Provisional text

JUDGMENT OF THE COURT (First Chamber)

7 December 2023 (*)

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 5(1)(a) – Principle of 'lawfulness' – Point (f) of the first subparagraph of Article 6(1) – Necessity of processing for the purposes of the legitimate interests pursued by the controller or by a third party – Article 17(1)(d) – Right to erasure where personal data have been unlawfully processed – Article 40 – Codes of conduct – Article 78(1) – Right to an effective judicial remedy against a supervisory authority – Decision taken by the supervisory authority on a complaint – Scope of judicial review of that decision – Credit information agencies – Storage of data from a public register relating to the discharge of remaining debts in favour of a person – Storage period)

In Joined Cases C-26/22 and C-64/22,

REQUESTS for a preliminary ruling under Article 267 TFEU from the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), made by decisions of 23 December 2021 and 31 January 2022, received at the Court on 11 January 2022 and 2 February 2022, in the proceedings

UF (C-26/22),

AB (C-64/22)

v

Land Hessen,

intervener:

SCHUFA Holding AG,

THE COURT (First Chamber),

composed of A. Arabadjiev, President of the Chamber, T. von Danwitz, P.G. Xuereb, A. Kumin (Rapporteur) and I. Ziemele, Judges,

Advocate General: P. Pikamäe,

Registrar: K. Hötzel, Administrator,

having regard to the written procedure and further to the hearing on 26 January 2023,

after considering the observations submitted on behalf of:

– UF and AB, by R. Rohrmoser and S. Tintemann, Rechtsanwälte,

– the Land Hessen, by M. Kottmann and G. Ziegenhorn, Rechtsanwälte,

– SCHUFA Holding AG, by G. Thüsing and U. Wuermeling, Rechtsanwalt,

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

– the Portuguese Government, by P. Barros da Costa, J. Ramos and C. Vieira Guerra, acting as Agents,

– the European Commission, by A. Bouchagiar, F. Erlbacher, H. Kranenborg and W. Wils, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 16 March 2023,

gives the following

Judgment

1 These requests for a preliminary ruling concern the interpretation of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter') and of point (f) of the first subparagraph of Article 6(1), Article 17(1)(d), Article 40, Article 77(1) and Article 78(1) of 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, and corrigendum OJ 2018 L 127, p. 2; 'the GDPR').

2 The requests have been made in two sets of proceedings between UF (Case C-26/22) and AB (Case C-64/22), on the one hand, and the Land Hessen (Federal State of Hesse, Germany), on the other hand, concerning the refusal of the Hessischer Beauftragter für Datenschutz und Informationsfreiheit (Data Protection and Freedom of Information Commissioner for the Federal State of Hesse, Germany; 'the HBDI') to order SCHUFA Holding AG ('SCHUFA') to delete data held by it relating to the discharge from remaining debts in favour of UF and of AB.

Legal context

European Union law

Directive 2008/48/EC

3 According to recitals 26 and 28 of Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC (OJ 2008 L 133, p. 66):

'(26) … In the expanding credit market, in particular, it is important that creditors should not engage in irresponsible lending or give out credit without prior assessment of creditworthiness, and the Member States should carry out the necessary supervision to avoid such behaviour and should determine the necessary means to sanction creditors in the event of their doing so. … [C]reditors should bear the responsibility of checking individually the creditworthiness of the consumer. …

…

(28) To assess the credit status of a consumer, the creditor should also consult relevant databases; the legal and actual circumstances may require that such consultations vary in scope. To prevent any distortion of competition among creditors, it should be ensured that creditors have access to private or public databases concerning consumers in a Member State where they are not established under non-discriminatory conditions compared with creditors in that Member State.'

4 Article 8(1) of that directive, that article being headed 'Obligation to assess the creditworthiness of the consumer', provides:

'Member States shall ensure that, before the conclusion of the credit agreement, the creditor assesses the consumer's creditworthiness on the basis of sufficient information, where appropriate obtained from the consumer and, where necessary, on the basis of a consultation of the relevant database. Member States whose legislation requires creditors to assess the creditworthiness of consumers on the basis of a consultation of the relevant database may retain this requirement.'

Directive 2014/17/EU

5 According to recitals 55 and 59 of Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 (OJ 2014 L 60, p. 34):

‘(55) It is essential that the consumer’s ability and propensity to repay the credit is assessed and verified before a credit agreement is concluded. That assessment of creditworthiness should take into consideration all necessary and relevant factors that could influence a consumer’s ability to repay the credit over its lifetime. …

…

(59) Consultation of a credit database is a useful element in the assessment of creditworthiness. …’

6 Entitled ‘Obligation to assess the creditworthiness of the consumer’, Article 18 of that directive provides, in paragraph 1 thereof:

‘Member States shall ensure that, before concluding a credit agreement, the creditor makes a thorough assessment of the consumer’s creditworthiness. That assessment shall take appropriate account of factors relevant to verifying the prospect of the consumer to meet his obligations under the credit agreement.’

7 Entitled ‘Database access’, Article 21 of that directive states, in paragraphs 1 and 2:

‘1. Each Member State shall ensure access for all creditors from all Member States to databases used in that Member State for assessing the creditworthiness of consumers and for the sole purpose of monitoring consumers’ compliance with the credit obligations over the life of the credit agreement. The conditions for such access shall be non-discriminatory.

