of Paragraph 116(1) of the Basic Law.'

25 Paragraph 28 of the PAuswG, which is entitled 'Invalidity', provides in subparagraph 3 thereof as follows:

'Malfunctioning which affects the electronic storage and processing medium shall not affect the validity of the identity card.'

II. The dispute in the main proceedings and the question referred for a preliminary ruling

26 On 30 November 2021, the applicant in the main proceedings applied to the City of Wiesbaden for a new identity card to be issued, on the ground that the electronic chip in his old card was defective. The applicant requested, however, that the new card should not contain his fingerprints.

27 The City of Wiesbaden rejected that application on two grounds. First, the applicant in the main proceedings was not entitled to have a new identity card issued, since he was already in possession of a valid identity document. In accordance with Paragraph 28(3) of the PAuswG, an identity card remains valid even if its electronic chip is defective. Second, and in any event, since 2 August 2021, the inclusion of two fingerprints in the storage medium of identity cards had been mandatory under Paragraph 5(9) of the PAuswG, which transposes Article 3(5) of Regulation 2019/1157.

28 On 21 December 2021, the applicant in the main proceedings brought an action before the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), which is the referring court, seeking an order requiring the City of Wiesbaden to issue him with an identity card with no fingerprints being collected.

29 The referring court has doubts regarding the lawfulness of the two grounds of the decision at issue in the main proceedings. As regards, in particular, the second ground, it tends toward the view that the validity of Regulation 2019/1157 or, at least, the validity of Article 3(5) thereof can be disputed.

30 In the first place, the referring court asks whether that regulation ought to have been adopted on the basis of Article 77(3) TFEU and, therefore, after the special legislative procedure provided for by that provision had been concluded, rather than on the basis of Article 21(2) TFEU and under the ordinary legislative procedure. First, Article 77(3) TFEU refers specifically to the competence of the European Union to adopt, inter alia, provisions on identity cards and is thus a more specific provision than Article 21(2) TFEU. Second, in the judgment of 17 October 2013, *Schwarz* (C-291/12, EU:C:2013:670), the Court held that Regulation No 2252/2004, in so far as it lays down standards for biometric elements in passports, was validly based on Article 62(2)(a) EC, which now corresponds to Article 77(3) TFEU.

31 In the second place, the referring court refers to the possible existence of a procedural defect vitiating the adoption of Regulation 2019/1157. As the European Data Protection Supervisor ('the EDPS') pointed out in Opinion 7/2018 of 10 August 2018 on the proposal for a regulation on strengthening the security of identity cards of Union citizens and other documents ('Opinion

7/2018'), the taking and storage of fingerprints constitute processing of personal data which must be the subject of an impact assessment under Article 35(10) of the GDPR. In the present case, no such assessment was carried out. In particular, the document accompanying that proposal for a regulation, entitled 'Impact assessment', cannot be regarded as being an impact assessment as provided for in that provision.

32 In the third place, the referring court asks, more specifically, whether Article 3(5) of Regulation 2019/1157 is compatible with Articles 7 and 8 of the Charter relating, respectively, to respect for private and family life and the protection of personal data. The obligation on the Member States to issue identity cards whose storage medium contains two fingerprints constitutes a limitation on the exercise of the rights recognised by those two provisions of the Charter, a limitation which can be justified only if it satisfies the conditions laid down in Article 52(1) of the Charter.

33 First, that limitation might not meet an objective of general interest. It is true that the Court accepted, in the judgment of 17 October 2013, *Schwarz* (C-291/12, EU:C:2013:670), that combating illegal entry by third-country nationals into the territory of the European Union is an objective recognised by EU law. However, an identity card is not, primarily, a travel document, as a passport is, and its objective is merely to enable the identity of an EU citizen to be verified in his or her dealings with administrative authorities and private third parties.

34 Second, assuming that that regulation pursues an objective of general interest recognised by EU law, there are doubts as to the proportionality of that limitation. The solution adopted by the Court in the judgment of 17 October 2013, *Schwarz* (C-291/12, EU:C:2013:670), is not transposable to Regulation 2019/1157, since it relates to passports, which it is optional to hold in Germany, unlike identity cards, and the use of which pursues a different objective.

35 On the other hand, it is apparent from Opinion 7/2018 that the inclusion and storage of fingerprints would have a wide-ranging impact on up to 370 million EU citizens, potentially subjecting 85% of the EU population to a mandatory requirement to have fingerprints taken. That wide-ranging impact, combined with the very sensitive nature of the data processed (a facial image combined with two fingerprints), means that the limitation placed on the exercise of the rights guaranteed in Articles 7 and 8 of the Charter, resulting from the compulsory collection of fingerprints for the purpose of producing identity cards, is greater than for passports, which, in turn, requires a stronger justification and a careful assessment of the measure at issue under a test of strict necessity.

36 In any event, the need to carry out a strict review of proportionality also follows from Article 9(1) of the GDPR, under which the processing of such biometric data is, in principle, prohibited and may be authorised only in exceptional and strictly limited situations.

37 In that context, while the referring court is of the opinion that the use of biometric data reduces the risk that a document may be falsified, it has doubts whether that fact alone can justify the extent of the limitation on the right to protection of personal data in the light, in particular, of the following reasons.

