THE SUPREME COURT
DECISIONS

announced in Stockholm on February 25, 2025

Target No
Ä 3457-24

PARTIES

Complainant

Panoptes Sweden AB, 559199-4503 Siren News Agency
Box 4211
102 65 Stockholm

Represented by: UI and EK, lawyers, and GT, lawyer

THE CASE

Disclosure of a public document

APPEALED DECISION

Court of Appeal for Upper Norrland decision 2024-04-09, dnr 2024/91

Visiting address
Riddarhustorget 8

Phone number
08-561 666 00

Opening hours
Monday-Friday
08:45-12:00
13:15-15:00

Postal address
Supreme Court
Box 2066
103 12 Stockholm

E-mail address
hogsta.domstolen@dom.se

Web site
www.hogstadomstolen.se

SUPREME COURT RULING

The reservation decided by the Court of Appeal shall be amended to read

– 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 name, social security number or address of an individual; and

– that Siren shall not otherwise offer the public or paying customers the possibility of searching documents in a way that gives access to the personal names, social security 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 inspect the requested documents without reservation.

REASONS

Background information

1. Panoptes Sweden AB's activities include the collection, processing, analysis and presentation of information. The company operates the Siren news agency.

2. Siren's core business consists of identifying and collecting material for news and providing such material to other news organizations or mass media, such as newspapers, magazines and broadcasters. As Siren is a news agency, the database (siren.se) in which, among other things, criminal convictions are provided is subject to constitutional protection under Chapter 1, Section 4 of the Basic Law on Freedom of Expression. 4 of the Basic Law on Freedom of Expression.

3. Siren has requested from the Court of Appeal a large number of public documents in criminal cases, such as judgments, decisions, diary sheets and summons applications.

4. The Court of Appeal has decided that the requested documents should be disclosed, but with the following reservations. 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 the decision, the Court of Appeal stated that it could be assumed that, after disclosure, the data would be processed in violation of the EU's Data Protection Regulation. 7 of the Public Access to Information and Secrecy Act (2009:400) applied and a reservation was an appropriate protective measure.

5. The company has appealed the decision to the Supreme Court. 9 of the Code of Judicial Procedure and the "Court of Appeal's diary" NJA 2015 p. 180 p. 5-7.)

The case in the Supreme Court

6. The case concerns the question of whether the requested information is confidential and, if so, whether the information should be disclosed with reservations. The case raises the relationship between Chapter 21. 7 § offentlighets- och sekretesslagen, 1 kap. 7 of the Act (2018:218) with supplementary provisions to the EU Data Protection Regulation (hereinafter the Data Protection Act) and the rules in the Data Protection Regulation.

---

[1] 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).

On disclosure of judgments and other court documents

7. In order to promote a free exchange of views, free and comprehensive information and free artistic creation, everyone has the right to access public documents to the extent that the rules on confidentiality do not prevent this (see Chapter 2, Sections 1 and 2 of the Freedom of the Press Ordinance).

8. Rules on confidentiality are contained 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 a public document or in some other way (see Chapter 3, Section 1 of the Freedom of Information and Secrecy Act).

9. The starting point is that criminal convictions are public. If a piece of information is included in a court judgment, any confidentiality for the information ceases to apply, unless the court decides on continued confidentiality (cf. Chapter 43, section 8 of the Freedom of Information and Secrecy Act).

10. In line with this, criminal judgments have generally been disclosed to the person who requested them, even when the amount involved was large. Other documents related to criminal proceedings, such as diary sheets and minutes, are also regularly disclosed, unless there is a specific confidentiality provision applicable to the information contained in them.

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 Freedom of Information and Protection of Privacy Act 7 of the Freedom of Information and Secrecy Act, which refers to the Data Protection Regulation - or the Data Protection Regulation as such - may constitute an obstacle to the disclosure of such documents.

The provision in Chapter 21. 7 of the Freedom of Information and Secrecy Act

12. According to Chapter 21. 7 of the Freedom of Information and Secrecy Act, confidentiality applies to personal data if it can be assumed that the data will be processed in violation of the Data Protection Regulation or the Data Protection Act after disclosure.

