Reports of Cases

OPINION OF ADVOCATE GENERAL
PIKAMÄE
delivered on 16 March 2023 [1]

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

UF (C-26/22)
AB (C-64/22)
v
Land Hesse,
Joined party:
SCHUFA Holding AG

(Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany))

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Point (f) of the first subparagraph of Article 6(1) – Lawfulness of processing – Article 17(1)(d) – Right to erasure where personal data have been unlawfully processed – Article 40 – Codes of conduct – Article 77(1) – Right to lodge a complaint – Article 78(1) – Right to an effective judicial remedy against a supervisory authority – Articles 7 and 8 of the Charter of Fundamental Rights of the European Union – Decision taken by the supervisory authority on a complaint – Scope of judicial review of that decision – Private credit information agencies – Storage of data from a public register – Legitimate interest – Storage period)

I. Introduction

1. The present requests for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany) under Article 267 TFEU 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) ('the GDPR'). [2]

[1] Original language: French.

[2] OJ 2016 L 119, p. 1.

2. The requests have been made in two sets of proceedings between, first, UF (Case C-26/22) and, second, AB (Case C-64/22) and Land Hessen, represented by the Hessischer Beauftragter für Datenschutz und Informationsfreiheit (Data Protection and Freedom of Information Commissioner for Land Hessen; 'HBDI'), concerning requests, made to the HBDI by UF and AB respectively, to take steps to ensure the deletion of an entry relating to discharge from remaining debts from the records of SCHUFA Holding AG ('SCHUFA').

3. The two cases raise a range of novel legal questions relating to, among other things, the legal nature of the decision taken by the supervisory authority hearing a complaint, and the scope of the judicial review which the court may exercise in the context of proceedings brought against such a decision. Those cases also concern the question of the lawfulness of the storage of personal data from public registers by credit information agencies.

II. Legal framework

A. European Union law

1. Regulation (EU) 2015/848

4. Under 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: [3]

'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.'

2. The GDPR

5. Article 5 of the GDPR provides, in paragraph 1:

'Personal data shall be:

…

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; … ("purpose limitation"):

…'

[3] OJ 2015 L 141, p. 19.

6. Article 6 of that regulation stipulates, in paragraph 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 ….

…'

7. Article 17 of the GDPR provides, in paragraph 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:

…

(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;

…'

8. Article 21 of that regulation stipulates, in paragraph 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.'

9. Article 40 of the regulation provides:

'1. The Member States, the supervisory authorities, the Board and the 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.

…'

10. Article 77 of the GDPR stipulates, in paragraph 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.'

11. Article 78 of that regulation provides:

'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.

…'

B. German law

12. Paragraph 9 of the Insolvenzordnung (Insolvency Code), in the version in force at the time of the facts in the main proceedings, provides, in its paragraph 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.'

13. Paragraph 3 of the Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet (Regulation on public notifications in insolvency proceedings on the internet) ('the InsBekV') stipulates, in its paragraphs 1 and 2:

'(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 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.'

III. The facts giving rise to the disputes, the main proceedings and the questions referred for a preliminary ruling

14. In the insolvency proceedings in respect of them, UF and AB were granted early discharge from remaining debts by judicial orders made on 17 December 2020 and 23 March 2021 respectively. Under Paragraph 9(1) of the Insolvency Code and Paragraph 3(1) and (2) of the InsBekV, this was subject to official notification on the internet, which was deleted after six months.

15. SCHUFA, a private credit information agency, enters published information relating to early discharges from remaining debts in its own databases but does not delete it until three years after entry.

16. When contacted by UF and AB respectively to request the erasure of the entries concerning them, SCHUFA informed them that its activity complied with the GDPR and that the time limit for erasure of six months under Paragraph 3(1) of the InsBekV was not applicable to it. UF and AB thereupon each lodged a complaint with the HBDI as the competent supervisory authority.

17. The HBDI ruled on those complaints by two decisions made on 1 March 2021 and 9 July 2021 respectively. In its view, SCHUFA is permitted to store negative entries concerning discharges from remaining debts beyond the period of discharge from a claim.

18. UF and AB each brought an action against the decision of the HBDI at the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden), the referring court. In this respect, they assert that the HBDI is obliged, within the scope of its duties and powers, to take measures in respect of SCHUFA to enforce deletion of the entries concerning them.

19. In this regard, the referring court considers it necessary, first, to clarify the legal nature of the decision made by the supervisory authority on a complaint lodged under Article 77(1) of the GDPR. The court explains that, in the view of the HBDI, the right provided for in Article 77(1) takes the form of a right of petition. It is thus subject to only limited judicial review, which is confined to examining whether the supervisory authority handled the complaint and informed the complainant of the progress and outcome of the complaint. By contrast, the substantive correctness of the decision on a complaint is not subject to judicial review.

20. Nevertheless, the referring court has doubts whether this analysis is compatible with the GDPR. It states that Article 78(1) of that regulation requires an effective judicial remedy. 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, the handling of the right to lodge a complaint cannot be interpreted restrictively. The referring court is therefore 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, while bearing in mind that that authority has both a margin of assessment and a discretion and that it can be obliged to take action only if lawful alternatives are not apparent.

21. Second, the referring court raises the question of the lawfulness of the storage of data from public registers by credit information agencies. The court states in this regard that these agencies receive all entries from the public registers, in this case the debtors' list and the insolvency register, from the State. Those data serve, according to the HBDI, to assess creditworthiness and can be stored for as long as is necessary for the purposes for which they were stored. Furthermore, 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.

22. According to the referring court, the question arises in the light of Articles 7 and 8 of the Charter as to whether the entries in the public registers can be transferred as such to privately kept registers without there being a specific reason for the storage of such data. This ultimately constitutes data retention, especially if the data have already been deleted from the national register because the retention period has expired. Furthermore, 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.

23. The referring court adds that processing and thus storage of data is permissible only if one of the conditions laid down in Article 6(1) of the GDPR is met, it being specified that only point (f) of the first subparagraph of Article 6(1) of that regulation enters into consideration in the present case. It is doubtful that a controller such as SCHUFA has a legitimate interest within the meaning of that provision. In any event, a credit information agency with a legitimate interest is able to query public registers for as long as the data are stored there.

24. 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. That provision is based on Article 79(5) of Regulation 2015/848, under 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, however, where the data are stored in a large number of private registers, in which case the data are stored for a longer time.

25. Moreover, even if it is deemed to be permissible for data from public registers to be stored by private credit information agencies, the question might arise as to whether the codes of conduct approved pursuant to Article 40 of the GDPR, which provide for a time limit for erasure of three years in respect of discharge from remaining debts, are to be included in the balancing of interests required for the assessment under point (f) of the first subparagraph of Article 6(1) of the GDPR.