38 First of all, in Opinion 7/2018, the EDPS stated that other secure printing techniques for identification documents, such as holograms or watermarks, are much less intrusive, while also enabling the falsification of those documents to be prevented and their authenticity to be

verified. Moreover, the fact that German law accepts that an identity card with a defective electronic chip remains valid demonstrates that the physical elements, in particular microprints or UV overprints, are sufficient to ensure the security of those cards.

39 Next, Article 3(7) of Regulation 2019/1157 authorises Member States to exempt children under the age of 12 years from the obligation to provide their fingerprints and, in any event, requires Member States to exempt children under the age of six years from that obligation, which demonstrates that it is not strictly necessary to take two fingerprints.

40 Furthermore, Article 3(5) of Regulation 2019/1157 would not comply with the principle of data minimisation, set out in Article 5 of the GDPR, from which it is apparent that the collection and use of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. While it facilitates interoperability between different types of systems, the collection of two complete fingerprints, rather than simply a subset of characteristics of those fingerprints ('the minutiae'), also increases the amount of personal data stored and therefore the risk of impersonation in the event of a data leak. That risk is, moreover, not negligible, since the electronic chips used in identity cards could be read by unauthorised scanners.

41 Finally, and in essence, the limitation on the exercise of the rights guaranteed in Articles 7 and 8 of the Charter could be non-legitimate since, in Opinion 7/2018, the EDPS noted that when Regulation 2019/1157 was adopted, the number of fraudulent identity cards was relatively small in proportion to the number of cards issued (38 870 fraudulent cards detected between 2013 and 2017) and that that number had been decreasing for a number of years.

42 In those circumstances, the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) decided to stay the proceedings and to refer the following question to the Court of Justice for a preliminary ruling:

'Does the obligation to take fingerprints and store them in identity cards in accordance with Article 3(5) of Regulation [2019/1157] 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?'

III. Consideration of the question referred

43 By its question, the referring court seeks, in essence, to ascertain whether Regulation 2019/1157 is invalid, as a whole or in part, on the grounds that (i) it was adopted on an incorrect legal basis, (ii) it infringes Article 35(10) of the GDPR and, (iii) it is contrary to Articles 7 and 8 of the Charter.

A. The first ground of invalidity: incorrect legal basis

44 The first ground of invalidity mentioned by the referring court concerns whether, having regard in particular to the explicit reference to identity cards in Article 77(3) TFEU and the solution adopted in the judgment of 17 October 2013, *Schwarz* (C-291/12, EU:C:2013:670), Regulation 2019/1157 ought to have been adopted on the basis of Article 77(3) TFEU and in accordance with the special legislative procedure laid down therein, and not, as was the case, on the basis of Article 21(2) TFEU.

1. Preliminary observations

45 According to settled case-law, the choice of legal basis for an EU measure must rest on objective factors that are amenable to judicial review; these include the aim and content of that measure (judgments of 16 February 2022, *Hungary* v *Parliament and Council*, C-156/21, EU:C:2022:97, paragraph 107, and of 16 February 2022, *Poland* v *Parliament and Council*, C-157/21, EU:C:2022:98, paragraph 121).

46 In addition, it should be noted that where the Treaties contain a more specific provision that is capable of constituting the legal basis for the measure in question, the measure must be founded on that provision (judgments of 6 September 2012, *Parliament* v *Council*, C-490/10, EU:C:2012:525, paragraph 44, and of 8 December 2020, *Poland* v *Parliament and Council*, C-626/18, EU:C:2020:1000, paragraph 48 and the case-law cited).

47 Lastly, if examination of an EU measure reveals that it pursues several purposes or that it comprises several components and if one of those purposes or components is identifiable as the main or predominant purpose or component, whereas the others are merely incidental or are only extremely limited in scope, the legal basis for adopting that measure must be determined in accordance with that main purpose or component (see, to that effect, judgment of 20 November 2018, *Commission* v *Council (Antarctic MPAs)*, C-626/15 and C-659/16, EU:C:2018:925, paragraph 77, and Opinion 1/19 *(Istanbul Convention)* of 6 October 2021, EU:C:2021:832, paragraph 286).

2. The respective scopes of Article 21(2) TFEU and Article 77(3) TFEU

48 Article 21(2) TFEU states that if action by the Union should prove necessary to guarantee every citizen of the European Union the right to move and reside freely within the territory of the Member States, and if the Treaties have not provided powers to that effect, 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 those rights.

49 It follows that that provision confers on the European Union a general competence to adopt provisions necessary for the purposes of facilitating the exercise of the right of citizens of the European Union to move and reside freely within the territory of the Member States referred to in Article 20(2)(a) TFEU, subject to the powers laid down to that effect by the Treaties.

50 Unlike Article 21(2) TFEU, Article 77(3) TFEU expressly lays down such powers in relation to the adoption of measures relating to passports, identity cards, residence permits or any other such document issued to citizens of the European Union for the purposes of facilitating the exercise of the right, referred to in Article 20(2)(a) TFEU, to move and reside freely within the territory of the Member States.

