

Provisional text

JUDGMENT OF THE COURT (Third Chamber)

11 December 2019 (*)

(Reference for a preliminary ruling — Protection of individuals with regard to the processing of personal data — Charter of Fundamental Rights of the European Union — Articles 7 and 8 — Directive 95/46/EC — Article 6(1)(c) and Article 7(f) — Making the processing of personal data legitimate — National legislation allowing video surveillance for the purposes of ensuring the safety and protection of individuals, property and valuables and for the pursuit of legitimate interests, without the data subject's consent — Installation of a video surveillance system in the common parts of a residential building)

In Case C-708/18,

REQUEST for a preliminary ruling under Article 267 TFEU from Tribunalul București (Regional Court, Bucharest, Romania), made by decision of 2 October 2018, received at the Court on 6 November 2018, in the proceedings

TK

v

Asociația de Proprietari bloc M5A-ScaraA,

THE COURT (Third Chamber),

composed of A. Prechal (Rapporteur), President of the Chamber, L.S. Rossi, J. Malenovský, F. Biltgen and N. Wahl, Judges,

Advocate General: G. Pitruzzella,

Registrar: A. Calot Escobar,

having regard to the written procedure,

after considering the observations submitted on behalf of:

- the Romanian Government, by C.-R. Canțăr, O.-C. Ichim and A. Wellman, acting as Agents,
- the Czech Government, by M. Smolek, J. Vláčil and O. Serdula, acting as Agents,
- the Danish Government, by J. Nymann-Lindegren, M. Wolff and P.Z.L. Ngo, acting as Agents,
- Ireland, by M. Browne, G. Hodge and A. Joyce, acting as Agents, and by D. Fenelly, Barrister-at-Law,
- the Austrian Government, initially by G. Hesse and J. Schmoll, and subsequently by J. Schmoll, acting as Agents,
- the Portuguese Government, by L. Inez Fernandes, P. Barros da Costa, L. Medeiros, I. Oliveira and M. Cancela Carvalho, acting as Agents,

– the European Commission, by H. Kranenborg, D. Nardi and L. Nicolae, acting as Agents, having decided, after hearing the Advocate General, to proceed to judgment without an Opinion, gives the following

Judgment

- 1 This request for a preliminary ruling concerns the interpretation of Article 6(1)(e) and Article 7(f) 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), and of Articles 8 and 52 of the Charter of Fundamental Rights of the European Union (‘the Charter’).
- 2 The request has been made in proceedings between TK and the Asociația de Proprietari bloc M5A-ScaraA (Association of co-owners of building M5A, staircase A, ‘the association of co-owners’) concerning TK’s application for an order that the association take out of operation the building’s video surveillance system and remove the cameras installed in the common parts of the building.

Legal context

EU law

- 3 Directive 95/46 was repealed and replaced, with effect from 25 May 2018, by 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 (OJ 2016 L 119, p. 1). However, given the date of the facts at issue in the main proceedings, those proceedings remain governed by Directive 95/46.
- 4 According to Article 1 thereof, Directive 95/46 seeks to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and to remove the obstacles to flows of those data.
- 5 Article 3(1) of that directive provided:

‘This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.’
- 6 Chapter II of that directive included Section I, entitled ‘Principles relating to Data Quality’, comprising Article 6 of the directive, which provided:
 - ‘1. Member States shall provide that personal data must be:
 - (a) processed fairly and lawfully;
 - (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
 - (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
 - (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
2. It shall be for the controller to ensure that paragraph 1 is complied with’.

7 In Section II of Chapter II, entitled ‘Criteria for Making Data Processing Legitimate’, Article 7 of Directive 95/46 was worded as follows:

‘Member States shall provide that personal data may be processed only if:

- (a) the data subject has unambiguously given his consent;
- or
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- or
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- or
- (d) processing is necessary in order to protect the vital interests of the data subject;
- or
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;
- or
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).’

Romanian law

8 Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Law No 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) (*Monitorul Oficial*, Part I, No 790 of 12 December 2001), as amended by Law No 102/2005 and Government Emergency Order No 36/2007, applicable *ratione temporis* to the main proceedings, was adopted in order to transpose Directive 95/46 into Romanian law.

9 Article 5 of Law No 667/2001 as amended provided:

‘1. Any personal data processing, except for the processing which refers to the categories mentioned in Article 7(1) and Articles 8 and 10, may be carried out only if the data subject has given his or her express and unequivocal consent for that processing.

