Reports of Cases

JUDGMENT OF THE COURT (Fifth Chamber)

20 November 2025 *

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of their personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data – Directive (EU) 2016/680 – Article 4(1)(c) and (e) – Minimisation of data processing – Storage limitation of personal data – Article 10 – Collection and storage of biometric and genetic data – Strict necessity – Article 6(a) – Obligation to make a distinction between personal data of different categories of persons – National legislation which provides for the collection of biometric and genetic data of any person suspected or accused of having committed an intentional criminal offence – Article 5 – Appropriate time limits for erasure or for a periodic review of the need for the storage of those data – No maximum time limit for storage – Assessment of the need for the storage of biometric and genetic data by the police on the basis of internal rules – Article 8(2) – Lawfulness of the processing of those data – Concept of 'Member State law' – Whether national case-law may be classified as 'Member State law')

In Case C-57/23,

REQUEST for a preliminary ruling under Article 267 TFEU from the Nejvyšší správní soud (Supreme Administrative Court, Czech Republic), made by decision of 26 January 2023, received at the Court on 2 February 2023, in the proceedings

JH

v

Policejní prezidium,

THE COURT (Fifth Chamber),

composed of M.L. Arastey Sahún, President of the Chamber, J. Passer, E. Regan (Rapporteur), D. Gratsias and B. Smulders, Judges,

Advocate General: J. Richard de la Tour,

Registrar: I. Illéssy, Administrator,

having regard to the written procedure and further to the hearing on 28 November 2024,

* Language of the case: Czech.

after considering the observations submitted on behalf of:

– JH, by M. Mandzák, L. Nezpěvák and L. Trojan, advokáti,

– the Czech Government, by M. Smolek, O. Serdula, J. Vláčil, T. Suchá and L. Březinová, acting as Agents,

– Ireland, by M. Browne, Chief State Solicitor, A. Joyce and D. O'Reilly, acting as Agents, and by A. Mulligan, Barrister-at-Law,

– the Netherlands Government, by J. Langer, acting as Agent,

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

– the European Commission, by A. Bouchagiar, H. Kranenborg, P. Němečková and F. Wilman, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 27 February 2025,

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 4(1)(c) and (e), Article 6, Article 8(2) and Article 10 of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89).

2 The request has been made in proceedings between JH and the Policejní prezidium (Police Directorate, Czech Republic) ('the Czech Police Directorate') concerning, in particular, the collection of JH's biometric and genetic data in the context of criminal proceedings and the storage of those data by the Czech police.

Legal context

European Union law

3 Recitals 1, 2, 26, 33, 37 and 96 of Directive 2016/680 are worded as follows:

'(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union ("the Charter") and Article 16(1) of the [FEU Treaty] provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. …

…

(26) Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done 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, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned. … Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate and relevant for the purposes for which they are processed. … Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Member States should lay down appropriate safeguards for personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use.

…

(33) Where this Directive refers to Member State law, a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights. Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

…

(37) 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. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term ‘racial origin’ in this Directive does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. Such personal data should not

be processed, unless processing is subject to appropriate safeguards for the rights and freedoms of the data subject laid down by law and is allowed in cases authorised by law; where not already authorised by such a law, the processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject. Appropriate safeguards for the rights and freedoms of the data subject could include the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data. …

…

(96) Member States should be allowed a period of not more than two years from the date of entry into force of this Directive to transpose it. Processing already under way on that date should be brought into conformity with this Directive within the period of two years after which this Directive enters into force. However, where such processing complies with the Union law applicable prior to the date of entry into force of this Directive, the requirements of this Directive concerning the prior consultation of the supervisory authority should not apply to the processing operations already under way on that date given that those requirements, by their very nature, are to be met prior to the processing. …

…'

4 Article 1 of that directive, entitled 'Subject matter and objectives', provides, in paragraph 1 thereof:

'This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities 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.'

5 Article 2 of that directive, entitled 'Scope', provides in paragraph 1 thereof:

'This Directive applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1).'

6 Article 3 of Directive 2016/680, entitled 'Definitions', states:

'For the purposes of this Directive:

(1) "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(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;

…

(12) “genetic data” means personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(13) “biometric data” means 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;

…’

7 Article 4 of Directive 2016/680, entitled ‘Principles relating to processing of personal data’, provides, in paragraph 1 thereof:

‘Member States shall provide for personal data to be:

(a) processed lawfully and fairly;

(b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

…’

8 Article 5 of that directive, entitled ‘Time limits for storage and review’, is worded as follows:

‘Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.’

9 Article 6 of that directive, entitled ‘Distinction between different categories of data subject’, provides:

‘Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as:

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

(b) persons convicted of a criminal offence;

(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and

(d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).'

10 Article 8 of that directive, entitled 'Lawfulness of processing', provides:

'1. Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.

2. Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.'

11 Under Article 10 of Directive 2016/680, entitled 'Processing of special categories of personal data':

'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 allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

(a) where authorised by Union or Member State law;

(b) to protect the vital interests of the data subject or of another natural person; or

(c) where such processing relates to data which are manifestly made public by the data subject.'

12 In accordance with Article 63(1) of that directive, Member States were to adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with that directive. Further, Member States are required to apply those provisions from that date.

13 In accordance with Article 64 of that directive, the Directive entered into force on 5 May 2016.

Czech law

14 Paragraph 11 of the zákon č. 273/2008 Sb., o Policii České republiky (Law No 273/2008 on the Police of the Czech Republic), in the version applicable to the dispute in the main proceedings ('the Law on the Czech Police'), entitled 'Proportionality of acts', provides:

'Police officers and other persons employed by the police shall:

…

(c) act in such a way that any interference with the rights and freedoms of persons who are the subject of procedures carried out by them or of persons not involved, does not exceed what is necessary in order to attain the objective of that procedure.'

