Supreme Court's DECISION

delivered in Stockholm on 25 February 2025

Case no.
Ä 3457-24

PARTIES

Appellant

Panoptes Sweden AB, 559199-4503

Nyhetsbyrån Siren

Box 4211

102 65 Stockholm

Counsel: Attorneys UI and EK and lawyer GT

THE MATTER

Disclosure of official documents

RULING APPEALED

Decision of the Court of Appeal for Northern Norrland of 09/24/2024, in case 2024/91

_____

Visiting address
Riddarhustorget 8

Telephone
+46 8 561 666 00

Office hours
Monday to Friday
08:45–12:00
13:15–15:00

Postal address
SUPREME COURT
Box 2066
103 12 Stockholm

E-mail
hogsta.domstolen@dom.se

Website
www.hogstadomstolen.se

THE SUPREME COURT'S RULING

The reservation issued by the Court of Appeal shall be amended to state:

- that the documents, in whatever form, may not be made available to the public or to paying customers if, as a result, the public or customers obtain the personal names, personal identity numbers or addresses of individuals; and

- that Siren shall not otherwise offer to the public or paying customers the possibility of searching documents in a way that gives access to the personal names, personal identity numbers or addresses of individuals.

CLAIMS IN THE SUPREME COURT

Panoptes Sweden AB has requested that the Supreme Court set aside the Court of Appeal's decision and grant the company's request to have access to the requested documents without reservation.

REASONS FOR THE DECISION

Background

1. The business of Panoptes Sweden AB includes collecting, processing, analysing and displaying information. The company operates Nyhetsbyrån Siren.

2. Siren's core business is to identify and gather news material and to disseminate such material to other news organisations and mass media, including newspapers, magazines and radio and television broadcasters. As Siren is a news agency, their database (siren.se) in which, among other things, verdicts in criminal cases are provided, is subject to constitutional protection under Chapter 1, Section 4 of the Fundamental Law on Freedom of Expression.

3. From the Court of Appeal, Siren has requested access to a large number of official documents in criminal cases, including judgments, decisions, case registers and indictments.

4. The Court of Appeal has ordered that the requested documents be disclosed, subject to the following reservation. The personal data contained in the documents may only be used for journalistic purposes, and the personal identity numbers, names and addresses of individuals may not be made available to the public or paying customers through the database or registers. As grounds for its decision, the Court of Appeal stated that it was presumable that, following disclosure, the data would be processed in breach of the EU Data Protection Regulation.[1] According to the Court of Appeal, the information was therefore subject to secrecy under Chapter 21, Section 7 of the Public Access to Information and Secrecy Act (2009:400), and the reservations constituted an appropriate protective measure.

5. The company has appealed the decision to the Supreme Court. (Leave to appeal is not required, cf. Chapter 54, Section 9 of the Code of Judicial Procedure and "Court of Appeal's Case Register" NJA 2015 p. 180 paras. 5–7).

At issue in the Supreme Court

6. The case concerns whether the information requested is subject to secrecy, and, if so, whether it should be disclosed with reservations. The case brings to the fore the relationship between Chapter 21, Section 7 of the Public Access to Information and Secrecy Act, Chapter 1, Section 7 of the

[1] Regulation (EU) 2016/679 of the European Parliament and 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).

Act on supplementary provisions to the EU General Data Protection Regulation (2018:218), hereinafter the Data Protection Act, and the rules in the General Data Protection Regulation (GDPR).

On disclosure of judgments and other court documents

7. In order to promote a free exchange of views, free and general knowledge and free artistic creation, everyone has the right to access official documents to the extent that the rules on secrecy do not prevent this (see Chapter 2, Sections 1 and 2 of the Freedom of the Press Act).

8. Rules on secrecy are set out in the Public Access to Information and Secrecy Act. Secrecy means that it is prohibited to disclose information that is subject to secrecy, regardless of whether this is done orally, by disclosure of an official document or in some other way (see Chapter 3, Section 1 of the Public Access to Information and Secrecy Act).

9. As a general rule, criminal judgments are public. If a piece of information is included in a court judgment, any secrecy for the information ceases to apply, unless the court orders continued secrecy (cf. Chapter 43, Section 8 of the Public Access to Information and Secrecy Act).

10. In line with this, criminal judgments have generally been disclosed to whoever has requested them, even where this involved large numbers of judgments. Other documents related to criminal proceedings, such as case registers and minutes, are also regularly disclosed, unless there is a specific secrecy provision applicable to the information they contain.

11. However, as stated in the Court of Appeal's decision, the question has been raised to what extent Chapter 21, Section 7 of the Public Access to Information and Secrecy Act, which refers to the GDPR – or the GDPR itself – may constitute an impediment to the disclosure of such documents.

