Anonymised version

Case C-26/22

Request for a preliminary ruling

Date lodged:

11 January 2022

Referring court:

Verwaltungsgericht Wiesbaden (Germany)

Date of the decision to refer:

23 December 2021

Applicant:

UF

Defendant:

Land Hesse

---

6 K 441/21.WI

VERWALTUNGSGERICHT WIESBADEN (ADMINISTRATIVE COURT, WIESBADEN)

ORDER

In the administrative proceedings
UF
[…]

Applicant

[…] **v**

Land Hesse,
represented by the Hessen Commissioner for Data Protection and Freedom of

Information,
[…] Defendant

Joined party:

SCHUFA Holding AG,
[…] **concerning** data protection law

the Administrative Court, Wiesbaden – 6th Chamber – […]

made the following order on 23 December 2021:

I. The proceedings are stayed.

II. The proceedings are referred to the Court of Justice of the European Union for a preliminary ruling pursuant to Article 267 TFEU with regard to the following questions:

1. Is Article 77(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 – 'GDPR'; OJ 2016 L 119, p. 1), 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

(a) 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 the GDPR 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

(b) 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 the GDPR, 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 the GDPR.

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 (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings (OJ 2015 L 141, p. 19), 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 of Fundamental Rights of the European Union of 12 December 2007 ('the Charter' – OJ 2007 C 303, p. 1)?

3a. 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 (EU) 2015/848, read in conjunction with the national law, permissible in principle?

3b. 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 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 Article 6(1) of the GDPR?

Grounds:

I.

1 By order of 31 August 2021 (6 K 226/21.Wl; C-552/21), the 6th Chamber of the Administrative Court, Wiesbaden, previously referred to the Court of Justice of the European Union the question as to the legal nature of the activity of, and notification by, the supervisory authority in relation to a complainant data subject. In addition, the 6th Chamber referred questions concerning entries from public registers, for example from the publications of the insolvency courts, which are transferred as such to privately kept registers. However, the action underlying the

request for a preliminary ruling in Case C-552/21 was withdrawn, with the result that the request could no longer be continued. The referring court considers that there is still a need for clarification with regard to the fundamental questions raised, and therefore refers them again in the present request for a preliminary ruling in a similar case.

2 The applicant in the present case likewise objects to the entry of a discharge from remaining debts (*Restschuldbefreiung*) in the records of the joined party SCHUFA Holding AG, a private credit information agency. He requests that the defendant take steps to ensure the deletion of the entry from the records of SCHUFA Holding AG, which reads as follows:

3 *Information from public registers*.

Discharge from remaining debts granted.	*This information is taken from the publications of the insolvency courts. We were notified of the granting of a discharge from remaining debts in respect of these insolvency proceedings.* *File reference 906IK1043-15PLZ30175.* *The event is registered with the insolvency courts under that file reference.*
Date of event 17.12.2020	

4 By order of the Amtsgericht Hannover (Local Court, Hanover) of 17 December 2020, the applicant was granted early discharge from remaining debts. That discharge was entered in the records kept at www.insolvenzbekanntmachungen.de. The entry on that website is deleted after 6 months. The joined party, SCHUFA Holding GmbH, also stores the entry in its database. The applicant contacted SCHUFA with a view to having the entry deleted. In response, the latter informed him that its activities are carried out in compliance with the GDPR. It stated that there is not an unconditional right to the deletion of personal data under Article 17 of the GDPR either. The entry concerning the discharge from remaining debts would be deleted after 3 years after its entry. The legislature has also recognised the need for information in commerce, such that creditworthiness information cannot be excluded from the credit information system. According to SCHUFA, the time limit for erasure under Paragraph 3(1) of the Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet (Regulation on public notifications in insolvency proceedings on the internet; 'the InsBekV') is not applicable to SCHUFA.

