Neutral Citation Number: [2026] EWCA Civ 140

Case No: CA-2024-002895

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE UPPER TRIBUNAL,
ADMINISTRATIVE APPEALS CHAMBER
Mrs Justice Heather Williams and Upper Tribunal Judges Wright and Stout
[2024] UKUT 287 (AAC)

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 19/02/2025

Before :

LORD JUSTICE MOYLAN
LADY JUSTICE ELISABETH LAING
and
LORD JUSTICE WARBY

- -

Between :

DSG RETAIL LIMITED	**Respondent/ Appellant**
- and -	
THE INFORMATION COMMISSIONER	**Appellant/ Respondent**

- -
- -

Julian Milford KC and Peter Lockley (instructed by the **ICO**) for the **Appellant**
Tim Pitt-Payne KC and Rupert Paines (instructed by **Pinsent Masons**) for the **Respondent**

Hearing date: 4 December 2025

- -

Approved Judgment

This judgment was handed down remotely at 10.00am on 19 February 2026 by circulation to the parties or their representatives by e-mail and by release to the National Archives.

.....

LORD JUSTICE WARBY:

Introduction and summary

1. This appeal is about the scope of the duty which data protection law imposes on data controllers to protect personal data of which they are the data controller by taking "appropriate technical and organisational measures". This is commonly known as the security duty. It is a protective duty, to take proportionate steps to guard against risk, not to guarantee a particular outcome. So it might equally be called a safeguarding duty. I shall use these terms interchangeably to refer to the same obligation.

2. The question raised by the appeal, simply stated, is whether the law requires a data controller to guard against the risk that data which relate to individuals who can be identified by the data controller will be subject to unauthorised or unlawful processing by a third party who cannot identify those individuals.

3. Today, the security duty is imposed in EU law by Articles 5(1)(f) and 32 of the General Data Protection Regulation ("GDPR") and, domestically, by the Assimilated General Data Protection Regulation ("UK GDPR"). But this case is concerned with events before the GDPR or UK GDPR came into force. So the legal context is provided by the Data Protection Act 1998 ("the 1998 Act"), which was enacted to give effect to the obligations imposed on the United Kingdom by the Data Protection Directive, 95/46/EC ("the Directive"). Section 4 of the 1998 Act required data controllers to comply with the data protection principles set out in Schedule 1 to the Act. The seventh data protection principle ("DPP7") imposed the security duty. DPP7 required data controllers to take appropriate technical and organisational measures (or "ATOMs") "against unauthorised or unlawful processing" of personal data and certain other eventualities.

4. The factual context for the appeal is that in 2017-2018 there was a cyber-attack on the systems of DSG Retail Limited ("DSG"), the owner and operator of well-known retail businesses including Dixons and Currys PC World. The critical feature of the attack, for present purposes, is that over a period of some nine months the attackers obtained millions of items of data by "scraping" transaction details from point-of-sale terminals, or card readers, as transactions were made, storing the data on DSG's servers, and attempting to exfiltrate the scraped data. More than 5.6 million payment cards were affected. In some 8,000 instances the attackers obtained the 16-digit card number or "PAN", the expiry date and the cardholder's name. But the great majority of the cards were protected by the "chip-and-pin" system, formally known as electro-magnetic verification ("EMV"). So, in those instances, the attackers only obtained the PAN and expiry date ("the EMV data"). They did not obtain the cardholders' names or any information that would enable them to identify the cardholders.

5. After an investigation, the Information Commissioner ("the Commissioner") found DSG in breach of DPP7 and served a monetary penalty notice ("MPN") in the maximum sum of £500,000. DSG appealed to the First-tier Tribunal ("FtT") contending, among other things, that DPP7 did not require them to take ATOMs against third-party acquisition of the EMV data because those would not be "personal data" in the "hands" of the third parties. The FtT rejected that contention, holding that it was sufficient that the EMV data were "personal data" in the "hands" of DSG. The FtT upheld the MPN, though it reduced the penalty by half.

6. DSG appealed to the Upper Tribunal ("UT"), which accepted DSG's case and reversed the findings of the FtT on this issue. The UT's key conclusion, for our purposes, was that the question of whether third-party acquisition of the EMV data involved personal data had to be analysed from the perspective of the third party. Viewed in that light, third-party acquisition of data was not "unauthorised or unlawful processing of personal data" against which ATOMs had to be taken, if the data themselves did not identify the individuals to whom they related and the third party had no other means of identifying those individuals.

7. The Commissioner now appeals to this court with permission granted by Elisabeth Laing LJ on the single ground that the UT erred in law "by holding that a data controller is not required to take appropriate technical and organisational measures against unauthorised or unlawful processing of data by a third party, where the data is personal data in the hands of the controller, but not in the hands of the third party." DSG resists the appeal, contending that the UT was right for the reasons it gave.

8. I have concluded that the UT's reasons for adopting a narrow interpretation of the statutory wording, though careful and thorough, are not in the end compelling. They lead to some surprising conclusions. In my judgment, a broader construction is more consistent with the language of the statute and its parent Directive, the identifiable purposes of the data protection legislation, and with the few decided cases that have any significant bearing on this issue. I would therefore allow the appeal and remit this case to the FtT to be determined in accordance with this judgment.

The issue further defined

9. It is unnecessary to add much to the summary I have already given. It is, however, appropriate to make these three points. First, the single issue before us is only one of a wider range of issues raised by the Commissioner's MPN and considered by the tribunals below. There were, for instance, findings that the attackers gained access to many millions of items of non-financial personal data. None of that is material to this appeal. Secondly, we are not deciding any factual issue about whether (as the Commissioner alleged in the proceedings below) there was a risk that attackers might obtain data which they could reasonably have identified as relating to an individual cardholder. We are addressing the single issue before us as one of legal principle, on the assumption that the cardholders were identifiable to DSG but not to the attackers. Thirdly, the legal issue is simply whether, on those assumptions, the company had any duty at all to take any ATOMs. We are not concerned with whether, if the duty does apply in that hypothetical scenario, the measures actually taken by DSG were "appropriate" or fell short of that standard. Nor are we concerned with the questions of whether any breaches of duty were serious enough to merit an MPN, or whether the MPN imposed was appropriate.