15 Paragraph 65 of the Law on the Czech Police provides as follows:

'(1) In performing their tasks, the police may, for the purpose of future identification of

(a) a person accused of having committed an intentional criminal offence or a person who has been informed that he or she is suspected of having committed such a criminal offence,

(b) a person serving a custodial sentence for committing an intentional criminal offence,

(c) a person subject to coercive medical measures or in preventive detention, or

(d) a wanted person who has been found and whose legal capacity is limited,

take fingerprints, identify physical features, perform measurements of the body, obtain visual, audio, and similar recordings, and take biological samples that make it possible to obtain information about his or her genetic make-up.

(2) If a procedure provided for in subparagraph 1 cannot be carried out because the person objects, the police officer shall be entitled to overrule that objection after unsuccessfully requesting the person to submit to it. The way in which the police officer overrules that objection must be proportionate to the strength of the objection. The police officer may not overrule a person's objection in the case of taking a blood sample or any other similar procedure violating his or her physical integrity.

(3) If a procedure provided for in subparagraph 1 cannot be carried out on the spot, the police officer shall be entitled to summon the person concerned in order to carry out that procedure. The police officer shall release the person once the procedure has been carried out.

(4) The police officer shall draw up a report on the procedures carried out.

(5) The police shall delete the personal data obtained pursuant to subparagraph 1 as soon as the processing of that data is no longer required for the prevention, investigation or detection of criminal activity or for the prosecution of criminal offences, or for ensuring the safety of the Czech Republic, public order or domestic security.'

16 Paragraph 79 of that law, entitled 'Basic provisions concerning the processing of personal data in the context of carrying out certain police tasks', provides:

'(1) Subparagraphs 2 to 6 and Paragraphs 79a to 88 shall apply to the processing of personal data for the prevention, investigation, detection or prosecution of criminal offences, for ensuring the safety of the Czech Republic, public order or domestic security, including for the purposes of tracing people and items.

(2) The police may process personal data where necessary in order to attain the objectives mentioned in subparagraph 1. The police may also process personal data in order to protect

important interests of a data subject that are linked to the objectives mentioned in subparagraph 1.

…’

17 Paragraph 82 of that law, entitled ‘Assessment of the need to carry out processing of personal data’ is worded as follows:

‘(1) The police shall verify at least once every three years that personal data processed for the purposes mentioned in Paragraph 79(1) are still necessary for the performance of its tasks in that area.

(2) For the purposes of the verification referred to in subparagraph 1, the police are authorised to require production of a criminal record certificate.

(3) The law enforcement and judicial authorities, the Ministerstvo spravedlnosti (Ministry of Justice, Czech Republic), the Ustavní soud (Constitutional Court, Czech Republic) and the Kancelář prezidenta republiky (Office of the President of the Republic, Czech Republic) shall keep the police continuously informed, within the limits of their competences, for the purposes of the verification referred to in subparagraph 1, of their final decisions, of the statute of limitations for criminal proceedings, of the enforcement of a sentence or of decisions of the President of the Republic relating to criminal proceedings, to sentences or to an amnesty or pardon granted.’

The dispute in the main proceedings and the questions referred for a preliminary ruling

18 By decision of 11 December 2015, the Unit for the Detection of Corruption and Financial Crime of the Criminal Investigation Police Department in the Plzeň section (Czech Republic), which is the unit of the Czech police with national competence, brought criminal proceedings against JH for the offence of breach of duty in the administration of the property of another.

19 On 13 January 2016, the Czech police first questioned JH in the context of criminal proceedings and ordered and carried out, despite JH’s objections, the following identification procedures: the taking of fingerprints from JH, the taking of a buccal smear from him, on the basis of which the police created a genetic profile, the taking of photographs of JH and the drawing up of a description of JH. The police subsequently recorded that information in the relevant databases.

20 By judgment of 15 March 2017, JH was convicted by the Městský soud v Praze (Prague City Court, Czech Republic) of the offence of breach of duty in the administration of the property of another by complicity and the serious offence of misconduct in public office. That court sentenced JH to a suspended custodial sentence of three years, a prohibition on performing management functions in the public service, including the management of moveable and immoveable assets for a period of four years, and ordered JH to pay compensation, within the limits of his means, for the damage caused.

21 On 8 March 2016, JH brought an action before the Městský soud v Praze (Prague City Court) seeking a declaration that the identification procedures carried out under Paragraph 65 of the Law on the Czech Police, the storage of the information and samples obtained and the creation of an entry in the databases of the Czech police in that connection constituted an unlawful interference with his fundamental right to respect for private life.

22 In view of the fact that, in the context of another pending case, the Městský soud v Praze (Prague City Court) had by then made a referral to the Ústavní soud (Constitutional Court, Czech Republic) for an assessment of the constitutionality of Paragraph 65 of the Law on the Czech Police, the Městský soud v Praze (Prague City Court) suspended its consideration of the action brought by JH.

23 By decision of 22 March 2022, the Ústavní soud (Constitutional Court) dismissed the referral made by the Městský soud v Praze (Prague City Court) seeking a declaration that Paragraph 65 of the Law on the Czech Police is unconstitutional. Further to that decision, the Městský soud v Praze (Prague City Court) resumed its consideration of the action brought by JH.

24 By judgment of 23 June 2022, the Městský soud v Praze (Prague City Court) upheld JH's action, finding that the procedures carried out by the Czech police on 13 January 2016 were unlawful. Accordingly, that court ordered the Czech police to erase all the personal data resulting from those procedures from its databases.

25 In that judgment, that court noted that the collection of genetic material represented a considerable interference with JH's fundamental right to respect for private life, which is protected in particular under Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 ('the ECHR'), and Article 10(3) of the Listina základních práv a svobod (Charter of Fundamental Rights and Freedoms of the Czech Republic). However, Paragraph 65 of the Law on the Czech Police does not provide sufficient guidance for assessing whether that interference is proportionate. The only verification required under Paragraph 65 is that the Czech police verify the 'intentional' nature of the offence committed before such a collection is carried out.

