



Reports of Cases

JUDGMENT OF THE COURT (Fifth Chamber)

16 November 2023*

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Directive (EU) 2016/680 – Article 17 – Exercise of the rights of the data subject through the supervisory authority – Verification of the lawfulness of the data processing – Article 17(3) – Obligation to provide the data subject with a minimum of information – Scope – Validity – Article 53 – Right to seek an effective judicial remedy against the supervisory authority – Concept of a ‘legally binding decision’ – Charter of Fundamental Rights of the European Union – Article 8(3) – Control by an independent authority – Article 47 – Right to effective judicial protection)

In Case C-333/22,

REQUEST for a preliminary ruling under Article 267 TFEU from the cour d’appel de Bruxelles (Court of Appeal, Brussels, Belgium), made by decision of 9 May 2022, received at the Court on 20 May 2022, in the proceedings

Ligue des droits humains ASBL,

BA

v

Organe de contrôle de l’information policière,

THE COURT (Fifth Chamber),

composed of E. Regan, President of the Chamber, Z. Csehi, M. Ilešič, I. Jarukaitis and D. Gratsias (Rapporteur), Judges,

Advocate General: L. Medina,

Registrar: M. Siekierzyńska, Administrator,

having regard to the written procedure and further to the hearing on 29 March 2023,

after considering the observations submitted on behalf of:

– Ligue des droits humains ASBL and BA, by C. Forget, avocate,

* Language of the case: French.

- the Organe de contrôle de l’information policière (OCIP), by J. Bosquet and J.-F. De Bock, advocaten,
- the Belgian Government, by P. Cottin, J.-C. Halleux, C. Pochet and A. Van Baelen, acting as Agents, and by N. Cariat, C. Fischer, B. Lombaert and J. Simba, avocats,
- the Czech Government, by O. Serdula, M. Smolek and J. Vláčil, acting as Agents,
- the French Government, by J. Illouz, acting as Agent,
- the European Parliament, by S. Alonso de León, O. Hrstková Šolcová, P. López-Carceller and M. Thibault, acting as Agents,
- the European Commission, by A. Bouchagiar, H. Kranenborg, A.-C. Simon and F. Wilman, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 15 June 2023,

gives the following

Judgment

- 1 This request for a preliminary ruling concerns, first, the interpretation of Article 8(3) and Article 47 of the Charter of Fundamental Rights of the European Union (‘the Charter’) and, secondly, the validity, in the light of the abovementioned provisions of the Charter, of Article 17 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 Ligue des droits humains ASBL and BA, on the one hand, and, on the other, the Organe de contrôle de l’information policière (OCIP) (Supervisory Body for Police Information (OCIP), Belgium) regarding the exercise, through that body, of BA’s rights relating to the personal data concerning him, processed by the Belgian police service and on the basis of which the Autorité nationale de sécurité (National Security Authority, Belgium) rejected a request for security clearance made by BA.

Legal context

European Union law

- 3 Recitals 7, 10, 43, 46, 48, 75, 82, 85 and 86 of Directive 2016/680 state:
 - ‘(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 Member 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 [European] 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.

...

- (43) A natural person should have the right of access to data which [have] been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. ...

...

- (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 at Rome on 4 November 1950], as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively, and in particular respect the essence of those rights and freedoms.

...

- (48) Where the controller denies a data subject his or her right to information, access to or rectification or erasure of personal data or restriction of processing, the data subject should have the right to request that the national supervisory authority verify the lawfulness of the processing. ...

...

- (75) The establishment in Member States of supervisory authorities that are able to exercise their functions with complete independence is an essential component of the protection of natural persons with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this Directive and should contribute to their consistent application throughout the Union in order to protect natural persons with regard to the processing of their personal data. ...

...

(82) In order to ensure effective, reliable and consistent monitoring of compliance with and enforcement of this Directive throughout the Union pursuant to the TFEU as interpreted by the Court of Justice, the supervisory authorities should have in each Member State the same tasks and effective powers, including investigative, corrective, and advisory powers which constitute necessary means to perform their tasks. ...

...