The legal context

10. Our task is to construe the statutory language. The primary text for consideration is that of the 1998 Act. However, we must interpret and apply the 1998 Act compatibly with the language and purposes of the Directive: *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, [2016] QB 1003. In discharging that duty we are bound by relevant decisions of the House of Lords. We are bound by relevant decisions of the Court of Justice of the European Union ("CJEU") made before IP Completion Day; and we "may have regard"

to relevant later decisions of the CJEU: *Farley v Paymaster (1836) Ltd t/a Equiniti* [2025] EWCA Civ 1117 [30].

The 1998 Act

11. The key concepts of "data", "personal data", "data subject" and "data controller" were all defined in s 1(1). This provided relevantly as follows:

> In this Act, unless the context otherwise requires—
>
> "*data*" means information which
>
> (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
>
> ...
>
> "*data controller*" means .... a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed
>
> ...
>
> "*data subject*" means an individual who is the subject of personal data;
>
> "*personal data*" means data which relate to a living individual who can be identified—
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller ...

12. The further key concept of "processing" was also defined by s 1(1) of the 1998 Act, in the following relevant terms:

> "*processing",* in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including
>
> (a) organisation, adaptation or alteration ...
>
> (b) retrieval, consultation or use ...,
>
> (c) disclosure ... by transmission, dissemination or otherwise making available, or
>
> (d) alignment, combination, blocking, erasure or destruction of the information or data;

13. Section 4(4) of the 1998 Act provided that, subject to some immaterial exceptions,

> it shall be the duty of a data controller to comply with the data protection principles **in relation to all personal data with respect to which he is the data controller.**

14. Schedule 1 Part I to the 1998 Act set out eight data protection principles. Each principle prescribed duties to be performed when processing personal data. DPP7, the provision with which we are directly concerned, was set out in paragraph 7, in these terms:

> Appropriate technical and organisational measures shall be taken against **unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data**.

15. Here and below I have emphasised in bold some key words. It will be clear already that the central question of interpretation is whether, by using the words I have emphasised in paragraphs [13] and [14] above, Parliament intended to impose a broad or a narrow duty. The broad duty would be one requiring the data controller ("C") to safeguard all information consisting of personal data of which C is a data controller against processing of any of the kinds identified in DPP7, including processing by a third party who could not identify the data subject(s). The narrow duty would be one to safeguard personal data of which C is a data controller from acts of C or a third party if, but only if, the act would amount to "unauthorised or unlawful processing" of data relating to a person who could be identified by the perpetrator of the act or, putting this in the language of the grounds of appeal, the data would be personal data "in the hands" of that person. The answer does not immediately emerge from the language of s 4(4) read with DPP7.

16. One possible source of guidance is Schedule 1 Part II to the 1998 Act, headed "Interpretation of the Principles in Part I". Paragraph 9 explained what was meant by "appropriate" measures:

> Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—
>
> (a) the harm that might result from s**uch** unauthorised or unlawful processing **or** accidental loss, destruction or damage **as are mentioned in the seventh principle**, and
>
> (b) **the nature of the data** to be protected

17. Also relevant, for reasons that will become apparent, are the first and second data protection principles. These were set out in paragraphs 1 and 2 of Schedule 1 Part I. The first principle required processing to be fair and lawful and to comply with certain conditions. Paragraph 2 set out the second principle, known today as "the transparency duty". This provided that

> personal data shall be **obtained only for one or more specified and lawful purposes**, and shall not be further processed in any manner incompatible with that purpose or those purposes.

18. These principles were further explained in Schedule 1 Part II, headed "Interpretation of the Data Protection Principles". Among the effects of Schedule 1 Part II paragraphs 2 and 5 were that, putting it broadly, the disclosure of personal data obtained from the data subject would be treated as unfair unless, at the time of collection, the data controller had given the data subject notice of the intended recipient(s) and purpose(s). Notices of this kind, known as "fair processing notices" are a familiar feature of online life.

The Directive

19. The Directive is also a potential source of interpretative guidance. Recital (26) identified the scope of the "principles of protection" that are implemented by the Directive. It included some language about identifiability that did not appear in the 1998 Act and was broader:

> (26) Whereas the principles of protection must apply to **any information concerning an identified or identifiable person;** whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used **either by the controller or by any other person** to identify the said person

Recital (26) went on to identify a proviso or limit to the principles, using language that did not appear in the 1998 Act:

> whereas **the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable ...**

20. The definition of personal data in Article 2 was, again, cast in broader terms than the definition in the 1998 Act. Article 2 provides:

> "For the purposes of this Directive:
>
> (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); **an identifiable person is one who can be identified directly or indirectly**, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"

21. Recital (46) identified the objectives that underlay the security duty, using these words:

> Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing .... whereas these measures must **ensure an appropriate level of security,** taking into account the state of the art and the costs of

> their implementation in relation to **the risks inherent in the processing** and the nature of the data to be protected

22. The substantive provisions which DPP7 was intended to implement were contained in Article 17(1) of the Directive, headed "Security of Processing". This provided as follows:

> Member States shall provide that the controller must implement appropriate technical and organisational measures **to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access**, in particular where the processing involves the transmission of data over a network, **and against all other unlawful forms of processing.**
>
> Having regard to the state of the art and the cost of their implementation, such measures shall **ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected**.

23. The origin of the transparency duty in respect of data obtained from the data subject was in Article 10 of the Directive. No relevant differences of substance. are apparent. This transparency duty is now contained in Article 13 of the GDPR and UK GDPR which is in similar terms.