The provision in Chapter 21, Section 7 of the Public Access to Information and Secrecy Act

12. According to Chapter 21, Section 7 of the Public Access to Information and Secrecy Act, secrecy applies to personal data if it is presumable that the data will be processed in violation of the GDPR or the Data Protection Act after disclosure.

13. The secrecy provision in Chapter 21, Section 7 differs from other secrecy provisions in that it does not refer to the information as such, but to what can be presumed to happen to it after disclosure. The provision requires the disclosing public authority to take into account what can be presumed about the imminent processing and its nature. A similar provision has existed since 1973. One of the reasons for this provision was the need to exert a degree of control over the possibilities of generating new registers, for purposes other than the original registers, by extracting personal data from existing registers (see Govt. bill 1973:33 p. 100 et seq.).

14. An assessment under this section only needs to be made if there are concrete circumstances indicating that the recipient will process the data in a manner contrary to data protection regulation, e.g., that mass extraction is carried out. There is no need to fully assess whether the processing will violate the GDPR or the Data Protection Act. (Cf. Govt. bill 2017/ 18:105 p. 135 et seq.)

GDPR

15. The GDPR is binding and directly applicable in all EU Member States (see Article 288, second paragraph, of the Treaty on the Functioning of the European Union). The Regulation was created to ensure, among other things, a uniform and high level of protection for natural persons that is equivalent in all Member States. It should be seen in the light of the fact

that the protection of natural persons in the processing of personal data is a fundamental right under the Charter of Fundamental Rights of the European Union. (See GDPR, recitals 1 and 10; see also Article 8 of the Charter and Article 16 of the Treaty on the Functioning of the European Union.)

16. Article 5 of the GDPR states that certain basic principles must be respected when processing personal data. These principles include that data must be processed lawfully, fairly and transparently, and that they must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Furthermore, they shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed and may be stored for longer periods only for certain purposes.

17. The principles set out in Article 5 are supplemented in Article 6 by more concrete requirements that must be met in order for the processing of the data to be lawful. One key requirement is that one of the grounds listed in the Article must apply in order for data to be processed. Examples of such grounds are the consent of the data subject or the necessity of the processing for compliance with a legal obligation.

18. Article 9 regulates the processing of certain special categories of personal data. These include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, data concerning health or data concerning a natural person’s sex life or sexual orientation. Processing of such data is prohibited unless the data subject has given his or her explicit consent or the processing is necessary for specified reasons.

19. Article 10 contains rules specifically aimed at the processing of personal data relating to criminal convictions and offences or related security measures. Processing of such data may only be carried out under the control of official authority or when the processing is authorised by

Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority. (For the CJEU's interpretation of the terms offences and convictions, see judgment of the Court of Justice of the European Union of 24 September 2019, *GC and Others*, C-136/17, EU:C:2019:773, para. 72.)

20. The purpose of Article 10 is to ensure a higher level of protection against processing of personal data which, by reason of its particularly sensitive nature, is likely to constitute a particularly serious interference with the fundamental right to respect for private life and protection of personal data enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (see judgment of the Court of Justice of the European Union of 22 June 2021, *Latvijas Republikas Saeima*, C-439/19, EU:C:2021:504, para. 74).

21. Article 85 of the GDPR requires Member States to reconcile by law the right to privacy under the Regulation with the freedom of expression and information. They shall also – if necessary to reconcile the right to privacy with the freedom of expression and information – provide for exemptions or derogations from certain enumerated parts of the Regulation (including Article 10) for certain processing operations, such as those carried out for journalistic purposes.

22. It follows from the case-law of the Court of Justice of the European Union that the concept of processing for journalistic purposes must be interpreted broadly. This includes disseminating information, opinions or ideas to the public. The technology used, or whether the activity is carried out for profit, has no bearing on the assessment. Processing of personal data where material collected from public authorities is made available commercially in an unaltered form may also constitute processing for

journalistic purposes. (See judgment of the Court of Justice of the European Union of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, EU:C:2008:727, paras. 55–62.)

23. In order to reconcile the public's right of access to official documents with the right to the protection of personal data under the Regulation, public authorities may, among other things, disclose personal data contained in official documents in accordance with applicable Union or Member State law (see Article 86).

24. Thus, Articles 85 and 86 of the regulation provide scope to restrict the right to the protection of personal data, but only on condition that such restrictions are provided for by law, are compatible with the essence of fundamental rights and fulfil the requirements arising from the principle of proportionality under Union law. This means, among other things, that the restrictions must not exceed what is strictly necessary, and it also requires that there are clear and precise rules governing the scope and application of the exceptions. (See, e.g., *Latvijas Republikas Saeima*, paras. 105 and 106 with further reference.)

25. This means that it is recognised that the protection of personal data may vary between Member States. At the same time, it is not guaranteed that any given reconciliation of interests is acceptable under Union law.

