Reports of Cases

JUDGMENT OF THE COURT (Grand Chamber)

4 October 2024*

(Reference for a preliminary ruling – 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 – Directive (EU) 2016/680 – Article 3(2) – Concept of 'processing' – Article 4 – Principles relating to processing of personal data – Article 4(1)(c) – Principle of 'data minimisation' – Articles 7, 8, 47 and Article 52(1) of the Charter of Fundamental Rights of the European Union – Requirement that a limitation on the exercise of a fundamental right must be 'provided for by law' – Proportionality – Assessment of proportionality in the light of all the relevant factors – Prior review by a court or independent administrative authority – Article 13 – Information to be made available or given to the data subject – Limits – Article 54 – Right to an effective judicial remedy against a controller or processor – Police investigation in relation to narcotics trafficking – Attempt, by the police, to unlock a mobile telephone in order to gain access, for the purposes of that investigation, to the personal data stored in that telephone)

In Case C-548/21,

REQUEST for a preliminary ruling under Article 267 TFEU from the Landesverwaltungsgericht Tirol (Regional Administrative Court, Tyrol, Austria), made by decision of 1 September 2021, received at the Court on 6 September 2021, in the proceedings

CG

v

Bezirkshauptmannschaft Landeck,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, K. Jürimäe, C. Lycourgos, E. Regan, T. von Danwitz, Z. Csehi and O. Spineanu-Matei, Presidents of Chambers, P.G. Xuereb (Rapporteur), I. Jarukaitis, A. Kumin, N. Jääskinen and M. Gavalec, Judges,

Advocate General: M. Campos Sánchez-Bordona,

Registrar: C. Di Bella, Administrator,

having regard to the written procedure and further to the hearing on 16 January 2023,

* Language of the case: German

after considering the observations submitted on behalf of:

– the Austrian Government, by A. Posch, J. Schmoll, K. Ibili and E. Riedl, acting as Agents,

– the Danish Government, by M.P.B. Jespersen, V. Pasternak Jørgensen, M. Søndahl Wolff and Y.T. Thyregod Kollberg, acting as Agents,

– the German Government, by J. Möller and M. Hellmann, acting as Agents,

– the Estonian Government, by M. Kriisa, acting as Agent,

– Ireland, by M. Browne, Chief State Solicitor, A. Joyce and M. Lane, acting as Agents, and by R. Farrell, Senior Counsel, D. Fennelly, Barrister-at-Law, and D. O'Reilly, Solicitor,

– the French Government, by R. Bénard, A. Daniel, A.-L. Desjonquères and J. Illouz, acting as Agents,

– the Cypriot Government, by I. Neophytou, acting as Agent,

– the Hungarian Government, by Zs. Biró-Tóth and M.Z. Fehér, acting as Agents,

– the Netherlands Government, by M.K. Bulterman, A. Hanje and J. Langer, acting as Agents,

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

– the Finnish Government, by A. Laine, acting as Agent,

– the Swedish Government, by J. Lundberg, H. Eklinder, C. Meyer-Seitz, A.M. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson, H. Shev and O. Simonsson, acting as Agents,

– the Norwegian Government, by F. Bergsjø, H. Busch, K. Moe Winther and P. Wennerås, acting as Agents,

– the European Commission, by G. Braun, S.L. Kalėda, H. Kranenborg and F. Wilman, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 20 April 2023,

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 5 and Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) ('Directive 2002/58'), read in the light of Articles 7, 8, 11, 41, 47 and Article 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter').

2 The request has been made in proceedings between CG and the Bezirkshauptmannschaft Landeck (District Administrative Authority, Landeck, Austria) concerning the seizure of CG's mobile telephone by the police and their attempts, in the context of a narcotics trafficking investigation, to unlock that telephone in order to access the data contained therein.

Legal context

European Union law

Directive 2002/58

3 Article 1 of Directive 2002/58, entitled 'Scope and aim', provides:

'1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

…

3. This Directive shall not apply to activities which fall outside the scope of the [TFEU], such as those covered by Titles V and VI of the [TEU], and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.'

4 Article 3 of that directive, headed 'Services concerned', provides:

'This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.'

5 Article 5 of that directive, entitled 'Confidentiality of the communications', provides in paragraph 1:

'Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.'

6 Article 15 of that directive, entitled 'Application of certain provisions of [Directive 95/46/EC]', states, in paragraph 1:

'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when

such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) [TEU].'

Directive (EU) 2016/680

7 Recitals 2, 4, 7, 10, 11, 15, 26, 37, 44, 46 and 104 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) are worded as follows:

'(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. This Directive is intended to contribute to the accomplishment of an area of freedom, security and justice.

…

(4) The free flow of personal data between 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 within the Union and the transfer of such personal data to third countries and international organisations, should be facilitated while ensuring a high level of protection of personal data. Those developments require the building of a strong and more coherent framework for the protection of personal data in the Union, backed by strong enforcement.

…

(7) Ensuring a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial cooperation in criminal matters and police cooperation. To that end, the level of protection of the rights and freedoms 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, should be equivalent in all Member States. Effective protection of personal data throughout the Union requires the strengthening of the rights of data

subjects and of the obligations of those who process personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.

…

(10) In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU may prove necessary because of the specific nature of those fields.

(11) It is therefore appropriate for those fields to be addressed by a directive that lays down the specific 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, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, 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)] applies. Regulation [2016/679] therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. …

…

(15) In order to ensure the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities, this Directive should provide for harmonised rules for the protection and the free movement of personal data processed 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. The approximation of Member States' laws should not result in any lessening of the personal data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union. Member States should not be precluded from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

…

(26) … The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose 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. …

…

(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. The processing of such data should also be allowed by law where the data subject has explicitly agreed to the processing that is particularly intrusive to him or her. However, the consent of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities.

…

(44) Member States should be able to adopt legislative measures delaying, restricting or omitting the information to data subjects or restricting, wholly or partly, the access to their personal data to the extent that and as long as such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others. The controller should assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted.

…

(46) Any restriction of the rights of the data subject must comply with the Charter and with the [Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950], as interpreted in the case-law of the Court of Justice [of the European Union] and by the European Court of Human Rights respectively, and in particular respect the essence of those rights and freedoms.

…

(104) This Directive respects the fundamental rights and observes the principles recognised in the Charter as enshrined in the TFEU, in particular the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on those rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.'