13. The confidentiality provision in Chapter 21. Section 7 differs from other confidentiality provisions in that it is not aimed at the information as such, but at what can be assumed to happen to it after disclosure. According to the provision, the disclosing authority must take into account what can be assumed about the forthcoming processing and its nature. A similar provision has existed since 1973. The provision was then justified, inter alia, by the need to create some control over the possibilities of building up new registers for purposes other than the original ones by obtaining personal data from existing registers (see Bill 1973:33 p. 100 f.).

14. An assessment under the section only needs to be made if there are concrete circumstances indicating that the recipient will process the data in a way that contravenes data protection regulations, e.g. that it is a matter of bulk extraction. A full assessment of whether the processing will contravene the GDPR or the Data Protection Act does not need to be made (see Government Bill 2017/18:105, p. 135 f.).

Data Protection Regulation

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). It was created, inter alia, to ensure 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 observed when processing personal data. These principles include that data must be processed lawfully, fairly and in a transparent manner, and that it must be adequate, relevant and not excessive relation to the purposes for which it is processed. Furthermore, they must not be kept in a form which permits identification of the data subject during
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 complemented in Article 6 by more concrete requirements that must be met in order for the processing of the data to be lawful. A key requirement is that one of the grounds listed in the Article must apply for a data processing operation to be allowed. 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, offenses that constitute crimes and related security measures. Processing of such data may be carried out only under the control of an authority or where processing is permitted by Union or Member State law, which lays down appropriate safeguards for the rights and freedoms of data subjects. A complete record of criminal convictions may be kept only under the control of an authority. (On the interpretation by the CJEU of the concepts of offences and convictions, see judgment of the Court of Justice of 24 September 2019, GC and Others, C-136/17, EU:C:2019:773, p. 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 as 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,
p. 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 must 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. It includes the dissemination of information, opinions or ideas to the public. The technology used

or whether the activity is carried out for profit does not affect 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 the 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, p. 55-62).

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

24. Thus, Articles 85 and 86 of the Regulation provide for the possibility of restricting the right to the protection of personal data, but only on condition that the restrictions are provided for by law, are compatible with the essence of fundamental rights and comply with the requirements arising from the principle of proportionality under EU law. That means, inter alia, that the restrictions must not go beyond what is strictly necessary and that there must be clear and precise rules governing the scope and application of the exceptions (see, for example, Latvijas Republikas Saeima, paragraphs 105 and 106 and the references therein).

25. This means that it is assumed that the protection of personal data may vary between Member States. At the same time, it is not clear that the reconciliations of interests that have been made are acceptable under EU law.

Data Protection Act

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

27. In Chapter 1. Section 7, first paragraph, stipulates that the General Data Protection Regulation 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 Basic Act on Freedom of Expression. The provision covers not only such application of the data protection regulation that would contravene freedom of the press and freedom of expression, but also that which would contravene the principle of public access to official records (cf. Government Bill 2017/18:105 p. 43).

28. The second paragraph of the section states that Articles 5-30 and 35-50 of the Data Protection Regulation 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 the case, it is primarily the exception for journalistic purposes that is of interest. The expression "processing for journalistic purposes" must be given the same meaning as under EU law (see p. 22, cf. "The Foundation's website" NJA 2001 p. 409).

Decisions of the European Court of Justice

29. In a couple of rulings, the European Court of Justice 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 requires a public body responsible for a register containing information on driver sanctions for traffic to make that information available to the public, without the person concerned having to

requesting access to the data needs to demonstrate that he or she has a specific interest in obtaining it. The GDPR was also considered to prevent the public body from transferring such data to economic operators for re-use, so that a person wishing to obtain information on a possible sting can contact those directly and obtain the data. (See Latvijas Republikas Saeima, pp. 122 and 129.)

31. In examining whether the national rules could be regarded as compatible with the GDPR, the Court assessed whether those rules, which thus restricted the protection afforded by the GDPR, were necessary and proportionate in relation to the objectives pursued by the legislation. In the context of that 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 kind of personal data must be considered more important. (See Latvijas Republika Saeima, pp. 102-121 and 126.)

32. Similarly, in a subsequent judgment, the CJEU 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 person for the purpose of ensuring public access to official documents, without the person requesting the disclosure having to demonstrate a specific interest in obtaining the information. (Judgment of the CJEU of 7 March 2024, C-740/22, Endemol Shine Finland, EU:C:2024:216, p. 58.)

Compatibility of the Swedish regime with EU law

33. The Supreme Court has to decide whether, and if so, in what way, the examination of a request for public documents that
contains data on criminal offenses are affected by the GDPR.