51 It is true that Article 77(3) TFEU is found in Title V of that treaty, which concerns the area of freedom, security and justice and, more specifically, in Chapter 2 of that Title V which is entitled 'Policies on border checks, asylum and immigration'. However, according to Article 77(1) TFEU, the European Union is to develop a policy with a view to ensuring the absence of any controls on persons, whatever their nationality, when crossing internal borders, to carrying out checks on persons and efficient monitoring of the crossing of external borders, and to the gradual introduction of an integrated management system for such borders. The provisions concerning passports, identity cards, residence permits or any other such document referred to in the competence laid down in Article 77(3) TFEU form an integral part of any such EU policy. As regards citizens of the European Union, those documents enable them, inter alia, to certify that they benefit from the right to move and reside freely within the territory of the Member States and therefore to exercise that right. Consequently, Article 77(3) is capable of providing the basis for the adoption of measures relating to those documents if such action appears necessary to facilitate the exercise of that right, laid down in Article 20(2)(a) TFEU.

52 That interpretation of the material scope of Article 77(3) TFEU cannot be invalidated either by the historical development of the Treaties in relation to European Union's competence to adopt measures relating to passports, identity cards, residence permits and other similar documents, to which the Parliament, the Council and the Commission refer, or by the fact, mentioned by the German Government, that that provision states that it is to apply 'if the Treaties have not provided the necessary powers'.

53 It is true that the Treaty of Lisbon removed the provision previously set out in Article 18(3) EC, which expressly precluded the EU legislature from having recourse to Article 18(2) EC (now Article 21(2) TFEU) as the legal basis for the adoption of 'provisions on passports, identity cards, residence permits or any other such document' and 'provisions on social security or social protection'. However, at the same time, that treaty expressly conferred on the European Union a power to take action in those two fields – namely (i) in Article 21(3) TFEU as regards social security and social protection and (ii) in Article 77(3) TFEU as regards the provisions on passports, identity cards, residence permits or any other such document, and made the adoption of measures in those fields subject to a special legislative procedure and, in particular, to unanimity in the Council.

54 In those circumstances, it cannot be inferred from the removal of the provision previously set out in Article 18(3) EC that it would from then on be possible to adopt 'provisions on passports, identity cards, residence permits or any other such document' on the basis of Article 21(2) TFEU. On the contrary, it follows from the historical treaty development that the authors of the Treaties intended, by means of Article 77(3) TFEU, to confer on the European Union a competence to adopt such provisions, intended to facilitate the exercise of the right to move and reside freely within the territory of the Member States guaranteed in Article 20(2)(a) TFEU, which is more specific than the more general competence laid down in Article 21(2) TFEU.

55 In addition, the statement in Article 77(3) TFEU that that provision is to apply 'if the Treaties have not provided the necessary powers' must be understood, having regard to the general scheme of the FEU Treaty, as meaning that the powers thereby referred to are conferred not by a provision with a more general scope, such as Article 21(2) TFEU, but by a provision which is even more specific.

56 Therefore, the adoption of Regulation 2019/1157 could be based on Article 21(2) TFEU only if the purpose or the main or predominant component of that regulation were to fall outside the specific scope of Article 77(3) TFEU, namely the issuing of passports, identity cards, residence permits or any other such document, for the purposes of facilitating the exercise of the right referred to in Article 20(2)(a) TFEU.

3. The purpose or the main or predominant component of Regulation 2019/1157

57 In the first place, as regards the purpose of Regulation 2019/1157, Article 1 thereof states that it is to strengthen the security standards applicable to identity cards issued by Member States to their nationals and to residence documents issued by Member States to Union citizens and their family members when exercising their right to free movement.

58 Similarly, recital 46 of that regulation states that the objectives of that regulation are to 'enhance security' of those travel and identity documents in order 'to facilitate the exercise of the rights of free movement by Union citizens and their family members', which is also confirmed by recitals 1, 2, 5, 17, 28, 29 and 36 of that regulation.

59 In the second place, as regards the content of Regulation 2019/1157, it should be noted that that regulation comprises 16 articles. Articles 1 and 2 of that regulation define, respectively, its subject matter and scope. Articles 3, 4, 6 and 7 of that regulation, which form the main components thereof, set out, inter alia, the requirements in terms of security, content, format or specifications with which identity cards and residence documents issued by the Member States must comply, while Articles 5 and 8 of that regulation provide for the phasing out of identity cards and residence cards which do not meet the requirements laid down by that regulation. Lastly, Articles 9 to 16 of Regulation 2019/1157 specify how the obligations laid down therein are to be implemented, in particular as regards the collection of biometric identifiers and the protection of personal data.

60 It is true that Article 2 of Regulation 2019/1157 states that that regulation applies not only to identity cards issued by Member States to their own nationals, but also to registration certificates issued in accordance with Article 8 of Directive 2004/38 to Union citizens residing for more than three months in a host Member State and to documents certifying permanent residence issued in accordance with Article 19 of that directive, which certificates and documents cannot be treated as similar to identity cards, passports or residence permits. However, Regulation 2019/1157 contains no provision governing those certificates and merely indicates, in point (f) of the first paragraph of Article 6 thereof, that residence documents issued by Member States to citizens of the European Union must contain the information to be included on registration certificates and documents certifying permanent residence issued in accordance with Articles 8 and 19 of Directive 2004/38 respectively. Accordingly, the purpose and the component of that regulation which relate to those certificates must be regarded as being extremely limited in scope, with the result that the legal basis of that regulation cannot be determined in the light of that purpose or that component.