8 Article 1 of Directive 2016/680, entitled 'Subject matter and objectives', provides, in paragraphs 1 and 2:

'1. 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.

2. In accordance with this Directive, Member States shall:

(a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and

(b) ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.'

9 Article 2 of Directive 2016/680, entitled 'Scope', provides, in paragraphs 1 and 3:

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

…

3. This Directive does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

…'

10 Article 3 of Directive 2016/680, headed '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;

…

(7) "competent authority" means:
(a) any public authority competent for 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; or
(b) any other body or entity entrusted by Member State law to exercise public authority and public powers 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;

…'

11 Article 4 of Directive 2016/680, headed 'Principles relating to processing of personal data', provides, in paragraph 1:

'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;

…'

12 Article 6 of Directive 2016/680, entitled 'Distinction between different categories of data subject', states:

'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).'

13 Article 10 of that directive, entitled 'Processing of special categories of personal data', is worded 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 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.'

14 Article 13 of Directive 2016/680, headed 'Information to be made available or given to the data subject', provides:

'1. Member States shall provide for the controller to make available to the data subject at least the following information:

(a) the identity and the contact details of the controller;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended;

(d) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority;

(e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

2. In addition to the information referred to in paragraph 1, Member States shall provide by law for the controller to give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights:

(a) the legal basis for the processing;

(b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;

(c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations;

(d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

3. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

…'

15 Article 54 of that directive, entitled 'Right to an effective judicial remedy against a controller or processor', states:

'Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 52, Member States shall provide for the right of a data subject to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions.'

Austrian law

16 Paragraph 27(1) of the Suchtmittelgesetz (Law on Narcotics) of 5 September 1997 (BGBl. I, 112/1997), in the version applicable to the dispute in the main proceedings, provides:

'Any person, who unlawfully,

1. Buys, possesses, produces, transports, imports or exports narcotics or offers, gives or supplies narcotics to another person,

…

shall be liable to a term of imprisonment of up to a year or a fine of up to 360 daily units.

…'

17 Paragraph 17 of the Strafgesetzbuch (Criminal Code) of 1 January 1975 (BGBl., 60/1974), in the version applicable to the main proceedings ('the StGB'), states:

'(1) Serious offences are acts committed with intent punishable by life imprisonment or more than three years' imprisonment.

(2) All other offences shall be minor offences.'

18 Paragraph 18 of the Strafprozessordnung (Criminal Procedure Code) of 30 December 1975 (BGBl., 631/1975), in the version applicable to the dispute in the main proceedings ('the StPO'), provides:

'(1) The criminal investigation police is entrusted with tasks in the service of the administration of criminal justice (Paragraph 10(1)(6) of the Bundes-Verfassungsgesetz [(Federal constitutional law)]).

(2) Criminal investigation police investigations fall under the responsibility of the security authorities, the organisation and territorial competence of which are governed by the provisions of the Sicherheitspolizeigesetz [(Security Police Law)] relating to the organisation of the administration of public security.

(3) The bodies of the public security service (subparagraph 2 of Paragraph 5 of the Sicherheitspolizeigesetz [(Security Police Law)] perform the executive function of the criminal investigation police which consists in investigating and prosecuting criminal offences in accordance with the provisions of this Law.

…'

19 Paragraph 99(1) of the StPO provides:

'The criminal investigation police conducts investigations on its own initiative or pursuant to a complaint; it must comply with the orders of the Public Prosecutor's Office and of the courts (subparagraph 2 of Paragraph 105).'

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

20 On 23 February 2021, while carrying out a narcotics check, officers of the customs office of Innsbruck (Austria) seized a package addressed to CG containing 85 grams of cannabis. That package was sent for examination to the central police station of St. Anton am Arlberg (Austria).

21 On 6 March 2021, two police officers of that station conducted a search of CG's residence in the course of which they questioned him regarding the consignor of that package and went through his home. During that search, the police officers asked for access to the connection data on CG's mobile telephone. Following CG's refusal, those police officers seized that mobile telephone, which contained a SIM card and an SD card, and gave CG the seizure report.

22 Subsequently, that mobile telephone was handed over to an expert of the Landeck District (Austria) police station with a view to unlocking it. That expert not having succeeded in unlocking the mobile telephone at issue, it was sent to the Vienna Bundeskriminalamt (Federal Office of the Criminal Investigation Police) (Austria) where a new attempt to unlock the telephone was made.

23 The seizure of CG's mobile telephone and the subsequent attempts to make use of that telephone were carried out at the personal initiative of the police officers concerned, without the authorisation of the Public Prosecutor's Office or a court.

24 On 31 March 2021, CG brought an action before the Landesverwaltungsgericht Tirol (Regional Administrative Court, Tyrol, Austria), the referring court, challenging the lawfulness of the seizure of his mobile telephone. That telephone was returned to CG on 20 April 2021.

25 CG was not informed promptly of the attempts to make use of his mobile telephone. He only became aware of those attempts when the police officer who seized that telephone and subsequently took the first steps to exploit its digital data was questioned as a witness in the proceedings pending before the referring court. Nor were those attempts documented in the file compiled by the criminal investigation police.

26 In the light of the foregoing, the referring court asks, in the first place, whether, in the light of paragraphs 52 to 61 of the judgment of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788), and the case-law cited therein, Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter, must be interpreted as meaning that full and uncontrolled access to all digital data contained in a mobile telephone, that is to say connection data, the content of communications, photos and browsing history – which can provide a very detailed and in-depth picture of almost all areas of the private life of the data subjects – constitutes so serious an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter that, as regards the prevention, investigation, detection and prosecution of criminal offences, that access must be limited to fighting serious offences.

27 In that regard, that court states that the offence of which CG is accused in the criminal investigation at issue in the main proceedings is set out in Paragraph 27(1) of the Law on Narcotics and is punishable by a term of imprisonment of up to a year and constitutes, in the light of the classification set out in Paragraph 17 of the StGB, only a minor offence.

28 In the second place, after recalling the lessons to be drawn from paragraphs 48 to 54 of the judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152), and the case-law cited therein, the referring court asks whether Article 15(1) of Directive 2002/58 precludes a national legal rule such as that stemming from the combined provisions of Paragraph 18 and Paragraph 99(1) of the StPO pursuant to which, in the course of a criminal investigation, the criminal investigation police can gain, without the authorisation of a court or independent administrative body, full and uncontrolled access to all digital data contained in a mobile telephone.