2. The data subject’s consent is not required in the following situations:

- (a) when the processing is required in order to carry out a contract or an agreement previous to that contract to which the data subject is a party, or in order to adopt measures, at his or her request, before the signing of the contract or previous agreement;
- (b) when the processing is required in order to protect the data subject’s life, physical integrity or health or those of a threatened third party;
- (c) when the processing is required in order to fulfil a legal obligation of the data controller;
- (d) when the processing is required in order to accomplish a measure of public interest or concerning the exercise of public powers of the data controller or the third party to whom the data are disclosed;
- (e) when the processing is necessary in order to accomplish a legitimate interest of the data controller or of the third party to whom the data are disclosed, on the condition that that interest does not adversely affect the interests or the fundamental rights and freedoms of the data subject;
- (f) when the processing concerns data which is obtained from publicly accessible documents, according to the law;
- (g) when the processing is performed exclusively for statistical purposes, historical or scientific research and the data remain anonymous throughout the entire processing.

3. The provisions of paragraph 2 are without prejudice to the legal texts governing the obligations of public authorities to respect and protect personal, family and private life.’

10 Decision No 52/2012 of the Autoritate Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (the National Authority for the Supervision of the Processing of Personal Data, Romania, ‘the ANSPDCP’) concerning the processing of personal data through the use of video surveillance systems, in the version applicable to the main proceedings, provided, in Article 1 thereof:

‘The collection, recording, storage, use, transmission, disclosure or any other operation for the processing of images by video surveillance means, which enable individuals to be identified directly or indirectly, constitute the processing of personal data falling within the scope of [Law No 677/2001].’

11 Article 4 of that decision provided:

‘Video surveillance may primarily be carried out for the following purposes:

- (a) the prevention and countering of crime;
- (b) road-traffic surveillance and the detection of road-traffic offences;
- (c) the safety and protection of persons, property and assets, and buildings and public facilities and their enclosures;
- (d) the implementation of public-interest measures or the exercise of public powers;
- (e) the pursuit of legitimate interests, provided that the rights and fundamental freedoms of data subjects are not adversely affected.’

12 Article 5(1) to (3) of that decision states:

- ‘1. Video surveillance may be carried out in open or public places and spaces, including on public-access roadways located on public or private land, subject to the conditions provided for by law.
2. Video surveillance cameras shall be installed so that they are visible.
3. The use of concealed video surveillance shall be prohibited, except in the cases provided for by law.’

13 Article 6 of that decision stated:

‘The processing of personal data using video surveillance means shall be carried out with the express and unequivocal consent of the data subject or in the cases referred to in Article 5(2) of Law No 677/2001’

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

14 TK lives in an apartment which he owns, located in the building M5A. At the request of certain co-owners of that building, the association of co-owners adopted, at a general assembly held on 7 April 2016, a decision approving the installation of video surveillance cameras in that building.

15 In implementation of that decision, three video surveillance cameras were installed in the common parts of the M5A building. The first camera was pointed towards the front of the building, whereas the second and third cameras were installed, respectively, in the ground-floor hallway and in the building’s lift.

16 TK objected to that video surveillance system being installed, on the ground that it constituted an infringement of the right to respect for private life.

17 Having found that, notwithstanding the numerous steps undertaken by him and the written acknowledgment of the association of co-owners that the video surveillance system installed was unlawful, that system continued to operate, TK brought an action before the referring court requesting that the association of co-owners be ordered to remove the three cameras and to take them out of operation definitively, failing which a penalty payment would be imposed.

18 TK argued before the referring court that the video surveillance system at issue infringed EU primary and secondary law, in particular the right to respect for private life both under EU and national law. He also stated that the association of co-owners had taken on the task of data controller for personal data without having followed the registration procedure in that regard provided for by law.

19 The association of co-owners stated that the decision to install a video surveillance system had been taken in order to monitor as effectively as possible who enters and leaves the building, since the lift had been vandalised on many occasions and there had been burglaries and thefts in several apartments and the common parts.

20 The association also stated that other measures which it had taken previously, namely the installation of an intercom/magnetic card entry system, had not prevented repeat offences of the same nature being committed.

21 In addition, the association of co-owners sent TK the memorandum which it had drawn up with the company which had installed the video surveillance cameras, stating that on 21 October 2016 the system’s hard drive had been erased and disconnected, that it had been taken out of operation and that the images recorded had been deleted.