Data Protection Act

26. The Data Protection Act contains supplementary provisions to the GDPR.

27. Chapter 1, Section 7, first paragraph, provides that the GDPR and the Data Protection Act shall not be applied to the extent that it would be contrary to the Freedom of the Press Act or the Fundamental Law on Freedom of Expression. This provision covers not only applications of data

protection regulation that would violate freedom of the press or freedom of expression, but also those that would violate the principle of public access to official documents (cf. Govt. bill 2017/18:105 p. 43).

28. The second paragraph of the Section states that Articles 5–30 and 35–50 of the GDPR and Chapters 2–5 of the Data Protection Act shall not apply to the processing of personal data for journalistic purposes or for academic, artistic or literary creation. In this case, it is mainly the exception for journalistic purposes that is relevant. The term "processing for journalistic purposes" is to be given the same meaning as under Union law (see para. 22, cf. "The Foundation's Website" NJA 2001 p. 409).

Decisions of the Court of Justice of the European Union

29. In a few judgments, the Court of Justice of the European Union has dealt with questions concerning the disclosure of personal data by public authorities in relation to, inter alia, Article 10 of the GDPR.

30. In *Latvijas Republikas Saeima*, the Court held that the provisions of the GDPR preclude national legislation which obliges a public body responsible for a register containing information on penalties imposed on drivers for traffic offences to make that information available to the public, without any requirement on the person requesting access to the data to demonstrate his or her specific interest in obtaining it. The GDPR was also considered to prevent the public body from transferring such information to economic operators for re-use, so that anyone wishing to obtain information regarding penalties can contact these operators directly and obtain the information. (See *Latvijas Republikas Saeima*, paras. 122 and 129.)

31. When examining whether the national rules could be considered compatible with the GDPR, an assessment was made as to whether those rules, which thus entailed a limitation of the protection provided by the GDPR, were

necessary and proportionate in relation to the objectives pursued by the regulation. In making this assessment, the Court took into account both the right to freedom of information under Article 85 and the right of public access to official documents under Article 86, but found that the right to protection of this type of personal data must be regarded as more important. (See *Latvijas Republika Saeima*, paras. 102–121 and 126.)

32. Similarly, in a subsequent judgment, the Court of Justice of the European Union held that the GDPR precludes the disclosure of information on criminal convictions of natural persons contained in a register kept by a court to any and all for the purpose of ensuring public access to official documents, unless the person requesting disclosure has demonstrated a specific interest in obtaining the information. (Judgment of the Court of Justice of the European Union of 7 March 2024, C-740/22, *Endemol Shine Finland*, EU:C:2024:216, para. 58.)

Compatibility of the Swedish regime with EU law

33. The Supreme Court must determine whether, and, if so, how, the examination of a request for official documents containing information on offences is affected by the GDPR.

34. As stated above, Chapter 1, Section 7, first paragraph, of the Data Protection Act provides that that Act and the GDPR are not to be applied to the extent that it would be contrary to the Freedom of the Press Act or the Fundamental Law on Freedom of Expression.

35. The intention of the Riksdag with the provision can be said to have been that the GDPR and the Data Protection Act should not apply at all in the constitutionally protected area. This would mean that, when carrying out an activity covered by the Freedom of the Press Act or the Fundamental Law on Freedom of Expression, there would be no need to comply with the

GDPR, nor would the GDPR restrict the public authorities' obligations to disclose personal data. (Cf. Govt. bill 2017/18:105 pp. 40 et seq., and Govt. bill 1997/98:44 p. 43 et seq. regarding the previous regulation).

36. Given such a starting point, it is consistent to understand Chapter 21, Section 7 of the Public Access to Information and Secrecy Act to entail that secrecy under the provision cannot exist in these cases; the provision presupposes an assessment of what can be presumed about the compatibility of the processing to be carried out with data protection regulations.

37. The same applies to cases where the exception in Chapter 1, Section 7, second paragraph, of the Data Protection Act applies, e.g. when processing personal data for journalistic purposes outside the constitutionally protected area. The paragraph provides that several key provisions of the GDPR, including Articles 5–10, do not apply to such processing.

38. However, when applying national regulation, the requirements of Union law must be taken into account. Member States are required, under Articles 85 and 86 of the GDPR, to reconcile, on the one hand, the interest in the right to freedom of expression and information as well as the public's right to access the official documents, with, on the other hand, the right to the protection of personal data. However, it is questionable whether a regulation requiring extensive disclosure of personal data relating to offences, while data protection regulation does not apply at all – or only partially – to the subsequent processing of the data, can be reconciled with the requirements of Union law.

39. Verdicts in criminal cases include a wide range of sensitive information. Their contents are not limited to the personal data of defendants and offenders, the offences to which a decision relates, and any penalty imposed. They also include a large amount of other personal data,

including information about victims and witnesses, and information regarding the circumstances of the offences charged, which can be linked to different individuals.