(85) Every data subject should have the right to lodge a complaint with a single supervisory authority and to an effective judicial remedy in accordance with Article 47 of the Charter where the data subject considers that his or her rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. ...

(86) Each natural or legal person should have the right to an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, that right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with Member State law. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.’

4 Article 1 of that directive, headed ‘Subject matter and objectives’, provides, in paragraphs 1 and 2 thereof:

‘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.’

5 That directive contains a Chapter III, entitled ‘Rights of the data subject’, which includes, inter alia, Articles 13 to 17 of the directive. Article 13 thereof, entitled ‘Information to be made available or given to the data subject’, sets out, in paragraph 1 thereof, the obligation for the Member States to provide that the controller must make available to the data subject a minimum degree of information, such as, inter alia, the identity and contact details of the controller. In

addition, it lists, in paragraph 2 thereof, the additional information that the Member States must, by law, require the controller to provide to the data subject in order to enable the exercise of his or her rights. In paragraphs 3 and 4 thereof, it states:

‘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.

4. Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under any of the points listed in paragraph 3.’

6 Article 14 of that directive, headed ‘Right of access by the data subject’, is worded as follows:

‘Subject to Article 15, Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data ...’

7 Under Article 15 of Directive 2016/680, entitled ‘Limitations to the right of access’:

‘1. Member States may adopt legislative measures restricting, wholly or partly, the data subject’s right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and 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.

2. Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under points (a) to (e) of paragraph 1.

3. In the cases referred to in paragraphs 1 and 2, Member States shall provide for the controller to inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under paragraph 1. Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.
4. Member States shall provide for the controller to document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.'
- 8 Article 16 of that directive, entitled 'Right to rectification or erasure of personal data and restriction of processing', provides:
- '1. Member States shall provide for the right of the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data relating to him or her. Taking into account the purposes of the processing, Member States shall provide for the data subject to have the right to have incomplete personal data completed, ...
2. Member States shall require the controller to erase personal data without undue delay and provide for the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay where processing infringes the provisions adopted pursuant to Article 4, 8 or 10, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject.
3. Instead of erasure, the controller shall restrict processing where:
- (a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or
- (b) the personal data must be maintained for the purposes of evidence.
- ...
4. Member States shall provide for the controller to inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. Member States may adopt legislative measures restricting, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and 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.

Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

...'

9 Article 17 of that directive, entitled 'Exercise of rights by the data subject and verification by the supervisory authority', provides:

'1. In the cases referred to in Article 13(3), Article 15(3) and Article 16(4) Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority.

2. Member States shall provide for the controller to inform the data subject of the possibility of exercising his or her rights through the supervisory authority pursuant to paragraph 1.

3. Where the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.'

10 Article 42 of that directive, entitled 'Independence', provides, in paragraph 1 thereof:

'Each Member State shall provide for each supervisory authority to act with complete independence in performing its tasks and exercising its powers in accordance with this Directive.'

11 Article 46 of Directive 2016/680, entitled 'Tasks', provides, in paragraph 1 thereof:

'Each Member State shall provide, on its territory, for each supervisory authority to:

(a) monitor and enforce the application of the provisions adopted pursuant to this Directive and its implementing measures;

...

(f) deal with complaints lodged by a data subject, ... and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, ...

(g) check the lawfulness of processing pursuant to Article 17, and inform the data subject within a reasonable period of the outcome of the check pursuant to paragraph 3 of that Article or of the reasons why the check has not been carried out;

...'

12 Under Article 47 of that directive, entitled 'Powers':

'1. Each Member State shall provide by law for each supervisory authority to have effective investigative powers. Those powers shall include at least the power to obtain from the controller

and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks.

2. Each Member State shall provide by law for each supervisory authority to have effective corrective powers such as, for example:

- (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions adopted pursuant to this Directive;
- (b) to order the controller or processor to bring processing operations into compliance with the provisions adopted pursuant to this Directive, where appropriate, in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data or restriction of processing pursuant to Article 16;
- (c) to impose a temporary or definitive limitation, including a ban, on processing.

...

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, as set out in Union and Member State law in accordance with the Charter.

...'