22 The association also communicated to TK another memorandum, dated 18 May 2017 from which it is apparent that the three video surveillance cameras had been uninstalled. That memorandum stated that the

association of co-owners had, in the meantime, completed the procedure enabling it to be registered as data controller responsible for personal data.

23 TK stated, however, before the referring court that the three video surveillance cameras were still in place.

24 The referring court notes that Article 5 of Law No 677/2001 provides, in a general manner, that processing of personal data, such as the recording of images by means of a video surveillance system, may be carried out only if the data subject has given his or her express and unequivocal consent. Paragraph 2 of that article sets out, however, a series of exceptions to that rule, which include the exception whereby the processing of personal data is required in order to protect the data subject's life, physical integrity or health or those of a threatened third party. Decision No 52/2012 of the ANSPDCP provides for the same type of exception.

25 The referring court makes reference, next, to Article 52(1) of the Charter enshrining the principle that there must be proportionality between the aim pursued by the interference with the rights and freedoms of citizens and the means used.

26 According to that court, the video surveillance system at issue before it does not seem to have been used in a manner or for a purpose not corresponding to the stated objective of the association of co-owners, which is that of protecting the life, physical integrity or health of the data subjects, namely the co-owners of the building in which that system was installed.

27 In those circumstances Tribunalul București (Regional Court, Bucharest, Romania) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

‘(1) Are Articles 8 and 52 of the Charter and Article 7(f) of Directive 95/46 to be interpreted as precluding provisions of national law such as those at issue in the main proceedings, namely Article 5(2) of [Law No 677/2001], and Article 6 of [Decision No 52/2012 of the ANSPDCP], in accordance with which video surveillance may be used to ensure the safety and protection of individuals, property and valuables and for the pursuit of legitimate interests, without the data subject's consent?

(2) Are Articles 8 and 52 of the Charter to be interpreted as meaning that the limitation of rights and freedoms which results from video surveillance is in accordance with the principle of proportionality, satisfies the requirement of being ‘necessary’ and ‘meets objectives of general interest or the need to protect the rights and freedoms of others’, where the controller is able to take other measures to protect the legitimate interest in question?

(3) Is Article 7(f) of Directive 95/46 to be interpreted as meaning that the ‘legitimate interests’ of the controller must be proven, present and effective at the time of the data processing?

(4) Is Article 6(1)(e) of Directive 95/46 to be interpreted as meaning that data processing (video surveillance) is excessive or inappropriate where the controller is able to take other measures to protect the legitimate interest in question?’

Consideration of the questions referred

28 First of all, it must be found that although the referring court does, by its fourth question, refer to Article 6(1)(e) of Directive 95/46, it provides no explanation as to the relevance of that provision to the outcome of the dispute in the main proceedings.

29 Article 6(1)(e) relates only to the requirements governing the storage of personal data. Nothing in the documents before the Court permits the inference that the dispute in the main proceedings concerns that aspect.

- 30 By contrast, in so far as by that question the referring court asks, in essence, whether the installation of a video surveillance system, such as that at issue before it, is proportionate to the purposes pursued, it must be found that the issue of whether personal data collected by that system meet the requirement of proportionality relates to the interpretation of Article 6(1)(c) of Directive 95/46.
- 31 Article 6(1)(c) of Directive 95/46 must be taken into account when verifying the second condition of application laid down in Article 7(f) of Directive 95/46, according to which the processing of personal data is ‘necessary’ for the purposes of the legitimate interests pursued.
- 32 Secondly, by its first and second questions, Tribunalul București (Regional Court, Bucharest, Romania) refers to Articles 8 and 52 of the Charter, taken in isolation or read in conjunction with Article 7(f) of Directive 95/46. The Court has made clear that the assessment of the condition laid down in that provision, relating to the existence of fundamental rights and freedoms of the data subject which override the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, necessitates a balancing of the opposing rights and interests concerned which depends on the individual circumstances of the particular case in question, and in the context of which account must be taken of the significance of the data subject’s rights arising from Articles 7 and 8 of the Charter (judgment of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito*, C-468/10 and C-469/10, EU:C:2011:777, paragraph 40). It follows that Articles 8 and 52 of the Charter must not, in the present case, be applied in isolation.
- 33 In the light of the foregoing, it must be found that, by its questions, which must be examined together, the referring court asks, in essence, whether Article 6(1)(c) and Article 7(f) of Directive 95/46, read in the light of Articles 7 and 8 of the Charter, must be interpreted as precluding national provisions which authorise the installation of a system of video surveillance, such as the system at issue in the main proceedings, installed in the common parts of a residential building, for the purposes of pursuing legitimate interests of ensuring the safety and protection of individuals and property, without the data subject’s consent.
- 34 It must be borne in mind that surveillance in the form of a video recording of persons, which is stored on a continuous recording device — the hard disk drive — constitutes, pursuant to Article 3(1) of Directive 95/46, the automatic processing of personal data (judgment of 11 December 2014, *Ryneš*, C-212/13, EU:C:2014:2428, paragraph 25).
- 35 Consequently, a video surveillance system using a camera must be characterised as the automatic processing of personal data, within the meaning of that provision, where the device installed enables personal data, such as images allowing natural persons to be identified, to be recorded and stored. It is for the referring court to ascertain whether the system at issue in the main proceedings has such characteristics.
- 36 In addition, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of Directive 95/46 and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of that directive (judgment of 13 May 2014, *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 71 and the case-law cited).
- 37 Article 7 of Directive 95/46 sets out an exhaustive and restrictive list of the cases in which the processing of personal data can be regarded as being lawful. The Member States cannot add new principles relating to the lawfulness of the processing of personal data in that article or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article (judgment of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 57).
- 38 It follows that, in order to be considered lawful, the processing of personal data must come within one of the six cases provided for in Article 7 of Directive 95/46.