40. If Chapter 1, Section 7, first paragraph, of the Data Protection Act is understood in the way the legislature may be said to have intended, the regulation means that the protection of these personal data – in the constitutionally protected area – will be based exclusively on the possibilities for intervention provided under the Freedom of the Press Act and the Fundamental Law on Freedom of Expression, which have essentially other purposes than protecting personal data. Nor, if the provision is understood in this way, are there any rules regarding how personal data may be processed, or conditions for exercising supervision with regard to data on offences.

41. Even in the cases referred to in Chapter 1, Section 7, second paragraph, such an arrangement (see paras. 35–37) means that the protection of personal data must to a very large extent take a back seat to the interest in freedom of expression and information.

42. The Supreme Court's overall assessment is that it cannot be considered compatible with Union law to have a system whereby verdicts in criminal cases are disclosed on a large scale, with the result that a significant amount of personal data relating to offences can subsequently be processed in a database and made available to others. In principle, there is thus no protection of the interest in privacy beyond what is provided by interventions based on the fundamental press laws and the Criminal Code. Such an arrangement almost completely undermines the protection in data processing related to offences that the GDPR aims to provide, and it cannot be considered to establish adequate protections for the rights and freedoms of data subjects as required by Article 10 of the GDPR. The assessment of

this incompatibility also applies in relation to processing carried out for journalistic purposes or other purposes referred to in Article 85.

43. It is therefore not possible to reconcile the Swedish regulation with the GDPR in the way that the legislature may have intended.

Consequences for the assessment to be made under Chapter 21, Section 7 of the Public Access to Information and Secrecy Act

Premises

44. It is not possible for the Supreme Court, with a single ruling, to resolve the issues associated with the Swedish regulation regarding the applicability of the GDPR more generally. The Court's task is to decide how the issues in the case are to be assessed, and in particular how Chapter 21, Section 7 of the Public Access to Information and Secrecy Act is to be applied.

45. It is to be kept in mind that the general issues related to insufficient protection of privacy interests in the processing of personal data in the constitutional area are far from new. Already at the time of the introduction of the system of certificates of no legal impediment to publication, in the Fundamental Law on Freedom of Expression, the Committee on the Constitution was concerned that the constitutional protection might extend to databases that constitute nothing less than personal registers, and that this might conflict with provisions aimed at protecting privacy (cf. report 2001/02:KU21 p. 31 et seq.).

46. There is also reason to note that two proposals have been presented to the Riksdag, aimed at better reconciling the interest in the freedom of the press and freedom of expression with protection of personal data as relates to offences (see Govt. bill 2017/18:49 and Govt. bill 2021/22:59) However, these bills have not become law. In addition, proposals have been made

again on this issue (see SOU 2024:75). In this context, mention can also be made of the Swedish Authority for Privacy Protection (IMY)'s legal opinion 2024:1, which is however limited to search services holding certificates of no legal impediment to publication.

47. In light of the above, the question arises whether it is possible to interpret and apply the Swedish regulatory framework in a way that can be reconciled with the GDPR.

The provision in Chapter 1, Section 7, first paragraph of the Data Protection Act

48. As can be seen from the above, the intention of the Riksdag can be surmised as seeking to prevent application of the GDPR and the Data Protection Act to the constitutionally protected area. It should be noted, however, that this is not reflected in the legal text. Chapter 1, Section 7, first paragraph of the Data Protection Act states that the GDPR shall not be applied "to the extent that it would be contrary to the Freedom of the Press Act or the Fundamental Law on Freedom of Expression". The wording of the provision thus suggests that the GDPR must give way only when conflict between the regulations arises.

49. It should be emphasised that the fact that secrecy applies to certain information as a rule cannot be considered to entail any conflict with the Freedom of the Press Act or the Fundamental Law on Freedom of Expression. On the contrary, the Freedom of the Press Act stipulates that the Riksdag may legislate on secrecy, and that secrecy then also applies in relation to activities covered by the Freedom of the Press Act or the Fundamental Law on Freedom of Expression.

50. It is also worth noting that Chapter 1, Section 7 of the Data Protection Act and Chapter 21, Section 7 of the Public Access to

Information and Secrecy Act, as far as is relevant here, were drafted in the same legislative context. The natural starting point should be that one provision does not exclude the application of the other. It should also be noted that there are no statements in the legislative history of Chapter 21, Section 7 addressing the question of whether secrecy should apply in relation to activities granted constitutional protection under the Freedom of the Press Act or the Fundamental Law on Freedom of Expression.

51. Against this background, the Supreme Court makes the assessment that there is scope to interpret Chapter 1, Section 7, first paragraph, of the Data Protection Act so that the provision does not prevent the requirements of the GDPR from being taken into account in the application of the special secrecy provision of Chapter 21, Section 7 of the Public Access to Information and Secrecy Act, even for activities in the constitutionally protected area. Such an interpretation should be made regardless of how one views the meaning of Chapter 1, Section 7, first paragraph, as regards the question whether the regulation can be applied to the subsequent processing in activities granted constitutional protection.