26 Moreover, that court noted that JH was prosecuted for a less serious offence, that is to say a criminal offence of lesser gravity; that his custodial sentence was suspended, which confirmed the lesser gravity of the alleged facts; that he had no previous criminal convictions; that it was unlikely that he would reoffend; and that it was not certain that the offences committed belonged to a category of offences in which perpetrators might commit in the future a criminal offence which the personal data stored on the databases could be used to identify. That court infers from this that the identification procedures carried out by the Czech police and with which the main proceedings are concerned did not satisfy the proportionality requirement.

27 The Czech Police Directorate lodged an appeal on a point of law against that judgment before the Nejvyšší správní soud (Supreme Administrative Court, Czech Republic), which is the referring court.

28 In support of its appeal, the Czech Police Directorate states that the purpose of the processing of personal data is clearly stated in Paragraph 65 of the Law on the Czech Police. It also states that, in this case, the competent services of the Czech police assessed the proportionality of the collection and storage of JH's personal data, taking into account the recidivism factor, the potential escalation of the actions and the fact that JH had committed several minor offences in the past.

29 In response, JH maintains, inter alia, that the Czech police carried out identification procedures without first examining the proportionality of the interference in question. JH also criticises the lack of publication of the Czech police's guidelines pertaining to the performance of identification procedures.

30 The referring court states that, in accordance with its recent case-law, merely respecting the formal requirements laid down in Paragraph 65(1) of the Law on the Czech Police, in particular as regards the classification of the criminal offence as 'intentional', is not sufficient to enable the collection and storage of the personal data referred to in that paragraph to be regarded as lawful. The police are therefore required to assess the proportionality of the collection in each specific case, taking into account, inter alia, the criminal history, the personality, and the conduct of the person concerned, the seriousness of the criminal offence in respect of which that person has been summoned in order to carry out identification procedures and, in the context of a request for erasure *ex post*, the time that has elapsed since the criminal offence concerned was committed.

31 By applying that case-law, the national courts would find identification procedures such as the collection of biometric and genetic data to be unlawful, in particular in the case of offences which do not involve any violence and which are committed by individuals who have no previous convictions.

32 It is in that context that the referring court asks whether the legal regime established by Paragraph 65 of the Law on the Czech Police is compatible with Directive 2016/680.

33 In the first place, that court asks whether the requirements laid down in Directive 2016/680 preclude the indiscriminate collection of biometric and genetic data in respect of any person suspected of having committed an intentional criminal offence.

34 First, it is apparent from the case-law of the European Court of Human Rights concerning the fundamental right to respect for private life, guaranteed by Article 8 ECHR, that the Contracting Parties are required to make a distinction between criminal offences in respect of which samples of deoxyribonucleic acid (DNA) are collected on the basis of the seriousness of those offences for society. The Contracting Parties cannot treat in the same way, on the one hand, the perpetrators of serious criminal offences, such as those committed with violence, in respect of which the collection and retention of DNA samples would be legitimate and, on the other hand, the perpetrators of less serious criminal offences.

35 Second, the requirements stemming from the principle of proportionality, such as, in particular, those laid down, within the scope of Directive 2016/680, in the form of the principle of minimisation of data processing and the obligation to make distinctions between different categories of data subjects, provided for in Article 4(1)(c) and Article 6 of that directive respectively, raise questions as regards whether it is sufficient to make distinctions *in abstracto* at the legislative level in accordance, in particular, with the gravity of the offences contemplated or whether it is necessary to assess *in concreto* the proportionality of the collection in each specific case.

36 In the second place, the referring court asks whether the requirements laid down in Directive 2016/680 preclude the storage of biometric and genetic data without a limitation in time being expressly provided for in that regard. Indeed, the national legislation applicable does not set a maximum limit for the period of storage of the identification data. However, the referring court's interpretation of the case-law of the European Court of Human Rights is that it does require a maximum limit to be established.

37 In the third place, the referring court asks whether the case-law of the Czech administrative courts may be classified as 'Member State law' within the meaning of Article 8 of Directive 2016/680, which lays down conditions for the lawful processing of personal data.

38 Paragraph 65 of the Law on the Czech Police does not specify either the specific conditions for storage and the type of information which may be extracted from the sample taken, or the conditions for storage and erasure of biometric and genetic data with the result that that article cannot satisfy, on its own, the requirements set out in Article 8(2) of Directive 2016/680, read in conjunction with Article 10 of that directive.

39 It is true that Paragraph 65 is supplemented by guidelines set by the President of the police which implement that paragraph, but because those guidelines are neither legislative texts nor published, the status of 'Member State law', within the meaning of Article 8(2) of Directive 2016/680, cannot, in any case, be recognised to those guidelines.

40 The question therefore arises as to whether Member State law can be regarded as providing sufficient substantive and procedural guarantees for the processing of sensitive data, within the meaning of Article 10 of that directive, such as biometric and genetic data, where those guarantees are established by case-law.

41 In those circumstances, the Nejvyšší správní soud (Supreme Administrative Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) What degree of distinction between individual data subjects is required by Article 4(1)(c) or Article 6 [of Directive 2016/680] in conjunction with Article 10 of [that directive]? Is it compliant with the obligation to minimise personal data processing, and with the obligation to distinguish between various categories of data subjects, for national law to permit the collection of genetic data in respect of all persons suspected or accused of having committed an intentional criminal offence?

(2) Is it in accordance with Article 4(1)(e) of Directive 2016/680 if the necessity of continued retention of a DNA profile is assessed, with a reference to the general prevention, investigation, and detection of criminal activity, by police authorities on the basis of their internal regulations, which frequently means in practice that sensitive personal data is retained for an unspecified period without a maximum limit for the duration of the retention of that personal data being set? If not, by what criteria should the proportionality of the period of the retention of the personal data collected and retained for that purpose be assessed?