2. Paragraph 1 shall apply both to databases which are operated by private credit bureaux or credit reference agencies and to public registers.’

Regulation (EU) 2015/848

8 Under recital 76 of Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings (OJ 2015 L 141, p. 19):

‘In order to improve the provision of information to relevant creditors and courts and to prevent the opening of parallel insolvency proceedings, Member States should be required to publish relevant information in cross-border insolvency cases in a publicly accessible electronic register. In order to facilitate access to that information for creditors and courts domiciled or located in other Member States, this Regulation should provide for the interconnection of such insolvency registers via the European e-Justice Portal. …’

9 Entitled ‘Responsibilities of Member States regarding the processing of personal data in national insolvency registers’, Article 79 of that regulation provides, in paragraphs 4 and 5 thereof:

‘4. Member States shall be responsible, in accordance with 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)], for the collection and storage of data in national databases and for decisions taken to make such data available in the interconnected register that can be consulted via the European e-Justice Portal.

5. As part of the information that should be provided to data subjects to enable them to exercise their rights, and in particular the right to the erasure of data, Member States shall inform data subjects of the accessibility period set for personal data stored in insolvency registers.’

The GDPR

10 Under recitals 10, 11, 47, 50, 98, 141 and 143 of the GDPR:

‘(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …

(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

…

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. …

…

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. … In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

…

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

…

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an

effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation 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. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. …

…

(143) … [E]ach natural or legal person should have 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, the right to an effective judicial remedy does not encompass measures taken by 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 that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. …'

11 Entitled 'Principles relating to processing of personal data', Article 5 of that regulation is worded as follows:

'1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

…

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");

…

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability")."

12 Headed 'Lawfulness of processing', Article 6 of that regulation provides:

'1. Processing shall be lawful only if and to the extent that at least one of the following applies:

…

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

…

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.'

13 Entitled 'Right to erasure ("right to be forgotten")', Article 17 of the GDPR provides, in paragraph 1 thereof:

'The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

…

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

…'

14 Entitled 'Right to object', Article 21 of that regulation provides, in paragraphs 1 and 2 thereof:

'1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.'

15 Entitled 'Codes of conduct', Article 40 of that regulation provides, in paragraphs 1, 2 and 5 thereof:

'1. The Member States, the supervisory authorities, the Board and the [European] Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this

Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

…

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.'

16 Entitled 'Supervisory authority', Article 51 of the GDPR provides, in paragraph 1 thereof:

'Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ("supervisory authority").'

17 Entitled 'Independence', Article 52 of that regulation provides, in paragraphs 1, 2 and 4 thereof:

'1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

…

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.'

18 Article 57(1) of that regulation, that article being entitled 'Tasks', provides:

'Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

…

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, 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, in particular if further investigation or coordination with another supervisory authority is necessary;

…'

19 Entitled 'Powers', Article 58 of the GDPR lists, in paragraph 1, the investigative powers available to each supervisory authority and, in paragraph 2, the corrective powers that it may have.

20 Under the heading ‘Right to lodge a complaint with a supervisory authority’, Article 77 of that regulation states:

‘1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.’

21 Under the heading ‘Right to an effective judicial remedy against a supervisory authority’, Article 78 of the GDPR provides, in paragraphs 1 and 2 thereof:

‘1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.’

22 Entitled ‘Right to an effective judicial remedy against a controller or processor’, Article 79 of the GDPR provides, in paragraph 1 thereof:

‘Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.’

German law

23 Under Paragraph 9(1) of the Insolvenzordnung (Insolvency Code) of 5 October 1994 (BGBl. 1994 I, p. 2866), in the version applicable to the facts in the main proceedings:

‘Public notification shall take place by means of centralised publication at national level on the internet; this may be done in extract form. The debtor must be precisely identified, and, in particular, his or her address and business sector must be stated. Notification is deemed to have been effected after two further days following the day of publication have elapsed.’

24 Paragraph 3 of the Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet (Regulation on public notifications in insolvency proceedings on the internet) of 12 February 2002 (BGBl. I, p. 677; ‘the InsoBekV’) stipulates, in subparagraphs 1 and 2 thereof:

‘(1) The publication of data from insolvency proceedings, including preliminary insolvency proceedings, in an electronic information and communication system shall be erased no later than six months after the insolvency proceedings are terminated or the order discontinuing the insolvency proceedings becomes final. If the proceedings are not opened, the period shall begin to run from the date on which the published protective measures are lifted.

(2) The first sentence of subparagraph 1 shall apply to publications in the proceedings for a discharge from remaining debts, including the order pursuant to Paragraph 289 of the Insolvency Code, subject to the proviso that the period begins to run from the date on which the decision on discharge from remaining debts becomes final.’

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

25 In the context of insolvency proceedings concerning them, UF and AB were granted early discharge from remaining debts by judicial decisions delivered on 17 December 2020 and 23 March 2021 respectively. In accordance with Paragraph 9(1) of the Insolvenzordnung and Paragraph 3(1) and (2) of the InsoBekV, the official publication of those decisions on the internet was discontinued after six months.

26 SCHUFA is a private credit information agency, which records and stores information from public registers in its own databases, in particular information relating to the discharge from remaining debts. It deletes that information three years after registration, in accordance with the code of conduct drawn up in Germany by the association of agencies providing credit information and approved by the competent supervisory authority.