29 In the third and last place, after stating that Paragraph 18 of the StPO, read in conjunction with Paragraph 99(1) thereof, does not impose any obligation on the police to document the measures for the digital exploitation of a mobile telephone, or to inform its owner of the existence of such measures, so that the latter may, as the case may be, object to such measures by means of a

preventive or *ex post facto* challenge before the courts, the referring court is uncertain whether those provisions of the StPO are compatible with the principle of equality of arms and the right to an effective judicial remedy within the meaning of Article 47 of the Charter.

30 In those circumstances the Landesverwaltungsgericht Tirol (Regional Administrative Court, Tyrol) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Is Article 15(1) [of Directive 2002/58 – as the case may be, in combination with Article 5 thereof –], read in the light of Articles 7 and 8 of the [Charter], to be interpreted as meaning that [access by public authorities] to data stored on mobile telephones [constitutes an] interference with [the] fundamental rights enshrined in those articles of the Charter which is sufficiently serious to [require] that that access [be] limited, in areas of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime?

(2) Is Article 15(1) of Directive [2002/58], read in the light of Articles 7, 8 and 11 and Article 52(1) of the [Charter], to be interpreted as meaning that it precludes a national rule, such as that enacted in Paragraph 18 of the [StPO], read in combination with Paragraph 99(1) thereof, which allows security authorities to grant themselves full and uncontrolled access to all digital data stored on a mobile telephone in the course of a criminal investigation without the authorisation of a court or independent administrative body?

(3) Is Article 47 of the [Charter], [as the case may be,] read in combination with Articles 41 and 52 thereof, to be interpreted, from the point of view of equality of arms and from the point of view of an effective remedy, as meaning that it precludes a national rule, such as that enacted in Paragraph 18 of the [StPO], read in combination with Paragraph 99(1) thereof, which allows [data stored on a mobile telephone to be exploited] without advising the data subject [of the measure concerned beforehand or, at the very least, after it is taken]?'

Procedure before the Court

31 On 20 October 2021, the Court sent a request for information to the referring court, by which it asked it whether Directive 2016/680 might be relevant in the dispute in main proceedings and, if so, to set out for the Court the provisions of national law transposing that directive into Austrian law which may apply in the present case.

32 On 11 November 2021, the referring court replied to that request, stating, inter alia, that the requirements of that directive had to be complied with in the present case. That reply was notified, together with the order for reference, to the interested persons referred to in Article 23 of the Statute of the Court of Justice of the European Union.

33 On 8 November 2022, pursuant to Article 61 of the Rules of Procedure of the Court, the Court requested the participants in the oral part of the procedure to concentrate in their oral submissions on Directive 2016/680 and to answer, at the hearing, certain questions concerning that directive.

The request to have the oral procedure reopened

34 Following delivery of the Advocate General's Opinion, by document lodged at the Court Registry on 17 May 2023, the Austrian Government submitted an application for rectification of that opinion on the ground that it presented incorrectly the position that government had expressed in both its written and oral observations and that it contained factual errors.

35 That government argues, first, that point 50 of the Advocate General's Opinion, read in conjunction with footnote 14 thereto, suggests that, according to that government, an attempt to access the data contained in a mobile telephone, such as that at issue in the main proceedings, cannot constitute processing of personal data for the purposes of Article 3(2) of Directive 2016/680. However, that government maintained the opposite at the hearing before the Court, by expressly endorsing the position set out by the Commission in its written observations, according to which it is apparent from a systemic interpretation of that directive, read in the light of its objectives, that it governs not only processing itself, but also operations taking place prior to such processing, such as a processing attempt, without the application of that directive being conditional on the success of that attempt.

36 Second, the Austrian Government submits that point 27 of the Advocate General's Opinion is based on incorrect facts, in that it suggests that the processing attempts referred to in paragraph 22 of the present judgment were not documented in the criminal investigation police's file. In that regard, that government states that, contrary to what is indicated in point 27 of the Opinion and the request for a preliminary ruling, it explained, in its written observations, that those processing attempts had been recorded in two reports drawn up by the police officers responsible for the investigation in the main proceedings and that those reports had subsequently been added to the file of the Public Prosecutor's Office.

37 By decision of the President of the Court of 23 May 2023, the Austrian Government's request for rectification of the Advocate General's Opinion was reclassified as a request that the oral part of the procedure be reopened, within the meaning of Article 83 of the Rules of Procedure.

38 In that regard, it should be recalled, first, that the Statute of the Court of Justice of the European Union and the Rules of Procedure make no provision for the parties or the interested persons referred to in Article 23 of that statute to submit observations in response to the Advocate General's Opinion. Second, under the second paragraph of Article 252 TFEU, the Advocate General, acting with complete impartiality and independence, is to make, in open court, reasoned submissions on cases which, in accordance with the Statute, require the Advocate General's involvement. The Court is not bound either by the Advocate General's submissions or by the reasoning which led to those submissions. Consequently, a party's disagreement with the Opinion of the Advocate General, irrespective of the questions that he or she examines in the Opinion, cannot in itself constitute grounds justifying the reopening of the oral part of the procedure (judgment of 14 March 2024, *f6 Cigarettenfabrik*, C-336/22, EU:C:2024:226, paragraph 25 and the case-law cited).

39 It is true that, in accordance with Article 83 of the Rules of Procedure, the Court may at any time, after hearing the Advocate General, order the reopening of the oral part of the procedure, in particular if it considers that it lacks sufficient information or where a party has, after the close of that part of the procedure, submitted a new fact which is of such a nature as to be a decisive factor for the decision of the Court, or where the case must be decided on the basis of an argument which has not yet been debated.

40 However, in the present case, the Court considers that it has, at the end of the written part of the procedure and the hearing held before it, all the information necessary to rule on the present request for a preliminary ruling. Moreover, the considerations put forward by the Austrian government in support of its request that the oral part of the procedure be reopened are not such as to have a decisive influence on the decision the Court is called upon to give in the present case.