(3) In the case of particularly sensitive personal data falling under Article 10 of Directive 2016/680, what is the minimal scope of the substantive or procedural conditions for obtaining, retaining, and deleting such data that must be regulated by a "provision of general application" in the law of a Member State? Can judicial case-law qualify as "Member State law" within the meaning of Article 8(2) in conjunction with Article 10 of Directive 2016/680?'

The questions referred for a preliminary ruling

The third question

42 By its third question, which it is appropriate to examine first, the referring court asks, in essence, whether Articles 8 and 10 of Directive 2016/680 must be interpreted as meaning that, as regards the collection, storage and erasure of biometric and genetic data, the concept of 'Member State law', within the meaning of those provisions, must be understood as referring only to a provision

of general application laying down the minimum conditions for collection, storage and erasure of those data or whether the case-law of the national courts which specifies those conditions can also fall within that concept.

43 In that regard, it must be borne in mind that, in accordance with Article 3(2) of Directive 2016/680, read in the light of Article 3(12) and (13) thereof, the collection, storage and erasure of biometric and genetic data constitute the processing of personal data within the meaning of that directive.

44 Article 4 of Directive 2016/680 sets out various principles to which that processing is subject, which convey, as is apparent from recitals 1 and 2 of that directive, the manner in which, within the limits provided for in Article 52 of the Charter, the EU legislature intended to give concrete expression, as regards that processing, to the fundamental right of natural persons to the protection of their personal data, enshrined in Article 8 of the Charter, which itself is closely connected to the right to respect for private life, enshrined in Article 7 of the Charter, by taking into account the specific nature of the activities of prevention and detection of criminal offences, investigations and prosecution of criminal offences or the execution of criminal penalties.

45 Among those principles, Article 4(1)(a) of Directive 2016/680 provides that any personal data must be processed lawfully and fairly.

46 Article 8(1) of Directive 2016/680 states, in that regard, that Member States are to provide for the processing of personal data which falls within the scope of that directive to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) of that directive and that it is based on EU or Member State law.

47 Moreover, under Article 8(2) of that directive, the processing of such data is possible only where Member State law regulating that processing specifies at least the objectives of that processing, the personal data to be processed and the purposes of that processing.

48 As regards certain categories of personal data, such as biometric or genetic data, Article 10 of Directive 2016/680 seeks to ensure enhanced protection by establishing strengthened conditions for the lawful processing of such data (see, to that effect, judgments of 30 January 2024, *Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR – Sofia*, C-118/22, EU:C:2024:97, paragraph 48, and of 4 October 2024, *Bezirkshauptmannschaft Landeck (Attempt to access personal data stored on a mobile telephone)*, C-548/21, EU:C:2024:830, paragraph 107). Those categories of data are, as stated in recital 37 of that directive, by their nature, particularly sensitive in relation to fundamental rights and freedoms as the context of their processing could create significant risks to the fundamental rights and freedoms of the data subjects.

49 Thus, in accordance with Article 10 of Directive 2016/680, any processing concerning personal data which falls into one of the categories exhaustively set out in that article ('sensitive personal data') must be authorised by EU law or by Member State law.

50 It follows that Articles 8 and 10 of Directive 2016/680 seek to define the scope of certain principles set out in Article 4 of that directive, which give concrete expression, in the area covered by that directive, inter alia, to the fundamental right of natural persons to the protection of their personal data recognised in Article 8 of the Charter.

51 Consequently, the concept of 'Member State law' used in Articles 8 and 10 must be understood as giving effect, in the area covered by Directive 2016/680, to the condition set out in Article 8(2) of the Charter, under which any processing of personal data that is not based on the consent of the person concerned must be carried out on some other legitimate basis laid down by law, a condition which itself only reflects the requirement of Article 52 of the Charter that any limitation on the exercise of the fundamental rights recognised by the Charter must be provided for by law. That concept thus relates to the validity of the use of national law as the legal basis for the processing of personal data.

52 First, as the Advocate General stated in point 82 of his Opinion, the Court, taking into account the settled case-law of the European Court of Human Rights, has held that the term 'law', used in Article 8(2) of the Charter, in the expression 'laid down by law', must be understood in its substantive sense and not its formal sense (judgment of 16 November 2023, *Roos and Others* v *Parliament*, C-458/22 P, not published, EU:C:2023:871, paragraph 61). Second, according to the case-law of the European Court of Human Rights, that sense of the term 'law' in the expression 'in accordance with the law', referred to in Article 8(2) ECHR, implies that that term refers to the provision in force as the competent courts have interpreted it (see, to that effect, ECtHR, 23 January 2025, *H. W. v. France*, CE:ECHR:2025:0123JUD 001380521, paragraph 65).

53 Moreover, as follows from the case-law of the Court, although the requirement that any limitation on the exercise of fundamental rights recognised by the Charter must be provided for by law implies that the act which permits the interference with those rights defines the scope of that limitation, that requirement does not however preclude, on the one hand, 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 competent court may, where appropriate, specify, by means of interpretation, the actual scope of that limitation in the light of the very wording of that act which allows the interference as well as the general scheme of that act and the objectives pursued by that limitation (see, by analogy, judgment of 21 June 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, paragraph 114).

54 Accordingly, the concept of 'Member State law', within the meaning of Articles 8 and 10 of Directive 2016/680, read in the light of Article 8(2) of the Charter, must be understood as being capable of referring to a provision expressly envisaging the carrying out of processing of personal data falling within the scope of that directive, as interpreted by the case-law of the national courts.

55 In any event, as stated in paragraph 47 above, Article 8(2) of Directive 2016/680 provides that the processing of personal data falling within the scope of that directive is possible only where Member State law regulating that processing specifies at least the objectives of it, the personal data to be processed and the purposes of the processing.