27 UF and AB applied to SCHUFA to have the entries relating to the decisions to discharge their remaining debts deleted. That agency refused to accede to their requests, after explaining that its activity was carried out in compliance with the GDPR and that the six-month deletion period provided for in Paragraph 3(1) of the InsoBekV did not apply to it.

28 UF and AB each lodged a complaint with the HBDI as the competent supervisory authority.

29 In decisions issued on 1 March 2021 and 9 July 2021 respectively, the HBDI found that SCHUFA's data processing was lawful.

30 UF and AB each brought an action against the decision of the HBDI before the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), the referring court. In support of their actions, they argued that the HBDI was obliged, within the scope of its duties and powers, to take measures in respect of SCHUFA to enforce deletion of the entries concerning them.

31 In its defence, the HBDI argued that the actions should be dismissed.

32 First, the HBDI argued that the right to lodge a complaint, provided for in Article 77(1) of the GDPR, is conceived solely as a right of petition. Thus, judicial review would be confined to examining whether the supervisory authority handled the complaint and informed the complainant of the progress and outcome of that complaint. By contrast, it is not the responsibility of the court hearing the case to review the substantive correctness of the decision handed down in response to the complaint.

33 Secondly, the HBDI emphasised that data to which credit information agencies have access may be stored for as long as is necessary for the purposes for which they were stored. In the absence of regulation by the national legislature, codes of conduct have been adopted by the supervisory authorities, and the one drawn up by the association of credit information agencies provides for the deletion of such data exactly three years after entry in the file.

34 In that regard, in the first place, the referring court considers it necessary to clarify the legal nature of the decision made by the supervisory authority after receiving a complaint under Article 77(1) of the GDPR.

35 In particular, that court has doubts about the HBDI's line of argument, since it would undermine the effectiveness of the judicial remedy referred to in Article 78(1) of the GDPR. In addition, having regard to the objective pursued by that regulation, which is to ensure, in the implementation of Articles 7 and 8 of the Charter, effective protection of fundamental rights and freedoms of natural persons, Articles 77 and 78 of the GDPR cannot be interpreted restrictively.

36 That court advocates an interpretation according to which the decision taken on the merits by the supervisory authority must be subject to full judicial review. However, that authority has both a degree of latitude and discretionary power, and may only be required to act where lawful options cannot be identified.

37 In the second place, the referring court raises the question, in two respects, of the lawfulness of the storage by credit information agencies of data relating to a person's solvency from public registers, such as the insolvency register.

38 First, there are doubts as to the lawfulness of a private agency such as SCHUFA storing data transferred from public registers in its own databases.

39 First of all, that storage does not take place in relation to a specific reason, but rather in the event that their contractual partners ask them for such information, and ultimately results in the data being retained, especially if the data have already been deleted from the public register because the retention period has expired.

40 Furthermore, processing and therefore retention of data is authorised only if one of the conditions set out in Article 6(1) of the GDPR is met. In this case, only the condition set out in point (f) of the first subparagraph of Article 6(1) of the GDPR is relevant. It is doubtful whether a credit information agency such as SCHUFA is pursuing a legitimate interest within the meaning of that provision.

41 Lastly, SCHUFA is only one of several credit information agencies and, consequently, data are often stored in multiple databases in Germany, entailing a massive encroachment on the fundamental right under Article 7 of the Charter.

42 Secondly, even supposing that the storage by private agencies of data from public registers were lawful as such, the question of the possible duration of such storage arises.

43 In that regard, the referring court is of the view that those private agencies should be required to comply with the six-month time limit laid down in Paragraph 3 of the InsoBekV relating to the retention in the insolvency register of decisions to discharge remaining debts. Thus, data which must be deleted from the public register would also have to be simultaneously deleted at all private credit information agencies which have stored those data.

44 Moreover, the question arises as to whether a code of conduct approved in accordance with Article 40 of the GDPR, which provides for a three-year deletion period for the entry relating to the discharge from remaining debts, should be taken into account in the balancing exercise to be carried out in the context of the assessment under point (f) of the first subparagraph of Article 6(1) of the GDPR.

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

‘(1) Is Article 77(1) of [the GDPR], read in conjunction with Article 78(1) thereof, to be understood as meaning that the outcome that the supervisory authority reaches and notifies to the data subject:

– has the character of a decision on a petition? This would mean that judicial review of a decision on a complaint taken by a supervisory authority in accordance with Article 78(1) of that regulation is, in principle, limited to the question of whether the authority has handled the complaint, investigated the subject matter of the complaint to the extent appropriate and informed the complainant of the outcome of the investigation,

or

– is to be understood as a decision on the merits taken by a public authority? This would mean that a decision on a complaint taken by a supervisory authority would be subject to a full substantive review by the court in accordance with Article 78(1) of that regulation, whereby, in individual cases – for example where discretion is reduced to zero – the supervisory authority may also be obliged by the court to take a specific measure within the meaning of Article 58 of that same regulation?

(2) Is the storage of data at a private credit information agency, where personal data from a public register, such as the "national databases" within the meaning of Article 79(4) and (5) of Regulation [2015/848] are stored without a specific reason in order to be able to provide information in the event of a request, compatible with Articles 7 and 8 of the [Charter]?