- 13 Article 52 of that directive, entitled 'Right to lodge a complaint with a supervisory authority', provides, in paragraph 1 thereof:

'Without prejudice to any other administrative or judicial remedy, Member States shall provide for every data subject to have the right to lodge a complaint with a single supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes provisions adopted pursuant to this Directive.'

- 14 Article 53 of that directive, entitled 'Right to an effective judicial remedy against a supervisory authority', states, in paragraph 1 thereof:

'Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.'

- 15 Article 54 of Directive 2016/680, entitled 'Right to an effective judicial remedy against a controller or processor', is worded as follows:

'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.'

Belgian law

16 The loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (Law on the protection of natural persons with regard to the processing of personal data) of 30 July 2018 (*Moniteur belge*, 5 September 2018, p. 68616) ('the LPD') transposes, in Title 2 thereof, Directive 2016/680. The rights set out in Articles 13 to 16 of that directive are provided for in Chapter III of that title, specifically in Articles 37 to 39 of that law.

17 Article 42 of the LPD provides:

'Any request to exercise the rights set out in this chapter with respect to the police services ... or to the Inspection générale de la police fédérale et de la police locale [(General Inspectorate of the Federal and Local Police, Belgium)] shall be made to the supervisory authority referred to in Article 71.

In the cases referred to in Articles 37(2), 38(2) [and] 39(4) ..., the supervisory authority referred to in Article 71 shall inform the data subject only that the necessary verifications have been carried out.

Notwithstanding paragraph 2, the supervisory authority referred to in Article 71 may communicate certain contextual information to the data subject.

The King shall determine, following opinion from the supervisory authority referred to in Article 71, the category of contextual information that may be communicated to the data subject by that authority.'

18 According to the cour d'appel de Bruxelles (Court of Appeal, Brussels, Belgium), the referring court, no Royal Decree has been adopted in order to implement the fourth paragraph of Article 42 of the LPD.

19 Under Article 71(1) of the LPD:

An independent supervisory authority for police information is hereby created at the Chamber of Representatives, under the name [Supervisory Body for Police Information].

...

[It shall be] responsible for:

1. supervising the application of this Title ...

2. monitoring the processing of the information and personal data covered by Articles 44/1 to 44/11/13 of the loi du 5 août 1992 sur la fonction de police (Law of 5 August 1992 on the police service), including that held in the data banks referred to in Article 44/2 of that law;

3. any other task organised by or under other laws.'

20 Chapter I of Title 5 of the LPD is entitled 'Action for an injunction'. Article 209, which is contained in that chapter, reads as follows:

'Without prejudice to any other judicial, administrative or extra-judicial remedy, the president of the court of first instance, sitting as if hearing interim proceedings, may determine that processing has been carried out which constitutes a breach of the statutory or regulatory provisions on the

protection of natural persons with regard to the processing of their personal data, and grant an injunction prohibiting such processing.

The president of the court of first instance, sitting as if hearing interim proceedings, shall hear any application relating to the right granted by or by virtue of the law to obtain access to personal data, as well as any application seeking rectification, erasure or prevention of the use of any personal data which are inaccurate or, having regard to the purpose of the processing, incomplete or irrelevant, or of which the recording, disclosure or storage is prohibited, to the processing of which the data subject has objected or which have been retained for longer than is permitted.'

21 Article 240(4) of the LPD provides that:

‘[The OCIP]

...

4. shall deal with complaints, investigate the subject matter of the complaint so far as necessary, and inform the complainant of the progress and the outcome of the investigation within a reasonable time, particularly where further investigation or cooperation with another supervisory authority is necessary. ...’

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

22 In 2016, BA, who at that time was employed on a part-time basis with a charity, sought security clearance from the National Security Authority in order to participate in the assembly and disassembly of the installations for the tenth ‘European Development Days’ event in Brussels (Belgium).

23 By letter of 22 June 2016, that authority refused BA security clearance, on the ground that it was apparent from the personal data which had been made available to it that that person had participated in 10 demonstrations between 2007 and 2016 and that such factors prevented him from being granted such clearance under the rules applicable, inter alia for reasons of State security and preservation of the constitutional democratic order. No appeal was brought against that decision.