61 In those circumstances, it follows from the purpose and main components of Regulation 2019/1157 that that regulation is one of the measures which falls within the specific scope of Article 77(3) TFEU, as identified in paragraphs 48 to 51 of the present judgment.

62 Accordingly, by adopting Regulation 2019/1157 on the basis of Article 21(2) TFEU, the EU legislature infringed Article 77(3) TFEU and had recourse to an inappropriate legislative procedure.

63 It follows that the first ground of invalidity mentioned by the referring court, alleging that Regulation 2019/1157 was adopted erroneously on the basis of Article 21(2) TFEU and under the ordinary legislative procedure, is such as to result in the invalidity of that regulation.

B. The second ground of invalidity: failure to comply with Article 35(10) of the GDPR

64 The second ground of invalidity mentioned by the referring court alleges that Regulation 2019/1157 was adopted without a data protection impact assessment having been carried out, contrary to Article 35(10) of the GDPR.

65 In that regard, it should be stated that Article 35(1) of the GDPR provides that where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller must, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Article 35(3) of that regulation states that such an analysis is to be required in the case of processing on a large scale of special categories of data referred to in Article 9(1) of that regulation, such as biometric data for the purpose of uniquely identifying a natural person.

66 Given that, in the present case, Regulation 2019/1157 does not itself undertake any operation applied to personal data or sets of personal data, but merely provides for Member States to carry out certain processing operations where an application for an identity card is made, it must be held that the adoption of that regulation was not subject to an assessment of the impact of the envisaged data processing operations within the meaning of Article 35(1) of the GDPR, first having been undertaken. Article 35(10) of that regulation establishes a derogation to Article 35(1) of that regulation.

67 It follows that, since, as is apparent from the foregoing, Article 35(1) of the GDPR did not apply when Regulation 2019/1157 was adopted, it was not possible for that adoption to infringe Article 35(10) of the GDPR.

68 In the light of the foregoing, the second ground alleging infringement of Article 35(10) of the GDPR is not such as to result in the invalidity of Regulation 2019/1157.

C. The third ground of invalidity: Article 3(5) of Regulation 2019/1157 is incompatible with Articles 7 and 8 of the Charter

69 The third ground of invalidity in respect of Regulation 2019/1157 referred to by the referring court concerns whether the obligation to include two complete fingerprints in the storage medium of identity cards issued by Member States, laid down in Article 3(5) of that regulation, entails an unjustified limitation of the rights guaranteed in Articles 7 and 8 of the Charter.

1. Whether there is a limitation

70 Article 7 of the Charter provides, inter alia, that everyone has the right to respect for his or her private life. Pursuant to Article 8(1) of the Charter, everyone has the right to the protection of personal data concerning him or her. It follows from a joint reading of those provisions that, as a general rule, any processing of personal data by a third party may constitute a threat to those rights (judgment of 17 October 2013, *Schwarz*, C-291/12, EU:C:2013:670, paragraph 25).

71 In the present case, Article 3(5) of Regulation 2019/1157 provides that the highly secure storage medium to be included in identity cards issued by Member States to their own nationals must contain biometric data, namely a facial image and two fingerprints in interoperable digital formats.

72 Such personal data allow for the precise identification of the natural persons concerned and are particularly sensitive due to the significant risks to the fundamental rights and freedoms which their use can constitute, as is apparent, in particular, from recital 51 of the GDPR, which applies to the data at issue, as stated in recital 40 of Regulation 2019/1157.

73 Therefore, the obligation to include two fingerprints in the storage medium of identity cards, laid down in Article 3(5) of Regulation 2019/1157, constitutes a limitation both of the right to respect for private life and of the right to the protection of personal data, enshrined in Articles 7 and 8 of the Charter respectively.

74 In addition, that obligation involves carrying out, in advance, two successive personal data processing operations, namely the collection of those fingerprints from the data subject, then the temporary storage of those fingerprints for the purposes of personalisation of identity cards, since those operations are governed by Article 10 of that regulation. Those operations also constitute limitations of the rights enshrined in Articles 7 and 8 of the Charter.

2. The justification for the limitation

75 As is apparent from settled case-law, the right to respect for private life and the right to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter respectively, are not absolute rights, but must be considered in relation to their function in society (see, to that effect, judgment of 20 September 2022, *SpaceNet and Telekom Deutschland*, C-793/19 and C-794/19, EU:C:2022:702, paragraph 63).

76 Limitations may therefore be placed on those rights, provided that, in accordance with the first sentence of Article 52(1) of the Charter, they are provided for by law and respect the essence of those rights. In addition, in accordance with the second sentence of that paragraph, in compliance with the principle of proportionality, such limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. In that regard, Article 8(2) of the Charter states that personal data must, inter alia, be processed ‘for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law’.