Case law

24. There appears to be no domestic or CJEU authority that bears directly on the issue before us. None has been identified by the parties. Nor, so far as we are aware, is there any decision on that issue in the jurisprudence of any other European country. We have however been referred to two main categories of case law which are said by one side or the other, or both, to have a bearing on our decision.

25. First, there is a body of UK case law about the operation of the exemption for "personal data" in the freedom of information legislation. The leading authority is the House of Lords' decision in *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47, [2008] 1 WLR 1550 *("CSA").* That case was concerned with the Freedom of Information (Scotland) Act 2002 ("FoI(S)A"), but that legislation is in materially identical terms to our Freedom of Information Act 2000 ("FoIA"). The House held, in short, that in principle, where a data controller renders personal data which it holds fully anonymous, these will no longer be "personal data" within the meaning of the 1998 Act and can be disclosed to a third party under FoI(S)A. The implications of *CSA* have been addressed in three decisions about FoIA that were cited to us: those of the UT in *APPGER v Information Commissioner* [2011] UKUT 153 (AAC) *("APPGER"),* the High Court (Cranston J) in *R (Department for Health) v Information Commissioner* [2011] EWHC 1430 (Admin) *("DoH"),* and the UT in *Information Commissioner v Miller* [2018] UKUT 229 (AAC) *("Miller").* These cases were all considered by the UT in the present case.

26. Secondly, there is some EU jurisprudence, comprising two cases: *Gesamtverband Autoleile-Handel EV v Scania CV AB* ("*Scania*") and *Single Resolution Board v*

European Data Protection Supervisor ("*SRB v EDPS*"). *Scania* is a decision of the CJEU (C-319/22, [2024] 2 CMLR 40) about when vehicle identification numbers ("VINs") amount to personal data within the meaning of the GDPR. That decision was handed down in November 2023 and was taken into account by the UT in this case. *SRB v EDPS* was about comments which shareholders of a Spanish bank had submitted to the SRB in response to a proposed scheme of resolution. The SRB passed pseudonymised versions of those comments to an external consultancy, Deloitte. The issue was whether, by doing this without giving the shareholders a fair processing notice, the SRB had infringed the transparency duty.[1] The EDPS determined that it had. In 2023, the General Court of the European Union ("GCEU") annulled that decision, reasoning that "in order to determine whether the information transmitted to Deloitte constituted personal data it is necessary to put oneself in Deloitte's position in order to determine whether the information transmitted to it relates to 'identifiable persons'", and that the EDPS had not done that: Case T-557/20, [2024] 2 CMLR 46 [97], [105]. In this case, the UT referred to and relied on the GCEU decision. The CJEU has since heard and allowed an appeal against that decision (C-413/23). We have the benefit of the CJEU's judgment dated 4 September 2025 and of the parties' submissions about that.

The FtT decision

27. The issue that is before us now was addressed at paragraphs [92]-[98] of the FtT's decision. The Tribunal set out a three-part analysis of the concept of personal data, as follows:-

> The primary definition of personal data, set out in s 1 of the DPA, read with Recital 26 of Directive 95/46/EC is data from which a living individual can be identified either directly, or from those data and other information, which is in the possession of or likely [reasonably] to come into the possession of, the data controller or a third party. Thus .... there are 3 limbs to the definition of personal data
>
> i. Data which identifies a living individual directly;
>
> ii. Data which identifies a living individual indirectly when combined with other information in the possession of (or likely reasonably to be in the possession of) the data controller; and
>
> iii. As (ii) but where the additional information is or is likely reasonably to be in the possession of a 3rd party.

28. The Tribunal considered it unnecessary to rule on the parties' arguments as to whether the EMV data were personal data within limb (i) or limb (iii). It was enough to conclude that the EMV data fell within limb (ii), for these reasons:-

> 92 ... in the context of these proceedings any PAN that identifies the bank account held solely by a living individual are personal

[1] In this instance, the duty was imposed by Article 15(1) of Regulation EU 2018/1725, which governs the processing of personal data by organs and agencies of the EU, but is materially identical to Article 13(1) of the GDPR.

> data for the purposes of DPP7 ... because a living individual could be identified indirectly from the PAN held by DSG when combined with additional information which is also in the possession of, or reasonably likely to come into the possession of, DSG.

29. The essence of the Tribunal's reasoning is encapsulated in the following passages:-

> 93. ...
>
> c. One of the purposes of the DPA is to create legal rights and obligations relating to personal data that are enforceable against the data controller. Unless exempt by virtue of s. 27(1), s. 4(4) requires a data controller to comply with all data protection principles in relation to all of the personal data in respect of which they are the data controller. In short, a data controller has obligations in relation to the personal data they are processing. None of the authorities to which we have been directed suggest that these obligations do not apply to data which is personal data when in the hands of the data controller, but which ceases to be personal data when in the possession of a 3rd party.
>
> d. The fact personal data may be anonymised to the extent that it becomes 'vanilla data' if or when it is published to the world at large, for example following an information request made pursuant s. 1 FOIA, does not preclude the data meeting the definition of personal data whilst it remains in possession of the data controller, provided the data controller is reasonably likely to have other information with which the data could be 'de-anonymised'. Whilst FOIA understandably points towards the DPA and related authorities for its definition of personal data, the DPA's definition of personal data is not limited by the contextual considerations of whether data remains personal data following publication as a result of a FOIA request.
>
> 94. We are ... satisfied that at least some of the PAN processed by DSG was capable of leading to the identification indirectly of a living individual, when combined with other data reasonably likely to be processed by DSG. ...
>
> 95 ... both Parties have focussed on the nature of a PAN once it has passed into the possession of 3rd parties, and on any consequent risks of harm. In our view this overlooks the fundamental purpose of the DPA and the Data Protection Principles, which imposes obligations on data controllers in relation to personal data when it is held by the data controller.
>
> 96 Put another way, the approach taken by the Parties in this case would, if taken to its logical conclusion, support a view

> whereby a data controller need only comply with DPP7 in relation to personal data that will continue to be personal data if and when it is unlawfully processed in isolation by a 3rd party. The fact that a record comprising personal data in the hands of a data controller will become purely 'data' in such circumstances must be relevant to any assessment of the risk of consequent damage and distress. However, this does not remove the requirement for appropriate technical and organisational measures to be in place in relation to the record while it remains personal data in the hands of the data controller.