41 So far as concerns, more specifically, the factual information referred to in paragraph 36 of this judgment, it should be borne in mind that, in preliminary ruling proceedings, the Court does not have the task of establishing the alleged facts but solely that of interpreting the relevant provisions of EU law (see, to that effect, judgment of 31 January 2023, *Puig Gordi and Others*, C-158/21, EU:C:2023:57, paragraph 36). According to the case-law of the Court, questions on the interpretation of EU law are referred by a national court in the factual and legislative context which that court is responsible for defining, the accuracy of which is not a matter for the Court to determine (see, to that effect, judgment of 18 June 2024, *Bundesrepublik Deutschland (Effect of a decision granting refugee status)*, C-753/22, EU:C:2024:524, paragraph 44 and the case-law cited).

42 In those circumstances, the Court considers, after hearing the Advocate General, that there is no need to order that the oral part of the procedure be reopened.

Admissibility of the request for a preliminary ruling

43 Several of the interested parties which submitted written observations in the present proceedings contested the admissibility of the request for a preliminary ruling in its entirety or of some of the questions asked by the referring court.

44 In the first place, the Austrian, French and Swedish Governments submit that the order for reference does not satisfy the requirements laid down in Article 94 of the Rules of Procedure, on the ground that it does not contain the factual and legal material necessary to give a useful answer to that court.

45 In the second place, the Austrian Government submits, first, that, by its second and third questions, the referring court seeks, in essence, to ascertain whether the provisions of Paragraphs 18 and 99 of the StPO, read together, are consistent with EU law. Since those provisions do not lay down the conditions under which the exploitation of data media must be performed, those questions bear no relation to the subject matter of the dispute in the main proceedings. It submits, second, that, under Austrian law, an order of the Public Prosecutor's Office is necessary in order to seize a mobile telephone or to attempt to access data contained in that telephone. That court should therefore find that there has been an infringement of Austrian law, with the result that the questions referred by that court are not necessary for the resolution of that dispute and that, therefore, there is no need to rule on the request for a preliminary ruling.

46 As a preliminary point, it should be noted that, according to settled case-law, in the context of the cooperation between the Court and the national courts provided for in Article 267 TFEU, it is solely for the national court before which a dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine, in the light of the particular circumstances of the case, both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court. Consequently, where

the questions submitted by the national court concern the interpretation of EU law, the Court is, in principle, bound to give a ruling (judgment of 24 July 2023, *Lin*, C-107/23 PPU, EU:C:2023:606, paragraph 61 and the case-law cited).

47 It follows that questions relating to EU law enjoy a presumption of relevance. 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 24 July 2023, *Lin*, C-107/23 PPU, EU:C:2023:606, paragraph 62 and the case-law cited).

48 Concerning, in the first place, the argument alleging failure to comply with the requirements laid down in Article 94 of the Rules of Procedure, it should be noted that, according to settled case-law, which is now reflected in Article 94(a) and (b) of the Rules of Procedure, the need to provide an interpretation of EU law which will be of use to the national court makes it necessary for the national court to define the factual and regulatory context of the questions it is asking or, at the very least, to explain the factual hypotheses on which those questions are based. Furthermore, it is essential, as stated in Article 94(c) of the Rules of Procedure, that the request for a preliminary ruling itself contain a statement of the reasons which prompted the referring court or tribunal to enquire about the interpretation or validity of certain provisions of EU law, and the connection between those provisions and the national legislation applicable to the dispute in the main proceedings (judgment of 21 December 2023, *European Superleague Company*, C-333/21, EU:C:2023:1011, paragraph 59 and the case-law cited).

49 In the present case, as regards the factual context, the referring court stated, in its request for a preliminary ruling, that the Austrian police authorities, after having seized CG's mobile telephone in a police investigation relating to narcotics trafficking, attempted, on two occasions, to gain access to the data contained in that telephone, at their own initiative, without prior authorisation from the Public Prosecutor's Office or a court. It also stated that CG had only become aware of the attempts to access the data contained in his mobile telephone when he heard the testimony of a police officer. Last, it stated that those attempts to gain access had not been documented in the file compiled by the criminal investigation police.

50 As regards the regulatory framework, that court stated that the national provisions which it referred to in the order for reference permitted an attempt to access data contained in a mobile telephone for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without (i) restricting that possibility solely to combating serious crime, (ii) making that attempt to access data subject to prior review by a judge or an independent administrative body, and (iii) providing for the data subjects to be informed of that attempt, with a view, in particular, of enabling them to oppose it by bringing a challenge before the courts.

51 In addition, that court has set out, as is apparent from paragraphs 26 to 29 of the present judgment, the reasons which led it to submit its request for a preliminary ruling to the Court and the link which, in its view, exists between the provisions of EU law and the Charter referred to in that request and the Austrian law provisions applicable, in its opinion, to the dispute in the main proceedings.

52 The information referred to in paragraphs 49 to 51 of the present judgment thus permits the inference that the request for a preliminary ruling meets the requirements laid down in Article 94 of the Rules of Procedure.

53 In the second place, so far as concerns the arguments alleging that the provisions of Austrian law referred to in the second and third questions referred are not relevant and that the referring court should have found an infringement of that law, it should be recalled that it is not for the Court to rule on the interpretation of provisions of national law or to decide whether the interpretation or application of those provisions by the national court is correct, since such an interpretation falls within the exclusive jurisdiction of the national court (judgment of 15 June 2023, *Getin Noble Bank (Suspension of the performance of a loan agreement)*, C-287/22, EU:C:2023:491, paragraph 32 and the case-law cited).

54 In the present case, it is apparent from the request for a preliminary ruling and, in particular, from the wording of the questions referred, that the referring court considers, first, that those provisions of Austrian law are applicable to the dispute in the main proceedings and, second, that an attempt to access data contained in a mobile telephone, without prior authorisation from the Public Prosecutor's Office or a court, such as that at issue in the main proceedings, is permitted under Austrian law. In accordance with the case-law cited in the preceding paragraph of the present judgment, it is not for the Court to rule on such an interpretation of those provisions.

55 It follows that the questions referred by the referring court are admissible.

Substance

56 The Austrian Government claims, in its written observations, that the Court does not have jurisdiction to answer the first and second questions referred for a preliminary ruling since those questions concern the interpretation of Article 5 and Article 15(1) of Directive 2002/58, when it is clear that that directive does not apply to the dispute in the main proceedings. At the hearing, several governments maintained that it was not possible to reformulate the questions referred in the light of Directive 2016/680. In particular, the Austrian Government stressed that the fact that the latter directive did not contain provisions equivalent to Article 5 and Article 15(1) of Directive 2002/58 precluded that reformulation. The French Government argued, for its part, that one of the limitations on the power to reformulate questions referred for a preliminary ruling can be found in the right of the Member States to submit written observations. According to that government, that right would be deprived of any effectiveness if it were possible for the legal framework of the procedure to be radically altered when the Court reformulates the questions referred for a preliminary ruling.