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

35. The legislator's intention with this provision may be said to have been that the GDPR and the Data Protection Act should not apply at all in the area protected by the Constitution. This would mean that in an activity covered by the Freedom of the Press Ordinance or the Freedom of Expression Act, there would be no need to comply with the Data Protection Ordinance and that the Ordinance would not restrict the authorities' obligations to disclose personal data. (See Government Bill 2017/18:105 p. 40 ff., cf. also Government Bill 1997/98:44 p. 43 ff. regarding the previously applicable regulation).

36. With such a starting point, it is consistent to understand Chapter 21, section 7 of the Freedom of Information and Secrecy Act as meaning that there cannot be secrecy under this provision. 7 of the Freedom of Information and Secrecy Act in such a way that secrecy under the provision cannot exist in these cases; the provision presupposes an assessment of what can be assumed about the future processing's compatibility with data protection regulations.

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

38. However, when applying the national regulation, the requirements of Union law must be taken into account. While Articles 85 and 86 of the GDPR require Member States to balance the interests of

freedom of expression and information and the right of public access to official documents on the one hand, and the right to protection of personal data on the other. However, it is questionable whether a regulation which provides for the extensive disclosure of personal data relating to breaches of the law, 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 EU law.

39. Criminal convictions contain a wide range of sensitive data. They not only contain personal data on the defendants and convicted persons, the offenses for which a decision has been made and the possible penalty imposed. They also contain a wide range of other personal data, including information on complainants and witnesses, and on the circumstances of the events charged that 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 legislator 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 Ordinance and the Basic Act on Freedom of Expression, which basically have other purposes than creating personal data protection. If the provision is understood in this way, there are also no rules on how personal data may be processed or any prerequisites for exercising supervision with regard to data on breaches of the law.

41. Even in the cases referred to in Chapter 1. Section 7, second paragraph, such a system (see paragraphs 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 EU law to have a system whereby criminal convictions are disclosed on a large scale, with the result that a significant amount of personal data relating to offenses can subsequently be processed in a database and made available to others. In principle, there is then no protection of the privacy interest other than that which may lie in interventions on the basis the media constitutions and the Criminal Code. Such an arrangement almost completely undermines the protection in the processing of data relating to criminal offenses that the GDPR aims to provide and cannot be considered to mean that appropriate safeguards have been established for the rights and freedoms of data subjects in the manner required by Article 10 of the GDPR. The assessment that this is not acceptable 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 legislator may have intended.

The consequences for the assessment to be made under Chapter 21. Section 7 of the Freedom of Information and Secrecy Act

Starting points

44. It is not possible for the Supreme Court to resolve the issues associated with the Swedish regulation of the applicability of the GDPR in a more general manner in an individual decision. The Court's task is to decide how the issues in the case are to be assessed and, in particular, how Chapter 21. 7 of the Freedom of Information and Secrecy Act should be applied.

45. It can be recalled that the general issues related to the lack of protection of privacy interests in the processing of personal data in the constitutional area are far from new.

Already in connection with the introduction of the system of voluntary publication certificates in the Freedom of Expression Act, the Committee on Constitutional Affairs was concerned that the constitutional protection might cover databases that constitute pure personal registers and that this might conflict with provisions aimed at protecting personal integrity (cf. 2001/02:KU21
p. 31 f.).

46. There is also reason to mention here that two proposals have been submitted to Parliament aimed at better balancing the interests of freedom of expression and freedom of information with the protection of personal data relating to breaches of the law (see Bill 2017/18:49 and Bill 2021/22:59). However, these have not led to legislation. In addition, proposals have again been put forward on this issue, among others (see SOU 2024:75). In this context, mention can also be made of the Swedish Authority for Privacy Protection's legal position 2024:1, which is, however, limited to search services with a publishing license.

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 stated above, the legislator's intention may be said to have been that the GDPR and the Data Protection Act should not apply at all to the constitutionally protected area. However, it may be noted that this is not expressed in the legislative text. Section 7, first paragraph
The Data Protection Act states that the GDPR shall not apply "to extent that it would be contrary to the Freedom of the Press Act or
the Basic Law on Freedom of Expression". The wording of the provision thus suggests that the GDPR only takes precedence when there is a conflict between the regulations.