The UT decision

30. The UT adopted the FtT's three-part analysis of the concept of personal data, but concluded that it was limbs (i) and (iii) that were important, not limb (ii). Its core reasons for taking that view appear from the following passages in its decisions.

> 112. For DPP7 purposes there is a distinction between the questions of who is subject to the duty and what data that duty applies to (on the one hand) and the question of what are the risks to protect against and whether that duty was breached (on the other) […] Here, the risk that the ICO considered DSG had failed to take appropriate steps to guard against was the risk of unauthorised or unlawful processing of personal data, that is to say unauthorised or unlawful processing of personal data by third parties. **Thus, it is necessary to consider what third parties would be able to obtain as a result of the alleged failings and to determine whether this would constitute personal data in their hands**. This necessarily involves considering the data from a limb (i) and a limb (iii) perspective, **not a limb (ii) perspective.**"
>
> ...
>
> 114 ... If a third party can only obtain anonymous data and the key to any pseudonymised material remains behind a completely secure wall then, consistent with the case law that we return to below, accessing that vanilla data would not amount to an "unauthorised or unlawful processing of personal data".

31. The UT went on at [122] to identify three propositions which it considered to be established by the domestic and European authorities:

(1) That "in instances of pseudonymisation, the same information may be personal data in the hands of the data controller (who retains the key to the identifying material), but not personal data in the hands of a third party, if the third parties do not have the means to access the additional information that the data controller holds which enables the identification of living individuals."

(2) That "whether the data that is said to constitute personal data is to be considered from a limb (ii) or a limb (iii) perspective, will depend upon the nature of the

statutory obligation and the processing under consideration." It was not the case that "both perspectives are taken into account in every instance" as the Commissioner had submitted.

(3) That "if outside of the hands of the data controller, no living individual can be identified from the data, **then at the moment of disclosure the information loses its character as 'personal data'**".

32. The UT concluded this part of its judgment at [123] as follows:

> Accordingly, when considering in relation to DPP7 whether ATOMS have been taken to protect against the particular risk of "unauthorised or unlawful processing of personal data", it is necessary to construe this risk in light of these principles. As the risk to be guarded against is the risk of data processing by third parties**, the question of whether personal data is involved is to be judged from the perspective of the data that the third parties can access** (rather than the entirety of the data held by the data controller), that is to say from a limb (iii) perspective (if the limb (i) definition is not met).

The appeal

33. The Commissioner's case is that the words I have emphasised in the quotations at [30]-[32] above reflect an error of law. The Commissioner submitted that the UT's interpretation was unduly narrow. It did not properly reflect the ordinary meaning of the language used by Parliament and the EU, nor did it give proper effect to the legislative purposes. It would leave gaps in the scope of protection, and would have practical consequences, which neither Parliament nor the EU is likely to have intended. On the UT's approach a data controller would, for instance, have no duty to protect against malicious third-party action to destroy or alter personal data held by the data controller, where the third party could not identify the data subjects. The Commissioner would have no basis for taking regulatory action against such a data controller. Finally, it was submitted that the case law cited by the UT does not, on a proper analysis, support its approach.

34. DSG submitted that the answer to this case is simple: it had no duty under the 1998 Act to prevent access to or use of personal data of which it was a data controller by a third party which could not identify the individual(s) to whom the data relate. In such a case, "[t]he data is not personal data in the hands of the third party, and so the third party would not be processing personal data" within the meaning of DPP7. This interpretation was said to be in accordance with the statutory language and prior authority. The Commissioner's contention that the UT's approach leaves unintended gaps in protection was said to beg the question at issue, and to be wrong as a matter of construction anyway. The Commissioner's own interpretation was described as "absurd". It was submitted that it would be "unfortunate, indeed bizarre" if data controllers were under a duty to protect information from access or use by third parties even if, so far as those third parties are concerned, it would be fully anonymised and therefore "not personal data at all".

Discussion and analysis

35. The relevant principles of statutory interpretation are well-known and not controversial. The court's task is "to ascertain the intention of Parliament expressed in the language under consideration"; "intention" here is not a subjective concept but an objective one, referring to "the intention which the court reasonably imputes to Parliament in respect of the language used": *R v Secretary of State for the Environment, Transport and the Regions ex p Spath Holme Ltd* [2001] AC 349, 396 (Lord Nicholls). The text of the particular enactment under examination and its natural and grammatical meaning are therefore the primary considerations, although the context and purpose of the enactment are both important: *R (O) v Secretary of State for the Home Department* [2022] UKSC 3, [2023] AC 255, [29] (Lord Hodge), *R v Luckhurst* [2022] UKSC 23, [2022] 1 WLR 3818, [23] (Lord Burrows). The potential consequences of competing constructions of the enactment are also relevant: *Fry v Inland Revenue Commissioners* [1959] Ch 86, 105 (Romer LJ).

36. We need, as I have said, to construe the 1998 Act compatibly with the Directive. We work on the assumption that Parliament intended its legislation to give effect to the UK's treaty obligations. We also need to take account of the UK and EU case law about the meaning of the term "personal data" that I have mentioned. This is for two reasons. First, we need to consider whether the decision in *CSA,* the *ratio* of which is binding upon us, dictates the answer to the question raised by this appeal. Secondly, and in any event, we must aim to ensure, as best we can, that this area of the law develops in a principled and coherent fashion.