26. 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:

(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 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

(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 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 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 that regulation?'

IV. Procedure before the Court

27. The order for reference in Case C-26/22, dated 23 December 2021, was received at the Court Registry on 11 January 2022. The order for reference in Case C-64/22, dated 31 January 2022, was received at the Court Registry on 2 February 2022.

28. By decision of the Court of 11 February 2022, those cases were joined for the purposes of the written and oral procedure and the judgment.

29. The parties to the main proceedings, SCHUFA, the German and Portuguese Governments and the European Commission submitted written observations within the period prescribed by Article 23 of the Statute of the Court of Justice of the European Union.

30. At the hearing on 26 January 2023, oral argument was presented by the legal representatives of the parties to the main proceedings and of SCHUFA and the agents of the Commission.

V. Legal analysis

A. Preliminary remarks

31. Since mutual confidence forms the basis for any contractual commitment in a market economy, it is understandable in principle, from a business point of view, that providers of goods and services wish to know about their clients and the risks inherent in such contractual commitment. Credit information agencies can help to establish this mutual confidence using statistical methods that allow undertakings to determine whether certain relevant criteria, including the creditworthiness of their clients, are met in a specific case. By doing so, they help undertakings to comply with various provisions of EU law which impose precisely that obligation on them for certain categories of contracts, in particular credit agreements.[4] That being said, those companies are not the only entities to provide such services. Aware of the need to ensure a degree of transparency and foreseeability in financial transactions, the EU legislature requires Member States to establish and maintain one or several registers in which information concerning insolvency proceedings is published.

32. It follows that several databases will exist in parallel: on the one hand, 'official' registers managed by public authorities and, on the other, databases administered by private agencies. This parallelism may lead to competition between systems or even give rise to legal conflicts if the legal arrangements governing those registers differ significantly. Regulatory differences can become especially problematical if they affect the protection of data since, whether the entity managing the register is public or private, it must respect the data subjects' interest in the way in which the data are managed and recorded. Because information concerning an individual's economic situation is sensitive from the point of view of respect for the right to protection of personal data and for private life, particular vigilance is required.

[4] These are specifically Articles 18 and 21 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), and Articles 8 and 9 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).

33. The GDPR, which has applied since 25 May 2018, established a legal framework which seeks to take account of the abovementioned interests throughout the European Union, particularly by imposing certain conditions on the processing of personal data. Thus, point (f) of the first subparagraph of Article 6(1) of the GDPR requires that 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 other words, the lawfulness of processing must be apparent from a balancing of the various interests at stake in which the legitimate interests pursued by the controller or by a third party must take precedence. It is for the supervisory authority, which, under Article 77(1) of the GDPR, will have to handle any complaint lodged by the data subject concerning the infringement of his or her fundamental rights, to ascertain whether those conditions are met. Lastly, if the data subject decided to seek a remedy against the decisions of the supervisory authority pursuant to Article 78(1) of the GDPR, it would be for the national courts to carry out an effective judicial review.

34. The preceding points of this Opinion briefly summarise the different legal aspects raised by the referring court in its requests for a preliminary ruling. The first question concerns the nature legal of a decision taken by the supervisory authority hearing a complaint and the scope of the judicial review to be exercised by the court in the context of proceedings brought against such a decision. The second to fifth questions relate, in essence, to the lawfulness of storage of personal data from public registers by credit information agencies. The questions referred will be examined below in the order in which they were asked by the referring court.

B. The first question referred for a preliminary ruling

35. Since the first question concerns the two stages of the administrative remedy, namely the complaint to the supervisory authority and the judicial remedy before the courts, governed by Articles 77 and 78 of the GDPR respectively, I think it appropriate to describe these two stages briefly and, in doing so, to address the legal aspects about which the referring court raises questions.

36. As I stated in my preliminary remarks, the GDPR seeks to ensure the protection of natural persons with regard to the processing of personal data, which is recognised as a fundamental right in Article 8(1) of the Charter and in Article 16(1) TFEU. Since any processing of personal data can have an impact on private life, mention should also be made of the protection guaranteed by Article 7 of the Charter.[5] Furthermore, it is clear from Article 1(2) of the GDPR, read together with recitals 10, 11 and 13 thereof, that the EU legislature confers this task on the EU bodies, offices and agencies, but also on the competent authorities of the Member States, which include supervisory authorities and national courts.[6]

1. The role of supervisory authorities, including the obligation to examine complaints

37. Article 8(3) of the Charter provides that compliance with the rules on protection of personal data is subject to control by an independent authority. Article 57(1)(a) of the GDPR implements this obligation stemming from primary law and provides that the task of each supervisory

[5] See Opinion of Advocate General Szpunar in *Latvijas Republikas Saeima (Penalty points)* (C-439/19, EU:C:2020:1054, point 48).

[6] Judgment of 15 June 2021, *Facebook Ireland and Others* (C-645/19, EU:C:2021:483, paragraphs 44 and 45).

authority is to *monitor and enforce the application of that regulation*. The handling of complaints lodged by a data subject is among its responsibilities, as is expressly stated in Article 57(1)(f) of the GDPR.

38. The Court has ruled that under that provision 'each supervisory authority *is required* on its territory *to handle complaints* which, in accordance with Article 77(1) of [the GDPR], 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'.[7] It should be pointed out in this connection that the Court has underlined the supervisory authority's obligation to 'handle such a complaint *with all due diligence*' in order to ensure compliance with the provisions of the GDPR. It should also be noted that recital 141 of the GDPR states that 'the investigation following a complaint should be *carried out … to the extent that is appropriate in the specific case*' (my emphasis).

39. All these factors suggest that the supervisory authority has a *binding obligation to handle complaints* lodged by data subjects with all due diligence that is appropriate in the specific case.[8] In so far as any infringement of the GDPR is, in principle, capable of constituting an infringement of fundamental rights, it would seem to be incompatible with the system established by that regulation to allow the supervisory authority discretion as to whether or not to handle complaints. Such an approach would undermine the crucial role conferred on it by the GDPR, which is to ensure compliance with the rules on the protection of personal data, and would therefore run counter to the objectives pursued by the EU legislature.[9] Ultimately, it should be borne in mind that complaints are an important source of information for the supervisory authority, enabling it to identify infringements.[10]

40. This interpretation is all the more convincing because Article 57(1)(f) of the GDPR imposes on the supervisory authority a number of requirements in connection with the handling of such a complaint, namely the obligation to investigate, to the extent appropriate, the subject matter of the complaint and to 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. Additionally, there is the obligation under Article 77(2) of the GDPR to inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78 of the GDPR. All these requirements, coming under the concept of 'good administration' which found expression in Article 41 of the Charter specifically with regard to the activities of the institutions and bodies of the European Union,[11] are intended to strengthen the complaints procedure in order to make it a *genuine administrative remedy*.