(3) (a) Are private databases (in particular databases of a credit information agency) which exist in parallel with, and are set up in addition to, the State databases and in which the data from the latter (*in casu*, insolvency announcements) are stored for longer than the period provided for within the narrow framework of Regulation 2015/848, read in conjunction with the national law, permissible in principle?

(b) If Question 3a is answered in the affirmative, does it follow from the "right to be forgotten" under Article 17(1)(d) of [the GDPR] that such data must be deleted where the processing period provided for in respect of the public register has expired?

(4) In so far as point (f) of [the first subparagraph of] Article 6(1) of [the GDPR] enters into consideration as the sole legal basis for the storage of data at private credit information agencies with regard to data also stored in public registers, is a credit information agency already to be regarded as pursuing a legitimate interest in the case where it imports data from the public register without a specific reason so that those data are then available in the event of a request?

(5) Is it permissible for codes of conduct which have been approved by the supervisory authorities in accordance with Article 40 of [the GDPR], and which provide for time limits for review and erasure that exceed the retention periods for public registers, to suspend the balancing of interests prescribed under point (f) of [the first subparagraph of] Article 6(1) of that regulation?'

46 By decision of the President of the Court of 11 February 2022, Cases C-26/22 and C-64/22 were joined for the purposes of the written and oral parts of the procedure and of the judgment.

Consideration of the questions referred

The first question

47 By its first question, the referring court asks, in essence, whether Article 78(1) of the GDPR must be interpreted as meaning that judicial review of a decision on a complaint taken by a supervisory authority is limited to the question whether that authority has handled the complaint, investigated the subject matter of the complaint to the extent appropriate and informed the complainant of the outcome of the investigation, or whether that decision is subject to a full judicial review, including the power of the court seised to require the supervisory authority to take a specific measure.

48 In order to answer that question, it should be borne in mind, as a preliminary point, that the interpretation of a provision of EU law requires that account be taken not only of its wording, but also of its context and the objectives and purpose pursued by the act of which it forms part (judgment of 22 June 2023, *Pankki S,* C-579/21, EU:C:2023:501, paragraph 38 and the case-law cited).

49 In respect of the wording of Article 78(1) of the GDPR, that provision provides that, without prejudice to any other administrative or non-judicial remedy, each natural or legal person is to have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

50 In this respect, it should be noted from the outset that, in the present case, the decisions adopted by the HBDI constitute legally binding decisions within the meaning of Article 78(1) of the GDPR. After examining the merits of the complaints lodged with it, that authority found that the processing of personal data challenged by the applicants in the main proceedings was lawful under the GDPR. Moreover, the legally binding nature of those decisions is confirmed by recital 143 of that regulation, according to which the dismissal or rejection of a complaint by a supervisory authority constitutes a decision producing legal effects with regard to the complainant.

51 It should also be noted that that provision, read in the light of recital 141 of the GDPR, explicitly states that any data subject has the right to an ‘effective’ judicial remedy, in accordance with Article 47 of the Charter.

52 Thus, the Court has already held that it follows from Article 78(1) of the GDPR, read in the light of recital 143 of that regulation, that courts seised of an action against a decision of a supervisory authority should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them (judgment of 12 January 2023, *Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-132/21, EU:C:2023:2, paragraph 41).

53 Therefore, Article 78(1) of the GDPR cannot be interpreted as meaning that judicial review of a decision on a complaint taken by a supervisory authority is limited to the question of whether the authority has handled the complaint, investigated the subject matter of the complaint to the extent appropriate and informed the complainant of the outcome of the investigation. On the contrary, for a judicial remedy to be ‘effective’, as required by that provision, such a decision must be subject to full judicial review.

54 That interpretation is supported by the context of Article 78(1) of the GDPR and by the objectives and purpose of the regulation.

55 As regards the context surrounding that provision, it is important to note that, in accordance with Article 8(3) of the Charter and Article 51(1) and Article 57(1)(a) of the GDPR, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of natural persons with regard to the processing of personal data (judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 107).

56 In particular, under Article 57(1)(f) of the GDPR, each supervisory authority is required on its territory to handle complaints which, in accordance with Article 77(1) of that regulation, any data subject is entitled to lodge where that data subject considers that the processing of his or her personal data infringes the regulation, and is required to examine the nature of that complaint as necessary. The supervisory authority must deal with such a complaint with all due diligence (judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 109).

57 In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority. Where, following its investigation, such an authority finds an infringement of the provisions of that regulation, it is required to react appropriately in order to remedy the shortcoming found. To that end, Article 58(2) of that regulation lists the various corrective measures that the supervisory authority may adopt (see, to that effect, judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 111).

58 It follows, as the Advocate General observed in point 42 of his Opinion, that the complaints procedure, which is not similar to that of a petition, is designed as a mechanism capable of effectively safeguarding the rights and interests of data subjects.

59 However, in view of the wide-ranging powers vested in the supervisory authority under the GDPR, the requirement for effective judicial protection would not be met if decisions concerning the exercise by such a supervisory authority of powers of investigation or the adoption of corrective measures were subject only to limited judicial review.

60 The same applies to decisions rejecting a complaint, as Article 78(1) of the GDPR makes no distinction according to the nature of the decision adopted by the supervisory authority.