37. For the reasons I shall explain, my opinion is that the language, context, and purposes of DPP7, and consideration of the consequences that would follow from the UT's interpretation, all point to the conclusion I have already identified: the security duty does require a data controller to take ATOMs against processing by a third party of data that relate to an individual who is identifiable to the data controller but not to the third party. That conclusion is consistent with the Directive. The decision and reasoning in *CSA* do not undermine it; that case addresses a different issue. And the EU jurisprudence is consistent with, indeed lends support to, the view at which I have arrived.

The legislative language and its immediate context

38. I begin with the body of the 1998 Act, and four features of the statutory language that seem to me significant. First, the general duty imposed on a data controller by s 4(4) is a duty to comply with the data protection principles in relation to "all personal data with respect to which he is the data controller". This is an unqualified duty in respect of any data that falls within the language quoted. Secondly, the definition of "personal data" in s 1 has only two categories. Category (a) is data which themselves enable a living individual to be identified, that is to say by anyone. Category (a) data, as they may be called, are defined by the criterion of direct identifiability. Category (b) comprises data relating to an individual who cannot be identified from the data themselves, but who can be identified from those data and other information which is, or is likely to come into the possession of, the data controller. Category (b) data, as they may be called, are defined by a criterion of indirect identifiability. Thirdly, it follows that on the face of the statute the s 4 duty is imposed (and imposed only) in respect of data that relate to a living individual who is directly identifiable, by anyone, from the data (category (a)) or

indirectly identifiable by the data controller (category (b)). Fourth, there is no reference here to the prospect of indirect identification by anyone other than the data controller. The language contains nothing that expressly or implicitly indicates that indirect identifiability by any third party is in any way a factor that expands, limits, or in any other way controls the scope of the duty.

39. Turning to the specific duty laid down by DPP7, I note that the object of this duty is, again, "personal data". This term appears twice in the text of DPP7. Applying ordinary principles of interpretation, it must bear the same meaning in both those places. And, unless there is some indication of a contrary intention, it must bear the same meaning in DPP7 as it does in s 4(4), that is to say, the meaning defined in s 1. There is nothing in the express terms of DPP7 that appears apt to limit or otherwise modify the scope of the defined term "personal data" in this context. Accordingly, the natural interpretation of DPP7, read in the context of ss 1 and 4(4), is that the security duty is imposed on a data controller in respect of all and any data which the controller is processing that relate to an individual who is directly identifiable from the data, or indirectly identifiable by the data controller. Nothing more but also nothing less. There is no reason, so far, to conclude that the data controller is relieved of this duty, or that the duty is qualified, in circumstances where the individual is not identifiable by a third party.

40. Next, it is necessary to consider the risks or eventualities against which the data controller is required to protect the personal data. That calls for interpretation of the list in DPP7. Up to a point, that is a relatively straightforward task. Grammatically, the list appears to involve two groups, linked by the word "and". The first group comprises "unauthorised or unlawful processing", and the second "accidental" loss, destruction or damage. The language of Schedule 1 paragraph 9 supports this analysis. Again, it places the risks in two groups, with a linking word (in this instance, "or"). So far, so good. And on the face of it, these might appear to be two separate and distinct groups of risk, one involving deliberate or non-accidental events, and the other various forms of accident. The task of interpretation is however complicated when one appreciates that the concept of "processing" is extraordinarily broad; that "destruction" is expressly identified in the non-exhaustive list of "processing" activities that appears in s 1(1) of the 1998 Act; and that "accidental" processing is liable to be "unauthorised" even if not "unlawful". It would therefore seem that these are two overlapping groups.

41. However that may be, it remains the case that, on the face of it, the risks against which a data controller is required to guard category (b) data include (though they are not limited to) non-accidental processing by a third party that is unauthorised or unlawful, whether or not the individual is identifiable to the third party. I can see nothing in the 1998 Act to support the submission of DSG, that the first part of DPP7 should be read as referring only to processing by someone other than the data controller to whom the individual is identifiable. That interpretation would require one to give the term "personal data" in this context a meaning different from and more limited than the one defined in s 1, and to the exclusion of that defined meaning. No reason for doing so is apparent. Personal data from which a person is indirectly identifiable by a data controller do not cease to have that character just because the data are also processed by someone else to whom the individual is not identifiable.

42. These conclusions about the 1998 Act need to be reviewed, of course, in the light of the Directive. As I have noted, Recital (26) and Article 2 define personal data in broader

terms than the 1998 Act. This is important. A domestic court must interpret and apply the language of the 1998 Act compatibly with the Directive. The court must, if necessary, disapply some of the statutory language, as in *Vidal-Hall*. The Directive therefore requires us to read category (b) of the definition of personal data in the 1998 Act as including data from which an individual is indirectly identifiable by anyone, including a third party. It is unnecessary to determine the mechanism for doing so, but one obvious means would be to read in the words "or any other person" that appear in the Directive. But I do not think this supports the UT's conclusions or assists the argument for DSG.

43. The language of the Directive gives the concept of "personal data" an expanded reach as compared to the ordinary meaning of the 1998 Act, not a more restricted one. Put another way, the Directive requires category (b) to be enlarged. The most obvious consequence for the security duty would be that the duty should be read more expansively, not less so. An available conclusion would be that the risks against which a data controller is required to guard include not only the ones I have already identified but also the risk of unauthorised or unlawful processing of data (and possibly other forms of processing) by a third party to whom the individual is indirectly identifiable, *even if* the individual is not identifiable to the data controller.