7 Judgment of 16 July 2020, *Facebook Ireland and Schrems* (C-311/18, EU:C:2020:559, paragraph 109).

8 See, to that effect, Kotschy, W., 'Article 77. Right to lodge a complaint with a supervisory authority', *The EU General Data Protection Regulation (GDPR)* (Kuner, C., Bygrave, L.A., Docksey, C. and Drechsler, L. (eds.), Oxford, 2020, p. 1123.

9 See, to that effect, Härting, N., Flisek, C. and Thiess, L., 'DSGVO: Der Verwaltungsakt wird zum Normalfall – Das neue Beschwerderecht', *Computer und Recht*, 5/2018, p. 299, who state that under Article 57(1)(a) of the GDPR the supervisory authority has the task of monitoring and enforcing the application of the GDPR in the interest of data subjects. According to the authors, it may not remain inactive when the rights of a citizen are infringed by processing of personal data. On the contrary, the supervisory authority is obliged to remedy the situation and exercise its powers under Article 58(2) of the GDPR.

10 See, to that effect, Hijmans, H., 'Article 55. Tasks', *The EU General Data Protection Regulation (GDPR)*, Kuner, C., Bygrave, L.A., Docksey, C. and Drechsler, L. (eds.), Oxford, 2020, pp. 934 and 936.

11 See my Opinion in *Parliament* v *UZ* (C-894/19 P, EU:C:2021:497, point 68) for a detailed explanation of the concept of 'good administration' in EU administrative law.

41. Although the supervisory authority, as guarantor of compliance with the provisions of the GDPR, is required to handle complaints lodged with it, several factors militate in favour of an interpretation to the effect that it enjoys a *margin of assessment in examining those complaints* and a *degree of latitude in the choice of the appropriate means* to carry out its tasks. Advocate General Saugmandsgaard Øe has noted that Article 58(1) of the GDPR 'confers on the supervisory authorities … significant investigative powers' and that they have, under Article 58(2) of that regulation, 'a wide range of means … of carrying out the task entrusted to [them]', referring in this connection to the various powers to adopt corrective measures listed in that provision.[12] It was then stated that, although the competent supervisory authority 'is required to carry out in full the supervisory task entrusted to it', 'the choice of the most effective means is a matter for [its] discretion … having regard to all the circumstances … at issue'.[13] I can only concur with this interpretation.

42. The detailed description of the supervisory authorities' power to adopt corrective measures shows that the EU legislature did not intend to make the complaint procedure similar to a petition procedure. On the contrary, the legislative objective seems to have been to establish a mechanism capable of *effectively safeguarding the rights and interests of individuals who lodge complaints*. It nevertheless seems clear that this latitude cannot be interpreted to mean that the supervisory authority has unlimited power, authorising it to act arbitrarily. On the contrary, the supervisory authority is obliged to exercise that latitude having regard to the limits imposed on it by EU law. For this reason too, it cannot be ruled out that the supervisory authority, as an administrative organ, will be forced to adopt a certain measure on account of the particular circumstances of the case, especially where there is a serious risk of an infringement of the fundamental rights of the data subject.

43. This interpretation, which allows the supervisory authority a degree of latitude in the choice of means, is corroborated by Article 58(4) of the GDPR, which provides that 'the exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including *effective judicial remedy*' (my emphasis) in accordance with Article 47 of the Charter. Furthermore, Article 78(1) and (2) of the GDPR recognises that each data subject has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them or where that authority fails to handle their complaint.

44. This brings us to the question of the *legal nature of decisions taken by the supervisory authority* which has been raised by the referring court in its requests for a preliminary ruling. Mention should be made in this regard of recital 141 of the GDPR, according to which 'every subject should have the right to lodge a complaint with a … supervisory authority … 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' (my emphasis). That recital takes account of the fact that a decision of the supervisory authority can adversely affect the data subject, particularly if it concludes that the complaint is unfounded or finds that there is no infringement of the GDPR and does not therefore take measures to rectify the situation which gave rise to the complaint. The EU legislature recognises *the legally binding effect of such a decision* and therefore makes a remedy available to the complainant before a national court.

12 Opinion of Advocate General Saugmandsgaard Øe in *Facebook Ireland and Schrems* (C-311/18, EU:C:2019:1145, points 146 and 147).

13 Opinion of Advocate General Saugmandsgaard Øe in *Facebook Ireland and Schrems* (C-311/18, EU:C:2019:1145, point 148).

45. Similarly, it should be noted that *it is not permissible for the supervisory authority not to take action* as, under Article 78(2) of the GDPR, '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'. This means that the complaint procedure cannot be viewed in the same way as a petition.

46. In the present case, as the referring court explained in its orders for reference, the supervisory authority adopted legally binding decisions in respect of the applicants in the main proceedings. It held, in essence, that the processing of the applicants' personal data by SCHUFA was lawful under Article 6(1)(b) and (f) of the GDPR and, on that basis, implicitly rejected recourse to an investigative or corrective measure.

2. The scope of judicial review of decisions taken by the supervisory authority

47. The legal remedy provided for in Article 78 of the GDPR represents the second stage of the administrative remedy under that regulation. It should be noted that both the 'complaint' to the supervisory authority and the 'legal remedy' are conceived as 'rights' of the data subject, which is perfectly understandable if it is presumed that Articles 77 to 79 of the GDPR seek to *implement the right to an effective remedy* enshrined in Article 47 of the Charter. As I stated above,[14] a combined reading of Article 58(4) and Article 78 of the GDPR, in the light of recital 141 of that regulation, makes it possible to identify that objective clearly.[15]

48. As regards *the scope of judicial review* of decisions taken by the supervisory authority, the national rules governing administrative procedure apply generally within the scope of procedural autonomy, subject to the principles of equivalence and effectiveness.[16] However, in my view, a remedy can be 'effective' within the meaning of Article 47 of the Charter and Article 78(1) of the GDPR only if the national court having jurisdiction has the power and is under an obligation to submit the supervisory authority's decision on the merits to a *full judicial review* in order to determine whether the supervisory authority has correctly applied the GDPR.

49. As the Court has held in its case-law, 'legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law'.[17]

50. In order to determine the scope of judicial review of decisions taken by the supervisory authority, it would seem appropriate to recall, first, recital 141 of the GDPR, according to which 'the investigation following a complaint should be carried out, *subject to judicial review*, to the

[14] See points 43 and 44 of this Opinion.

[15] See judgment of the EFTA Court of 10 December 2020 in Joined Cases E-11/19 and E-12/19, *Adpublisher AG* v *J and K*, paragraph 58, in which that Court notes that Article 58(4) and Article 78 of the GDPR 'give expression to the right to an effective judicial remedy'.