61 As regards the objectives pursued by the GDPR, it is apparent, in particular, from recital 10 thereof that the aim of that regulation is to ensure a high level of protection of natural persons with regard to the processing of personal data within the European Union. Moreover, recital 11 of that regulation states that effective protection of such data requires the strengthening of the rights of data subjects.

62 If Article 78(1) of that regulation were to be interpreted as meaning that the judicial review referred to therein is limited to verifying whether the supervisory authority has handled the complaint, investigated

the subject matter of the complaint to the extent appropriate and informed the complainant of the outcome of the investigation, the attainment of the objectives and the pursuit of the purpose of the regulation would necessarily be compromised.

63 Furthermore, an interpretation of that provision according to which a decision on a complaint adopted by a supervisory authority is subject to full judicial review does not call into question the guarantees of independence enjoyed by supervisory authorities, nor the right to an effective judicial remedy against a controller or processor.

64 In the first place, it is true that, in accordance with Article 8(3) of the Charter, compliance with the rules on the protection of personal data is subject to control by an independent authority. In that context, Article 52 of the GDPR specifies, in particular, that each supervisory authority is to act with complete independence in performing its tasks and exercising its powers in accordance with that regulation (paragraph 1), that, in the performance of their tasks and exercise of their powers, the member or members of each supervisory authority are to remain free from external influence (paragraph 2), and that each Member State is to ensure that each supervisory authority has the resources necessary for the effective performance of its duties and the exercise of its powers (paragraph 4).

65 However, those guarantees of independence are in no way compromised by the fact that the legally binding decisions of a supervisory authority are subject to full judicial review.

66 In the second place, as regards the right to an effective judicial remedy against a controller or processor provided for in Article 79(1) of the GDPR, it should be noted that, according to the case-law of the Court, the remedies provided for, respectively, in Article 78(1) and Article 79(1) of that regulation may be exercised concurrently with and independently of each other (judgment of 12 January 2023, *Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-132/21, EU:C:2023:2, paragraph 35 and operative part). In that context, the Court has held, inter alia, that making several remedies available strengthens the objective set out in recital 141 of that regulation of guaranteeing for every data subject who considers that his or her rights under that regulation are infringed the right to an effective judicial remedy in accordance with Article 47 of the Charter (judgment of 12 January 2023, *Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-132/21, EU:C:2023:2, paragraph 44).

67 Therefore, and even though it is for the Member States, in accordance with the principle of procedural autonomy, to lay down the detailed rules for the coordination of those remedies (judgment of 12 January 2023, *Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-132/21, EU:C:2023:2, paragraph 45 and operative part), the existence of the right to an effective judicial remedy against a controller or processor, provided for in Article 79(1) of the GDPR, does not affect the scope of the judicial review exercised, in the context of an action brought under Article 78(1) of that regulation, over a decision on a complaint adopted by a supervisory authority.

68 However, it should be added that, while, as pointed out in paragraph 56 of this judgment, the supervisory authority must deal with a complaint with all due diligence, that authority has, as regards the remedies listed in Article 58(2) of the GDPR, a margin of discretion as to the choice of appropriate and necessary means (see, to that effect, judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 112).

69 While the national court hearing an action under Article 78(1) of the GDPR must, as noted in paragraph 52 of this judgment, have full jurisdiction to examine all questions of fact and law relating to the dispute concerned, the guarantee of effective judicial protection does not imply that it is entitled to substitute its assessment of the choice of appropriate and necessary remedies for that of that authority, but requires that court to examine whether the supervisory authority has complied with the limits of its discretion.

70 In the light of all the foregoing considerations, the answer to the first question is that Article 78(1) of the GDPR must be interpreted as meaning that a decision on a complaint adopted by a supervisory authority is subject to full judicial review.

The second to fifth questions

71 By its second to fifth questions, which it is appropriate to consider together, the referring court asks, in essence,

– whether Article 5(1)(a) of the GDPR, read in conjunction with point (f) of the first subparagraph of Article 6(1) of that regulation, must be interpreted as precluding a practice of private credit information agencies consisting in retaining, in their own databases, information from a public register relating to the grant of a discharge from remaining debts in favour of natural persons, and in deleting that information after a period of three years, in accordance with a code of conduct within the meaning of Article 40 of that regulation, whereas the period of retention of that information in the public register is six months, and,

– whether Article 17(1)(c) and (d) of the GDPR must be interpreted as meaning that a private credit information agency which has acquired information relating to the grant of a discharge from remaining debts from a public register is obliged to delete that information.

Article 5(1)(a) of the GDPR

72 Article 5(1)(a) of the GDPR provides that personal data is to be processed lawfully, fairly and in a transparent manner in relation to the data subject.

73 In that context, the first subparagraph of Article 6(1) of that regulation sets out an exhaustive and restrictive list of the cases in which processing of personal data can be regarded as lawful. Thus, in order to be capable of being regarded as such, processing must fall within one of the cases provided for in that provision (judgment of 4 July 2023, *Meta Platforms and Others (General terms of use of a social network)*, C-252/21, EU:C:2023:537, paragraph 90 and the case-law cited).