52. This means that the public authority which must carry out the review under Chapter 21, Section 7 of the Public Access to Information and Secrecy Act must assess whether the information, after disclosure, will presumably be processed in breach of the provisions of the GDPR, without taking a position on the extent to which the Swedish act means that the regulation does not apply to the activities of the person who has requested the data. In the application of Chapter 21, Section 7, the GDPR can then be seen as a freestanding yardstick for when secrecy applies to information that would otherwise be public.

53. In this way, the requirements of the Regulation can be taken into account when deciding whether to disclose public documents containing personal data.

The provision in Chapter 1, Section 7, second paragraph of the Data Protection Act

54. Chapter 1, Section 7, second paragraph states that exemptions from the application of the GDPR shall be made in principle in all parts where the Regulation allows for exemptions. More specifically, as explained, Articles 5–30 and 35–50 of the GDPR are exempted. Here, the legislature has more clearly utilised the national reconciliation mechanism provided for in Article 85 of the GDPR.

55. The legislative history shows that the main purpose of the exemption in the second paragraph was to ensure that, among other things, journalistic activities which are not covered by the Freedom of the Press Act and the Fundamental Law on Freedom of Expression are exempted from parts of the GDPR and the Data Protection Act. A starting point in the drafting of the provision has been that exemptions should be introduced to the extent that the Regulation permits (see Govt. bill 2017/18:105 pp. 44 et seq. and 187). It may be noted that, although the provision is intended to cover activities not covered by the Freedom of the Press Act or the Fundamental Law on Freedom of Expression, its wording also covers activities that are protected by the constitution.

56. The wording of the second paragraph does not leave the same room for interpretation in accordance with Union law as the first paragraph. However, the two paragraphs must be seen in context. The second paragraph cannot reasonably be interpreted as meaning that the exception to the application of the GDPR for non-constitutionally protected activities is

more far-reaching than the exception relating to the constitutionally protected area.

57. The second paragraph should therefore, in the same way as the first paragraph, be applied so that it does not prevent the GDPR from being fully taken into account in a review under Chapter 21, Section 7 of the Public Access to Information and Secrecy Act. The public authority responsible for the review must therefore assess whether, following disclosure, the data are likely to be processed in breach of the provisions of the GDPR, without taking a position on whether the exempted articles of the GDPR apply to the activities of the party requesting the data.

Summary conclusion

58. Taken together, the above means that Chapter 1, Section 7 of the Data Protection Act – assessed in the light of Union law – does not prevent the GDPR from being taken into account in the application of the secrecy provision in Chapter 21, Section 7 of the Public Access to Information and Secrecy Act.

The assessment in this case

Does secrecy apply under Chapter 21, Section 7 of the Public Access to Information and Secrecy Act?

59. In order for secrecy under Chapter 21, Section 7 of the Public Access to Information and Secrecy Act to apply to the information that Nyhetsbyrån Siren has requested be disclosed, it must be possible to presume that the information will be processed after disclosure in a way that is incompatible with the GDPR. This presumption must be based on the existence of concrete circumstances indicating this, but a full assessment of whether the processing that will presumably be carried out is indeed incompatible with the GDPR need not be made (see para. 14). The extent to

which the Regulation applies to Siren's activities is not to be determined, but the Regulation should be used as a freestanding yardstick in the assessment (see paras. 51 and 57).

60. Siren has requested a large number of criminal judgments and other documents related to criminal cases, such as decisions, case registers and indictments. These documents contain information on offences and other sensitive data. Siren has repeatedly requested official documents from the Court of Appeal in a similar manner. Against this background, and taking into account the extensive processing of personal data of this kind that takes place at Siren, it can be presumed that the personal data contained in the requested documents will be processed in a way that is incompatible with Article 10 of the GDPR (cf. para. 42). Consequently, the personal data contained in the documents requested are subject to secrecy.

Are there conditions under which the documents can be released with reservations?

61. If a public authority finds that the risk of damage, harm or other inconvenience which, under a provision on secrecy, prevents the disclosure of information to an individual can be eliminated by a reservation restricting the individual's right to pass on or utilise the information, the public authority shall make such a reservation at the time the information is disclosed to the individual (Chapter 10, Section 14, first paragraph of the Public Access to Information and Secrecy Act).

62. It seems clear that this provision was written with a view to those secrecy provisions whose application requires consideration of harm, damage or other inconvenience. Any reference to such factors is not found in Chapter 21, Section 7 of the Public Access to Information and Secrecy Act, but nor does any exception in Chapter 10, Section 14, entail that it cannot be applied in the case of secrecy under Chapter 21, Section 7. The

latter provision, like several other secrecy rules, further aims to protect information about individuals' personal circumstances. Disclosure of information that is incompatible with the GDPR may therefore be deemed likely to cause damage, harm or other inconvenience. Even if the result of a reservation is not entirely the same as in other cases, the provision in Chapter 10, Section 14, first paragraph should therefore also be applicable when secrecy applies under Chapter 21, Section 7.