[16] Judgment of 7 September 2021, *Klaipėdos regiono atliekų tvarkymo centras* (C-927/19, EU:C:2021:700, paragraph 146).

[17] See judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650, paragraph 95).

extent that is appropriate in the specific case' (my emphasis). Second, mention should be made of recital 143 of the GDPR, which states that 'each 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*' (my emphasis). In my view, these passages should be understood to mean that the judicial review to be carried out by the national court under Article 78 of the GDPR must be full, that is to say, it must extend to all relevant aspects which fall within the margin of assessment available to the supervisory authority in examining the subject matter of a complaint and within its discretion in respect of the choice of investigative and corrective measures.

51. The EU legislature's objective of guaranteeing a full judicial review of any decision of a supervisory authority which produces legal effects in respect of the data subject who lodged a complaint with it becomes particularly clear if consideration is given to another passage of recital 143 of the GDPR, which states that '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*' (my emphasis). [18] In my view, only a judicial review having this scope satisfies the requirements laid down in Article 47 of the Charter. [19]

52. By contrast, the arguments raised by SCHUFA and the HBDI in favour of a limited judicial review of decisions of the supervisory authorities do not seem convincing. First, the aim of the 'independence' conferred on the supervisory authority under Article 52 of the GDPR, which gives specific expression to the requirement laid down in Article 8(3) of the Charter, is to protect that authority from any undue interference, but it does not exempt it from the obligation to exercise its duties and powers in full compliance with EU law and to submit its decisions to effective judicial review, like any other national authority. Second, the existence of a right to a judicial remedy against the controller, provided for in Article 79 of the GDPR, does not preclude the right to seek a remedy against a decision taken by the supervisory authority under Article 78 of the GDPR. These remedies coexist independently, neither remedy being subsidiary to the other, such that they may be exercised in parallel. [20] The applicants cannot therefore be criticised for having acted unlawfully in defending their rights protected by the GDPR on the ground that they gave precedence to a certain remedy. These arguments must therefore be rejected.

53. In the light of the above considerations, the answer to the first question must be that Article 78(1) of the GDPR must be interpreted as meaning that under that provision a legally binding decision of a supervisory authority is subject to a full substantive judicial review.

[18] See judgment of 12 January 2023, *Nemzeti Adatvédelmi és Információszabadság Hatóság* (C-132/21, EU:C:2023:2, paragraph 41).

[19] See, to that effect, Kotschy, W., 'Article 77. Right to lodge a complaint with a supervisory authority', *The EU General Data Protection Regulation (GDPR)*, Kuner, C., Bygrave, L.A., Docksey, C. and Drechsler, L. (eds.), Oxford, 2020, pp. 1127 to 1130.

[20] See Opinion of Advocate General Richard de the Tour in *Nemzeti Adatvédelmi és Információszabadság Hatóság* (C-132/21, EU:C:2022:661, point 43 et seq.).

C. The second to fifth questions referred for a preliminary ruling

54. The second to fifth questions referred for as preliminary ruling relate, in essence, to the lawfulness of storage of personal data from public registers by credit information agencies. The questions asked by the referring court raise a number of legal problems connected with this practice, which must be examined in a structured manner. For the sake of clarity, the questions should be grouped thematically and addressed in that order.

55. In order to provide the referring court with an answer which will be of use to it and enable it to determine the case before it, the Court will be required to interpret a number of provisions of the GDPR which, although not expressly mentioned in the questions, nevertheless appear to be relevant. This approach is possible since, according to settled case-law, the Court may extract from all the information provided by the referring court, in particular from the grounds of the order for reference, the legislation and the principles of EU law that require interpretation in view of the subject matter of the dispute in the main proceedings. [21]

56. It seems all the more necessary to conduct a detailed analysis because at times the national court refers solely to Articles 7 and 8 of the Charter in its questions even though those provisions are not applicable in isolation, as has been explained by the Court, but are to be taken into account in the balancing of interests under point (f) of the first subparagraph of Article 6(1) of the GDPR. [22] It should also be borne in mind in this context that, in so far as the provisions of the GDPR implement the fundamental rights at issue, the logical starting point for any exegesis is the interpretation of secondary law, which must be read in the light of primary law, of which the Charter forms an integral part. [23] I will therefore include in the analysis below all provisions which seem relevant.

1. Compliance of the practice of credit information agencies with the principles governing the processing of personal data enshrined in the GDPR

57. Chapter II of the GDPR, entitled 'Principles', lays down the principles relating to processing of personal data. I will examine below whether the practice of credit information agencies of storing personal data from public registers for a period of three years complies with the principles which seem most relevant in the present context, namely the principles of lawfulness, purpose limitation and data minimisation.

58. For the purposes of this analysis, I will rely on the information provided by the referring court and SCHUFA, while emphasising that it is for SCHUFA, as the controller, to demonstrate compliance with the abovementioned principles in accordance with the principle of accountability laid down in Article 5(2) of the GDPR.

[21] Judgments of 11 November 2020, *DenizBank* (C-287/19, EU:C:2020:897, paragraph 59), and of 24 February 2022, *Glavna direktsia 'Pozharna bezopasnost i zashtita na naselenieto'* (C-262/20, EU:C:2022:117, paragraph 33).

[22] Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA* (C-708/18, EU:C:2019:1064, paragraph 32).

[23] Judgment of 26 April 2022, *Poland* v *Parliament and Council* (C-401/19, EU:C:2022:297, paragraph 47).

(a) Compliance with the principle of lawfulness (point (f) of the first subparagraph of Article 6(1) of the GDPR)

59. Article 5(1)(a) of the GDPR provides that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. Under Article 6(1) of the GDPR, processing of personal data is lawful only if one of the grounds set out therein applies. As the Court has ruled, this is an exhaustive and restrictive list of the cases in which such processing can be regarded as lawful.[24] The referring court wishes to know, in essence, whether point (f) of the first subparagraph of Article 6(1) of the GDPR authorises a private credit information agency to store personal data from public registers in order to make those data available to a client in the event of a request.

60. According to the Court's case-law,[25] point (f) of the first subparagraph of Article 6(1) of the GDPR lays down three cumulative conditions in order for the processing of personal data to be lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or third parties to which the data are communicated; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence. While it is for the referring court to assess whether these conditions are satisfied, the Court must guide it in making that assessment by clarifying the questions of law raised.

(1) The existence of a 'legitimate interest'

61. First, with regard to the pursuit of a 'legitimate interest', I would point out that the GDPR and the case-law recognise a wide range of interests considered legitimate,[26] while specifying that, according to Article 13(1)(d) of the GDPR, it is the responsibility of the controller to indicate the legitimate interests pursued under point (f) of the first subparagraph of Article 6(1) of the GDPR.