5 The applicant challenged those statements by letter to the defendant of 10 February 2021. He stated that the storage of the discharge from remaining debts in SCHUFA's records is unlawful. Such storage is not in fact necessary for the protection of interests. The interests of the data subject clearly prevail. It is not acceptable to equate a discharge from remaining debts which has been granted with unsettled payment irregularities. Even if it were accepted that processing of

the event is legitimate, it is no longer necessary after the expiry of a period of one year.

6 In response to that letter, the defendant informed the applicant by decision of 1 March 2021 that, while it understands the applicant's position, SCHUFA is permitted to store negative entries concerning discharges from remaining debts beyond the period of discharge from a claim. The legal basis is point (b) and point (f) of Article 6(1) of the GDPR and Paragraph 31 of the Bundesdatenschutzgesetz (Federal Law on data protection) of 30 June 2017 (BGBl. I, p. 2 097, last amended by the Law of 23 June 2021, BGBl. I, p. 1 858 – 'the BDSG'). Personal data required for a credit check can be stored for as long as is necessary for the purposes for which they were stored. In determining creditworthiness, it is permissible to draw on the behaviour of part of a group of persons to form probabilities in respect of the behaviour of other persons also belonging to that group and to establish statistical significance.

7 The applicant brought an action against that decision by written submission of his authorised representative of 6 April 2021. He claims that the joined party did not carry out a balancing of interests, and the defendant did not object to that omission. However, according to the applicant, the defendant is obliged, within the scope of its duties and powers, to take measures to enforce deletion.

II.

1. Charter of Fundamental Rights of the European Union ('the Charter')

8 Article 7 of the Charter

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

9 Article 8 of the Charter

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

10 Article 47 of the Charter

Right to an effective remedy and to a fair trial Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.

Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

2. 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)

11 Article 78

Data protection

1. National rules implementing Directive 95/46/EC shall apply to the processing of personal data carried out in the Member States pursuant to this Regulation, provided that processing operations referred to in Article 3(2) of Directive 95/46/EC are not concerned.

2. Regulation (EC) No 45/2001 shall apply to the processing of personal data carried out by the Commission pursuant to this Regulation.

12 **Article 79**

Responsibilities of Member States regarding the processing of personal data in national insolvency registers

1. Each Member State shall communicate to the Commission the name of the natural or legal person, public authority, agency or any other body designated by national law to exercise the functions of controller in accordance with point (d) of Article 2 of Directive 95/46/EC, with a view to its publication on the European e-Justice Portal.

2. Member States shall ensure that the technical measures for ensuring the security of personal data processed in their national insolvency registers referred to in Article 24 are implemented.

3. Member States shall be responsible for verifying that the controller, designated by national law in accordance with point (d) of Article 2 of Directive 95/46/EC, ensures compliance with the principles of data quality, in particular the accuracy and the updating of data stored in national insolvency registers.

4. Member States shall be responsible, in accordance with Directive 95/46/EC, 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.

3. 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 – GDPR) (OJ 2016 L 119, p. 1)

13 **Article 6 of the GDPR**

Lawfulness of processing

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

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(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;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(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;

(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.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

(…)

14 **Article 17 of the GDPR**

Right to erasure (‘right to be forgotten’)

1. 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:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(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;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

15 **Article 77 of the GDPR**

Right to lodge a complaint with a supervisory authority

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.

16 **Article 78 of the GDPR**

Right to an effective judicial remedy against a supervisory authority

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.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Insolvenzordnung (Insolvency Code; 'the InsO') of 5 October 1994 (BGBl. I p. 2 866), last amended by Article 5 of the Law of 16 July 2021 (BGBl. I, p. 2 947)

17 **Paragraph 9 of the InsO – Public notification**

(1) 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.

(2) The insolvency court may arrange for further publications to the extent provided for by regional law. The Federal Ministry of Justice and Consumer Protection is empowered to regulate, by ordinance, with the consent of the Bundesrat, the details of the centralised publication at national level on the internet. In that respect, provision shall be made for, in particular, time limits for erasure and rules to ensure that the publications

1. remain intact, complete and up-to-date,

2. can be traced back to their origin at any time.