56 In that regard, it must be noted, first, that the reference to Member State 'law' 'regulating' the processing at issue implies that the objectives of the processing, the personal data to be processed and the purposes of the processing are, at least in principle, laid down in a provision of general application. Second, Article 8(2) seeks to ensure, as follows expressly from recital 33 of that directive, that Member State law regulating the processing is clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court and the European Court of Human Rights.

57 According to the case-law of the European Court of Human Rights, any measure which forms the legal basis for the processing of personal data must have certain qualities, namely, in essence, that measure must comply, first, with higher-ranking law, next, be accessible and, lastly, sufficiently foreseeable, that is to say to a degree that is reasonable in the circumstances, to enable the individuals concerned to regulate their conduct, which requires that measure to define the scope and the manner for exercising the powers conferred on the competent authorities with sufficient clarity (see, to that effect, inter alia, ECtHR, 26 April 1979, *the Sunday Times v. the United Kingdom*, CE:ECHR:1979:0426JUD00065387, §§ 25 and 52; ECtHR, 1 July 2008, *Liberty and Others v. the United Kingdom*, CE:ECHR:2008:0701JUD005824300, §§ 62 and 63; and ECtHR, 4 December 2008, *S and Marper v. the United Kingdom*, CE:ECHR:2008:1204JUD003056204, § 95).

58 Similarly, according to the case-law of the Court, to meet the requirement, set out in Article 52 of the Charter, to be provided for by law, legislation involving an interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards so that the persons whose personal data are concerned have sufficient guarantees to protect effectively their data against the risk of abuse and against any unlawful access and use of those data (see judgments of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 54, and of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 91).

59 In view of the fact that Article 8(2) of Directive 2016/680 seeks to ensure compliance with the requirements set out in paragraphs 56 and 57 above, it follows that the objectives pursued, the personal data concerned and the purposes of the processing covered by that directive must be apparent, with sufficient clarity and precision, from the legislative provision regulating that processing itself, so that that processing can be regarded as meeting the requirements to be provided for by law, within the meaning of the case-law of the European Court of Human Rights and Article 52 of the Charter.

60 Having regard to all the foregoing, the answer to the third question is that Articles 8 and 10 of Directive 2016/680 must be interpreted as meaning that, as regards the collection, storage and erasure of biometric and genetic data, the concept of 'Member State law', within the meaning of those articles, must be understood as referring to a provision of general application laying down the minimum conditions for collection, storage and erasure of those data, as interpreted by the case-law of the national courts, in so far as that case-law is accessible and sufficiently foreseeable.

The first question

Admissibility

61 In its written observations, the European Commission submits that the first question is inadmissible on the ground that the collection of JH's biometric and genetic data by the Czech police took place on 13 January 2016, that is to say, before the entry into force of Directive 2016/680 on 5 May 2016, and before the expiry of the transposition period of that directive, set by Article 63(1) thereof to occur on 6 May 2018.

62 In that regard, it must be borne in mind that the Court may refuse to rule on a question referred by a national court for a preliminary ruling only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose,

where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (judgment of 20 March 2025, *Anib and Others*, C-728/22 to C-730/22, EU:C:2025:200, paragraph 48).

63 In the present case, Article 64 of Directive 2016/680 provides that that directive is to enter into force on 5 May 2016, while Article 63 of that directive states that the Member States are to adopt and publish the laws, regulations and administrative provisions necessary to comply with that directive by 6 May 2018.

64 However, it is apparent from the documents before the Court that the personal data concerning JH, taken from his genetic and biometric samples collected on 13 January 2016, continued to be stored on the databases of the Czech police and therefore to be processed after 6 May 2018.

65 Subject to the situations provided for in Article 4(2) of Directive 2016/680, under Article 4(1)(b) of that directive personal data cannot be processed where their collection was not justified by legitimate purposes.

66 Consequently, as the Advocate General pointed out in point 34 of his Opinion, the personal data covered by Directive 2016/680 that were collected lawfully before the date of the entry into force of that directive, but which would have been collected in breach of the principles laid down by that directive if they had been collected after the date that that directive was transposed or, failing that, after the deadline for the transposition of that directive, namely 6 May 2018, cannot be stored after the date that that directive was transposed or, failing that, after the deadline for its transposition.

67 Thus, in the present case, it is not obvious that the first question is necessarily devoid of any relation to the actual facts of the main action or its purpose or that the problem raised is hypothetical, on the ground, relied on by the Commission, that it concerns biometric and genetic data collected before the entry into force of Directive 2016/680.

68 Furthermore, in so far as the Court has before it the factual and legal material necessary to give a useful answer to the first question submitted to it, that question must be held to be admissible.

Substance

69 By its first question, the referring court asks, in essence, whether Article 6 or Article 4(1)(c) of Directive 2016/680, read in conjunction with Article 10 of that directive, must be interpreted as precluding national legislation which permits the indiscriminate collection of biometric and genetic data of any person accused or suspected of having committed an intentional criminal offence.

70 In that regard, so far as concerns, in the first place, Article 6 of Directive 2016/680, it must be borne in mind that that article requires Member States to provide for the controller, 'where applicable and as far as possible', to make a clear distinction between the personal data of different categories of data subjects, such as those referred to in Article 6(a) to (d) of that directive, that is to say, respectively; persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence; persons convicted of a criminal offence; victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and, lastly, other parties to a criminal offence, such as persons who might be called on to testify in

investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in Article 6(a) and (b) of Directive 2016/680.

71 In accordance with that provision, Member States must therefore ensure that the controller, 'where applicable and as far as possible', makes a clear distinction between the data of different categories of data subjects in such a way that they are not subject without distinction to the same degree of interference with their fundamental right to protection of their personal data, regardless of the category to which they belong, since those categories must be established essentially in accordance with the criminal status of the person concerned.