44. The CJEU decision in *Scania* provides some support for this view. Independent operators in the motor vehicle industry asserted that Regulation 2018/858 (access to vehicle repair and maintenance information) required vehicle manufacturers to provide them with access to VINs. The question arose of whether that would involve the "processing" of "personal data" within the meaning of the GDPR. The CJEU held that it would. VINs were not "in themselves and in all cases" personal data, because they did not identify any natural person. But they would be "personal data" if they were made available to the operators, and the operators had lawful access to the means of identifying the vehicle owners, such as by combining the VINs with registration certificates containing personal details of the vehicle owners. That was because data of this kind "becomes personal as regards someone who reasonably has means enabling that datum to be associated with a specific person": [46]. Accordingly, in a case where the operator might reasonably have the means enabling them to link a VIN to a natural person "the VIN constitutes personal data for them ... and, indirectly, for the vehicle manufacturers making it available...": [49]. For the controller (the manufacturer) to make the VINs available would amount to "processing": [51].

45. The GDPR definition of "personal data" is materially identical to that of the Directive. There was no suggestion in *Scania* that the manufacturers had access to registration certificates or to any other means by which they could indirectly identify any natural person as the vehicle owner or keeper or driver. The Court appears to have concluded that if and so long as the VINs would amount to personal data "as regards" the recipient operators, the disclosure of the VINs to them by the manufacturer would amount to processing of personal data within the meaning of the GDPR. It did not matter if, as seems to have been assumed, the data would not be "personal data" "as regards" the manufacturer. At [84] of its later judgment in *SRB v EDPS* the CJEU summarised the principle established in the *Scania* case as follows:

> Data which are in themselves impersonal may become 'personal' in nature where the controller puts them at the disposal of other persons who have means reasonably likely to enable the data

> subject to be identified .... where those data are put at their disposal – those data are personal data both for those persons and, indirectly, for the controller.

46. Regardless of this analysis, and returning to the question at issue, two fundamental observations remain. First, that - on the face of both the 1998 Act and the Directive - data are "personal data" if and for as long as the individual to whom they relate is indirectly identifiable to the data controller. Secondly, the fact that the concept of "personal data" is broader in the Directive than it is in the 1998 Act does not logically lead to a narrower or different interpretation of the security duty. The next question is whether there is anything else in the Directive that supports a narrower view of the scope of that duty.

47. The key provisions are in Recital (46) and Article 17(1). I can see nothing in the Recital that calls for a more limited approach. Nor do I see any such material in Article 17(1). That Article is framed in a different way from DPP7. The three concepts of unauthorised, unlawful and accidental activity are all included, but they are not presented in the same order or in the same way. The list of events against which ATOMs must be taken is not clearly divided into two, and it includes some events that are not mentioned in DPP7: "alteration", "disclosure" and "access". The internal logic is not immediately apparent. So Article 17(1) does pose interpretative challenges.

48. In my judgment, however, four conclusions can reliably be drawn: (1) the relevant provisions of the Directive rely on a concept of personal data which is broadly defined, and includes data relating to an individual who is indirectly identifiable to the data controller; (2) Article 17 contains a non-exhaustive list of events that involve some form of processing of personal data, so defined; (3) in its ordinary meaning, Article 17 encompasses a duty to guard against at least some forms of non-accidental processing by a third party of information which is being processed by the data controller, and which is personal data because the individual concerned is indirectly identifiable to the data controller; (4) the language of Article 17 provides no support for the view advanced by DSG, that the duty does not extend to processing that results in data coming into the "hands" of a third party who lacks the means of identification.

49. In reaching this fourth conclusion I have borne in mind that I am now dealing with a definition of "personal data" that goes beyond category (b) as defined on the face of the 1998 Act, and includes data from which an individual is indirectly identifiable by a third party. But this does not in my opinion provide any sound basis for concluding that, as DSG contend, the term "personal data" in DPP7 should be interpreted or applied in a restricted fashion. I note that DSG's core submissions include the proposition that "third party conduct with regard to the EMV data would not be **processing of personal data**" (my emphasis). The thrust of the point is that this language denotes processing carried out by someone *to whom* the data are "personal data". This is, to my mind, a weak and unconvincing submission. And such force as it has relies on the terminology of DPP7, not that of Article 17, which nowhere includes the composite phrase "processing of personal data".

50. In my judgment, the broader context buttresses these conclusions. In most cases, the data controller is likely to have obtained personal data from the data subject, or with the consent of the data subject, after giving the data subject a fair processing notice setting out to whom and for what purposes the data may be disclosed by the data

controller. It can fairly be said that as a rule (albeit a rule with some exceptions) the data subject has confided or entrusted their personal data to the data controller on terms, with a view to its being processed in stated ways and for stated purposes and not otherwise. It is against that background that the Directive and the 1998 Act impose duties on the data controller and confer correlative rights on the data subject. The security duty may be viewed as an obligation owed to the data subject by the data controller, to protect that which has been entrusted by the one to the other. It seems inherently unlikely that the legislators intended, without clearly indicating as much, to restrict the scope of that duty so that a data controller has no obligation to safeguard some parts of such data.

The purposes of the Directive

51. The Recitals seem to me to contain a degree of additional, general, support for the conclusions I have already expressed. They recognised that, as data processing systems were "designed to serve man", they must "respect their fundamental freedoms, notably the right to privacy ... and contribute to ... the well-being of individuals": Recital (2). The principles of protection included that "the fundamental rights of individuals should be safeguarded": Recital (3). The object of national laws on the processing of personal data being "to protect fundamental rights and freedoms, notably the right to privacy" recognised in Article 8 of the Convention, the approximation of those laws should "seek to ensure a high level of protection in the Community": Recital (10). The rights guaranteed by Article 8 are broad and incapable of exhaustive definition. They do not depend upon the individual being identifiable to the wrongdoer. Furthermore, the scope of protection is not limited to Article 8. It extends to the protection of other fundamental rights and to well-being. There is certainly nothing here to suggest that the protection afforded to personal data is limited in such a way that its disclosure to or processing by those who cannot identify the individual concerned falls out of scope.