(a) Whether the principle of legality has been complied with

77 As regards the requirement laid down in the first sentence of Article 52(1) of the Charter that any limitation on the exercise of rights recognised by the Charter must be provided for by law, it should be recalled that that requirement implies that the act which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned, bearing in mind, on the one hand, that that requirement does not preclude the limitation in question from being formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances and, on the other hand, that the Court may, where appropriate, specify, by means of interpretation, the actual scope of the limitation in the light of the very wording of the EU legislation in question as well as its general scheme and the objectives it pursues, as interpreted in view of the fundamental rights guaranteed by the Charter (judgment of 21 June 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, paragraph 114).

78 In the present case, the limitations on the exercise of the fundamental rights guaranteed in Articles 7 and 8 of the Charter arising from the obligation to include two complete fingerprints in the storage medium of identity cards issued by Member States and the conditions for application and the scope of those limitations are defined clearly and precisely by Article 3(5) and Article 10(1) and (3) of Regulation 2019/1157, which were adopted by the EU legislature in accordance with the ordinary legislative procedure and the effects of which will be maintained by the present judgment.

79 Therefore, those limitations on the exercise of the fundamental rights guaranteed in Articles 7 and 8 of the Charter comply with the principle of legality referred to in the first sentence of Article 52(1) of the Charter.

(b) Compliance with the essence of the fundamental rights guaranteed in Articles 7 and 8 of the Charter

80 It should be stated that the information provided by fingerprints does not, in itself, make it possible to have an overview of the private and family life of data subjects.

81 In those circumstances, the limitation entailed by the obligation to include two fingerprints in the storage medium of identity cards issued by the Member States, laid down in Article 3(5) of Regulation 2019/1157, does not adversely affect the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter (see, by analogy, judgment of 21 June 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, paragraph 120).

(c) Whether the principle of proportionality has been complied with

82 As is apparent from the second sentence of Article 52(1) of the Charter, in order for limitations on the exercise of the fundamental rights guaranteed by the Charter to be made in accordance with the principle of proportionality, those limitations must be necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

83 More specifically, derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary, it being understood that where there is a choice between several measures appropriate to meeting the legitimate objectives pursued, recourse must be had to the least onerous. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure at issue, by properly balancing the objective of general interest against the rights concerned, in order to ensure that the disadvantages caused by that measure are not disproportionate to the aims pursued. Thus, the question whether a limitation on the rights guaranteed in Articles 7 and 8 of the Charter can be justified must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness (judgment of 22 November 2022, *Luxembourg Business Registers*, C-37/20 and C-601/20, EU:C:2022:912, paragraph 64 and the case-law cited).

84 Accordingly, in order to ascertain whether, in the present case, the interference with the rights guaranteed in Articles 7 and 8 of the Charter resulting from the obligation to include two fingerprints in the storage medium of identity cards, provided for in Article 3(5) of Regulation 2019/1157, comply with the principle of proportionality, it is necessary to examine, first, whether that measure pursues one or more objectives of general interest recognised by the European Union and is actually appropriate for attaining those objectives, second, whether the resulting interferences are limited to what is strictly necessary, in the sense that those objectives could not reasonably be achieved in an equally effective manner by other means less prejudicial to those fundamental rights of the data subjects, and, third, whether those interferences are not disproportionate to the objectives, which implies, in particular, a balancing of those objectives and the seriousness of those interferences (see, to that effect, judgments of 22 November 2022, *Luxembourg Business Registers*, C-37/20 and C-601/20, EU:C:2022:912, paragraph 66, and of 8 December 2022, *Orde van Vlaamse Balies and Others*, C-694/20, EU:C:2022:963, paragraph 42).

(1) Whether one or more objectives of general interest recognised by the European Union is pursued and whether the measure to attain those objectives is appropriate

(i) Whether the objectives pursued by the measure at issue are of general interest

85 Article 1 of Regulation 2019/1157 states that the purpose of that regulation is to strengthen the security standards applicable, inter alia, to identity cards issued by Member States to their nationals when exercising their right to free movement.

86 More specifically, and as is apparent from recitals 4, 5, 17 to 20 and 32 of Regulation 2019/1157, the inclusion of biometric data, including two complete fingerprints, in the storage medium of identity cards is intended to ensure the authenticity of those cards and to enable the holder of that card to be reliably identified, while contributing, in accordance with recitals 23 and 33 and Article 3(5) of that regulation, to the interoperability of identification document verification systems, with a view to reducing the risk of falsification and document fraud.

87 The Court has already had occasion to rule on the issuing of passports (see, to that effect, judgment of 17 October 2013, *Schwarz*, C-291/12, EU:C:2013:670, paragraphs 36 to 38) and the establishment of an identification file for third-country nationals (see, to that effect, judgment of 3 October 2019, *A and Others*, C-70/18, EU:C:2019:823, paragraph 46 and the case-law cited), that

combating document fraud, which includes, inter alia, combating the production of false identity cards and identity theft, constitutes an objective of general interest recognised by the European Union.