74 In the present case, it is common ground that the lawfulness of the processing of personal data at issue in the main proceedings must be assessed solely in the light of point (f) of the first subparagraph of Article 6(1) of the GDPR. Under that provision, the processing of personal data is lawful only if and to the extent that it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

75 Accordingly, that provision lays down three cumulative conditions for the processing of personal data to be lawful, namely, first, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or freedoms and fundamental rights of the person concerned by the data protection do not take precedence (judgment of 4 July 2023, *Meta Platforms and Others (General terms of use of a social network)*, C-252/21, EU:C:2023:537, paragraph 106 and the case-law cited).

76 As regards, first, the condition relating to the pursuit of a ‘legitimate interest’, in the absence of a definition of that concept in the GDPR, it should be emphasised, as the Advocate General observed in point 61 of his Opinion, that a wide range of interests is, in principle, capable of being regarded as legitimate.

77 Second, with regard to the condition that the processing of personal data be necessary for the purposes of the legitimate interests pursued, that condition requires the referring court to ascertain that the legitimate data processing interests pursued cannot reasonably be achieved just as effectively 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 (judgment of 4 July 2023, *Meta Platforms and Others (General terms of use of a social network)*, C-252/21, EU:C:2023:537, paragraph 108 and the case-law cited).

78 In that context, it should also be recalled that the condition relating to the need for processing must be examined in conjunction with the ‘data minimisation’ principle enshrined in Article 5(1)(c) of the GDPR, in accordance with which personal data must be ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’ (judgment of 4 July 2023, *Meta*

Platforms and Others (General terms of use of a social network), C-252/21, EU:C:2023:537, paragraph 109 and the case-law cited).

79 Third, with regard to the condition that the interests or fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interests of the controller or of a third party, the Court has already held that that condition entails a balancing of the opposing rights and interests at issue which depends in principle on the specific circumstances of the particular case and that, consequently, it is for the referring court to carry out that balancing exercise, taking account of those specific circumstances (judgment of 4 July 2023, *Meta Platforms and Others (General terms of use of a social network)*, C-252/21, EU:C:2023:537, paragraph 110 and the case-law cited).

80 Furthermore, as can be seen from recital 47 of the GDPR, the interests and fundamental rights of the data subject may in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect such processing (judgment of 4 July 2023, *Meta Platforms and Others (General terms of use of a social network)*, C-252/21, EU:C:2023:537, paragraph 112).

81 While it is therefore ultimately for the national court to assess whether, in relation to the processing of personal data at issue in the main proceedings, the three conditions referred to in paragraph 75 of this judgment are satisfied, it is open to the Court, when giving a preliminary ruling on a reference, to give clarifications to guide the national court in that determination (see, to that effect, judgment of 20 October 2022, *Digi*, C-77/21, EU:C:2022:805, paragraph 39 and the case-law cited).

82 In this case, with regard to the pursuit of a legitimate interest, SCHUFA argues that credit information agencies process the data necessary for the assessment of the creditworthiness of persons or undertakings in order to be able to make that information available to their contractual partners. In addition to protecting the economic interests of agencies wishing to enter into credit-linked contracts, the determination of creditworthiness and the provision of information on creditworthiness form the basis of credit and the economy’s ability to function. The activity of those agencies also helps to clarify the business requirements of persons involved in credit-related transactions as the report allows a quick and non-bureaucratic examination of those transactions.

83 In that regard, while the processing of personal data such as that at issue in the main proceedings serves SCHUFA’s economic interests, that processing also serves to pursue the legitimate interest of SCHUFA’s contractual partners, who intend to conclude credit agreements with individuals, in being able to assess the creditworthiness of those individuals, and thus the interests of the credit sector from a socio-economic point of view.

84 In the case of consumer credit agreements, Article 8 of Directive 2008/48, read in the light of recital 28 thereof, states that, before the conclusion of the credit agreement, the creditor is required to assess the consumer’s creditworthiness on the basis of sufficient information, including, where appropriate, information from public and private databases.

85 Furthermore, as regards consumer credit agreements relating to residential immovable property, it follows from Articles 18(1) and 21(1) of Directive 2014/17, read in the light of recitals 55 and 59 thereof, that the creditor must make a thorough assessment of the consumer’s creditworthiness and that he or she must have access to credit databases, the consultation of such databases being a useful element for the purposes of that assessment.

86 It should be added that the obligation to assess the creditworthiness of consumers, as laid down in Directives 2008/48 and 2014/17, is intended not only to protect the credit applicant but also, as pointed out in recital 26 of Directive 2008/48, to ensure the proper functioning of the credit system as a whole.

87 However, the data processing must also be necessary in order to achieve the legitimate interests pursued by the controller or by a third party and the interests or fundamental freedoms and rights of the data subject must not override those interests. In the context of that balancing of the opposing rights and interests at issue, namely, those of the controller and of the third parties involved, on the one hand, and those of the data subject, on the other, account must be taken, as has been noted in paragraph 80 of this judgment, in particular of the reasonable expectations of the data subject as well as the scale of the

processing at issue and its impact on that person (see judgment of 4 July 2023, *Meta Platforms and Others (General terms of use of a social network)*, C-252/21, EU:C:2023:537, paragraph 116).