Consequences and practicalities

52. The interpretation adopted by the UT, and supported by DSG, has consequences that would, in my view, be surprising in the light of the express purposes and overall scheme of the Directive. There would, in particular, be no obligation for a data controller to take any measures against the risk of deliberate third-party interference with data held by the data controller, such as malicious encryption, deletion, alteration, or indeed extraction, where the third party was unable to identify the individuals to whom such data relate.

53. I think it legitimate for this court to take judicial notice that third-party interventions of this kind are common. Blackmail activities based upon hacking into corporate databases have been a well-established feature of modern life for some years: see for instance *Clarkson plc v Persons Unknown* [2018] EWHC 417 (QB). The Commissioner maintains that ransomware attacks, in which an attacker exfiltrates or encrypts data and demands a ransom for its return or release, are "a growing and pernicious threat in the UK". I agree that this is notorious. Sometimes these events are litigated: see for instance *University College Union v Persons Unknown* [2025] EWHC 192 (KB). It is implicit in the reasoning of the UT, and in DSG's submissions, that such interventions are essentially harmless from the perspective of data subjects, so long as the malicious actor

is not able to identify the people to whom the data relate, so that a duty to guard against them would be pointlessly burdensome. I do not accept that.

54. The impact of such attacks is not dependent on the attacker's ability to identify the data subjects. I consider it self-evident that such activities are capable of causing significant material and non-material harm to data subjects. As for the other side of the balance sheet, it is to be borne in mind that the security duty requires a data controller to conduct a risk assessment, and to consider prospectively what measures are appropriate to guard against the risks identified. On any view, when it comes to data that relate to an individual but do not themselves contain the means of identification, the data controller will need to assess the risk of "jigsaw" identification. That has always been difficult. In modern conditions, the task is harder still. Huge amounts of information about individuals are publicly accessible, and available to be processed automatically. Technology has vastly increased in sophistication. The ability to locate, assemble and combine disparate items to elicit information about individuals is greatly enhanced. It will often prove impossible to rule out the risk that unauthorised access to part of a data set, which does not itself identify any individual, could lead to processing by some unknown third party with (legitimate) access to the means of identification. A data controller in possession of a set of information that amounts to personal data "in its hands" will only be able confidently to draw a clear line around its security duty if it has first conducted a thorough analysis of that issue. I therefore do not see that the interpretation I favour would be likely to add significantly to the burden of the security duty. The exercise would not be fundamentally different. It is, moreover, difficult to impute to those responsible for this legislation an intention that the scope of the security duty should turn on such difficult and finely-balanced judgments.

Authority

55. As a general proposition, indirect identifiability by a third party may be sufficient to mean that data that relate to an individual qualify as "personal data", the processing of which must be conducted in accordance with data protection principles. *Scania* makes that point in the context of the GDPR, and it seems to me that the same reasoning must hold good, in general, for the Directive and the 1998 Act as well. The *Scania* decision does not, however, bear directly on the issue that is critical to the present appeal, namely whether indirect third-party identifiability is a necessary condition for category (b) data to be "personal data" in the context of DPP7.

56. When addressing that issue, the UT placed weight on the GCEU decision in *SRB v EDPS* and, in particular, the observation I have quoted, that in order to decide whether data relating to an individual were "personal data" it was necessary to place oneself "in the position of" the recipient and assess whether the individual was identifiable to them. This was a foundation of the first and the third of the key propositions which the UT drew from the authorities. The CJEU's decision on appeal from the GCEU undermines that analysis.

57. The CJEU rejected the broad-brush argument advanced by the EDPS, that pseudonymised data such as those transmitted to Deloitte are "in all cases" personal data "solely because of the existence of information enabling the data subject to be identified". The Court held that pseudonymisation may or may not make the data subjects unidentifiable to a third-party recipient. It will depend on what means of identification are lawfully available and reasonably likely to be used by the third party.

But the Court agreed with the EDPS that, in the context of the transparency duty, the GCEU had been wrong to assess the identifiability of the data subject solely from the perspective of the controller.

58. The CJEU noted that the GDPR does not specify the relevant perspective for assessing whether the data subject was identifiable: [98]. It said that the case law showed that "the relevant perspective for assessing whether the data subject is identifiable depends, in essence, on the circumstances of the processing of the data in each individual case": [100]. The transparency duty was one that had to be performed at the time of collection of the data. That was because its purposes included enabling data subjects to make an informed decision on whether to provide or refuse to provide the personal data, and to defend their rights against third parties later. At [110]-[111] the court held that the transparency duty was "part of the legal relationship between the data subject and the controller"; that it "concerns the information in relation to that data subject as it was transmitted to that controller, thus before any potential transfer to a third party"; and that accordingly, for this purpose, "the identifiable nature of the data subject must be assessed at the time of collection of the data and from the point of view of the controller".

59. Applying these principles to the duty with which we are concerned in this case, my conclusion is that the same approach should be adopted to the security duty under the 1998 Act. The security duty is, as already observed, an incident of the legal relationship between the data subject and the data controller. It is an obligation owed to the former by the latter in respect of all and any data that are entrusted to the data controller and are personal data. When determining whether data are "personal data" in this context and for this purpose it is sufficient if they qualify as such from the perspective of the data controller. Temporally, the duty first arises when the data controller is processing the data and they are personal data from the data controller's point of view - that is to say, the individual to whom they relate is indirectly identifiable to the data controller. It will continue to apply for so long as those two conditions are met. It will come to an end if and when either condition ceases to be satisfied.

60. In my opinion, the domestic case law about the personal data exemption in freedom of information law is consistent with this analysis. I shall focus on *CSA*, which is the only authority that binds us. I have summarised the legal context, and outcome of that case but should provide some further detail. The CSA was a public health body that had collected information about childhood leukaemia in a part of Scotland that housed a military firing range and various nuclear facilities. A researcher, acting for an MSP, applied under FoI(S)A for details of the incidence of the disease, broken down by age, location, and time. The CSA refused, maintaining that the disease was so rare and the numbers so small that release in this form would render individuals identifiable; the data sought would therefore be "personal data" within the meaning of s 1 of the 1998 Act; disclosure of the data as requested would contravene the data protection principles; and they were accordingly exempted from disclosure by s 38 of FoI(S)A. The Commissioner ordered the agency to perform an operation called "barnardisation" which, it was said, would make it impossible to identify any of the individuals. On a challenge by the CSA the House of Lords agreed that the information as it stood was personal data but held that if barnardisation could achieve what was claimed for it, the information would no longer be personal data.