(3) Public notification shall be sufficient to serve as proof of service on all parties, even where this law requires a specific type of service in addition thereto.

18 **Paragraph 286 of the InsO – Principle**

If the debtor is a natural person, he or she shall be discharged, in accordance with Paragraphs 287 to 303a, from the liabilities towards the insolvency creditors which had not been discharged in the insolvency proceedings.

19 **Paragraph 287a of the InsO – Decision of the insolvency court**

(1) If the application for discharge from remaining debts is admissible, the insolvency court shall establish, by order, that the debtor is granted discharge from remaining debts, provided that he or she complies with the obligations under Paragraphs 295 and 295a and that the conditions for refusal under Paragraphs 290 and 297 to 298 are not met. 2 The order shall be notified to the public. 3 The debtor has a right of immediate appeal against the order.

5. Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet (Regulation on public notifications in insolvency proceedings on the internet) of 12 February 2002 (BGBl. I 2002, p. 677; 'the InsBekV')

20 **Paragraph 1**

Public notifications in insolvency proceedings on the internet must comply with the requirements of this Regulation. The publication may contain only the data which are to be published pursuant to the Insolvency Code or other provisions prescribing public notification in insolvency proceedings.

21 **Paragraph 3 Time limits for erasure**

(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 protective measures published are lifted.

(2) The first sentence of subparagraph 1 shall apply to the 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 the discharge from remaining debts becomes final.

(3) Other publications under the Insolvency Code shall be erased one month after the first day of publication.

6. Bundesdatenschutzgesetz (Federal Law on data protection; 'the BDSG') of 30 June 2017 (BGBl. I, p. 2 097, last amended by the Law of 23 June 2021, BGBl. I, p. 1 858)

22 **Paragraph 31 of the BDSG**

Protection of trade and commerce in the context of scoring and credit reports

(1) The use of a probability value regarding specific future behaviour of a natural person for the purpose of deciding on the establishment, implementation or

termination of a contractual relationship with that person (scoring) shall be permissible only if

1. the provisions of data protection law have been complied with,

2. the data used to calculate the probability value are demonstrably relevant to the calculation of the probability of the specific behaviour, on the basis of a scientifically recognised mathematical statistical method,

3. the data used for the calculation of the probability value were not exclusively address data, and

4. where address data are used, the data subject has been notified of the intended use of such data before the calculation of the probability value; the notification must be documented.

(…)

III.

1. The first question referred

23 In the context of an application for leave to appeal in a case which also concerned a discharge from remaining debts and SCHUFA Holding AG (Administrative Court, Wiesbaden), judgment of 7 June 2021, Case 6 K 307/20.WI), the defendant supervisory authority took the view that Article 77(1) of the GDPR does not provide that the substantive correctness of a decision on a complaint is subject to judicial review. Rather, that provision contains a right of complaint which takes the form of a right of petition, which is subject to only limited judicial review. Within the framework of the judicial review, 'effective' judicial protection is limited to the authority handling the data subject's complaint in the first place and informing him or her of the progress and outcome of the complaint within the timeframes specified. Article 78(1) of the GDPR does not provide for more extensive judicial review.

24 There are different legal views on the legal nature of the decision of the national supervisory authority pursuant to Article 77 of the GDPR. In the case-law, the view is expressed, on the one hand, that the processing of a complaint is to be measured against the standard of review for petitions, that is to say, the processing of the complaint is to be regarded as appropriate if the defendant establishes the facts of the case and does not substantiate its legal assessment regarding both the submission and the subject matter of the complaint in a merely formulaic manner and informs the complainant of that outcome […]. The case-law which proceeds on the assumption that the right is similar to a right of petition argues that Article 77(1) of the GDPR has not changed anything in relation to the situation under the old law (Article 28(4) of Directive 95/46/EC).