62. SCHUFA asserts that the processing of data in question serves the pursuit of legitimate interests of great importance. More specifically, 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. This also protects the economic interests of undertakings wishing to conclude contracts linked to credit. In addition, the determination of creditworthiness and the provision of credit information form the basis for credit and for 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.

63. In my view, there is in principle no objective reason to doubt the legitimacy of SCHUFA's interest in providing the business service described above to its clients or the interest of SCHUFA's clients in utilising its services to assess the creditworthiness of potential business partners along those lines. Whilst it is true that the purpose of providing this kind of service is to obtain remuneration and it therefore constitutes the economic model of a private company, this is not sufficient, in itself, to alter the fact that the first condition laid down in point (f) of the first subparagraph of Article 6(1) of the GDPR is satisfied in the present case.

[24] Judgments of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)* (C-439/19, EU:C:2021:504, paragraph 99), and of 1 August 2022, *Vyriausioji tarnybinės etikos komisija* (C-184/20, EU:C:2022:601, paragraph 67).

[25] Judgment of 17 June 2021, *M.I.C.M.* (C-597/19, EU:C:2021:492, paragraph 106).

[26] See, in this regard, Opinion of Advocate General Rantos in *Meta Platforms and Others (General terms of use of a social network)* (C-252/21, EU:C:2022:704, point 60).

64. This holds a fortiori where the objective pursued by the service in question is essentially similar to that which the EU legislature had in view in adopting Article 24 of Regulation 2015/848, which requires Member States to establish and maintain in their territory one or several registers in which information concerning insolvency proceedings is published. As is apparent from recital 76 of that regulation, the objective of those public registers is to 'improve the provision of information to relevant creditors and courts and to prevent the opening of parallel insolvency proceedings'. It seems that the service offered by SCHUFA has no other purpose. The question whether the parallelism of systems can give rise to legal conflicts will be examined below. It is sufficient to note at this stage in the analysis that, given that the objectives are the same, the processing of data by SCHUFA must be considered to serve a legitimate interest within the meaning of point (f) of the first subparagraph of Article 6(1) of the GDPR.

(2) The 'need' to process for the purposes of the legitimate interest

65. As to the condition relating to the need to process personal data for the purposes of the legitimate interests pursued, according to the case-law of the Court of Justice, derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.[27] It is necessary therefore for a close link to exist between the processing and the interest pursued, in the absence of alternatives that are more data-protection friendly, since it is not enough for the processing merely to be of use to the controller.

66. In this case, it would have to be demonstrated that the retrieval of personal data concerning insolvency from public registers and the private storage of those data are the only means for SCHUFA to offer that precise information to its clients for business purposes. It is possible that SCHUFA is able to offer the business service and provide credit information on individuals by having recourse to other available sources of data. It is for the referring court to determine whether this possibility would still allow SCHUFA profitably to offer this business service to its clients.

67. SCHUFA submits that the processing of data is necessary. In its view, if a credit information agency waited for a specific request before starting to collect data, it would be impossible to provide a report in good time. SCHUFA maintains that the fact that data are (also) available to the public for a certain time has no impact on the legitimate interests of credit information agencies or on the need for processing.

68. If the storage of personal data from public registers was not necessary in order to enable SCHUFA to offer its business service to its clients, that processing could not be lawful on the basis of point (f) of the first subparagraph of Article 6(1) of the GDPR. On the other hand, if the second condition under that provision was satisfied, the referring court would still also have to examine the third and last cumulative condition under that provision.

[27] See judgments of 4 May 2017, *Rīgas satiksme* (C-13/16, EU:C:2017:336, paragraph 30), and of 17 June 2021, *M.I.C.M.* (C-597/19, EU:C:2021:492, paragraph 110).

(3) Balancing of the different interests at stake

69. As regards, lastly, the balancing of the interests of the controller and the interests or fundamental rights and freedoms of the data subject, according to the case-law of the Court of Justice, it is for the referring court to weigh the interests at stake.[28] In this regard, the guidelines of the former Article 29 Working Party, now the 'European Data Protection Board', whose tasks are defined in Article 70 of the GDPR, set out the following criteria to be considered when applying that balancing test: (i) assessing the controller's legitimate interest; (ii) impact on the data subjects; (iii) provisional balance; and (iv) additional safeguards applied by the controller to prevent any undue impact on the data subjects.[29] In the interest of a detailed and logical analysis, I propose that these criteria be applied to the cases in the main proceedings. This approach will, moreover, contribute to a more coherent application of the GDPR in accordance with the objectives pursued by the EU legislature.

(i) Assessing the controller's 'legitimate interest'

70. As regards the first criterion, it must be stated that the interest of both SCHUFA and its clients is *purely economic*. Private agencies store personal data imported from public registers in order to offer their clients a service consisting in providing information on the creditworthiness of the data subject based inter alia on those data. As I explained above,[30] such an interest seems legitimate for the purposes of this analysis.

(ii) Impact of processing on the data subjects

71. As far as the second criterion is concerned, that is to say, the impact of processing on the data subject, the *period after which data must be erased* appears to be the relevant factor. The longer the period for which data are stored in the databases of private credit information agencies, the greater the consequences for the data subject. In the present case, the personal data of the applicants in the main proceedings were processed in the public register in order to 'improve the provision of information to relevant creditors and courts and to prevent the opening of parallel insolvency proceedings', as is required by recital 76 of Regulation 2015/848. In balancing the different interests, the German legislature took the view that the period for which publication of data from insolvency proceedings in such public registers was necessary in order to achieve that objective was six months. The storage of personal data beyond that period of six months therefore seems a priori to have a significant negative impact on the data subject.

72. According to the Court's case-law, other factors must be taken into account in this analysis, namely the *methods of access to databases* and the *facilities available for the dissemination of personal data*.[31] In simple terms, the more easily accessible the information is to the public, the more serious the interference with the fundamental rights of the data subject. This is particularly so where a large *number of users* have access to the data of the data subject.[32] It therefore seems clear that, even if data are already available in public registers for that period of six months, the

[28] Judgments of 4 May 2017, *Rīgas satiksme* (C-13/16, EU:C:2017:336, paragraph 31), and of 17 June 2021, *M.I.C.M.* (C-597/19, EU:C:2021:492, paragraph 111).

[29] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217, 9 April 2014, section III.3.4 ('Key factors to be considered when applying the balancing test').

[30] See points 61 to 63 of this Opinion.

[31] Judgments of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraphs 86 and 87), and of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA* (C-708/18, EU:C:2019:1064, paragraph 57).