57 In that regard, it should be recalled that the Court has held, relying in particular on Article 1(1) and (3) and Article 3 of Directive 2002/58, that, where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by Directive 2002/58, but by national law only, subject to the application of Directive 2016/680 (judgments of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraph 48, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 103).

58 It is common ground that the dispute in the main proceedings concerns an attempt by the police directly to access personal data contained in a mobile telephone, without any intervention on the part of a provider of electronic communications services having been sought.

59 It is therefore clear that that dispute does not fall within the scope of Directive 2002/58, to which reference is made in the first and second questions referred.

60 Nevertheless, it should be recalled that, in accordance with settled case-law, under the procedure laid down by Article 267 TFEU, which provides for cooperation between national courts and the Court of Justice, it is for the latter to provide the national court with an answer which will be of use to it and enable it to determine the case before it. To that end, the Court should, where necessary, reformulate the questions referred to it. The Court may also find it necessary to consider provisions of EU law which the national court has not referred to in its questions (judgments of 15 July 2021, *Ministrstvo za obrambo*, C-742/19, EU:C:2021:597, paragraph 31 and the case-law cited, and of 18 June 2024, *Generalstaatsanwaltschaft Hamm (Request for the extradition of a refugee to Türkiye)*, C-352/22, EU:C:2024:521, paragraph 47).

61 The fact that a national court has, formally speaking, worded a question referred for a preliminary ruling with reference to certain provisions of EU law does not prevent the Court from providing the national court with all the points of interpretation which may be of assistance in adjudicating on the case pending before it, whether or not that court has referred to them in its questions. In that regard, it is for the Court to extract from all the information provided by the national court, in particular from the grounds of the decision referring the questions, the points of EU law which require interpretation, having regard to the subject matter of the dispute (judgment of 22 June 2022, *Volvo and DAF Trucks*, C-267/20, EU:C:2022:494, paragraph 28 and the case-law cited).

62 Admittedly, in accordance with settled case-law, the information provided in the order for reference must not only be such as to enable the Court to reply usefully but must also give the governments of the Member States and other interested persons an opportunity to submit observations pursuant to Article 23 of the Statute of the Court of Justice of the European Union (judgment of 21 December 2023, *Royal Antwerp Football Club*, C-680/21, EU:C:2023:1010, paragraph 32 and the case-law cited).

63 However, as is apparent from paragraphs 31 to 33 of the present judgment, in response to the Court's request for information addressed to the referring court, the latter stated that Directive 2016/680 was applicable to the dispute in the main proceedings. The interested parties were able, in their written observations, to express their views on the interpretation of that directive and its relevance to the case in the main proceedings. In addition, for the purposes of the hearing, the Court asked the participants in the oral part of the procedure to answer, at that hearing, certain questions concerning that directive. In particular, it asked them to state their position on the relevance of Article 4 of that directive for answering the first question referred for a preliminary ruling and on that of Articles 13 and 54 of that directive for answering the third question referred.

64 Consequently, the fact that the first and second questions referred for a preliminary ruling concern the interpretation of Article 5 and Article 15(1) of Directive 2002/58, and not that of Directive 2016/680, does not preclude the questions referred by the national court from being reformulated in the light of the provisions of Directive 2016/580 which are relevant in the present case and, therefore, does not prevent the Court from having jurisdiction to answer those questions.

65 That conclusion is not called into question by the argument of Ireland and of the French and Norwegian Governments that an attempt to access personal data does not fall within the scope of Directive 2016/680, since that directive applies only to processing which has actually been carried out.

66 Those governments submit, in that regard, that the interpretation of the provisions of that directive is not relevant for the resolution of the dispute in the main proceedings; the same is true of the interpretation of the Charter, since it applies only in situations in which the Member States are implementing EU law.

67 However, where it is not obvious that the interpretation of an act of EU law bears no relation to the facts of the dispute in the main proceedings or its purpose, as is the case of Directive 2016/680 here, the objection alleging the inapplicability of that act to the case in the main proceedings concerns the substance of the questions raised (see, by analogy, judgment of 24 July 2023, *Lin*, C-107/23 PPU, EU:C:2023:606, paragraph 66 and the case-law cited).

68 Accordingly, it is necessary, as a preliminary point, to examine whether an attempt by the police to access the data contained in a mobile telephone falls within the material scope of that directive.

The application of Directive 2016/680 to an attempt to access data contained in a mobile telephone

69 Article 2(1) of Directive 2016/680 defines its material scope. According to that provision, that directive 'applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1) [thereof]', that is to say, inter alia, 'the prevention, investigation, detection or prosecution of criminal offences'.

70 Article 3(2) of that directive defines the concept of 'processing' as including '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 … retrieval, consultation' or also 'dissemination or otherwise making available'.

71 It is thus apparent from the very wording of Article 3(2) of Directive 2016/680 and, in particular, from the use of the expressions 'any operation', 'any set of operations' and 'otherwise making available' that the EU legislature intended the concept of 'processing' to be broad in scope and, consequently, for the material scope of that directive to be wide. That interpretation is supported by the non-exhaustive nature, expressed by the expression 'such as', of the list of operations mentioned in that provision (see, by analogy, judgment of 24 February 2022, *Valsts ieņēmumu dienests (Processing of personal data for tax purposes)*, C-175/20, EU:C:2022:124, paragraph 35).

72 Those textual elements thus argue in favour of an interpretation according to which, where the police seize a telephone and handle it with a view to extracting and consulting personal data contained therein, they begin processing within the meaning of Article 3(2) of Directive 2016/680, even if they do not, for technical reasons, succeed in accessing those data.

73 That interpretation is confirmed by the context of Article 3(2) of Directive 2016/680. Under Article 4(1)(b) of that directive, Member States are to provide that personal data are to be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes. The latter provision lays down the principle of purpose limitation (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 122). The effectiveness of that principle necessarily requires that the purpose of the collection be determined as from when the competent authorities attempt to access personal data since such an attempt, if successful, is such as to enable those authorities, inter alia, to collect, extract or consult the data in question immediately.