88 As regards point (f) of the first subparagraph of Article 6(1) of the GDPR, the Court has held that that provision must be interpreted as meaning that processing can be regarded as necessary for the purposes of the legitimate interests pursued by the controller or by a third party, within the meaning of that provision, only if such processing is carried out in so far as is strictly necessary for the purposes of that legitimate interest and if it is apparent from a balancing of the opposing interests, having regard to all the relevant circumstances, that the interests or fundamental freedoms and rights of the persons concerned by the processing at issue do not override that legitimate interest of the controller or of a third party (see, to that effect, judgments of 4 May 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336, paragraph 30, and of 4 July 2023, *Meta Platforms and Others (General terms of use of a social network)*, C-252/21, EU:C:2023:537, paragraph 126).

89 In that context, the referring court refers to two aspects of the processing of personal data at issue in the main proceedings. In the first place, that processing would involve storing the data in a variety of ways, namely not only in a public register but also in the databases of the credit information agencies, it being specified that those agencies store the data not in relation to a specific reason but rather in the event that their contractual partners ask them for such information. In the second place, those agencies store the data for three years, on the basis of a code of conduct within the meaning of Article 40 of the GDPR, whereas the national legislation provides for a storage period of only six months in the case of the public register.

90 With regard to the first of those aspects, SCHUFA argues that it would be impossible to provide information in a timely manner if a credit information agency had to wait for a specific request before it could start collecting data.

91 In that regard, it is for the referring court to ascertain whether the storage of the data at issue by SCHUFA in its own databases is limited to what is strictly necessary in order to achieve the legitimate interest pursued, when the data at issue can be consulted in the public register and without a commercial undertaking having requested information in a specific case. If this were not the case, the storage of such data by SCHUFA could not be considered necessary for the period during which the data are made available to the public.

92 As regards the length of time for which the data are stored, it must be held that the examinations of the second and third conditions referred to in paragraph 75 of this judgment merge in so far as the assessment of whether, in the present case, the legitimate interests pursued by the processing of personal data at issue in the main proceedings cannot reasonably be achieved by a shorter period for storing the data requires a balancing of the opposing rights and interests at issue.

93 As regards the balancing of the legitimate interests pursued, it should be noted that, in so far as the analysis provided by a credit information agency makes it possible to assess objectively and reliably the creditworthiness of the potential customers of the contractual partners of the agency supplying that credit information, it makes it possible to compensate for disparities in information and therefore to reduce the risks of fraud and other uncertainties.

94 On the other hand, as regards the rights and interests of the data subject, the processing of data relating to the granting of a discharge from remaining debts, by a credit information agency, such as the storage, analysis and communication of such data to a third party, constitutes a serious interference with the fundamental rights of the data subject, enshrined in Articles 7 and 8 of the Charter. Such data is used as a negative factor when assessing the data subject's creditworthiness and therefore constitutes sensitive information about his or her private life (see, to that effect, judgment of 13 May 2014, *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraph 98). The processing of such data is likely to be considerably detrimental to the interests of the data subject in so far as such disclosure is likely to make it significantly more difficult for him or her to exercise his or her freedoms, particularly where basic needs are concerned.

95 Furthermore, as the Commission has pointed out, the longer the data in question is stored by credit information agencies, the greater the impact on the interests and private life of the data subject and the

greater the requirements relating to the lawfulness of the storage of that information.

96 It should also be noted that, as stated in recital 76 of Regulation 2015/848, the purpose of a public insolvency register is to improve the provision of information to creditors as well as to the courts concerned. In that context, Article 79(5) of that regulation merely provides that Member States are to inform data subjects of the accessibility period set for personal data stored in insolvency registers, without setting a time limit for the retention of such data. By contrast, it is apparent from Article 79(4) of the GDPR that Member States are responsible, in accordance with that regulation, for the collection and storage of personal data in national databases. The retention period for such data must then be set in compliance with the GDPR.

97 In this case, the German legislature provides that information relating to the granting of a discharge from remaining debts is kept in the insolvency register for only six months. It therefore considers that, after the expiry of a six-month period, the rights and interests of the data subject take precedence over those of the public to have access to that information.

98 Moreover, as the Advocate General observed in point 75 of his Opinion, the discharge from remaining debts is intended to allow the person who benefits from it to re-enter economic life and is therefore generally of existential importance to that person. The attainment of that objective would be jeopardised if credit information agencies could, for the purposes of assessing the economic situation of a person, retain data relating to a discharge from remaining debts and use such data after they have been deleted from the public insolvency register, in so far as those data are still used as a negative factor when assessing the solvency of such a person.

99 In those circumstances, the interests of the credit sector in having access to information on a discharge from remaining debts cannot justify the processing of personal data such as that at issue in the main proceedings beyond the period for which the data are kept in the public insolvency register, so that the retention of those data by a credit information agency cannot be based on point (f) of the first subparagraph of Article 6(1) of the GDPR as regards the period following the deletion of those data from a public insolvency register.

100 As regards the six-month period during which the data in question are also available in that public register, it should be noted that, although the effects of parallel storage of those data in the databases of such agencies may be regarded as less serious than after the six months have elapsed, such storage nevertheless constitutes an interference with the rights enshrined in Articles 7 and 8 of the Charter. In that regard, the Court has already held that the presence of the same personal data in several sources reinforces the interference with the individual's right to privacy (see judgment of 13 May 2014, *Google Spain and Google*, C-131/12, EU:C:2014:317, paragraphs 86 and 87). It is for the referring court to weigh up the interests involved and the impact on the data subject concerned, in order to establish whether the parallel storage of those data by private credit information agencies can be regarded as being limited to what is strictly necessary, as required by the case-law of the Court cited in paragraph 88 of this judgment.