- 39 The questions raised by the referring court concern, in particular, the principle relating to making data processing legitimate referred to in Article 7(f) of Directive 95/46; that provision was transposed into Romanian law by Article 5(2)(e) of Law No 677/2001, and that article is also referred to in Article 6 of Decision No 52/2012 of the ANSPDCP as regards specifically the processing of personal data by video surveillance means.
- 40 In that regard, Article 7(f) of Directive 95/46 lays down three cumulative conditions in order for the processing of personal data to be lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; secondly, the need to process personal data for the purposes of the legitimate interests pursued; and thirdly, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interest pursued (judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336, paragraph 28).
- 41 It must be stated that Article 7(f) of Directive 95/46 does not require the data subject's consent. Such consent, as a condition to which the processing of personal data is made subject, appears, however, only in Article 7(a) of that directive.
- 42 In the present case, the objective which the controller essentially seeks to achieve when he or she installs a video surveillance system such as that at issue in the main proceedings, namely protecting the property, health and life of the co-owners of a building, is likely to be characterised as a 'legitimate interest', within the meaning of Article 7(f) of Directive 95/46. The first condition laid down in that provision appears, therefore, in principle, to be fulfilled (see, by analogy, judgment of 11 December 2014, *Ryneš*, C-212/13, EU:C:2014:2428, paragraph 34).
- 43 The referring court is, however, uncertain whether the first of the conditions laid down in Article 7(f) must be understood as meaning that the interests pursued by the controller at issue must, first, be 'proven' and, secondly be 'present and effective at the time of the data processing'.
- 44 In that regard, it must be found that, as the Romanian and Czech Governments, Ireland, the Austrian Government, the Portuguese Government and the Commission have argued, since, in accordance with Article 7(f) of Directive 95/46, the controller responsible for the processing of personal data or the third party to whom those data are disclosed must pursue legitimate interests justifying that processing, those interests must be present and effective as at the date of the data processing and must not be hypothetical at that date. It cannot, however, be necessarily required, at the time of examining all the circumstances of the case, that the safety of property and individuals was previously compromised.
- 45 In the present case, in a situation such as that at issue in the main proceedings, the condition relating to the existence of a present and effective interest seems in any event to be fulfilled, since the referring court notes that thefts, burglaries and acts of vandalism had occurred before the video surveillance system was installed and that was despite the previous installation, in the entrance to the building, of a security system comprising an intercom/magnetic card entry.
- 46 As regards the second condition laid down in Article 7(f) of Directive 95/46, relating to the need to process personal data for the purposes of the legitimate interests pursued, the Court has pointed out that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336, paragraph 30 and the case-law cited).
- 47 That condition requires the referring court to ascertain that the legitimate data processing interests pursued by the video surveillance at issue in the main proceedings — which consist, in essence, in ensuring the security of property and individuals and preventing crime — cannot reasonably be as effectively achieved by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter.