24 On 4 February 2020, BA’s legal adviser requested the OCIP to identify the controllers responsible for processing the personal data at issue and to order them to provide his client with access to all the information concerning him in order to enable him to exercise his rights within an appropriate period.

25 By email of 6 February 2020, the OCIP acknowledged receipt of that request. It indicated that BA only had an indirect right of access to those data, while also stating that it was itself going to verify the lawfulness of any data processing in the Banque de données nationale générale (General National Data Bank), namely the database used by all the national police services. It also stated that it had the power to order the police to erase or amend data, if necessary, and that once the checks had been completed, it would inform BA that the necessary verifications have been carried out.

26 By email of 22 June 2020, the OCIP stated as follows to BA’s legal adviser:

‘…

I inform you, in accordance with Article 42 of [the LPD], that the [OCIP] has carried out the necessary verifications.

This means that your client’s personal data have been checked against the police data banks with a view to ensuring the lawfulness of any processing.

If necessary, the personal data have been amended or erased.

As I informed you in my email of 2 June, Article 42 of the LPD does not permit the [OCIP] to provide any further information.’

27 On 2 September 2020, Ligue des droits humains and BA, on the basis of the second paragraph of Article 209 of the LPD, submitted an application for interim relief before the tribunal de première instance francophone de Bruxelles (Brussels Court of First Instance (French-speaking), Belgium).

28 In the first place, the applicants in the main proceedings requested that court to declare the application for interim relief admissible, and, in the alternative, to refer a question to the Court of Justice on whether, in essence, Article 47(4) of Directive 2016/680, read in the light of recitals 85 and 86 of that directive and in conjunction with Article 8(3) and Article 47 of the Charter, precluded Articles 42 and 71 of the LPD, inasmuch as those provisions did not provide for any judicial remedy against decisions taken by the OCIP.

29 In the second place, as to the substance, they requested access to all personal data concerning BA, through the OCIP, and the identification, by the latter, of the controllers and any recipients of those data.

30 In the event that the court seized were to hold that Article 42(2) of the LPD allowed access to the personal data processed by the police services to be systematically restricted, they requested, in the alternative, that a question be referred to the Court of Justice concerning, in essence, whether Articles 14, 15 and 17 of Directive 2016/680, read in conjunction with Articles 8 and 47 and Article 52(1) of the Charter, were to be interpreted as precluding national legislation allowing a general and systematic derogation from the right of access to personal data where, first, that right was exercised through the supervisory authority and, secondly, that authority could merely state to the data subject that it had carried out all the necessary verifications without informing him or her of the personal data being processed and of the recipients, irrespective of the intended purpose.

31 By order of 17 May 2021, the tribunal de première instance francophone de Bruxelles (Brussels Court of First Instance (French-speaking)) declared that it had ‘no jurisdiction’ to hear and determine that application for interim relief.

32 On 15 June 2021, the applicants in the main proceedings brought an appeal against that order before the cour d’appel de Bruxelles (Court of Appeal, Brussels), the referring court. In essence, they reiterated the requests they had made at first instance.

- 33 In that context, the referring court observes, *inter alia*, in essence that, in the event that a person does not have the right to exercise in person the rights provided for by Directive 2016/680, the action for an injunction provided for in Article 209 et seq. of the LPD cannot be put into effect. First, such an action can be brought against the controller, but not against the supervisory authority itself. Secondly, nor can it be exercised by that person, in the present case, BA, against the controller, since the exercise of that person's rights is entrusted to that authority. Lastly, the very succinct information provided by the OCIP to BA does not enable either BA or a court to determine whether that supervisory authority has exercised BA's rights correctly. It adds that, although the LPD provides that that action for an injunction is without prejudice to any other judicial, administrative or extra-judicial remedy, any other such remedy sought by BA would encounter the same problems.
- 34 In those circumstances, the *cour d'appel de Bruxelles* (Court of Appeal, Brussels) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:
- '(1) Do Articles 47 and 8(3) of [the Charter] require provision to be made for a judicial remedy against an independent supervisory authority such as the [OCIP] where it exercises the rights of the data subject *vis-à-vis* the controller?
- (2) Does Article 17 of Directive 2016/680 comply with Articles 47 and 8(3) of [the Charter], as interpreted by the Court of Justice, in that it obliges the supervisory authority – which exercises the rights of the data subject *vis-à-vis* the controller – only to inform the data subject “that all necessary verifications or a review by the supervisory authority have taken place” and “of his or her right to seek a judicial remedy”, when such information does not enable any *a posteriori* review to be conducted as regards the action taken and assessment made by the supervisory authority in the light of the data of the data subject and the obligations of the controller?'