49. It should be emphasized that the fact that confidentiality applies to certain information as a starting point cannot be considered to mean that there is a conflict with the Freedom of the Press Act or the Basic Freedom of Expression Act. On the contrary, the Freedom of the Press Ordinance provides that the Riksdag may legislate on secrecy and that secrecy then also applies in relation to activities covered by the Freedom of the Press Ordinance or the Fundamental Law on Freedom of Expression.

50. It is also worth noting that Chapter 1. 7 of the Data Protection Act and Chapter 21. 7 of the Freedom of Information and Secrecy Act, as far as is now relevant, 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 preparatory works to Chapter 21, section 7 that concern the issue of confidentiality. 7 that concern the question of whether confidentiality should apply in relation to activities covered by constitutional protection under the Freedom of the Press Ordinance or the Basic Freedom of Expression Act.

51. Against this background, the Supreme Court concludes that there is scope to interpret Chapter 1 7, first paragraph, of the Data Protection Act so that the provision does not prevent the requirements of the Data Protection Regulation from being taken into account in the application of the special confidentiality provision in Chapter 21, section 7 of the Freedom of Information and Secrecy Act. 7 of the Freedom of Information and Secrecy Act also in the constitutionally protected area. And such an interpretation should be made regardless of how one is to view the meaning of Chapter 1. 7, first paragraph, as regards the question of whether the Regulation can be applied to the subsequent processing in the activity covered by the constitutional protection.

52. This means that the authority that has to carry out an assessment under Chapter 21, section 7 of the Freedom of Information and Secrecy Act must 7 of the Freedom of Information and Secrecy Act must assess whether the information, after disclosure, can be assumed to be processed in violation of

the provisions of the GDPR, without taking a position on the extent to which the Swedish regulation means that the Regulation does not apply to the activities of the person who has requested the information. In the application of Chapter 21, section 7, the Data Protection Regulation can then be seen as a deadline. 7 can then be seen as an independent yardstick for when confidentiality applies to information that would otherwise have been 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. In Chapter 1. Section 7, second paragraph states that exemptions from the application of the Data Protection Regulation shall be made in principle in all parts where the Regulation allows for exemptions. More specifically, as stated, Articles 5-30 and 35-50 of the GDPR are exempted. Here, the legislator has more clearly used the system of national adaptation provided for in Article 85 of the GDPR.

55. The preparatory works show that the main purpose of the exception in the second paragraph has been to ensure that, among other things, journalistic activities that are not covered by the Freedom of the Press Act and the Freedom of Expression Act are exempted from parts of the Data Protection Regulation and the Data Protection Act. A starting point in the design of the provision
has been that exceptions should be introduced to the extent permitted by the Ordinance (see Government Bill 2017/18:105, pp. 44 et seq. and 187). It can be noted that the provision - although it aims to cover activities that are not covered by the Freedom of the Press Ordinance or the Basic Freedom of Expression Act - according to its wording also covers activities that have constitutional protection.

56. The wording of the second subparagraph does not leave the same scope for interpretation in accordance with Union law as the first subparagraph. However, the two paragraphs must be seen in context. The second paragraph cannot reasonably be interpreted as meaning that the exemption from the application of the GDPR for nonconstitutionally protected activities is more far-reaching than the exemption 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 Data Protection Regulation from being fully taken into account in an examination under Chapter 21. 7 of the Freedom of Information and Secrecy Act. The authority that has to carry out the review shall thus assess whether the data, after disclosure, can be assumed to be processed in contravention of the provisions of the Data Protection Regulation, without taking a position on whether the exempted articles of the Regulation are to be applied in the activities carried out by the person who has requested the data.

Overall conclusion

58. Taken together, the above means that Chapter 1 7 of the Data Protection Act - assessed in the light of EU law - does not prevent the GDPR from being taken into account in the application of the confidentiality provision in Chapter 21. 7 of the Freedom of Information and Secrecy Act.

The assessment in this case

Does confidentiality apply under Chapter 21. 7 of the Freedom of Information and Secrecy Act?

59. In order for confidentiality under Chapter 21. 7 of the Public Access to Information and Secrecy Act to apply to the information that Nyhetsbyrån Siren has requested to be disclosed, it is required that it can be assumed that the information will be processed after disclosure

in a way that is incompatible with the GDPR. The presumption must be based on the existence of concrete circumstances indicating this, but there is no need to make a full assessment of whether the processing operation likely to be carried out is incompatible with the GDPR (see point 14). There is no need to take a position on the extent to which the Regulation applies to SIRENE's activities, but the Regulation must be used as an independent yardstick in the assessment (see paragraphs 52 and 57).