72 As is clear from the phrase 'where applicable and as far as possible', which Article 6 of Directive 2016/680 contains, the obligation to make a distinction between certain categories of person which that article imposes on the Member States is not absolute but depends, inter alia, on whether, in each individual case, a clear distinction between those categories of persons may be made (see, to that effect, judgment of 26 January 2023, *Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)*, C-205/21, EU:C:2023:49, paragraph 84) and the purposes of the processing.

73 In the present case, the Czech Government submits that the reference made, by the referring court, to the category of suspected persons must be understood as referring to persons who, in the context of expedited preliminary proceedings, have been informed that they are suspects, which, in the national legislation at issue in the main proceedings, would necessitate, as for accused persons, that sufficient material to demonstrate that those persons have committed an offence has been gathered.

74 Should that be the case, which is for the referring court to verify, those two categories of person could both be regarded as falling within the category referred to in Article 6(a) of Directive 2016/680 for the purposes of any given processing, in so far as the objectives pursued by the processing concerned do not require a distinction to be made between those two categories.

75 Consequently, Article 6 of Directive 2016/680 must be interpreted as not precluding national legislation which allows for the indiscriminate collection of biometric and genetic data of persons falling within the category of persons 'accused of having committed an intentional criminal offence' and persons falling within the category of persons 'suspected of having committed such an offence' within the meaning of national law, where the purposes of that collection do not require a distinction to be made between those two categories of persons whose data may be collected on the basis of that regulation.

76 As regards, in the second place, Article 4(1)(c) of Directive 2016/680, read in conjunction with Article 10 of that directive, the first of those articles provides that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are processed. That latter requirement thus calls for the Member States to comply with the principle of minimisation of data processing as regards the objective and purpose pursued by the processing concerned.

77 Article 10 of that directive provides that, so far as concerns sensitive personal data, including biometric and genetic data, the processing must satisfy, in addition to the condition of falling within one of the three cases listed exhaustively in points (a) to (c), two further conditions, namely, first, that there must be appropriate safeguards for the rights and freedoms of the data subject and, second, that the envisaged processing must be strictly necessary.

78 As regards that last condition, first of all, that condition implies that the necessity is to be assessed with particular rigour in respect of the purposes pursued by the processing in question and that, accordingly, such processing can be regarded as necessary solely in a limited number of cases (see, to that effect, judgment of 26 January 2023, *Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)*, C-205/21, EU:C:2023:49, paragraph 118).

79 Thus, the purposes of processing biometric and genetic personal data cannot be indicated in terms that are too general, but have to be defined sufficiently precisely and specifically to enable assessment of whether that processing is 'strictly necessary' (judgment of 26 January 2023, *Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)*, C-205/21, EU:C:2023:49, paragraph 124).

80 In that regard, while Directive 2016/680 does not define the concept of 'purposes of the processing', it may be noted that Article 8(2) of that directive expressly distinguishes that notion from 'objectives of processing'. Article 4(1)(b) of that directive provides that the purposes pursued by the processing of personal data must be, inter alia, specified and explicit and that those data cannot be processed in a manner that is incompatible with those purposes, while Article 4(1)(c) of that directive provides that it is in relation to those purposes that the adequate, relevant and not excessive nature of the processing to which the personal data is subject is to be assessed.

81 Accordingly, it can be inferred that the concept of 'objectives of processing' within the meaning of Article 8(2) of Directive 2016/680, refers to the more general objectives, stated in Article 1(1) of Directive 2016/680, that the processing must pursue to be within the scope of that directive, whereas the concept of 'purposes of the processing' within the meaning, inter alia, of Article 8(2) of that directive, must be understood as referring to the specific and real aims pursued by the processing of personal data in the light of the task of the controller, such as a specific task connected with the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties.

82 Next, given that, as is apparent from recital 26 of Directive 2016/680, read in the light of the proportionality principle, for non-sensitive personal data, the condition of necessity, for the purposes of that directive, is satisfied where the purpose of the processing concerned cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of data subjects, it must therefore be concluded that the condition that the processing of sensitive personal data must be strictly necessary, requires the controller, for its part, to ensure that the purpose pursued by the processing in question cannot be achieved just as effectively by having recourse to categories of data other than those listed in Article 10 of Directive 2016/680 (see, to that effect, judgment of 26 January 2023, *Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)*, C-205/21, EU:C:2023:49, paragraph 126).

83 Furthermore, having regard to the significant risks that the processing of sensitive personal data poses to the rights and freedoms of data subjects, in particular in the context of the tasks of the competent authorities for the purposes set out in Article 1(1) of Directive 2016/680, the 'strictly

necessary' condition requires account to be taken of the specific importance of the purpose of the processing concerned. Such importance may be assessed on the basis of the very nature of the purpose pursued – in particular of the fact that the processing serves a specific objective connected with the prevention of criminal offences or threats to public security displaying a certain degree of seriousness, the punishment of such offences or protection against such threats – and in the light of the specific circumstances in which that processing is carried out (see, to that effect, judgment of 26 January 2023, *Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)*, C-205/21, EU:C:2023:49, paragraph 127).

84 In any event, as regards the collection of biometric and genetic data of persons accused or suspected of having committed an intentional criminal offence for the purposes of future identification and comparison of those persons, the strictly necessary nature of that collection must take into account all of the relevant factors, such as, in particular, the nature and gravity of the presumed offence of which they are accused, the particular circumstances of that offence, any link between that offence and other procedures in progress, and the criminal record or individual profile of the persons in question (see, to that effect, judgment of 26 January 2023, *Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)*, C-205/21, EU:C:2023:49, paragraph 132).

85 Lastly, the 'strictly necessary' condition entails particularly strict checking as to whether the principle of minimisation of processing of the data concerned, set out in Article 4(1)(c) of that directive, is observed (see judgment of 26 January 2023, *Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)*, C-205/21, EU:C:2023:49, paragraph 125).