74 As regards the objectives of Directive 2016/680, that directive seeks, inter alia, as is apparent from recitals 4, 7 and 15 thereof, to ensure a high level of protection of the personal data of natural persons.

75 That objective would be undermined should it not be possible to classify an attempt to access personal data contained in a mobile telephone as 'processing' of that data. An interpretation of Directive 2016/680 to that effect would expose the persons concerned by such an access attempt to a significant risk that it will no longer be possible to prevent the principles established by that directive from being breached.

76 It should also be noted that such an interpretation is consistent with the principle of legal certainty, which, in accordance with the Court's settled case-law, requires the application of rules of law to be foreseeable by those subject to them, in particular where they may have adverse consequences (judgment of 27 June 2024, *Gestore dei Servizi Energetici*, C-148/23, EU:C:2024:555, paragraph 42 and the case-law cited). An interpretation according to which the applicability of Directive 2016/680 depends on the success of the attempt to access personal data contained in a mobile telephone would create uncertainty incompatible with that principle for both the competent national authorities and individuals.

77 It follows from the foregoing that an attempt by the police to access the data contained in a mobile telephone for the purposes of a criminal investigation, such as that at issue in the main proceedings, falls, as the Advocate General stated in point 53 of his Opinion, within the scope of Directive 2016/680.

The first and second questions

78 The referring court expressly referred, in its first and second questions, first, to Article 15(1) of Directive 2002/58, which requires, inter alia, that the legislative measures which it allows the Member States to adopt to restrict the scope of the rights and obligations laid down in several provisions of that directive, constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security – that is to say, State security – defence and public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, and, second, to Article 52(1) of the Charter, which enshrines the principle of proportionality in the context of limitations on the exercise of the rights and freedoms recognised by the Charter.

79 Under Article 4(1)(c) of Directive 2016/680, Member States are to provide for personal data to be adequate, relevant and not excessive in relation to the purposes for which they are processed. That provision thus requires the Member States to observe the principle of 'data minimisation', which gives expression to the principle of proportionality (judgment of 30 January 2024, *Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR – Sofia*, C-118/22, EU:C:2024:97, paragraph 41 and the case-law cited).

80 It follows that, in particular, the collection of personal data in the context of criminal proceedings and their storage by police authorities, for the purposes set out in Article 1(1) of that directive, must, like any processing falling within the scope of that directive, comply with that principle (judgment of 30 January 2024, *Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR – Sofia*, C-118/22, EU:C:2024:97, paragraph 42 and the case-law cited).

81 Thus, it must be held that, by its first and second questions, which it is appropriate to examine together, the referring court asks, in essence, whether Article 4(1)(c) of Directive 2016/680, read in the light of Articles 7 and 8 of the Charter and Article 52(1) thereof, precludes national legal rules which afford the competent authorities the possibility of accessing data contained in a mobile telephone, for the purposes of preventing, investigating, detecting and prosecuting criminal offences in general, and which do not make reliance on that possibility subject to prior review by a court or an independent administrative body.

82 As a preliminary point, it should be noted that, as is apparent from recitals 2 and 4 of Directive 2016/680, while establishing a strong and coherent framework for the protection of personal data in order to ensure respect for the fundamental right of protection of natural persons with regard to the processing of their personal data, recognised in Article 8(1) of the Charter and Article 16(1) TFEU, that directive is intended to contribute to the accomplishment of an area of freedom, security and justice within the European Union (see, to that effect, judgment of 25 February 2021, *Commission* v *Spain (Personal Data Directive – Criminal law)*, C-658/19, EU:C:2021:138, paragraph 75).

83 To that end, Directive 2016/680 seeks, inter alia, as has been noted in paragraph 74 of the present judgment, to ensure a high level of protection of the personal data of natural persons.

84 In that regard, it should be recalled that, as recital 104 of Directive 2016/680 highlights, the limitations which, under that directive, can be placed on the right to the protection of personal data, provided for in Article 8 of the Charter, and on the right to respect for private and family life, protected by Article 7 of the Charter, must be interpreted in accordance with the requirements of Article 52(1) thereof, which include respect for the principle of proportionality (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 33).

85 Those fundamental rights are not absolute rights, but must be considered in relation to their function in society and be weighed against other fundamental rights. Any limitation on the exercise of those fundamental rights must, in accordance with Article 52(1) of the Charter, be provided for by law, respect the essence of those fundamental rights and observe the principle of proportionality. Under the principle of proportionality, 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. They must apply only in so far as is strictly necessary and the legislation which entails the limitations in question must lay down clear and precise rules governing the scope and application of those limitations (judgment of 30 January 2024, *Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR – Sofia*, C-118/22, EU:C:2024:97, paragraph 39 and the case-law cited).

86 As regards, in the first place, the objective of general interest capable of justifying a limitation on the exercise of the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as that arising from the legal rule at issue in the main proceedings, it should be noted that the processing of personal data in the context of a police investigation aimed at the prosecution of a criminal

offence – such as an attempt to access the data contained in a mobile telephone – must be regarded, in principle, as genuinely meeting an objective of general interest recognised by the European Union, within the meaning of Article 52(1) of the Charter.

87 As far as concerns, in the second place, the requirement that such a limitation be necessary, as stated, in essence, in recital 26 of Directive 2016/680, that requirement is not met where the objective of general interest pursued can reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of the data subjects (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 40 and the case-law cited).

88 By contrast, the requirement of necessity is met where the objective pursued by the data processing at issue cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed in Articles 7 and 8 of the Charter (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 and the case-law cited).

89 As regards, in the third place, the proportionate nature of the limitation on the exercise of the fundamental rights guaranteed in Articles 7 and 8 of the Charter, resulting from such processing, it involves balancing all the relevant factors in the individual case (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 62 and 63 and the case-law cited).

90 Such factors include, inter alia, the seriousness of the limitation thus placed on the exercise of the fundamental rights at issue, which depends on the nature and sensitivity of the data to which the competent police authorities may have access, the importance of the objective of general interest pursued by that limitation, the link existing between the owner of the mobile telephone and the criminal offence in question and the relevance of the data in question for the purpose of establishing the facts.

91 As regards, first, the seriousness of the limitation on fundamental rights resulting from a legal rule such as that at issue in the main proceedings, it is apparent from the order for reference that that rule authorises the competent police authorities to access, without prior authorisation, the data contained in a mobile telephone.