60. SIRENE has requested a large number of criminal convictions and other documents related to criminal cases, such as decisions, diary sheets and summons applications. These documents contain information on breaches of the law and other sensitive data. Siren has repeatedly requested public documents from the Court of Appeal in a similar way. Against this background, and taking into account the extensive processing of personal data of this kind that takes place at SIRENE, it can be assumed that the personal data contained in the requested documents will be processed in a way that is incompatible with Article 10 of the Data Protection Regulation (cf. p. 42). Consequently, confidentiality applies to the personal data contained in the documents requested.

Are there conditions for conditional release of the documents?

61. If an authority finds that such a risk of damage, harm or other inconvenience which, according to a provision on confidentiality, prevents the disclosure of information to an individual can be eliminated by a reservation that restricts the individual's right to pass on the information or use it, the authority shall make such a reservation when the information is disclosed to the individual (Chapter 10, Section 14, first paragraph of the Freedom of Information and Secrecy Act).

62. It seems clear that the provision is written with a view to those confidentiality provisions whose application requires consideration of damage, harm or other inconvenience. No reference to such factors

is not found in Chapter 21. 7 of the Public Access to Information and Secrecy Act, but there is also no exception in Chapter 10, section 14, which means that it cannot be applied in the case of confidentiality under Chapter 21. 7 §. The latter provision, like several other secrecy rules, also aims to protect information about individuals' personal circumstances. Disclosure of information that is incompatible with the GDPR may therefore be considered to be likely to cause damage, harm or other inconvenience. Even if the result of a reservation is not fully the same as in other cases, the provision in Chapter 10, Section 14, first paragraph, should therefore also be applicable when confidentiality applies under
Chapter 21. 7 §.

63. Setting a reservation under Chapter 10, Section 14 when disclosing documents can be a way of achieving to some extent a balance between different interests as required by the GDPR. This applies in particular when the interest in freedom of expression and information is to be combined with the right to privacy.

64. Given the nature of Siren's activities, it can be assumed that the data 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 a reservation which balances the interest in being able to carry out journalistic activities against the interest in privacy. There is reason to take into account, when formulating the reservation, that Siren makes available via its database, inter alia, editorially processed news text.

65. A reasonable balance between the different interests can be achieved if the reservation is designed to prevent the documents - with the personal data contained in them - from being made available by SIRENE or from being made searchable by others, but does not prevent the personal data from being searched.

the data are used in, for example, news texts or news material produced by Siren.

66. In those circumstances, there is reason to amend the Court of Appeal's decision so as to give effect to the reservation:

– 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 name, social security number or address of an individual; and

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

Judges Anders Eka, Henrik Jermsten (dissenting), Kristina Ståhl, Agneta Bäcklund (dissenting), Thomas Bull (dissenting), Petter Asp (Rapporteur) and Cecilia Renfors took part in the judgment.
The rapporteur was Malin Falkmer, Registrar.

DISSENTING OPINION

Mr. Justice Jermsten and Mr. Justice Bull dissent and consider the appeal should be allowed. In their opinion, the grounds should read as follows.

REASONS

Background information

1. Panoptes Sweden AB's activities include the collection, processing, analysis and presentation of information. The company operates the Siren news agency.

2. Siren focuses on monitoring the authorities and its core business is to identify and collect information for news and to pass on such information to other news organizations or mass media, such as newspapers, magazines and broadcasters. As Siren is a news agency, information from its database is subject to constitutional protection under Chapter 1, Section 4 of the Basic Law on Freedom of Expression. 4 of the Basic Law on Freedom of Expression.

3. Siren has asked the Court of Appeal for a large number of public documents in criminal cases, such as judgments, decisions, diary sheets and summons applications.

4. The Court of Appeal has decided to release the requested documents but with a reservation. The reservation means that the personal data contained in the documents may only be used for journalistic purposes and that 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 the decision, the Court of Appeal stated that it could be assumed that, after 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 confidentiality under Chapter 21. 7 of the Public Access to Information and Secrecy Act (2009:400) applied and a reservation was an appropriate protective measure.

On disclosure of judgments etc.