Consideration of the questions referred

The first question

- 35 As a preliminary point, it is apparent from the request for a preliminary ruling that the questions of the referring court concern the existence, on the basis of Article 53(1) of Directive 2016/680, read in the light of Article 47 of the Charter, of an obligation for the Member States to provide for a right to an effective judicial remedy against the competent national supervisory authority, when a provision of national law is implemented which transposes Article 17 of that directive, according to which, in the cases covered by Article 13(3), Article 15(3) and Article 16(4) of that directive, the rights of the data subject may be exercised through such a supervisory authority.
- 36 In addition, it must be observed that the answer to that question is dependent on the nature and scope of the task and powers of the supervisory authority in connection with the exercise of the data subject's rights, provided for in Article 17 of Directive 2016/680. That task and those powers are set out in Article 46(1)(g) and Article 47(1) and (2) of that directive and must be analysed in the light of Article 8(3) of the Charter, which requires that compliance with the rules on the protection of personal data, set out in paragraphs 1 and 2 of Article 8 thereof, is to be subject to control by an independent authority.

- 37 Therefore, the referring court must be understood as asking, in essence, by its first question, whether Article 17 of Directive 2016/680, read in conjunction with Article 46(1)(g), Article 47(1) and (2) and Article 53(1) of that directive, and with Article 8(3) and Article 47 of the Charter, must be interpreted as meaning that, where the rights of a data subject have been exercised, pursuant to Article 17 of that directive, through the competent supervisory authority, that data subject must have available to him or her an effective judicial remedy against that authority.
- 38 It must be recalled at the outset that, under Article 53(1) of Directive 2016/680, Member States must provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.
- 39 It must therefore be determined whether a supervisory authority adopts such a decision where, pursuant to Article 17 of that directive, the rights of the data subject set out by that directive are exercised through that supervisory authority.
- 40 In this connection, under Article 17(1) of Directive 2016/680, ‘in the cases referred to in Article 13(3), Article 15(3) and Article 16(4)’ of that directive, Member States are under an obligation to adopt measures ‘providing that the rights of the data subject may also be exercised through the competent supervisory authority’.
- 41 As indicated by the use of the adverb ‘also’ and as the Advocate General in essence observed in points 41 and 42 of her Opinion, the indirect exercise of the rights of the data subject through the competent supervisory authority, provided for in that provision, is an additional guarantee offered to that data subject that his or her personal data are processed lawfully, where national legislative provisions limit the direct exercise before the controller of the right to receive further information, referred to in Article 13(2) of Directive 2016/680, the right of access to those data, set out in Article 14 of that directive, or of the right to obtain their rectification, erasure or a restriction of processing under the conditions of Article 16(1) to (3) of that directive.
- 42 Having regard to the specific nature of the purposes for which the data processing covered by that directive is carried out, to which attention is drawn, in particular, in recital 10 thereof, Article 13(3) and Article 15(1) of Directive 2016/680 authorise the national legislature to limit the direct exercise, on the one hand, of the right to information, and, on the other hand, of the right of access, ‘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’, in order to ‘avoid obstructing official or legal inquiries, investigations or procedures’, ‘avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties’, ‘protect public security’, ‘protect national security’ or ‘protect the rights and freedoms of others’. In addition, Article 15(3) of that directive provides that the controller may omit to inform the data subject of any refusal or restriction of access and of the reasons for the refusal or the restriction where the provision of that information would undermine one of the abovementioned public interest purposes.
- 43 Likewise, Article 16(4) of that directive authorises the national legislature to restrict the obligation on the controller to ‘inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal’ for the same public interest purposes, ‘to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned’.