101 Finally, with regard to the existence, as in the present case, of a code of conduct providing that a credit information agency must delete data relating to a release from remaining debts after a period of three years, it should be recalled that, in accordance with Article 40(1) and (2) of the GDPR, codes of conduct are intended to contribute to the proper application of that regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises. Thus, associations and other bodies representing categories of data controllers or processors may draw up, amend or extend codes of conduct, for the purpose of specifying the application of that regulation, such as with regard to fair and transparent processing, the legitimate interests pursued by controllers in specific contexts and the collection of personal data.

102 In addition, under Article 40(5) of the GDPR, a draft code is to be submitted to the competent supervisory authority, which is to approve it if it finds that it provides sufficient appropriate safeguards.

103 In the present case, the code of conduct at issue in the main proceedings was drawn up by the association of German credit information agencies and approved by the competent supervisory authority.

104 That being so, while, in accordance with Article 40(1) and (2) of the GDPR, a code of conduct is intended to contribute to the proper application of that regulation and to specify the application of that regulation, the fact remains, as the Advocate General observed in points 103 and 104 of his Opinion, that the conditions for the lawfulness of the processing of personal data laid down by such a code cannot differ from the conditions laid down in Article 6(1) of the GDPR.

105 Thus, a code of conduct that leads to an assessment different from that obtained pursuant to point (f) of the first subparagraph of Article 6(1) of the GDPR cannot be taken into account in the balance of interests under that provision.

Article 17 of the GDPR

106 Lastly, the referring court raises the question, in essence, of the obligations incumbent on a credit information agency under Article 17 of the GDPR.

107 In that regard, it should be borne in mind that, under Article 17(1)(d) of the GDPR, to which the referring court refers, the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller has the obligation to erase personal data without undue delay where the personal data have been unlawfully processed.

108 Therefore, according to the clear wording of that provision, if the national court were to conclude from its assessment of the lawfulness of the processing of personal data at issue in the main proceedings that that processing was not lawful, it would be incumbent on the controller, in this case SCHUFA, to delete the data concerned as soon as possible. This would be the case, as noted in paragraph 99 of this judgment, in respect of the processing of personal data beyond the six-month period for which the data are kept in the public insolvency register.

109 As regards the processing at issue during the six-month period in which the data are available in the public insolvency register, if the referring court were to conclude that the processing complied with point (f) of the first subparagraph of Article 6(1) of the GDPR, Article 17(1)(c) of that regulation would apply.

110 That provision establishes the right to erasure of personal data where the data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no ‘overriding legitimate grounds for the processing’. Under the latter provision, the data subject is to have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of the first subparagraph of Article 6(1) of the GDPR. The controller is no longer required to process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

111 As the Advocate General observed in point 93 of his Opinion, it follows from a combined reading of those provisions that the data subject enjoys a right to object to processing and a right to erasure, unless there are overriding legitimate grounds which take precedence over the interests and rights and freedoms of that person within the meaning of Article 21(1) of the GDPR, which it is for the controller to demonstrate.

112 Consequently, if the controller fails to provide such proof, the data subject is entitled to request the erasure of the data on the basis of Article 17(1)(c) of the GDPR, where he or she objects to the processing in accordance with Article 21(1) of that regulation. It is for the referring court to examine whether, exceptionally, there are overriding legitimate grounds capable of justifying the processing in question.

113 In the light of all the foregoing considerations, the second to fifth questions should be answered as follows:

– Article 5(1)(a) of the GDPR, read in conjunction with point (f) of the first subparagraph of Article 6(1) of that regulation, must be interpreted as precluding a practice of private credit information agencies consisting in retaining, in their own databases, information from a public

register relating to the grant of a discharge from remaining debts in favour of natural persons in order to be able to provide information on the solvency of those persons, for a period extending beyond that during which the data are kept in the public register;

– Article 17(1)(c) of the GDPR must be interpreted as meaning that the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where he or she objects to the processing pursuant to Article 21(1) of that regulation and there are no overriding legitimate grounds capable of justifying, exceptionally, the processing in question;

– Article 17(1)(d) of the GDPR must be interpreted as meaning that the controller is required to erase unlawfully processed personal data as soon as possible.

Costs

114 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 (First Chamber) hereby rules:

1. **Article 78(1) of 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)**

   must be interpreted as meaning that a decision on a complaint adopted by a supervisory authority is subject to full judicial review.

2. **Article 5(1)(a) of Regulation 2016/679, read in conjunction with point (f) of the first subparagraph of Article 6(1) of that regulation,**

   must be interpreted as precluding a practice of private credit information agencies consisting in retaining, in their own databases, information from a public register relating to the grant of a discharge from remaining debts in favour of natural persons in order to be able to provide information on the solvency of those persons, for a period extending beyond that during which the data are kept in the public register.

3. **Article 17(1)(c) of Regulation 2016/679**

   must be interpreted as meaning that the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where he or she objects to the processing pursuant to Article 21(1) of that regulation and there are no overriding legitimate grounds capable of justifying, exceptionally, the processing in question.

4. **Article 17(1)(d) of Regulation 2016/679**

   must be interpreted as meaning that the controller is required to erase unlawfully processed personal data as soon as possible.

[Signatures]

* Language of the case: German.