25 The referring court has doubts as to whether that view is compatible with Article 77(1) of the GDPR. It is precisely not sufficient under Article 77(1) of the GDPR for the authority merely to handle the complaint, investigate the subject matter of the complaint to the extent appropriate and inform the data subject of the outcome of the assessment. This is because the principles established by the case-law in that regard correspond to those relating to a petition and therefore limit the right to an effective judicial remedy against the supervisory authority pursuant to Article 78(1) of the GDPR.

26 It is true that the original Article 28(4) of Directive 95/46/EC was worded similarly to Article 77(1) of the GDPR in force today and that a procedure resembling that for petitions had been adopted under the old law in Germany. However, Directive 95/46/EC did not contain a requirement for an effective remedy, as is now the case (Article 78 of the GDPR; see also Article 53 of Directive (EU) 2016/680). This is because the effective remedy under Article 47 of the Charter is now included under EU law (see Article 1(2) of the GDPR and Article 1(2) of Directive (EU) 2016/680). The EU legislature has therefore made a clear distinction between an ***effective*** legal remedy and a petition (see Article 44 of the Charter). Treatment resembling that applicable to petitions would not in any event lead to an effective remedy in the present case, but only to 'any kind of' remedy.

27 The enforcement of the GDPR would then be very much dependent on the seeking of remedies in a private capacity within the meaning of Article 79 of the GDPR and thus primarily on a task carried out in a private capacity. The fact that this cannot be in line with the spirit of the GDPR follows from the fact that the implementation of the requirements of the GDPR is the task of the Member States and their national administrations (Article 57(1)(a) of the GDPR). In particular, the mandate of national supervisory authorities to protect the fundamental rights and freedoms of natural persons in relation to processing, as expressly established in Article 51(1) of the GDPR, would be devoid of purpose if the supervisory authorities could not be required, by way of effective remedies, to perform their duties. Such a conclusion can also be drawn from recital 141, according to which natural persons have an effective judicial remedy where 'the supervisory authority does not act on a complaint […] where such action is necessary to protect the rights of the data subject'.

28 Having regard to the objective pursued by the GDPR, but also by Directive (EU) 2016/680, which is to ensure, in implementation of Articles 7 and 8 of the Charter, effective protection of the freedoms and fundamental rights of individuals, in particular, their right to protection of privacy and the protection of personal data, the handling of the right to lodge a complaint cannot be interpreted so restrictively that the supervisory authority need only act in just 'any manner' (see also, to that effect, CJEU, judgment of 15 June 2021, Case C-645/19, EU:C:2021:483, paragraph 91). Having regard also to the fact that, in the case of cross-border processing, the supervisory authority of another Member State could also establish that the processing of data in question is in breach of the rules contained in the

GDPR (see CJEU, judgment of 15 June 2021, Case C-645/19), it is *a fortiori* necessary for there to be a power of judicial review with regard to such a decision of the national supervisory authority in the complaint procedure under Articles 77 and 78 of the GDPR.

29 The Oberverwaltungsgericht Koblenz (Higher Administrative Court, Koblenz), which ruled, in its judgment of 26 October 2020 (Case 10 A 10613/20.OVG) in the case before it, that a complainant is entitled neither to a decision with specific content nor to a specific decision on the merits, did not refer the question concerning Regulation (EU) 2016/679 – *in casu*, Article 78(1) of the GDPR – to the Court of Justice of the European Union for definitive clarification in the case before it.

30 However, the court takes the view that the supervisory authority has a margin of assessment and discretion. According to Article 57(1)(a) of the GDPR, each supervisory authority must monitor and enforce the application of the GDPR. Article 58 of the GDPR regulates the powers of the supervisory authority (see also, in that regard, CJEU, judgment of 14 June 2021 in Case C-645/19). In that respect, the procedure does not differ in any way from triangular situations in national law, in which the party seeking judicial protection attempts to bring about official action at the expense of a private third party in order to enforce an individual public-law right. In that respect, too, the authority must fully investigate the facts of the case on the basis of the complainant's submission and act within the scope of its discretion to intervene. However, the discretion is reduced to zero if individual public-law rights have been infringed. In that respect, there is not the slightest argument in the present case against treating the complaint proceedings brought against the supervisory authority by a third party – the complainant – under the GDPR in the same way as has been the practice of the German administrative courts in national law for decades.