[32] Judgment of 1 August 2022, *Vyriausioji tarnybinės etikos komisija* (C-184/20, EU:C:2022:601, paragraph 92).

fact that they are stored and available in parallel in the databases of private credit information agencies has a further impact on the private life of the individual in addition to the negative consequences of those data being available in public registers.

73. An additional factor to be taken into account in the analysis is *the potentially sensitive nature of the data* at issue. [33] Generally speaking, the impact on the data subject increases according to the sensitivity of the personal data. It is clear from the Court's case-law that personal data concerning recovery of debts are actually sensitive data for the data subject's private life. [34] Making this kind of data available to a *number of users which is unlimited in principle* must therefore be regarded as a significant interference with the fundamental rights of the data subject. [35]

74. Lastly, it also seems crucial to take into account the *time factor*. Even lawful processing of data may cease to comply with the GDPR over time where those data are not or are no longer relevant or are excessive having regard to the purpose for which they were originally collected. With this in mind, I seriously question how the storage of personal data could be justified for a period of three years when the national legislature considers a storage period of six months, a much shorter time, to be broadly sufficient in order to take account of the business interests of economic operators. I must point out that SCHUFA was not able to give a clear and convincing answer to this question [36] even though under Article 5(2) of the GDPR it must demonstrate compliance with the principles relating to processing of personal data. [37]

(iii) Provisional balance

75. On the basis of an assessment of all the factors mentioned in the preceding points, I must conclude that the considerable negative consequences that the storage of data will have on the data subject after the period of six months in question seem to override the commercial interest of the private agency and its clients in storing the data after that period. Against this background, it should be stressed that the discharge from remaining debts granted is intended to *allow the beneficiary to re-enter economic life*. [38] The applicants in the main proceedings and the Commission also highlighted this aspect at the hearing. This objective would be frustrated if private credit information agencies were authorised to store personal data in their databases after the data have been erased from the public register.

(iv) Additional safeguards

76. Lastly, as regards additional safeguards possibly applied by the controller to prevent any undue impact on the data subjects, there is nothing in the order for reference or in the observations submitted by SCHUFA to indicate the existence of such safeguards.

[33] Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA* (C-708/18, EU:C:2019:1064, paragraph 57).

[34] Judgment of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 98).

[35] See judgment of 22 November 2022, *Luxembourg Business Registers* (C-37/20 and C-601/20, EU:C:2022:912, paragraphs 39 to 42), in which the Court considered making information on the beneficial owners of corporate and other legal entities available to the general public to be an infringement of the rights guaranteed in Articles 7 and 8 of the Charter. In its reasoning, the Court took into account the sensitive nature of the personal data at issue and the fact that the information was accessible to a potentially unlimited number of persons.

[36] At the hearing, SCHUFA referred to the fact that some people would become insolvent again, which, it claims, justifies a storage period of three years.

[37] Gutowski, M., 'OLG Schleswig: Eintragung erfolgter Restschuldbefreiung in Datenbanken von Auskunfteien über die Löschungsfrist für das Insolvenzbekanntmachungsportal hinaus', *Neue Zeitschrift für Insolvenz- und Sanierungsrecht*, 18/2021, p. 799, expresses doubts whether it is beneficial to provide for the storage of a person's data for three years in order to determine his or her economic situation.

[38] See, to that effect, Heyer, H.-U., 'Schein-Datenschutz', *Zeitschrift für Verbraucher-, Privat- und Nachlassinsolvenz*, 2019, p. 46.

(4) Interim conclusion

77. In the light of the above considerations, I take the view that the storage of data by a private credit information agency cannot be lawful under point (f) of the first subparagraph of Article 6(1) of the GDPR once the personal data concerning insolvency have been erased from public registers.

78. As regards the period of six months during which the personal data are also available in public registers, it is for the referring court to balance the abovementioned interests and impacts on the data subject in order to determine whether the parallel storage of those data by private credit information agencies is lawful under point (f) of the first subparagraph of Article 6(1) of the GDPR.

(b) Compliance with the principles of purpose limitation and data minimisation (Article 5(1)(b) and (c) of the GDPR)

79. In accordance with the principle of purpose limitation, which is laid down in Article 5(1)(b) of the GDPR, it must be ensured that personal data collected for a specified purpose are not further processed in a manner that is incompatible with those purposes. In the present case, the data concerning insolvency and discharge from remaining debts were processed by public authorities in the performance of legal obligations.

80. However, as regards the further use of data by a private agency, it must be examined, in the light of the GDPR and applying the criteria set out in Article 6(4) of that regulation, whether the specified purpose is compatible with the initial purpose. Points (a), (b) and (d) of that provision are particularly relevant in this case. They lay down the following criteria: (i) the link between the initial purpose and the further purpose; (ii) the context in which the data have been collected and, in particular, the relationship between data subjects and the controller, and (iii) the possible consequences of the intended further processing for the data subject.

81. First, it seems that the *link between the purposes is tenuous*, not least because the initial purpose is laid down by law, more specifically by EU law, which requires Member States to establish and maintain registers,[39] and because the controller is a public authority acting within the framework of the tasks conferred on it by law, whereas the further purpose is pursued by a private entity in the context of a business activity consisting in providing economic information on individuals.

82. Second, as regards the context in which the data have been collected, *there is no link between the controller and the data subject* since data are collected indirectly through registers and data subjects are not therefore aware that their data can be further used, or by whom, or for what purpose. I consider this aspect to be particularly serious from the point of view of protection of personal data since, as a general rule, a person cannot reasonably expect further processing of his or her personal data.[40] Because the law prescribes a specified period for the storage of data in public registers, it is reasonable to assume that the data at issue will be erased after that period has expired.

[39] See point 31 of this Opinion.

[40] See judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA* (C-708/18, EU:C:2019:1064, paragraph 58).

83. Third, with respect to the possible consequences which the further processing of data may have for the data subjects, it must be stated that information concerning insolvency proceedings will always be used as a *negative factor in a future assessment of the creditworthiness and ability to pay* of the natural person concerned, which has a significant impact on that person's rights. A false picture of their economic situation can produce detrimental effects for data subjects by complicating significantly the exercise of their freedoms or even by stigmatising them in society. In so far as data subjects can be denied goods and services, they may suffer unjustified discrimination.

84. In the light of these three criteria, which must be satisfied for the use of personal data to be consistent with the initial purpose, as required by Article 6(4) of the GDPR, it appears doubtful that the further use of those data can be consistent with that purpose.