88 The objective of interoperability of identification document verification systems is also of general interest since, as is apparent from recital 17 of Regulation 2019/1157, it contributes to facilitating the exercise by EU citizens of the right granted to them by Article 20 TFEU to move and reside freely within the territory of the Member States.

(ii) Whether the measure at issue is appropriate for actually meeting the objectives of general interest pursued

89 In the present case, the inclusion of two complete fingerprints in the storage medium of identity cards is appropriate for attaining the general interest objectives of combating the production of false identity cards and identity theft as well as the interoperability of verification systems, put forward by the EU legislature in order to justify that measure.

90 First of all, the inclusion of biometric data, such as fingerprints, in identity cards is liable to make it more difficult to produce false identity cards, in so far as, inter alia, in accordance with Article 3(5) of Regulation 2019/1157, read in conjunction with Article 14(1) and (2) of that regulation, such data must be stored in accordance with precise technical specifications and be capable of being kept secret.

91 Next, the inclusion of such biometric data is a means making it possible, in accordance with Article 11(6) and recitals 18 and 19 of Regulation 2019/1157, reliably to verify the authenticity of the identity card and the identity of the cardholder, and thereby to reduce the risk of fraud.

92 Finally, the choice made by the EU legislature to provide for complete fingerprints to be included also appears to be appropriate for achieving the objective of interoperability of identity card verification systems since the use of complete fingerprints makes it possible to ensure compatibility with all automated systems for the identification of fingerprints used by the Member States, even though such systems do not necessarily use the same identification mechanism.

93 The referring court also observes that the first subparagraph of Article 3(7) of Regulation 2019/1157 authorises Member States to exempt from the collection of their fingerprints, inter alia, children under the age of 12 and even requires them, in its second subparagraph, to exempt children under the age of six from that collection.

94 It is true that legislation is appropriate for ensuring that the objective pursued is attained only if the measures it lays down genuinely reflect a concern to attain it and if they are implemented in a consistent and systematic manner (see, by analogy, judgment of 5 December 2023, *Nordic Info*, C-128/22, EU:C:2023:951, paragraph 84 and the case-law cited).

95 However, Regulation 2019/1157 meets that requirement even though it lays down exemptions from the obligation to collect children's fingerprints since, as is apparent from recital 26 thereof, those exemptions are intended to take into account the best interests of the child.

96 The same is true of the rule laid down in Article 5 of Regulation 2019/1157 that identity cards which do not meet the requirements set out in Article 3 of that regulation only cease to be valid at their expiry or by 3 August 2031 at the latest. The EU legislature was entitled to take the view

that such a transition period was appropriate in order to avoid the burden on Member States of issuing new identity cards for all persons concerned within a very short period, without, for that reason, calling into question the long-term effectiveness of the measures laid down by that regulation.

97 As to the fact that certain Member States provide in their legislation that the identity cards which they issue remain valid notwithstanding the electronic storage medium being defective, it is sufficient to note that such legislation is compatible with Regulation 2019/1157 only in so far as the transition period mentioned in the preceding paragraph has not expired.

(2) Whether recourse to the measure at issue is necessary for the purpose of attaining the objectives of general interest pursued

98 As regards, in the first place, the very principle of including fingerprints in the storage medium of identity cards, it must be stated that fingerprints are a reliable and effective means of establishing, with certainty, the identity of a person and that the process used to collect those fingerprints is simple to implement.

99 In particular, as the Advocate General observed in point 90 of her Opinion, simply inserting a facial image is a less effective means of identification than inserting two fingerprints in addition to that image, since ageing, lifestyle, illness, plastic surgery or reconstructive surgery may also alter the anatomical characteristics of the face.

100 It is true that the impact assessment carried out by the Commission which accompanied the proposal for a regulation which gave rise to Regulation 2019/1157 indicated that the option of not requiring two fingerprints to be included in the storage medium of identity cards was to be preferred.

101 However, apart from the fact that the Commission itself did not select that option in its legislative proposal, it should be noted that, while paragraph 14 of the Interinstitutional Agreement provides that, upon considering Commission legislative proposals, the Parliament and the Council must take full account of the Commission's impact assessments, that agreement states, in paragraph 12, that such assessments 'are a tool to help the three Institutions reach well-informed decisions and not a substitute for political decisions within the democratic decision-making process'. Therefore, while the Parliament and the Council are required to take account of the Commission's impact assessments, the content of such assessments is not binding on them, in particular as regards the evaluations contained therein (see, to that effect, judgment of 21 June 2018, *Poland* v *Parliament and Council*, C-5/16, EU:C:2018:483, paragraph 159 and the case-law cited).

102 Accordingly, the mere fact that the EU legislature adopted a different and, as the case may be, more onerous measure than that recommended following the impact assessment is not such as to demonstrate that it exceeded the limits of what was necessary in order to attain the stated objective (see, to that effect, judgment of 4 May 2016, *Pillbox 38*, C-477/14, EU:C:2016:324, paragraph 65).

103 In the present case, the impact assessment carried out by the Commission found that the option of requiring fingerprints to be included in the storage medium of identity cards was the most effective for the purposes of attaining the specific objective of combating the production of false identity cards and improving document authentication. In those circumstances, the option of not

making such inclusion mandatory cannot, in any event, call into question whether the measure adopted by the EU legislature was necessary, as provided for in the case-law referred to in paragraph 84 of the present judgment.