- 48 In addition, as the Commission maintained, the condition relating to the need for processing must be examined in conjunction with the ‘data minimisation’ principle enshrined in Article 6(1)(c) of Directive 95/46, in accordance with which personal data must be ‘adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed’.
- 49 It is apparent from the documents before the Court that the requirements linked to the proportionality of the processing of data at issue in the main proceedings seem to have been taken into account. It is not in dispute that alternative measures consisting in a security system, installed in the entrance to the building, and comprising an intercom/magnetic card entry, were initially put in place, but proved to be insufficient. In addition, the video surveillance device at issue is limited only to the common parts of the building in co-ownership and the approach to it.
- 50 However, the proportionality of the data processing by a video surveillance device must be assessed by taking into account the specific methods of installing and operating that device, which must limit the effect thereof on the rights and freedoms of data subjects while ensuring the effectiveness of the video surveillance system at issue.
- 51 Consequently, as the Commission contended, the condition relating to the need for processing implies that the controller must examine, for example, whether it is sufficient that the video surveillance operates only at night or outside normal working hours, and block or obscure the images taken in areas where surveillance is unnecessary.
- 52 Lastly, as regards the third condition laid down in Article 7(f) of Directive 95/46, relating to the existence of fundamental rights and freedoms of the data subject whose data require protection, which might override the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, it must be borne in mind, as mentioned in paragraph 32 above, that the assessment of that condition necessitates a balancing of the opposing rights and interests concerned which depends on the individual circumstances of the particular case in question, and in the context of which account must be taken of the significance of the data subject’s rights arising from Articles 7 and 8 of the Charter.
- 53 In that context, the Court has held that Article 7(f) of Directive 95/46 precludes Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case. Thus, Member States cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case (judgment of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 62).
- 54 It is also apparent from the case-law of the Court that it is possible to take into consideration, for the purposes of that balancing, the fact that the seriousness of the infringement of the data subject’s fundamental rights resulting from that processing can vary depending on the possibility of accessing the data at issue in public sources (see, to that effect, judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336, paragraph 32).
- 55 Unlike the processing of data from public sources, the processing of data from non-public sources implies that information relating to the data subject’s private life will thereafter be known by the data controller and, as the case may be, by the third party or parties to whom the data are disclosed. This more serious infringement of the data subject’s rights enshrined in Articles 7 and 8 of the Charter must be taken into account and be balanced against the legitimate interest pursued by the data controller or by the third party or parties to whom the data are disclosed (see, to that effect, judgment of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito*, C-468/10 and C-469/10, EU:C:2011:777, paragraph 45).
- 56 The criterion relating to the seriousness of the infringement of the data subject’s rights and freedoms is an essential component of the weighing or balancing exercise on a case-by-case basis, required by Article 7(f)

of Directive 95/46.

- 57 In this respect, account must be taken, inter alia, of the nature of the personal data at issue, in particular of the potentially sensitive nature of those data, and of the nature and specific methods of processing the data at issue, in particular of the number of persons having access to those data and the methods of accessing them.
- 58 The data subject's reasonable expectations that his or her personal data will not be processed when, in the circumstance of the case, that person cannot reasonably expect further processing of those data, are also relevant for the purposes of the balancing exercise.
- 59 Lastly, those factors must be balanced against the importance, for all the co-owners of the building concerned, of the legitimate interests pursued in the instant case by the video surveillance system at issue, inasmuch as it seeks essentially to ensure that the property, health and life of those co-owners are protected.
- 60 In the light of the foregoing, the answer to the questions raised is that Article 6(1)(c) and Article 7(f) of Directive 95/46, read in the light of Articles 7 and 8 of the Charter, must be interpreted as not precluding national provisions which authorise the installation of a video surveillance system, such as the system at issue in the main proceedings, installed in the common parts of a residential building, for the purposes of pursuing legitimate interests of ensuring the safety and protection of individuals and property, without the consent of the data subjects, if the processing of personal data carried out by means of the video surveillance system at issue fulfils the conditions laid down in Article 7(f), which it is for the referring court to determine.

Costs

- 61 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national 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 (Third Chamber) hereby rules:

Article 6(1)(c) and Article 7(f) 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, read in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, must be interpreted as not precluding national provisions which authorise the installation of a video surveillance system, such as the system at issue in the main proceedings, installed in the common parts of a residential building, for the purposes of pursuing legitimate interests of ensuring the safety and protection of individuals and property, without the consent of the data subjects, if the processing of personal data carried out by means of the video surveillance system at issue fulfils the conditions laid down in Article 7(f), which it is for the referring court to determine.

[Signatures]

* Language of the case: Romanian.