92 Such access is liable to concern, depending on the content of the mobile telephone in question and the choices made by the police, not only traffic and location data, but also photographs and the internet browsing history on that telephone, or even a part of the content of the communications made with that telephone, in particular by consulting the messages stored therein.

93 Access to such a set of data is liable to allow very precise conclusions to be drawn concerning the private life of the data subject, such as his or her everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of that data subject and the places he or she frequents socially.

94 Last, it cannot be ruled out that the data contained in a mobile telephone may include particularly sensitive data, such as personal data revealing racial or ethnic origin, political opinions and religious or philosophical beliefs, such sensitivity justifying the specific protection afforded to them by Article 10 of Directive 2016/680, which also extends to data revealing information of

that nature indirectly, following an intellectual operation involving deduction or cross-referencing (see, by analogy, judgment of 5 June 2023, *Commission* v *Poland (Independence and private life of judges)*, C-204/21, EU:C:2023:442, paragraph 344).

95 The interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter to which the application of a rule such as that at issue in the main proceedings may give rise must therefore be regarded as serious, or even particularly serious.

96 As regards, second, the importance of the objective pursued, it should be noted that the seriousness of the offence which is the subject matter of the investigation is one of the main parameters when examining the proportionality of the serious interference which access to the personal data contained in a mobile telephone constitutes and which allow precise conclusions to be drawn concerning the private life of the data subject.

97 However, to consider that only combating serious crime may justify access to data contained in a mobile telephone would limit the investigative powers of the competent authorities, within the meaning of Directive 2016/680, in relation to criminal offences in general. This would increase the risk of impunity for such offences, given the importance that such data may have for criminal investigations. Accordingly, such a limitation would disregard the specific nature of the tasks performed by those authorities for the purposes set out in Article 1(1) of that directive, highlighted in recitals 10 and 11 thereof, and would undermine the objective of achieving an area of freedom, security and justice within the European Union pursued by that directive.

98 That being so, those considerations are without prejudice to the requirement, arising from Article 52(1) of the Charter, that any limitation on the exercise of a fundamental right must be 'provided for by law', that requirement implying that the legal basis authorising such a limitation must define its scope sufficiently clearly and precisely (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 65 and the case-law cited).

99 In order to satisfy that requirement, it is for the national legislature to define with sufficient precision the factors, in particular the nature or categories of the offences concerned, which must be taken into account.

100 As regards, third, the link that exists between the owner of the mobile telephone and the criminal offence in question and the relevance of the data in question for the purpose of establishing the facts, it is apparent from Article 6 of Directive 2016/680 that the concept of 'data subject' covers different categories of persons, namely, in essence, persons suspected, on serious grounds, of having committed or being about to commit a criminal offence, persons convicted of a criminal offence, victims or potential victims of such offences, and others parties to a criminal offence which may be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings. According to that article, Member States are required to 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.

101 In that regard, so far as concerns, in particular, access to the data contained in the mobile telephone of a person who is subject to a criminal investigation, as in the case in the main proceedings, it is important that the existence of reasonable suspicions in relation to that

person – in the sense that that person has committed, commits or plans to commit an offence, or that he or she is involved in one way or another in such an offence – is supported by objective and sufficient evidence.

102 It is essential – in particular in order to ensure that the principle of proportionality is observed in each specific case by balancing all the relevant factors – that, where access to personal data by the competent national authorities carries the risk of serious, or even particularly serious, interference with the fundamental rights of the data subject, that access be subject to a prior review carried out either by a court or by an independent administrative body.

103 That prior review requires that the court or independent administrative body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various legitimate interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the legitimate interests relating to the needs of the investigation in the context of combating crime and, on the other hand, the fundamental rights to respect for private life and protection of personal data of the persons whose data are concerned by the access.

104 That independent review, in a situation such as that referred to in paragraph 102 of the present judgment, must take place prior to any attempt to access the data concerned, except in cases of duly justified urgency, in which case that review must take place within a short time. A subsequent review would not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met.

105 In particular, the court or independent administrative body, acting in the context of a prior review carried out following a reasoned request for access falling within the scope of Directive 2016/680, must be entitled to refuse or restrict that access where it finds that the interference with fundamental rights which that access would constitute would be disproportionate in the light of all the relevant factors.

106 A refusal to authorise the competent police authorities to access the data contained in a mobile telephone, or a restriction on that access, is therefore necessary if, taking into account the seriousness of the offence and the needs of the investigation, access to the content of the communications or to sensitive data does not appear to be justified.

107 As regards, in particular, the processing of sensitive data, account must be taken of the requirements laid down in Article 10 of Directive 2016/680, the purpose of which is to ensure enhanced protection with regard to that processing which is liable, as is apparent from recital 37 of that directive, to create significant risks to fundamental rights and freedoms, such as the right to respect for private and family life and the right to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter. To that end, as follows from the very terms of Article 10 of Directive 2016/680, the requirement that the processing of such data be allowed ‘only where strictly necessary’ must be interpreted as establishing strengthened conditions for lawful processing of sensitive data, compared with those which follow from Article 4(1)(b) and (c) and Article 8(1) of that directive and refer only to the ‘necessity’ of data processing that falls generally, within the directive’s scope (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, paragraphs 116 and 117 and the case-law cited).

108 Thus, first, the use of the adverb 'only' before the words 'where strictly necessary' underlines that the processing of special categories of data, within the meaning of Article 10 of Directive 2016/680, will be capable of being regarded as necessary solely in a limited number of cases. Second, the fact that the necessity for processing of such data is an 'absolute' one signifies that that necessity is to be assessed with particular rigour (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).

109 In the present case, the referring court states that, in the course of criminal investigation proceedings, the Austrian police are authorised to access data contained in a mobile telephone. In addition, it states that such access is not, in principle, subject to the prior authorisation of a court or independent administrative authority. It is, however, for that court alone to draw the appropriate conclusions from the clarifications provided, inter alia, in paragraphs 102 to 108 of the present judgment in the main proceedings.

110 It follows from the foregoing that the answer to the first and second questions is that Article 4(1)(c) of Directive 2016/680, read in the light of Articles 7 and 8 and Article 52(1) of the Charter, must be interpreted as not precluding national legal rules which afford the competent authorities the possibility to access data contained in a mobile telephone for the purposes of the prevention, investigation, detection and prosecution of criminal offences in general, provided those rules:

– define with sufficient precision the nature or categories of offences concerned,

– ensure respect for the principle of proportionality, and

– make reliance on that possibility, except in duly justified cases of urgency, subject to prior review by a judge or an independent administrative body.