63. Making a reservation under Chapter 10, Section 14 when disclosing documents may be a way of reconciling, to some extent, the different interests as required by the GDPR. This is particularly the case when the interest in freedom of expression and information has to be reconciled with the right to privacy.

64. Given the nature of Siren's business, it can be assumed that the data contained in the requested documents will be processed to a significant extent for journalistic purposes. The documents should therefore, as the Court of Appeal has found, be disclosed, but with reservations that reconcile the interest in conducting journalistic activities with the interest in privacy. When drafting this reservation, it should be borne in mind that Siren makes available, via its database, edited news articles, among other things.

65. A satisfactory reconciliation of the different interests can be achieved if the reservation is designed to prevent the documents – and the personal data contained therein – from being made available by Siren or from being made searchable by others, but does not prevent the personal data from being used in, for example, news articles or other news material produced by Siren.

66. In those circumstances, there is reason to amend the Court of Appeal's order, giving the following meaning to the reservation:

- that the documents, in whatever form, may not be made available to the public or to paying customers if, as a result, the public or customers obtain the personal names, personal identity numbers or addresses of individuals; and

- that Siren shall not otherwise offer to the public or paying customers the possibility of searching documents in a way that gives access to the personal names, personal identity numbers or addresses of individuals.

_____

_____ _____ _____

_____ _____

_____ _____

Justices of the Supreme Court Anders Eka, Henrik Jermsten (dissenting), Kristina Ståhl, Agneta Bäcklund (dissenting), Thomas Bull (dissenting), Petter Asp (reporting Justice) and Cecilia Renfors participated in the ruling. Judge referee: Malin Falkmer.

DISSENTING OPINION

Justices Henrik Jermsten and Thomas Bull dissent and would grant the appeal. They state the following.

REASONS FOR THE DECISION

Background

1. The business of Panoptes Sweden AB includes collecting, processing, analysing and displaying information. The company operates Nyhetsbyrån Siren.

2. Siren focuses on monitoring public authorities, and its core business is to identify and gather news material and to disseminate such material to other news organisations and mass media, including newspapers, magazines and radio and television broadcasters. As Siren is a news agency, information from its database is subject to constitutional protection under Chapter 1, Section 4 of the Fundamental Law on Freedom of Expression.

3. From the Court of Appeal, Siren has requested access to a large number of official documents in criminal cases, including judgments, decisions, case registers and indictments.

4. The Court of Appeal has decided to release the requested documents, but with a reservation. The reservation stipulates that the personal data contained in the documents may only be used for journalistic purposes, and the personal identity numbers, names and addresses of individuals may not be made available to the public or paying customers through the database/registers.

5. As grounds for its decision, the Court of Appeal stated that it was presumable that, following disclosure, the data would be processed in

breach of the EU Data Protection Regulation. According to the Court of Appeal, the information was therefore subject to secrecy under Chapter 21, Section 7 of the Public Access to Information and Secrecy Act (2009:400), and the reservations constituted an appropriate protective measure.

On disclosure of judgments, etc.

6. In order to promote a free exchange of views, free and general knowledge and free artistic creation, everyone has the right to access official documents to the extent that the rules on secrecy do not prevent this (Chapter 2, Sections 1 and 2 of the Freedom of the Press Act).

7. According to Chapter 21, Section 7 of the Public Access to Information and Secrecy Act, secrecy applies to personal data if it is presumable that the data will be processed in violation of the EU's GDPR or the Act on supplementary provisions to the EU General Data Protection Regulation (2018:218) (Data Protection Act).

8. The secrecy provision at issue differs from other secrecy provisions in that it does not refer to the information as such, but to what can be presumed to happen to it after disclosure. An assessment under this section only needs to be made if there are concrete circumstances indicating that the recipient will process the data in a manner contrary to data protection regulation, e.g., that mass extraction is carried out. There is no need to fully assess whether the processing will violate the GDPR or the Data Protection Act. (Cf. Govt. bill 2017/ 18:105 p. 135 et seq.)

9. The GDPR sets out, in Articles 5 and 6, certain basic requirements for the processing of personal data, including that it must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Furthermore, the data must be processed lawfully, fairly and transparently in relation to the data

subject, and they must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. One key requirement is also that one of the grounds listed in Article 6 must apply in order for a data to be processed. Examples of such grounds are the consent of the data subject or the necessity of the processing for compliance with a legal obligation.

10. Article 9 regulates the processing of certain special categories of personal data. These include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, data concerning health or data concerning a natural person's sex life or sexual orientation. Processing of such data is prohibited unless the data subject has given his or her explicit consent or the processing is necessary for specified reasons.