85. Furthermore, by fixing at six months the maximum period for which the insolvency and the judicial decision concerning discharge from remaining debts may be published if the legal conditions are met, *the national legislature has already taken into account the attainment of the public interest* and balanced the interest of creditors, on the one hand, and the interests and rights of insolvent persons, on the other.[41] The processing of personal data by private agencies for a period six times longer than is prescribed by law for public registers *seems excessive and penalises the data subject de facto, even though clearly nothing of the kind is envisaged by the law*. As I have already noted, the discharge from remaining debts granted is intended to allow the beneficiary to re-enter economic life. This objective would be frustrated if private credit information agencies were authorised to store personal data in their databases after the data have been erased from the public register.[42] In the absence of evidence to the contrary, it is likely that the conditions of access to the database may have been conceived with the intention of *circumventing the national legislation* adopted by the Member State in order to fulfil its obligations under EU law.[43]

86. Furthermore, it seems disproportionate to 'reuse' a past situation which has already been given legal clarification, such as discharge from remaining debts, in future evaluations rather than using updated factors for the risk assessment in order to ensure a more precise and objective evaluation of the data subject's economic situation. Questions might be asked about *the value of information concerning a person's economic situation which is several years old*. Personal data relating to a situation which dates back some time will hardly provide reliable information on the data subject's current economic situation. The German legislature seems to have recognised this problem and to have drawn the right conclusions, opting for a much shorter data storage period.

87. Lastly, I think that the approach taken by credit information agencies runs counter to the principle of data minimisation enshrined in Article 5(1)(c) of the GDPR, under which personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In this regard, the question actually arises as to *what is the purpose of*

[41] The argument put forward by SCHUFA at the hearing that the German legislature has taken no steps to shorten the period of three years applied by SCHUFA would not seem to invalidate this finding. There may be various reasons why a Member State has not yet addressed the issue of parallel databases. The purpose of the requests for a preliminary ruling from the referring court is precisely to find answers to this issue in order to establish a situation that complies with the requirements of the GDPR.

[42] See point 75 of this Opinion.

[43] Ehmann, E., 'Bundesdatenschutzgesetz', Simitis, S., Hornung, G. and Spiecker, I. (eds.), *Datenschutzrecht – DSGVO mit BDSG*, 8th edition, Baden-Baden, 2014, Paragraph 29, point 192, considers that there is no longer a legitimate interest in the dissemination of personal data by a database managed by a private agency where a period prescribed by national legislation for their publication in a public register has expired, otherwise the legislative objective would be frustrated.

making available personal data which are already accessible to the public in the registers established by Member States. It seems likely that such activity could lead to dissemination of sensitive information which is not absolutely necessary to meet the business interests of economic operators. [44]

88. For the reasons set out above, I consider that the practice of a private credit information agency of storing those data is not consistent with the principles of purpose limitation and data minimisation, enshrined in points (b) and (c) of Article 5(1) of the GDPR respectively.

(c) Interim conclusion

89. The above analysis leads me to conclude that the practice of credit information agencies of storing personal data from public registers for a period of three years is not consistent with the principles governing the processing of personal data enshrined in the GDPR. That being said, this conclusion is based on an assessment of the facts for which the referring court hearing the dispute is ultimately responsible.

2. Recourse to the right to erasure (Article 17(1) of the GDPR)

90. The referring court also wishes to know whether the 'right to be forgotten' enshrined in Article 17 of the GDPR means that personal data are to be erased from the databases of a private credit information agency which exist in parallel with public registers and contain the same data. The referring court draws a distinction between the period during which personal data are also available in the public register and the period during which those data are no longer available there.

91. Article 17(1)(d) of the GDPR provides for the *absolute right* of data subjects to have their personal data erased where they have been unlawfully processed. [45] Consequently, in the event that, in the light of the conclusion that I have reached in my analysis, [46] the referring court were to take the view that SCHUFA was not able to process the applicants' personal data lawfully on the basis of point (f) of the first subparagraph of Article 6(1)) of the GDPR, such processing would be unlawful if none of the other grounds referred to in Article 6(1) of the GDPR applied. In that case, SCHUFA would be required to erase the applicants' personal data and the applicants would have a right to erasure irrespective of whether they requested that the data be erased in the period before or after their erasure from the public register. Such an outcome also seems to comply with the requirements laid down by Article 5(1)(e) of the GDPR, which provides that personal data are to be 'kept in a form which permits identification of data subjects *for no longer than is necessary for the purposes for which the personal data are processed*' (my emphasis).

92. In this regard, I would like to draw attention to Article 79(5) of Regulation 2015/848, which illustrates the importance which the EU legislature attached to the right to erasure, especially where the authorities process particularly sensitive personal data, such as data relating to the creditworthiness of data subjects. Under that provision '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*

[44] See judgment of 1 August 2022, *Vyriausioji tarnybinės etikos komisija* (C-184/20, EU:C:2022:601, paragraph 93), according to which the condition relating to the 'necessity of processing' must be examined in conjunction with the 'data minimisation' principle.

[45] Dix, A., *Datenschutzrecht – DSGVO mit BDSG*, Simitis, S., Hornung, G.and Spiecker, I. (eds.), Baden-Baden, 2018, Article 17, point 14.

[46] See point 77 of this Opinion.

erasure of data, Member States shall inform data subjects of the accessibility period set for personal data stored in insolvency registers' (my emphasis). The EU legislature clearly recognised the need to erase data of this nature where their storage is no longer justified.

93. Although the request for a preliminary ruling concerns only the interpretation of point (d) of Article 17(1) of the GDPR, I consider that point (c) of that paragraph 1 may also prove to be relevant to the judgment to be delivered in the present cases, that is to say, if the referring court were to take the view, contrary to the conclusion that I have reached on the basis of the available information, that SCHUFA was able to process the applicants' personal data lawfully under point (f) of the first subparagraph of Article 6(1) of the GDPR. 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. This wording implies that any 'overriding legitimate grounds for the processing' constitutes an exception to the right of data subjects to object to the processing and to obtain the erasure of their personal data. Accordingly, the data subject is presumed to enjoy a right to object to processing and a right to erasure if there are no overriding legitimate grounds. [47]

94. In the interest of effective protection of personal data, there should be no significant obstacles to the exercise of the right to erasure, in particular where there are a number of credit information agencies on the market which store data in parallel to the public register. If the exercise of that right were to be rendered excessively difficult by reason of a strict interpretation of Article 17(1) of the GDPR, the protection which the GDPR seeks to offer could easily be circumvented by competitors. It should be recalled that the aim of the EU legislature is that '*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' (my emphasis), as is stated in recital 10 of the GDPR. Data subjects must therefore be able to assert their rights vis-à-vis any agencies that infringe those rules. Since SCHUFA is only one of many large credit information agencies in Germany, it will be necessary to establish whether the storage of personal data in parallel to the public register is common practice among those agencies.