6. In order to promote a free exchange of views, free and comprehensive information and free artistic creation, everyone has the right to access public 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 Ordinance).

7. According to Chapter 21. Section 7 of the Public Access and Secrecy Act, confidentiality applies to personal data if it can be assumed that after disclosure, the data will be processed in contravention of the EU General Data Protection Regulation or the Act (2018:218) with supplementary provisions to the EU General Data Protection Regulation (Data Protection Act).

8. The confidentiality provision in question differs from other confidentiality provisions in that it does not refer to the data as such, but to what is likely to happen to them after disclosure. An assessment under the section only needs to be made if there are concrete circumstances indicating that the recipient will process the data in a way that is contrary to data protection regulations, e.g. that it is a question of mass extraction. A full assessment of whether the processing will contravene the GDPR or the Data Protection Act does not need to be made (see Government Bill 2017/18:105, p. 135 f.).

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 subsequently processed in a way incompatible with those purposes. Furthermore, the data must be processed lawfully, fairly and in a transparent manner in relation to the data subject, and must be adequate, relevant and not excessive in relation to the purposes for which they are processed. Furthermore, a key requirement is that one of the grounds set out in Article 6 must apply in order for a data to be processed. Examples of such grounds are the existence of the data subject's consent 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, offenses that constitute crimes and related security measures. Processing of such data may be carried out only under the control of an authority or where processing is permitted by Union or Member State law, which lays down appropriate safeguards for the rights and freedoms of data subjects. A complete register of criminal convictions may be kept only under the control of an 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. They shall furthermore for processing carried out for such purposes - if necessary

in order 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 Articles 5, 6, 9 and 10.

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

The 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 settled case law that the provisions of regulations generally have direct effect in national legal systems, without the need for national authorities to take any implementing measures (judgment of the Court of Justice of the European Union in
15 May 2021, Facebook Ireland and Others, C-645/19, EU:C:2021:483, p. 110 and case-law cited).

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

16. The reconciliation and reconciliation of freedom of expression, freedom of information and the protection of personal data is thus not clear from the GDPR. Moreover, there is room for differences

between 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, p. 69).

17. It is clear that several Member States have made extensive exemptions from the provisions of the Data Protection Regulation for journalistic activities (see SOU 2024:75 p. 120 ff. regarding Norway, Denmark and Finland). Even countries such as the Netherlands and Austria have, in a way similar to the Swedish regulation in substance, excluded activities that are journalistic from the scope of the Regulation.

18. In addition, the reconciliation under Article 85 must take into account that the rights in the Charter of Fundamental Rights of the European Union have an equal status. 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 in case of conflict they must be balanced against each other.

19. According to Swedish law, the GDPR shall not be applied to the extent that it would be contrary to the Freedom of the Press Act or the Freedom of Expression Act (Bill 2017/18:105, p. 40 ff.). Furthermore, Articles 5, 6, 9 and 10 of the GDPR shall not apply to the processing of personal data for journalistic purposes, even outside the constitutionally protected area.

20. Based on Article 85 of the GDPR, this position can be said to mean that the Swedish legislator has deemed it necessary from a freedom of expression perspective to fully exempt such actors covered by

of constitutional protection from the provisions of the Regulation, and that the same should essentially apply to those actors without constitutional protection but whose activities have journalistic purposes. The practical effect of this is that personal data processing is essentially unregulated.

21. 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
However, in the case of Endemol Shine Finland (C-740/22, EU:C:2024:216), the question may be asked whether the Swedish regulation strikes a balance between freedom of expression, freedom of information and the protection of personal data that is fully compatible with EU law.

22. In the opinion of the Supreme Court, there is reason to note the following at the outset 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 Data Protection Regulation between the right to public documents and the right to protection of personal data and concerned Article 85 only in so far 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 a national reconciliation based on that interest were not addressed. The judgment therefore has no direct bearing on the present situation.

23. In the second ruling, the Court found that respect for private life and the protection of personal data must be considered to outweigh the public interest in access to public documents. Furthermore, it was held that the right to freedom of information under Article 85 of the Data Protection Regulation should not be interpreted as justifying the disclosure of personal data relating to criminal convictions any person requesting such data (paragraphs 55 and 56).

24. The CJEU's reasoning thus focused on the balance of interests between the protection of personal data relating to criminal offenses and public access to public documents and freedom of information in general. The ruling therefore has no direct bearing on situations where an operator requests such information for journalistic purposes.