11. Article 10 contains rules specifically aimed at the processing of personal data relating to criminal convictions and offences or related security measures. Processing of such data may only be carried out under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

12. Article 85 of the Regulation requires Member States to reconcile by law the right to privacy under the GDPR with the freedom of expression and information, including processing carried out for journalistic purposes or for the purposes of academic, artistic or literary creation. For processing carried out for such purposes, and if necessary to reconcile the right to privacy with the freedom of expression and information, exemptions or derogations from certain enumerated parts of the Regulation, including Articles 5, 6, 9 and 10, shall also be provided.

13. Chapter 1, Section 7, first paragraph, of the Data Protection Act provides that the GDPR and the Data Protection Act shall not be applied to the extent that it would be contrary to the Freedom of the Press Act or the Fundamental Law on Freedom of Expression. The second paragraph of the same Section states that, inter alia, Articles 5, 6, 9 and 10 of the GDPR shall not apply to the processing of personal data for journalistic purposes or for academic, artistic or literary creation.

Swedish reconciliation under Article 85

14. As a preliminary remark, it should be noted that an EU regulation is binding in its entirety and directly applicable in each Member State. It is settled case-law that the provisions of regulations generally have immediate effect in national legal systems, without any implementing measures by the national authorities being required (judgment of the Court of Justice of the European Union of 15 May 2021, *Facebook Ireland and Others*, C-645/19, EU:C:2021:483, p. 110 and the case-law cited).

15. However, some articles of the GDPR do not constitute a complete regulation, and the GDPR requires complementary regulation in national law. This is the case, for example, with the GDPR's requirement for national reconciliation of the GDPR's rules on personal data protection with freedom of expression and information.

16. How to reconcile and harmonise freedom of expression, freedom of information and the protection of personal data is thus not clear from the GDPR. There is also room for variation among Member States as regards the content of provisions reconciling the right to the protection of personal data with freedom of expression and information (judgment of the Court of Justice of the European Union of 24 September 2019, *Google*, C-507/17, EU:C:2019:772, para. 69).

17. It is clear that several Member States have made extensive exemptions from the provisions of the GDPR for journalistic activities (see SOU 2024:75, p. 120 et seq. regarding Norway, Denmark and Finland). Countries such as the Netherlands and Austria have also excluded journalistic activities from the scope of the GDPR, in a manner similar in substance to the Swedish regulation.

18. In addition, reconciliation under Article 85 has to take into account the equal status of the rights recognised in the Charter of Fundamental Rights of the European Union. The protection of personal data is governed by Article 8, and freedom of expression and information is protected by Article 11. Thus, from the point of view of Union law, neither right has a stronger position than the other, but where they conflict, they must be balanced against each other.

19. Under Swedish law, the GDPR is therefore not to be applied to the extent that it would be contrary to the Freedom of the Press Act or the Fundamental Law on Freedom of Expression (Govt. bill 2017/18:105 p. 40 et seq.). Furthermore, Articles 5, 6, 9 and 10 of the GDPR, among others, shall not apply to the processing of personal data for journalistic purposes, even outside the constitutionally protected area.

20. On the basis of Article 85 of the GDPR, this position can be said to mean that the Swedish legislature has deemed it necessary, from the perspective of freedom of expression, to completely exempt entities covered by constitutional protection from the provisions of the GDPR, and that the same should essentially apply to those entities that lack constitutional protection but whose activities have journalistic purposes. In practice, personal data processing by such entities is essentially unregulated.

21. However, in the light of the judgments of the Court of Justice of the European Union of 22 June 2021 in *Latvijas Republika Saeima* (C-439/19,

EU:C:2021:504) and of 7 March 2024 in *Endemol Shine Finland* (C-740/22, EU:C:2024:216), the question may nevertheless be asked whether the Swedish legislation reconciling freedom of expression and freedom of information with the protection of personal data is fully compatible with Union law.

22. In the opinion of the Supreme Court, there is first of all reason to note the following with regard to the rulings of the Court of Justice of the European Union The first case concerned the reconciliation, under Article 86 of the GDPR, of the right to official documents with the right to the protection of personal data, and only concerned Article 85 insofar as it deals with the right to freedom of information. There was no freedom of expression aspect to the case, and the requirements of Article 85 for national reconciliation based on that interest were not addressed. The judgment therefore has no direct relevance to the present situation.

23. In the second judgment, the Court of Justice of the European Union found that the respect for private life and the protection of personal data must be considered to outweigh the public interest in access to official documents. Furthermore, it was emphasised that the right to freedom of information under Article 85 of the GDPR should not be interpreted as justifying the disclosure of personal data relating to criminal convictions to any person requesting such data (paras. 55 and 56).