31 In order to achieve a uniform interpretation, it is necessary to obtain an answer to Question 1. In accordance with the foregoing, the referring court is inclined towards an interpretation to the effect that the supervisory authority's decision on the merits is to be subject to full review by the court, whereby the supervisory authority can, however, be obliged to take action only if lawful alternatives are not apparent (as in the abovementioned case where discretion is reduced to zero). Only in that way can effective judicial protection be ensured. Even if the supervisory authority is completely independent (see CJEU, judgment of 9 March 2010, Case C-518/07, EU:C:2010:125), that independence cannot lead to arbitrary action taken with impunity, which would be the case, however, if the procedure were of a nature resembling that applicable to petitions.

2. The second to fifth questions referred

32 Private credit information agencies receive all entries from the public registers, in this case the debtors' list and the insolvency register, from the State – *in casu*, the

joined party Schufa Holding AG receives such entries from the judicial administration service of Rhineland-Palatinate. The present case specifically concerns the entry and public announcement of the discharge from remaining debts on the website 'insolvenzbekanntmachungen.de' operated by North Rhine-Westphalia on behalf of the German *Länder*. In that context, it is unclear whether there is a regime governing a joint procedure pursuant to Article 26 of the GDPR.

33 In that respect, the question arises, in the light of Articles 6 and 7 of the Charter, as to whether the entries from the public registers can be transferred as such to privately kept registers without there being a specific reason for the storage of such data with the private credit information agency. Rather, the purpose of the storage is to be able to use the data in the event of a possible request for information by an economic operator, for example a bank. In that context, the question of whether such information is ever requested is completely open. This ultimately leads to data retention, especially if the data have already been deleted from the national register because the retention period has expired.

34 National law (Paragraph 31 of the BDSG) contains rules for scoring carried out by credit agencies, but makes them subject, in turn, to compatibility with (European) data protection law (point 1 of Paragraph 31(1) of the BDSG). National law does not contain a time limit for erasure in respect of the databases of credit information agencies.

35 In the present case, the defendant proceeds on the assumption that those personal data serve to assess creditworthiness and can 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, the supervisory authorities, together with the association of credit information agencies, have created 'Codes of conduct', which provide for erasure precisely three years after the entry in the file of the credit information agency concerned (see 'Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien' (Codes of conduct concerning the time limits for review and erasure by German credit information agencies) of 25 May 2018 of the association 'Die Wirtschaftsauskunfteien e. V.', which have been approved by the supervisory authorities in accordance with Article 40 of the GDPR).

36 This means that the discharge from remaining debts which is at issue in present case must be erased from the public register of insolvency announcements after 6 months, but, in the case of the private credit information agencies (just seven large companies), it can be stored for a much longer period, possibly for another three years, and can be processed for the purposes of providing information.

37 The referring court takes the view that there are already doubts as to whether it is permissible at all for such data to be held at a large number of private companies 'in parallel' to the State registers. In that respect, it should be borne in mind that the joined party Schufa Holding AG is only one of several credit information agencies and, consequently, data is often stored in this way in Germany, entailing

a massive encroachment on the fundamental right under Article 7 of the Charter. This is the case above all because such 'data retention' is not regulated by law and is capable of massively interfering with the economic activity of a data subject, both with and without justification […].

38 In addition, under the GDPR, processing and thus storage of data is permissible only if one of the conditions of Article 6(1) of the GDPR is met. Only point (f) of Article 6(1) of the GDPR enters into consideration in the present case. This is because, as an economically active company, the joined party does not perform a task carried out in the public interest or in the exercise of official authority (point (e) of Article 6(1) of the GDPR) […].