- 44 Therefore, in that context, as is apparent from recital 48 of that directive, the indirect exercise of the rights referred to in paragraph 41 above through the competent supervisory authority must be regarded as necessary for the protection of those rights, their direct exercise before the controller being difficult or even impossible.
- 45 To that end, Article 46(1)(g) of Directive 2016/680 requires that each competent national authority must be entrusted with the task of checking the lawfulness of processing pursuant to Article 17 of that directive, that is to say following a request made on the basis of the latter provision.
- 46 Moreover, it is apparent, *inter alia*, from Article 47(1) and (2) of that directive that each supervisory authority must have, under the national legislation, not only ‘effective investigative powers’ but also ‘effective corrective powers’.
- 47 Those provisions must be read in the light of the requirement stated in Article 8(3) of the Charter, that compliance with the rules on the right of everyone to the protection of personal data, set out in paragraphs 1 and 2 of that article, must be ‘subject to control by an independent authority’, and, in particular, the requirement set out in the second sentence of paragraph 2 thereof, that ‘everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified’. As is confirmed by settled case-law, the establishment of an independent supervisory authority is intended to ensure the effectiveness and reliability of the monitoring of compliance with the rules concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim (see, to that effect, Opinion 1/15 (*EU-Canada PNR Agreement*) of 26 July 2017, EU:C:2017:592, paragraph 229 and the case-law cited).
- 48 Thus, where such a supervisory authority acts in order to ensure the exercise of the rights of the data subject on the basis of Article 17 of Directive 2016/680, its task falls entirely within the definition, in EU primary law, of its role, since that definition entails, *inter alia*, the monitoring of compliance with the data subject’s rights of access and of rectification. It follows that, in accomplishing that specific task, as with any other task, the supervisory authority must be able to exercise the powers which are conferred on it under Article 47 of that directive by acting with complete independence, in accordance with the Charter and as stated in recital 75 of that directive.
- 49 In addition, at the end of the verification of the lawfulness of processing, the competent supervisory authority must, under the first sentence of Article 17(3) of that directive, inform the data subject ‘at least that all necessary verifications or a review by the supervisory authority have taken place’.
- 50 As observed, in essence, by the Advocate General in point 65 of her Opinion, it must be inferred from all those provisions that, when the competent supervisory authority informs the data subject of the result of the verifications made, it brings to his or her knowledge the decision it has made in his or her regard to close the verification process, that decision necessarily affecting the legal position of the data subject. That decision therefore constitutes a ‘legally binding decision’ with regard to the data subject, within the meaning of Article 53(1) of Directive 2016/680, irrespective of whether and to what extent that authority has found the processing of the data concerning that subject to be lawful or adopted corrective measures.

- 51 Indeed, recital 86 of that directive states that the concept of ‘legally binding decision’ within the meaning of that directive must be understood as referring to a decision which produces legal effects concerning the data subject, in particular, a decision concerning the exercise of investigative, corrective and authorisation powers by the supervisory authority or concerning the dismissal or rejection of complaints.
- 52 Therefore, the data subject must be able to obtain judicial review of the merits of such a decision on the basis of Article 53(1) of Directive 2016/680, and, in particular, of the manner in which the supervisory authority performed its obligation, resulting from Article 17 of that directive and to which Article 46(1)(g) of that directive refers, to carry out ‘all necessary verifications’ and, as the case may be, exercised its corrective powers.
- 53 That conclusion is, moreover, borne out by recital 85 of Directive 2016/680, from which it is apparent that any data subject should have the right to an effective judicial remedy against a supervisory authority where that authority ‘does not act where such action is necessary to protect the rights of the data subject’.
- 54 Lastly, such an interpretation is in accordance with Article 47 of the Charter, since, as is apparent from settled case-law, that right must be accorded to any person relying on rights or freedoms guaranteed by EU law against a decision adversely affecting him or her which is such as to undermine those rights or freedoms (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 87 and the case-law cited).
- 55 Having regard to all the foregoing considerations, the answer to the first question is that Article 17 of Directive 2016/680, read in conjunction with Article 46(1)(g), Article 47(1) and (2) and Article 53(1) of that directive, and with Article 8(3) and Article 47 of the Charter, must be interpreted as meaning that where the rights of a data subject have been exercised, pursuant to Article 17 of that directive, through the competent supervisory authority and that authority informs that data subject of the result of the verifications carried out, that data subject must have an effective judicial remedy against the decision of that authority to close the verification process.