95. It must therefore be stated at this stage in the analysis that the applicants may, in principle, rely on a right to erasure under Article 17(1) of the GDPR. It would be otherwise only if a private credit information agency successfully 'demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject' in accordance with Article 21(1) of the GDPR. In so far as the information available does not reveal any compelling grounds which might exist in the dispute in the main proceedings, it is for the referring court to establish the facts and, if necessary, to balance the interests at stake.

96. In the light of the above considerations, Article 17(1)(d) of the GDPR is to 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 those data have been unlawfully processed in accordance with Article 6(1) thereof. Article 17(1)(c) of the GDPR is to be interpreted as meaning that the data subject has, in principle, the right to obtain from the

[47] Kranenborg, H., 'Article 17. Right to erasure ("right to be forgotten")', *The EU General Data Protection Regulation (GDPR)*, Kuner, C., Bygrave, L.A., Docksey, C. and Drechsler, L. (eds.), Oxford, 2020, p. 481, explains that Article 21(1) of the GDPR reverses the burden of proof such that the data controller, rather than the data subject, must demonstrate overriding legitimate grounds in order to justify processing. If that controller is not able to do so, the data in question must be erased.

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. It is for the referring court to examine if, exceptionally, there are overriding legitimate grounds for the processing.

3. Recourse to a code of conduct within the meaning of Article 40 of the GDPR in order to provide for time limits for review and erasure that exceed the retention periods for public registers

97. The referring court also wishes to know whether it is consistent with EU law to provide, in a code of conduct within the meaning of Article 40 of the GDPR, for time limits for review and erasure that exceed the retention periods for public registers without it being necessary to carry out the balancing of interests prescribed under point (f) of the first subparagraph of Article 6(1) of that regulation.

98. In this regard, it must be observed at the outset that, according to the referring court, at present national legislation does not lay down time limits for erasure in respect of databases held by credit information agencies. However, it seems that the interested parties regard the code of conduct jointly adopted by the supervisory authorities and the association of credit information agencies as a kind of 'legal basis' capable of legitimising the practice described above. That view seems legally objectionable for the following reasons.

99. From a legal point of view, such a code of conduct is merely a *voluntary undertaking* on the part of those who drew it up and adopted it, that is to say, the abovementioned association and its members. Similarly, the fact that that code of conduct was approved by a supervisory authority only means that it *considers itself to be bound by that code of conduct* as an administrative authority. It nevertheless seems clear that it has no binding force on third parties in accordance with the legal principle '*pacta tertiis nec nocent nec prosunt*'. Otherwise, not only would natural persons whose data are processed be affected, but also agencies that were not involved in drawing up such a code of conduct.

100. By definition, a code of conduct has no normative value in a legal order but is intended to *specify the provisions of a normative act so as to facilitate its application*. This interpretation is supported by paragraphs 1 and 2 of Article 40 of the GDPR, under which the codes of conduct to be prepared by associations and other bodies representing categories of controllers or processors are intended, first, 'to *contribute* to the proper application' and, second, to '*specify* … the application' of that regulation (my emphasis). Consequently, in so far as the function of the code of conduct in question is confined to ensuring the proper application of the GDPR in a certain sector, it cannot in itself constitute the legal basis justifying processing of personal data. [48]

[48] It should be pointed out that the code of conduct in question ('Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien vom 25.05.2018') (Code of Conduct on Time Limits for Verification and Deletion of Personal Data by German Private Companies Providing Business Information of 25 May 2018) states that its rules 'do not contain *any provisions regulating the material justification for storage* of personal data'. The code of conduct also states that 'the regulation of storage and deletion periods *does not indicate the lawfulness of their storage*. The following deletion and storage periods apply, whether the underlying data were collected and stored *on a statutory basis* or on the basis of consent' (my emphasis). In my view, this shows that the authors of that code must have been aware that the code of conduct does not constitute a legal basis capable of legitimising data processing.

101. The legal basis justifying such processing can be found only in Article 6 of the GDPR or, if there is an applicable opening clause, in national law. I have already stated in this Opinion that Article 6 of the GDPR sets out an exhaustive and restrictive list of the cases in which such processing can be regarded as lawful. [49] Consequently, the rules of the code of conduct *could not have the effect of extending that list* without at the same time infringing EU law.

102. It would appear that this is precisely the case where, as in this instance, those rules impose on credit information agencies the obligation to store the data of data subjects for a period of three years, that is to say, for an extended period of time which cannot be justified having regard to the principles governing the processing of personal data enshrined in the GDPR. More specifically, as I have shown in my analysis, the storage of those data cannot be considered lawful under point (f) of the first subparagraph of Article 6(1) of the GDPR for the period following the erasure of personal data concerning insolvency from public registers. [50]

103. It must therefore be concluded at this stage in the analysis that codes of conduct which would lead to a *different result* from that which would have been obtained pursuant to point (f) of the first subparagraph of Article 6(1) of the GDPR could not be taken into consideration in the balance of interests under that provision. As 'controllers' within the meaning of Article 4(7) of the GDPR, credit information agencies cannot hide behind the rules of the code of conduct which they have themselves drawn up in order legitimately to escape their obligations under that regulation.

104. In the light of the above considerations, I take the view that Article 40(2) and (5) of the GDPR is to be interpreted as meaning that codes of conduct drawn up in accordance with those provisions and possibly approved by the supervisory authority may not lay down in a legally binding manner conditions for lawful processing of personal data which differ from those set out in Article 6(1) of the GDPR.

VI. Conclusion

105. In the light of the above considerations, I propose that the Court answer the questions referred for a preliminary ruling by the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany) as follows:

(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 under that provision a legally binding decision of a supervisory authority is subject to a full substantive judicial review.

(2) Point (f) of the first subparagraph of Article 6(1) of Regulation 2016/679

[49] See point 59 of this Opinion.

[50] See point 77 of this Opinion.

must be interpreted as meaning that it precludes the storage by a private credit information agency of 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 for a period beyond that for which the data are stored in the public register. It is for the referring court to determine whether the storage of data for the period authorised for the public register satisfies the conditions laid down in point (f) of the first subparagraph of Article 6(1) of Regulation 2016/679.

(3) Article 17(1)(d) 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 those data have been unlawfully processed in accordance with Article 6(1) of that regulation.

Article 17(1)(c) of Regulation (EU) 2016/679

must be interpreted as meaning that the data subject has, in principle, 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. It is for the referring court to examine if, exceptionally, there are overriding legitimate grounds for the processing.

(4) Article 40(2) and (5) of Regulation 2016/679

must be interpreted as meaning that codes of conduct drawn up in accordance with those provisions and possibly approved by the supervisory authority may not lay down in a legally binding manner conditions for lawful processing of personal data which differ from those set out in Article 6(1) of that regulation.