104 In the second place, as regards the inclusion of two complete fingerprints rather than just some of the characteristics of those fingerprints ('the minutiae'), first, as the Advocate General observed in point 93 of her Opinion, the minutiae do not offer the same guarantees as a complete fingerprint. Second, the inclusion of a complete fingerprint is necessary for identification document verification systems to be interoperable, which is one of the essential objectives pursued. As is apparent from paragraph 47 of Opinion 7/2018 and as the referring court also points out, Member States use different fingerprint identification technologies, with the result that the inclusion in the storage medium of the identity card of only certain fingerprint characteristics has the effect of compromising the attainment of the interoperability objective pursued by Regulation 2019/1157 in respect of identification document verification systems.

105 It follows from the foregoing considerations that the limitations placed on the fundamental rights guaranteed in Articles 7 and 8 of the Charter which arise from the obligation to include two complete fingerprints in the storage medium appear to comply with what is strictly necessary.

(3) Whether there is a balance between, on the one hand, the seriousness of the interference with the fundamental rights involved, and, on the other hand, the objectives pursued by that measure

(i) The seriousness of the interference caused by the limitation on the exercise of the rights guaranteed in Articles 7 and 8 of the Charter

106 The assessment of the seriousness of the interference caused by a limitation on the rights guaranteed in Articles 7 and 8 of the Charter entails account being taken of the nature of the personal data concerned, in particular whether those data may be sensitive, as well as of the nature and specific arrangements for the processing of the data, in particular the number of persons who have access to those data and the arrangements for access to them. Where appropriate, account must also be taken of the existence of measures intended to prevent those data being the subject of unlawful processing.

107 In the present case, it is true that the limitation on the exercise of the rights guaranteed in Articles 7 and 8 of the Charter resulting from Regulation 2019/1157 is capable of affecting a large number of persons, the Commission in its impact assessment having evaluated that number at 370 million of the then 440 million citizens of the European Union. Fingerprints, as biometric data, are by their nature particularly sensitive and, as is apparent in particular from recital 51 of the GDPR, enjoy specific protection under EU law.

108 However, it is important to point out that the collection and storage of two complete fingerprints are permitted by Regulation 2019/1157 only for the purpose of including those fingerprints in the storage medium of identity cards.

109 In addition, it follows from Article 3(5) of that regulation, read in conjunction with Article 10(3) thereof, that, once that those fingerprints have been included and the identity card collected by the person concerned, the fingerprints collected are to be stored only in the storage medium of that card, which is, in principle, in the physical possession of that person.

110 Lastly, Regulation 2019/1157 lays down a set of safeguards intended to limit the risks that, when it is implemented, personal data may be collected or used for purposes other than the attainment of the objectives which it pursues, not only as regards the personal data processing operations which that regulation makes mandatory, but also with regard to the main processing operations to which fingerprints included in the storage medium of identity cards may be subject.

111 Accordingly, as regards, first, data collection, Article 10(1) and (2) of Regulation 2019/1157 states that biometric identifiers are to be collected 'solely by qualified and duly authorised staff' and that those staff must comply with 'appropriate and effective procedures for the collection of biometric identifiers', since those procedures must observe the rights and principles set out in the Charter, the Convention for the Protection of Human Rights and Fundamental Freedoms and the United Nations Convention on the Rights of the Child. In addition, as has been pointed out in paragraph 93 of the present judgment, Article 3(7) of that regulation contains special rules for children under the age of 12 years (first and second subparagraphs) and for persons in respect of whom fingerprinting is physically impossible (third subparagraph), those persons being 'exempt from the requirement to give fingerprints'.

112 As regards, second, data storage, on the one hand, Regulation 2019/1157 requires Member States to store, as biometric data, a facial image and two fingerprints. In that regard, recital 21 of that regulation expressly states that that regulation does not provide 'a legal basis for setting up or maintaining databases at national level for the storage of biometric data in Member States, which is a matter of national law that needs to comply with Union law regarding data protection', nor does it provide 'a legal basis for setting up or maintaining a centralised database at Union level'. On the other hand, Article 10(3) of that regulation provides that those 'biometric identifiers … shall be kept … only until the date of collection of the document and, in any case, no longer than 90 days from the date of issue' and states that, 'after this period, these biometric identifiers shall be immediately erased or destroyed'.

113 It follows, in particular, that Article 10(3) of Regulation 2019/1157 does not permit Member States to process biometric data for purposes other than those laid down in that regulation. In addition, that provision precludes the centralised storage of fingerprints which goes beyond the temporary storage of those fingerprints for the purpose of personalising identity cards.

114 Lastly, Article 11(6) of Regulation 2019/1157 refers to the possibility that biometric data contained in the secure storage medium may be used, in accordance with EU and national law, by duly authorised staff of the competent national authorities and EU agencies.

115 Article 11(6)(a) of that regulation permits the use of biometric data stored in the storage medium of identity cards and residence documents only for the purpose of verifying the authenticity of the identity card or residence document.