The second question

- 56 By its second question, the referring court asks, in essence, whether Article 17(3) of Directive 2016/680 is valid having regard to Article 8(3) and Article 47 of the Charter in so far as it obliges the supervisory authority only to inform the data subject (i) that all necessary verifications or a review by the supervisory authority have taken place and (ii) that that person has a right to seek a judicial remedy, since such information does not allow any judicial review of the action taken and the assessment made by the supervisory authority, in the light of the data processed and of the obligations of the controller.
- 57 First, it should be noted in this respect that, in accordance with a general principle of interpretation, an EU act must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter. Thus, if the wording of secondary EU legislation is open to more than one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with primary law (judgment of 21 June 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, paragraph 86 and the case-law cited).

- 58 Secondly, 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 (see, to that effect, judgment of 4 June 2013, ZZ, C-300/11, EU:C:2013:363, paragraph 53 and the case-law cited).
- 59 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 26 January 2023, *Ministerstvo na vatreshnite raboti (Recording of biometric and genetic data by the police)*, C-205/21, EU:C:2023:49, paragraph 89 and the case-law cited).
- 60 In the present case, it must be observed that, so far as concerns the decision of the competent supervisory authority identified in paragraph 50 above, Article 17(3) of Directive 2016/680 establishes, with respect to that supervisory authority, an obligation to provide a minimum of information, providing that it is to inform the data subject ‘at least that all necessary verifications or a review by the supervisory authority have taken place’ and of ‘his or her right to seek a judicial remedy’.
- 61 It follows that, since that provision does not preclude, in certain situations, in accordance with the rules adopted by the national legislature to implement it, the supervisory authority from being able, or even obliged, to confine itself to providing the minimum information referred to in the preceding paragraph, without any other details, in particular where those rules seek to avoid compromising the public interest purposes provided for in Article 13(3), Article 15(1) and Article 16(4) of that directive, as set out in paragraphs 42 and 43 above, it is liable to give rise to a limitation on the right to an effective judicial remedy, guaranteed in Article 47 of the Charter.
- 62 That said, in the first place, it must be noted that such a limitation is expressly provided for by Directive 2016/680 and that it therefore complies with the condition laid down in Article 52(1) of the Charter, according to which any limitation on the exercise of a fundamental right must be ‘provided for by law’.
- 63 In the second place, the fact that Article 17(3) of Directive 2016/680 allows Member States to restrict, in certain cases, the statement of reasons for that decision to the minimum particulars set out in that provision, does not mean, as the Advocate General in essence states in point 89 of her Opinion, that it is possible in all circumstances to reduce the information provided to the data subject to solely those particulars.
- 64 That provision must be interpreted in the light of Article 52(1) of the Charter, so that the other criteria set out in that latter provision must be satisfied. That means holding that Article 17(3) of that directive requires Member States to ensure that the provisions of national law implementing it, first, respect the essence of the data subject’s right to effective judicial protection and, secondly, are based on a weighing up of the public interest purposes warranting limitation of that information and of the fundamental rights and legitimate interests of that data subject, in

accordance with the principles of necessity and of proportionality, like the weighing up which must be carried out by the national legislature when it implements the limitations provided for in Article 13(3), Article 15(3) and Article 16(4) of that directive.