86 In particular, as regards the storage and use of data extracted from the DNA of persons for the purposes of identification or comparison, such a principle implies that, in order to assess whether such processing is strictly necessary, due consideration should be given to the possibility of relying exclusively on polymorphisms present in non-coding areas of DNA, namely areas that are not known to provide any information about those persons' ethnicity or genetic diseases.

87 Consequently, while a Member State may comply with Directive 2016/680 either by delegating to the competent authorities the responsibility of ensuring, in each individual case, that for all processing of sensitive personal data the condition that that processing is strictly necessary is satisfied, or by laying down in legislation the assessment criteria that the authorities must apply subsequently in a non-discriminatory manner, the fact remains that, in that second situation, those criteria must be capable of meeting the requirements that arise from that same condition, as set out in paragraphs 77 to 83 above.

88 Thus, in the judgment of 26 January 2023, *Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)* (C-205/21, EU:C:2023:49, paragraph 135), the Court held that national legislation which provides for the systematic collection of biometric and genetic data of any person accused of an intentional offence subject to public prosecution in order for them to be entered in a record, without laying down an obligation on the competent authority to verify and demonstrate that, first, their collection is strictly necessary for achieving the specific objectives pursued and, second, that those objectives cannot be achieved by measures constituting a less serious interference with the rights and freedoms of the person concerned, is contrary to the 'strictly necessary' condition.

89 That being so, while the collection provided for by the legislation at issue in the case which gave rise to that judgment applied mandatorily to all persons accused of intentional offences subject to public prosecution, the first question concerns legislation which merely gives police the right to take samples of biometric and genetic data in respect of persons accused or suspected of having committed an intentional offence.

90 The fact that legislation confers such a right on the police does not mean that the law of the Member State concerned allows for that collection to be systematic or that it can done in breach, inter alia, of the principle of minimisation of data processing, set out in Article 4(1)(c) of Directive 2016/680, or of the condition that the processing concerned is strictly necessary, laid down in Article 10 of that directive, in so far as that law, which includes the case-law of the national courts, defines in an appropriate and sufficiently precise manner the purposes pursued by such processing of biometric and genetic data, that is to say, the specific and real aims pursued by the processing of personal data as regards the task for which the controller is responsible, and that that right is carried out in accordance with the requirements set out in paragraphs 77 to 83 above.

91 Thus, it is apparent from the information before the Court that, in the present case, the national case-law sets out certain requirements which seek to ensure that that principle is adhered to, such as the obligation for the police, before taking a DNA sample, to take into account, inter alia, the criminal history of the perpetrator of the offence committed, the seriousness of that offence in relation to the type of offence in question and the specific circumstances of that offence which require a sample to be taken, as well as the personality of the perpetrator.

92 In that situation, it is for the national courts to determine, in each case, whether the police have carried out the collection in breach of the principles governing the processing of personal data, laid down in Article 4 of Directive 2016/680 and of the specific requirements applicable to the processing of sensitive personal data, laid down in Article 10 of that directive, as interpreted in the light of Articles 7 and 8 of the Charter.

93 In that regard, it must again be stated that the mere fact that the offence allegedly committed by a person is economic in nature and that the collection of that person's biometric and genetic data takes place before he or she has been convicted by final judgment is not sufficient to exclude that collection from being regarded as strictly necessary, since, in the light of the objectives pursued, that collection, including as regards the type of data concerned, may prove strictly necessary, inter alia to make it possible to establish whether, because of that person's possible involvement in a criminal organisation, he or she may have been involved in other offences for which that type of data could be relevant or, where there is a risk that that person will flee, to enable that person to be identified.

94 In the light of all of the above, the answer to the first question is that Article 6 and Article 4(1)(c) of Directive 2016/680, read in conjunction with Article 10 of that directive, must be interpreted as not precluding national legislation which permits the indiscriminate collection of biometric and genetic data of any person accused or suspected of having committed an intentional criminal offence, in so far as, first, the purposes of that collection do not require a distinction to be made between those two categories of persons and, second, the controllers are required, in accordance with national law, including the case-law of the national courts, to comply with all of the principles and specific requirements laid down in Articles 4 and 10 of that directive.

The second question

95 It must be noted, at the outset, that where, in the formulation of the second question, the referring court mentions national legislation which has the effect that the personal data concerned are, in most cases, stored for an 'unspecified period', it is apparent from the documents before the Court of Justice that by 'unspecified period', that court intends, in reality, to refer to the fact that no maximum period of storage is specified and not that such storage would be unlimited in time.

96 Consequently, the Court of Justice understands that by its second question, the referring court asks, in essence, whether Article 4(1)(e) of Directive 2016/680 must be interpreted as precluding national legislation under which the need for continued storage of biometric and genetic data is assessed by the police on the basis of internal rules, without that legislation laying down a maximum period for storage.

97 In that regard, Article 4(1)(e) of Directive 2016/680 states that Member States are to provide for personal data to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed.

98 As regards, in the first place, the fact that the national legislation concerned does not provide for a maximum period for storage, it must be borne in mind that, in accordance with the requirements of Article 4(1)(e) of Directive 2016/680, Article 5 of that directive requires Member States to provide for appropriate time limits to be established for erasure of personal data or for a periodic review of the need for the storage of those data and for procedural measures to ensure that those time limits are observed.

99 By contrast, Article 5 of that directive leaves it to the Member States to determine those time limits, in so far as they are 'appropriate', and to decide whether those time limits concern the erasure of those data or the periodic review of the need to store them.

100 Article 4(1)(e) and Article 5 of Directive 2016/680 must be read in conjunction, inter alia, with Article 10 of that directive, with the result that the storage of the biometric or genetic data must be strictly necessary and there must be appropriate safeguards for the rights and freedoms of the data subject.