116 Article 11(6)(b) of that regulation provides that biometric data stored on the storage medium of identity cards and residence documents may be used to verify the identity of the holder 'by means of directly available comparable features where the identity card or residence document is required to be produced by law'. Since such processing is capable of providing additional information on the private life of data subjects, it may be carried out only for purposes which are strictly limited to identifying the data subject and subject to conditions which are defined precisely by law requiring the identity card or residence document to be presented.

117 As regards, third, the consultation of biometric data recorded in the storage medium of identity cards, it should be noted that recital 19 of Regulation 2019/1157 lays down an order of priority for the use of methods of verifying the authenticity of the document and the identity of the holder, by providing that the Member States must 'primarily verify the facial image' and, where necessary, 'verify the fingerprints' in order to confirm without doubt the authenticity of the document and the identity of the holder.

118 As regards, fourth, the risk of unauthorised access to the data stored, Article 3(5) and (6) of Regulation 2019/1157 provides, in order to minimise that risk as far as possible, that fingerprints are to be stored on a 'highly secure storage medium', which has 'sufficient capacity and capability to guarantee the integrity, authenticity and confidentiality of the data'. Moreover, it follows from Article 3(10) of that regulation that 'when Member States store data for electronic services such as e-government and e-business in the identity cards, such national data shall be physically or logically separated', in particular, from fingerprints collected and stored on the basis of that regulation. Lastly, it is apparent from recitals 41 and 42 and Article 11(4) of that regulation that the Member States remain responsible for the proper processing of biometric data, including when they cooperate with external service providers.

(ii) The significance of the objectives pursued

119 As has been recalled at paragraph 86 of the present judgment, the inclusion of two fingerprints in the storage medium of identity cards is intended to combat the production of false identity cards and identity theft and to ensure the interoperability of identification document verification systems. On that basis, it is capable of contributing to the protection of the privacy of data subjects as well as, more broadly, to combating crime and terrorism.

120 In addition, such a measure makes it possible to meet the requirement for every EU citizen to have a means of identifying himself or herself which is reliable and, for the Member States, to ensure that the persons relying on rights conferred by EU law do indeed hold those rights. It thereby contributes, in particular, to facilitating the exercise by EU citizens of their right to free movement and residence, which is also a fundamental right guaranteed by Article 45 of the Charter. Accordingly, the objectives pursued by Regulation 2019/1157, in particular by the inclusion of two fingerprints in the storage medium of identity cards, are of particular importance not only for the European Union and the Member States, but also for EU citizens.

121 Furthermore, the legitimacy and significance of those objectives are in no way called into question by the fact, mentioned by the referring court, that paragraphs 24 to 26 of Opinion 7/2018 stated that only 38 870 cases of fraudulent identity cards were detected between 2013 and 2017 and that that figure had been falling for a number of years.

122 Even if it were considered that the number of fraudulent identity cards was low, the EU legislature was not required to wait for that number to increase in order to be able to adopt measures to prevent the risk of such cards being used, but could, particularly with a view to managing risks, anticipate such an increase, provided that the other conditions relating to compliance with the principle of proportionality were observed.

(iii) Balancing

123 In the light of the foregoing, it must be found that the limitation on the exercise of the rights guaranteed in Articles 7 and 8 of the Charter resulting from the inclusion of two fingerprints in the storage medium of identity cards does not appear to be – having regard to the nature of the data at issue, the nature of the processing operations and the manner in which they are carried out and the safeguards laid down – of a seriousness which is disproportionate when compared with the significance of the various objectives pursued by that measure. Accordingly, such a measure must be regarded as being based on a fair balance between, on the one hand, those objectives and, on the other, the fundamental rights involved.

124 Therefore, the limitation on the exercise of the rights guaranteed in Articles 7 and 8 of the Charter is not contrary to the principle of proportionality, with the result that the third ground is not such as to result in the invalidity of Regulation 2019/1157.

125 It follows from all the foregoing that Regulation 2019/1157 is invalid in so far as it was adopted on the basis of Article 21(2) TFEU.

IV. Maintaining the effects of Regulation 2019/1157 for a certain time

126 The effects of an act which has been declared invalid may be maintained on grounds of legal certainty, in particular where the immediate effects of the judgment finding such invalidity would give rise to serious negative consequences for the persons concerned (see, to that effect, judgment of 17 March 2016, *Parliament* v *Commission*, C-286/14, EU:C:2016:183, paragraph 67).

127 In the present case, Regulation 2019/1157 being invalid with immediate effect would be likely to have serious negative consequences for a significant number of EU citizens, in particular for their safety in the area of freedom, security and justice.

128 In those circumstances, the Court holds that the effects of Regulation 2019/1157 must be maintained until the entry into force, within a reasonable period which may not exceed two years from 1 January of the year following the date of delivery of the present judgment, of a new regulation based on Article 77(3) TFEU and intended to replace it.

V. Costs

129 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. **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 is invalid.**

2. The effects of Regulation 2019/1157 are to be maintained until the entry into force, within a reasonable period which may not exceed two years from 1 January of the year following the date of delivery of the present judgment, of a new regulation based on Article 77(3) TFEU and intended to replace it.

[Signatures]