- 65 In particular, where (i) it is required by the protection of the right of the data subject to an effective judicial remedy against the decision to close the verification process and (ii) it is not precluded by the public interest purposes referred to in Article 13(3), Article 15(3) and Article 16(4) of Directive 2016/680, the onus is on the Member States to provide that the information disclosed to the data subject may go beyond the minimum information provided for by Article 17(3) of that directive, so as to make it possible for him or her to defend his or her rights and to decide, with full knowledge of the facts, whether there is any point in him or her applying to the court with jurisdiction.
- 66 Likewise, the national measures implementing that latter provision must, to the extent possible, leave a degree of discretion to the competent supervisory authority, in accordance with the independence characterising such an authority under Article 8(3) of the Charter, to determine whether the framework established by the national legislation in line with the requirements noted in paragraph 65 above precludes it from communicating to that data subject, at least in brief, the result of its verifications and any corrective measures which it has taken. In this connection, as the Advocate General observed, in essence, in points 73 and 74 of her Opinion, it is for that authority, in compliance with that national legislative framework, to engage in a confidential dialogue with the controller and, at the end of that dialogue, to decide on which information is necessary for the data subject to exercise his or her right to an effective judicial remedy and may be communicated to him or her without compromising the public interest purposes referred to in paragraph 65 above.
- 67 Moreover, should that framework require that the information provided by the supervisory authority be limited to that provided for in Article 17(3) of Directive 2016/680, it is nevertheless for the Member States, in the exercise of their procedural autonomy, to implement the measures necessary to guarantee, in accordance with Article 53(1) of that directive, an effective judicial review both of the existence and of the merits of the reasons which warranted the limitation on that information and of the correct execution, by the supervisory authority, of its task of verifying the lawfulness of the processing. In that regard, the concept of ‘effective judicial remedy’ referred to in the latter provision must be read in the light of recital 86 of that directive, under which the courts before which actions against a supervisory authority are brought ‘should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it’.
- 68 In particular, Member States must ensure that the court with jurisdiction has at its disposal and applies techniques and rules of procedural law which accommodate, on the one hand, legitimate considerations in relation to the public interest purposes referred to in Article 13(3), Article 15(3) and Article 16(4) of Directive 2016/680, those purposes having been taken into consideration by the national legislation to limit the information provided to the data subject and, on the other hand, the need to ensure sufficient compliance with the data subject’s procedural rights, such as the right to be heard and the adversarial principle (see, to that effect, judgment of 4 June 2013, ZZ, C-300/11, EU:C:2013:363, paragraph 57 and the case-law cited).
- 69 In the context of the judicial review of the correct application of Article 17 of that directive by the supervisory authority, it is incumbent upon the Member States to lay down rules enabling the court with jurisdiction to examine both all the grounds and the related evidence on the basis of

which that authority based, within that framework, the verification of the lawfulness of the processing of the data at issue as well as the conclusions which it drew from that verification (see, to that effect, judgment of 4 June 2013, ZZ, C-300/11, EU:C:2013:363, paragraph 59 and the case-law cited).

- 70 In that regard, as the European Parliament noted in its observations, Article 15(4) of Directive 2016/680 provides that the controller must document the factual or legal reasons on which it has based the decision by which it limited, wholly or partly, the rights of access of the data subject and that that information must be made available to the supervisory authorities. As that institution suggested, that provision, read in conjunction with Articles 17 and 53 of that directive and in the light of Article 47 of the Charter, as interpreted by the case-law recalled in paragraphs 68 and 69 above, implies that that information must also be made available to the court before which an action against the supervisory authority has been brought, seeking review of the correct application of Article 17 of that directive.
- 71 Thus, it is apparent from paragraphs 63 to 70 above that the limitation provided for in Article 17 of Directive 2016/680 respects the essence of the data subject's right to an effective judicial remedy against the supervisory authority's decision to close the procedure provided for in that provision and the principles of necessity and proportionality, in accordance with Article 52(1) of the Charter.
- 72 Having regard to all the foregoing considerations, it must be concluded that the examination of the second question has revealed nothing capable of affecting the validity of Article 17(3) of Directive 2016/680.

Costs

- 73 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. Article 17 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 conjunction with Article 46(1)(g), Article 47(1) and (2) and Article 53(1) of that directive and with Article 8(3) and Article 47 of the Charter of Fundamental Rights of the European Union,**

must be interpreted as meaning that where the rights of a data subject have been exercised, pursuant to Article 17 of that directive, through the competent supervisory authority and that authority informs that data subject of the result of the verifications carried out, that data subject must have an effective judicial remedy against the decision of that authority to close the verification process.

2. The examination of the second question has revealed nothing capable of affecting the validity of Article 17(3) of Directive 2016/680.

[Signatures]