24. The reasoning of the Court of Justice of the European Union thus focused on balancing the interests of safeguarding personal data relating to offences, on the one hand, and public access to official documents and freedom of information in general, on the other. The ruling therefore has no direct bearing on situations where an entity requests such information for journalistic purposes.

25. The conclusion that can be drawn from the rulings of the Court of Justice of the European Union is that the reconciliation of freedom of information with the protection of personal data must respect the principle of proportionality, and the national rules introduced must not go beyond what is necessary. However, it is not clear what this means in practice in a context where interests other than those at stake in the two cases are in conflict.

26. Another observation that can be made from the two cases is that the Court of Justice of the European Union's assessment of whether reconciliation under Articles 85 and 86 of the GDPR is acceptable has been based on the specific circumstances of the individual case. Although it must be possible to take account of the design of a national system at an abstract level, it is thus the effects in the specific case that are decisive in determining whether or not, for example, the requirement of proportionality is met.

The assessment in this case

27. The case in question concerns a request for access to official documents by an entity enjoying so-called 'automatic constitutional protection', i.e. protection following directly from the constitution (Chapter 1, Section 4 of the Fundamental Law on Freedom of Expression).

28. From a constitutional point of view, this means that the starting point is that Siren is an entity whose business presumably aligns with the purpose of the Fundamental Law on Freedom of Expression, i.e., to ensure a free exchange of views, free and general knowledge and free artistic creation. These are all purposes that almost entirely coincide with the areas where exemptions from the provisions of the GDPR are authorised under Article 85.

29. The information on Siren's business is as follows. Siren is a member of the Swedish Media Publishers' Association (*Tidningsutgivarna*). Siren identifies and collects news material in order to provide such material to other news organisations and mass media. Siren manages, assesses and prepares material on the basis of documents provided by courts, public authorities and others. This processing is in various ways intended for publication. It is the editorial staff who analyse the material and make independent news assessments. The processed material may then be used for publication by other mass media or in Siren's own database.

30. It must be considered clear that the collection of personal data by Siren is for journalistic purposes. Thus, although it is questionable whether the Swedish regulation reconciles freedom of expression and freedom of information with a protection of personal data which fulfils the requirements of Union law in all respects, there is nothing to suggest that, in the case of an operator such as Siren, it would not be acceptable to reconcile the various interests under Article 85 of the GDPR in the way that the Swedish legislature has done.

31. It cannot therefore be considered contrary to Union law to apply constitutional protection to Siren's request for access to official documents in the manner intended by the Swedish legislature.

32. As the Court of Appeal has noted, the requested documents are public and must be disclosed unless secrecy applies under Chapter 21, Section 7 of the Public Access to Information and Secrecy Act. According to this Section, secrecy applies to personal data if it is presumable that the data will be processed in violation of the GDPR after disclosure.

33. However, it cannot be presumed that Siren will process the personal data contained in the documents requested by Siren in breach of the GDPR,

as the processing of personal data by Siren is not subject to the provisions of the GDPR.

34. Secrecy under Chapter 21, Section 7 of the Public Access to Information and Secrecy Act therefore does not apply. The appeal is therefore granted.

_____

DISSENTING OPINION

Justice Agneta Bäcklund dissents and considers further proceedings in the case are to be dismissed. The reasons for the judgment should, she finds, read as follows from para. 61.

61. If a public authority finds that the risk of damage, harm or other inconvenience which, under a provision on secrecy, prevents the disclosure of information to an individual can be eliminated by a reservation restricting the individual's right to pass on or utilise the information, the public authority shall make such a reservation at the time the information is disclosed to the individual (Chapter 10, Section 14, first paragraph of the Public Access to Information and Secrecy Act).

62. It seems clear that this provision was written with a view to those secrecy provisions whose application requires consideration of harm, damage or other inconvenience. There is no reference to such factors in Chapter 21, Section 7 of the Public Access to Information and Secrecy Act.

63. It is difficult to see that a reservation would fully satisfy the possibility of balancing the interest of privacy and the interest of conducting journalistic activities where the processing of large amounts of data relating to offences is at issue. The risk that the provision in Chapter 21, Section 7 is intended to prevent – namely, that the data will be processed in breach of the GDPR after disclosure – can thus not be eliminated by a reservation.

64. Given the interpretation of the relationship between Chapter 1, Section 7 of the Data Protection Act and Chapter 21, Section 7 by the Supreme Court, it is also hardly possible to lay down any rules regarding the processing of data on offences which are disclosed, without considering whether Article 10 of the GDPR applies to such processing. Nor does a

reservation prohibiting the disclosure of certain data seem appropriate, in view of the right to freely communicate information on any subject.

65. In conclusion, there are no grounds for disclosure with certain reservations. Nor does disclosure with certain reservations seem an appropriate measure in this case.

66. Since the documents to which the action relates have been disclosed with reservations to Siren, the appeal should not give rise to any further measure and further proceedings in the case should be dismissed.

_____