101 However, where a Member State determines appropriate time limits for a periodic review of the need to store personal data and, at the time of that review, it is necessary to assess whether extending that storage is strictly necessary, the Member State law concerned must be regarded as meeting those requirements. Thus, even where the data stored are sensitive personal data, such a Member State is not required to define the absolute time limits for the storage of those data, beyond which those data must be automatically erased (see, to that effect, judgment of 30 January 2024, *Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR – Sofia*, C-118/22, EU:C:2024:97, paragraph 52).

102 By contrast, the appropriate nature of those time limits for a periodic review requires that, first, in accordance with Article 4(1)(c) and (e) of Directive 2016/680, read in the light of Article 52(1) of the Charter, those personal data that have been stored until then must be erased under the conditions laid down in Article 16(2) and (3) of that directive where, at the time that one of the reviews is carried out, the storage of those data no longer appears to be strictly necessary and,

therefore, proves excessive as regards the purposes pursued (see, to that effect, judgment of 30 January 2024, *Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR – Sofia*, C-118/22, EU:C:2024:97, paragraphs 45, 48 and 50 and the case-law cited).

103 Second, having regard to the requirements, under Article 4(1)(c) of Directive 2016/680, that all personal data are to be adequate, relevant and not excessive in relation to the purposes for which they have been processed, the fact that that provision and Article 8 of that directive must be read in the light of the requirements that arise under Article 52 of the Charter and the obligation, under Article 6 of that directive, for the controller, where applicable, to make a clear distinction between personal data of different categories of data subjects, those time limits for review cannot be regarded as being appropriate where the changes to the criminal status of the data subject, considered to be relevant in respect of the purpose pursued by that storage, does not result in an obligation, on the controller, to re-examine within a reasonable period of time the need to store the data of that person.

104 As regards, in the second place, the fact that the need to continue storage of the biometric and genetic data is assessed by the police on the basis of internal rules, that fact is not in itself contrary to Article 8(2) of Directive 2016/680, in so far as those internal rules require the police to ensure that the condition that the storage of those data is strictly necessary is satisfied and that the discretion of the police is governed by a sufficient framework under national law, including the case-law of the national courts.

105 Where the fact that the rules are internal, and therefore are not accessible to all persons whose personal data may be processed, has the consequence that those rules cannot be relied on by the competent authorities to demonstrate that they comply with the requirements that are imposed on them, that fact does not however have the consequence of automatically making the processing of personal data decided upon in accordance with those rules unlawful, but implies that, where applicable, in case of an action against the decision to proceed with one of those cases of processing, the police are to establish before the competent court, independently of those internal rules, that the 'strictly necessary' condition has been duly satisfied.

106 In the present case, first, according to the Czech Government, it is apparent, inter alia, from Paragraph 65(5) of the Law on the Czech Police, which is for the referring court to verify, that the DNA profiles of the persons suspected or accused of having committed an intentional criminal offence must be erased where their storage is no longer necessary as regards the objectives pursued, that is to say, where those persons are no longer accused or suspected and that those persons are not accused or suspected in any other criminal proceedings or that they have not previously committed other serious crimes or other offences.

107 In that regard, it must be borne in mind, however, that the storage of biometric and genetic data can be regarded as meeting the requirement that it is to be allowed only 'where strictly necessary', within the meaning of Article 10 of Directive 2016/680, solely where it takes into consideration not only the data subject's possible connection with other ongoing proceedings or the background or profile of that person, but also the nature and seriousness of the offence which led to the final criminal conviction, or other circumstances such as the particular context in which that offence was committed (see, to that effect, judgment of 30 January 2024, *Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR – Sofia*, C-118/22, EU:C:2024:97, paragraph 67).

108 Second, although Czech law does not provide for a maximum period for storage of personal data collected under Paragraph 65(1) of the Law on the Czech Police, Paragraph 82(1) of that law nevertheless imposes an obligation on the police to review at least once every three years that the storage of those data is still necessary for the performance of their tasks.

109 Therefore, it is for the referring court to establish whether, having regard to the purposes pursued by the storage of the biometric and genetic data concerned, such a time limit of three years may be regarded as appropriate, it being specified however that, in the contrary case, the erasure of those data would not be required if it were established that their continued storage remained, in any event, strictly necessary.

110 Having regard to all of the foregoing, the answer to the second question is that Article 4(1)(e) of Directive 2016/680 must be interpreted as not precluding national legislation under which the need for the continued storage of biometric and genetic data is assessed by the police on the basis of internal rules, without that legislation laying down a maximum period of storage, in so far as that legislation sets appropriate time limits for a periodic review of the need to store those data and, at the time of that review, the strict necessity of extending their storage is assessed.

Costs

111 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 (Fifth Chamber) hereby rules:

1. **Articles 8 and 10 of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA**

   must be interpreted as meaning that, as regards the collection, storage and erasure of biometric and genetic data, the concept of 'Member State law', within the meaning of those articles, must be understood as referring to a provision of general application laying down the minimum conditions for collection, storage and erasure of those data, as interpreted by the case-law of the national courts, in so far as that case-law is accessible and sufficiently foreseeable.

2. **Article 6 and Article 4(1)(c) of Directive 2016/680, read in conjunction with Article 10 of that directive**

   must be interpreted as not precluding national legislation which permits the indiscriminate collection of biometric and genetic data of any person accused or suspected of having committed an intentional criminal offence, in so far as, first, the purposes of that collection do not require a distinction to be made between those two categories of persons and, second, the controllers are required, in accordance with

national law, including the case-law of the national courts, to comply with all of the principles and specific requirements laid down in Articles 4 and 10 of that directive.

3. Article 4(1)(e) of Directive 2016/680

must be interpreted as not precluding national legislation under which the need for the continued storage of biometric and genetic data is assessed by the police on the basis of internal rules, without that legislation laying down a maximum period for storage, in so far as that legislation sets appropriate time limits for a periodic review of the need to store those data and, at the time of that review, the strict necessity of extending their storage is assessed.

[Signatures]