The third question

111 It is apparent from the order for reference that, by its third question, the referring court seeks, in essence, to determine whether CG should have been informed of the attempts to access the data contained in his mobile telephone in order to be able to exercise his right to an effective remedy guaranteed in Article 47 of the Charter.

112 In that regard, the relevant provisions of Directive 2016/680 are, first, Article 13 of that directive, entitled 'Information to be made available or given to the data subject', and, second, Article 54 of that directive, entitled 'Right to an effective judicial remedy against a controller or processor'.

113 It must also be borne in mind that, as recital 104 of Directive 2016/680 highlights, the limitations imposed by that directive on the right to an effective remedy and to a fair trial, protected by Article 47 of the Charter, must be interpreted in accordance with the requirements of Article 52(1) thereof, which include respect for the principle of proportionality.

114 It must therefore be held that, by its third question, the referring court asks, in essence, whether Articles 13 and 54 of Directive 2016/680, read in the light of Article 47 and Article 52(1) of the Charter, must be interpreted as precluding national legal rules which authorise the competent authorities in criminal matters to attempt to access data contained in a mobile telephone without informing the data subject.

115 It follows from Article 13(2)(d) of Directive 2016/680 that, in addition to the information referred to in paragraph 1, such as the identity of the controller, the purpose of that processing and the right to lodge a complaint with a supervisory authority which must be made available to the data subject, Member States are to provide by law for the controller to give the data subject further information to enable him or her to exercise his or her rights, where necessary, in particular where the personal data are collected without the knowledge of the data subject.

116 However, Article 13(3)(a) and (b) of Directive 2016/680 allows the national legislature to restrict the provision of information to the data subject pursuant to paragraph 2, or to omit to provide that information 'to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned', inter alia, to 'avoid obstructing official or legal inquiries, investigations or procedures' or to 'avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties'.

117 Last, it should be noted that Article 54 of Directive 2016/680, which gives expression to Article 47 of the Charter, requires Member States to provide that, where a person considers that his or her rights laid down in the provisions adopted pursuant to that directive have been infringed as a result of the processing of his or her personal data in breach of those provisions, that person has the right to an effective judicial remedy.

118 It is apparent from the case-law that the right to an effective judicial remedy, guaranteed in Article 47 of the Charter, requires, in principle, that the person concerned must be able to ascertain the reasons on which the decision taken in relation to him or her is based, so as to make it possible for him or her to defend his or her rights in the best possible conditions and to decide, with full knowledge of the relevant facts, whether there is any point in his or her applying to the court with jurisdiction, and in order to put the latter fully in a position in which it may carry out the review of the lawfulness of that decision (judgment of 16 November 2023, *Ligue des droits humains (Verification by the supervisory authority of data processing)*, C-333/22, EU:C:2023:874, paragraph 58).

119 Although that right is not an absolute right and, in accordance with Article 52(1) of the Charter, limitations may be placed upon it, that is on condition that those limitations are provided for by law, they respect the essence of the rights and freedoms at issue and, in compliance with the principle of proportionality, 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 (judgment of 16 November 2023, *Ligue des droits humains (Verification by the supervisory authority of data processing)*, C-333/22, EU:C:2023:874, paragraph 59).

120 Therefore, it follows from the provisions cited in paragraphs 115 to 119 above that it is for the competent national authorities which have been authorised by a court or an independent administrative body to access the data stored to inform the data subjects, within the framework of the applicable national procedural rules, of the grounds on which that authorisation is based, as soon as such information is not liable to jeopardise the investigations carried out by those authorities, and to make available to them all the information referred to in Article 13(1) of Directive 2016/680. That information is indeed necessary to enable those persons to exercise, inter alia, the right to a remedy expressly provided for in Article 54 of Directive 2016/680 (see, to that effect, judgment of 17 November 2022, *Spetsializirana prokuratura (Retention of traffic and location data)*, C-350/21, EU:C:2022:896, paragraph 70 and the case-law cited).

121 By contrast, national legal rules which exclude as a general rule any right to obtain such information are not consistent with EU law (see, to that effect, judgment of 17 November 2022, *Spetsializirana prokuratura (Retention of traffic and location data)*, C-350/21, EU:C:2022:896, paragraph 71).

122 In the present case, it is apparent from the order for reference that CG knew that his mobile telephone had been seized when the Austrian police attempted in vain to unlock it in order to access the data contained therein. In those circumstances, it does not appear that informing CG of the fact that those authorities were going to attempt to access those data was liable to prejudice the investigations; accordingly, he should have been informed of those attempts beforehand.

123 It follows from the foregoing that the answer to the third question is that Articles 13 and 54 of Directive 2016/680, read in the light of Article 47 and Article 52(1) of the Charter, must be interpreted as precluding national legal rules which authorise the competent authorities to attempt to access data contained in a mobile telephone without informing the data subject, within the framework of the applicable national procedural rules, of the grounds on which the authorisation to access such data, issued by a court or an independent administrative body, is based, once the communication of that information is no longer liable to jeopardise the tasks of those authorities under that directive.

Costs

124 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. **Articles 4(1)(c) 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, read in the light of Articles 7, 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union,**

   must be interpreted as not precluding national legal rules which afford the competent authorities the possibility to access data contained in a mobile telephone for the purposes of the prevention, investigation, detection and prosecution of criminal offences in general, provided those rules:

   – **define with sufficient precision the nature or categories of offences concerned,**

   – **ensure respect for the principle of proportionality, and**

   – **make reliance on that possibility, except in duly justified cases of urgency, subject to prior review by a judge or an independent administrative body.**

2. **Articles 13 and 54 of Directive 2016/680, read in the light of Article 47 and Article 52(1) of the Charter of Fundamental Rights,**

must be interpreted as precluding national legal rules which authorise the competent authorities to attempt to access data contained in a mobile telephone without informing the data subject, within the framework of the applicable national procedural rules, of the grounds on which the authorisation to access such data, issued by a court or an independent administrative body, is based, once the communication of that information is no longer liable to jeopardise the tasks of those authorities under that directive.

[Signatures]