39 It is also more than doubtful that there is a legitimate general interest pursued by the controller (*in casu*, Schufa Holding AG) or by a third party (for example a lending bank) pursuant to point (f) of Article 6(1) of the GDPR. At best, the credit information agency has a fundamental interest in storing the discharge from remaining debts because it is an economically relevant piece of data by means of which the joined party earns its revenue if it also assesses it in a credit check.

40 However, this is contrary to the legislative spirit of Paragraph 3 of the InsBekV, which proceeds on the basis of a retention period of (only) six months in the insolvency register […]. The required balancing of interests should lead to entitlement to process data only if the data from the insolvency register are in fact imperatively needed to provide information on a financial situation.

41 In addition, in Paragraph 3 of the InsBekV, the German legislature provides for only a relatively short storage period of six months for discharges from remaining debts in the insolvency register. The provision made in Paragraph 3 of the InsBekV is based, in turn, on Article 79(5) of Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings (OJ L 141, p. 19), according to which Member States are to inform data subjects of the accessibility period set for personal data stored in insolvency registers so as to enable them to exercise their rights, and in particular the right to the erasure of data. That right does not apply where the data are stored in a large number of 'private' registers, in which case the data are stored for longer.

42 This leads to the fundamental question of whether data from the insolvency register may be transferred in their entirety to a 'private' database at all, since a credit information agency with a legitimate interest is in any event able to query the insolvency register for as long as the data are stored there. If credit information agencies were permitted to store data, this would lead to parallel data retention and would deprive the data subject of the possibility to exercise the right to erasure of data before the insolvency court. Thus, the credit information agencies storing the data would be carrying out a form of data retention. The referring court takes the view that such retention should not be permissible in the context of Article 8 of the Charter and point (f) of Article 6(1) of the GDPR. In many cases, the data subject would also have to assert his or her rights against all

the credit information agencies, which would ultimately mean that multiple requests for erasure would have to be made and effective legal protection would be more difficult to obtain.

43 In so far as it is deemed to be permissible for data from public registers to be stored at private companies (credit information agencies), as is currently assumed by the supervisory authority, the question then arises as to whether the approved private codes of conduct pursuant to Article 40 of the GDPR, which provide for standard time limits for erasure, are to be included in the balancing of interests under point (f) of Article 6(1) of the GDPR. Accordingly, both the joined party and the defendant supervisory authority consider that there is 'authorisation to store data' in respect of the discharge from remaining debts for a period of three years under the 'codes of conduct'.

44 In that respect, the present Chamber shares the view taken by the Oberlandesgericht Schleswig-Holstein (Higher Regional Court, Schleswig-Holstein), according to which the time limits for review and erasure under point II.2.b) of the codes of conduct concerning discharges from remaining debts run counter to the provisions in Paragraph 9 of the InsO and Paragraph 3 of the InsBekV (Higher Regional Court, Schleswig-Holstein, judgment of 4 June 2021, Case 17 U 15/21, II. 1. (c) (cc). Therefore, the codes of conduct do not make the data processing (storage) lawful. Consequently, those codes – even if approved by the supervisory authorities – must not be included in the required balancing of interests pursuant to point (f) of Article 6(1) of the GDPR, either with regard to the case where a credit agency has a legitimate interest or with regard to the retention period and thus the time limits for erasure.

45 Rather, in the event that it is permissible for data from public registers to be stored at credit information agencies, the time limits for retention and erasure that are applicable to such 'private parties' should at most be the same as those applicable to public registers. This would mean that data which must be deleted from the public register would also have to be simultaneously deleted at all private credit information agencies which have additionally stored those data.

46 Since the present case concerns the fundamental question of whether data from public registers can be stored at private companies and, if that question is answered in the affirmative, the question of when such data must be deleted at those companies, the present proceedings are stayed and the matter is referred to the Court of Justice. Proceeding on the basis of the Court of Justice's answers to these highly contentious questions concerning Articles 7 and 8 of the Charter and point (f) of Article 6(1) of the GDPR, it will be possible to rule definitively on the case.

IV.

47 The order is not open to appeal.

[…] Wiesbaden, 5 January 2022

[…] [Note regarding official copies]