25. The conclusion that can be drawn from the CJEU's rulings is that the reconciliation between freedom of information and the protection of personal data must respect the principle of proportionality and that 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 CJEU's assessment of whether reconciliation under Articles 85 and 86 of the GDPR is acceptable has been based on the concrete circumstances of the individual case. Although it must be possible to take into account the design of a national system at an abstract level, it is thus the effects in the concrete case that are decisive for the assessment of 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 public documents by an actor who has so-called automatic constitutional protection, i.e. constitutional protection follows directly from the Constitution (Chapter 1, Section 4 of the Freedom of Expression Act).

28. From a constitutional point of view, this means that the starting point is that SIREN is an actor whose activities can be assumed to be in line with the purpose of the Basic Law on Freedom of Expression, i.e. to ensure a free exchange of opinions, a free and

general education and freedom of artistic creation. These are all purposes that almost entirely coincide with the areas where exemptions from the provisions of the GDPR are allowed under Article 85.

29. The information on Siren's activities is as follows. Siren is a member of the Association of Newspaper Publishers. Siren identifies and collects news material in order to provide such material to other news organizations or mass media. Siren processes, evaluates and prepares documentation on the basis of documents provided by courts, authorities and others. This processing is intended for publication in various ways. It is the editorial staff who analyze the material and make independent news assessments. The processed material can then be used for publication in other mass media or in Siren's own database.

30. It is clear that SIRENE collects personal data for journalistic purposes. Thus, although it is questionable whether the Swedish regulation strikes a balance between freedom of expression, freedom of information and the protection of personal data which meets the requirements of EU law in all respects, there is nothing to suggest that, in the case of an actor such as SIREN, it would not be acceptable to carry out the balancing of interests under Article 85 of the GDPR in the way that the Swedish legislature has done.

31. It cannot therefore be considered contrary to European Union law to apply constitutional protection to SIREN's request access to public 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 confidentiality applies under Chapter 21. 7 of the Freedom of Information and Secrecy Act. Under that section, confidentiality applies to

personal data if it is likely that, after disclosure, the data will be processed in breach of the GDPR.

33. However, it cannot be assumed that SIRENE will process the personal data contained in the documents requested by SIRENE in breach of the GDPR as the processing of personal data by SIRENE is not subject to the provisions of the GDPR.

34. Secrecy under Chapter 21. 7 of the Freedom of Information and Secrecy Act does not apply. The appeal shall therefore be granted.

_____

DISSENTING OPINION

Justice Agneta Bäcklund dissents and considers that the case should be dismissed from further consideration. She considers that the recitals from paragraph 61 onwards should read as follows.

61. If an authority finds that the risk of damage, harm or other inconvenience which, according to a provision on confidentiality, prevents the disclosure of information to an individual can be eliminated by a reservation that restricts the individual's right to pass on the information or use it, the authority shall make such a reservation when the information is disclosed to the individual (Chapter 10, Section 14, first paragraph of the Freedom of Information and Secrecy Act).

62. It seems clear that the provision is written with such confidentiality provisions in mind, the application of which requires consideration damage, harm or other inconvenience. There is no reference to such factors in Chapter 21. 7 of the Freedom of Information and Secrecy Act.

63. It is difficult to see that a reservation would fully satisfy the possibility of balancing the interest in privacy and the interest in conducting journalistic activities when it is a question of processing a large amount of data relating to breaches of the law. The risk that the provision in Chapter 21. 7 is intended to prevent - that the data, after disclosure, will be processed in breach of the General Data Protection Regulation - cannot therefore be eliminated by a reservation.

64. With the interpretation of the relationship between Chapter 1. 7 of the Data Protection Act and Chapter 21. 7 by the Supreme Court, it is also hardly possible to lay down any rules on the processing of the disclosed data on infringements of the law, without considering whether Article 10 of the

GDPR applies to that processing. Furthermore, a reservation prohibiting the disclosure of certain information does not seem appropriate in view of the right to communicate freely on any subject.

65. The conclusion is therefore that there are no grounds for conditional disclosure. Nor does conditional disclosure appear to be an appropriate measure.

66. Since the documents to which the action relates have been disclosed to SIREN with reservations, the appeal should not give rise to any further action and the case should be removed from the register.

_____