61. The principal speech was given by Lord Hope, who spoke for the majority. Lord Rodger and Lady Hale delivered speeches offering different reasons for reaching the same overall conclusions, but Lord Rodger agreed with Lord Hope's reasoning in the alternative. The cases have taken different views of the status of Lord Hope's reasoning, as a matter of precedent. In *APPGER* the UT considered that Lord Hope's reasoning was not binding and that it could reach its own view. In *DoH,* to which I return, Cranston J rejected that approach as impermissible. He concluded at [45] that "our system of precedent demands that the High Court treat Lord Hope's speech as determinative". I agree, and the same applies in the Court of Appeal.

62. The key passages of Lord Hope's speech are at [24]-[27]. At [24], he conducted a close analysis of the definition of "personal data" in s 1 of the 1998 Act. He concluded that its effect was that data would only fall within category (b) if an individual was indirectly identifiable to someone from the data "taken together" with "other information". As he put it, "each of these two components must have a contribution to make to the result". If the data were "put into a form from which" no individual could be identified "even with the assistance of other information from which they were derived" they would not be personal data. It would not matter even if the "other information" itself identified the individual(s). In that situation "it will be the other information only, and not anything in 'those data'" that would lead him to the result. At [25], Lord Hope cited Recital 26 to the Directive and noted the proviso concerning data "rendered anonymous in such a way that the data subject is no longer identifiable". He concluded that "Read in the light of the Directive ... the definition in section 1(1) of the 1998 Act must be taken to permit the release of information which meets this test without having to subject the process to the rigour of the data protection principles."

63. Lord Hope went on to consider the question of perspective:

> 26 ... The question is whether the data controller, or anybody else who was in possession of the barnardised data, would be able to identify the living individual or individuals to whom the data in that form related. If it were impossible for the recipient of the barnardised data to identify those individuals, the information would not constitute "personal data" in his hands. But **we are concerned in this case with its status while it is still in the hands of the data controller**, as the question is whether it is or is not exempt from the duty of disclosure that the 2002 Act says must be observed by him.
>
> 27 In this case it is not disputed that the agency itself holds the key to identifying the children that the barnardised information would relate to, as it holds or has access to all the statistical information about the incidence of the disease in the health board's area from which the barnardised information would be derived. But in my opinion **the fact that the agency has access to this information does not disable it from processing it in such a way, consistently with recital 26 of the Directive, that it becomes data from which a living individual can no longer be identified**. If barnardisation can achieve this, the way will be then open for the information to be released in that form because it will no longer be personal data. Whether it can do this is a

> question of fact for the commissioner on which he must make a finding. ...

64. In *DoH,* Cranston J said at [49] that it would "wrong to pretend that the interpretation of the *CSA* case is an easy matter". I agree. Cranston J's conclusion was that the key to understanding the decision lay in the order proposed by Lord Hope, which showed that "although the [CSA] held the information as to the identities of the children to whom the requested information related, it did not follow from that that the information, sufficiently anonymised, would still be personal data when publicly disclosed": [51]. The critical consideration, in Cranston J's view, was not "the status of information in the data controller's hands" but "the implications of disclosure by the data controller" and "whether any living individuals can be identified by the public following the disclosure of the information": [52]. In *Miller* at [10] the UT drew from these decisions the conclusion that indirect third-party identifiability is the sole criterion when deciding whether information "is personal data when disclosed", and that this is so "even though the data controller holds the key to identification of individuals to which the data relates".

65. That may be the correct interpretation of the cases. For my part, I think the ratio of *CSA* is narrower still. I have added the emphasis above to highlight what I consider to be the essential and narrow grounds of this decision. These are that if, under the regime enacted by the 1998 Act, a data controller deliberately processed an existing set of personal data so as to create and then disclose a separate and independent sub-set of those data which was truly anonymised, in the sense that it contained nothing that identified or was capable of contributing to the identification by anyone of any individual to whom the data related, then the resulting sub-set would not be "personal data" *even to the data controller* and its disclosure would not involve the processing of "personal data". The decision was framed as giving effect to the language and purposes of the proviso to Recital 26, and the legitimate policy objectives. The reasoning places weight on the word "rendered" in the proviso, and on the deliberate and transformative nature of the anonymising operations thereby envisaged. It is noteworthy that the conclusions arrived at were decisions of principle, leaving open for decision the key question of fact, whether the data set could indeed be rendered truly anonymous.

66. Whichever is the correct analysis of *CSA* I am satisfied that the case provides no material assistance with the resolution of the issue before us on this appeal. That is for the following reasons. First, if I am right, then the ratio of *CSA* is that on the true interpretation of the 1998 Act, read in the light of the proviso to Recital 26, information that relates to an individual is not "personal data" at the time of its disclosure to the public if it has been "rendered anonymous" before such disclosure, in the way I have outlined. That conclusion has no bearing on the issue before us, which arises on the assumption that the individuals to whom the data relate remain indirectly identifiable to the data controller throughout, so that the information remains "personal data" from that perspective: see paragraphs [2], [7] and [9] of this judgment, above.

67. Secondly, and on any view, *CSA* was concerned with the data protection implications of deliberate disclosure by the data controller in a specific context of a newly created sub-set of information previously held as "personal data". The House's conclusion was driven by what the court inferred to be the legislative intentions as to the outcome, in that particular context. The present case is concerned with an entirely different context. It would be inappropriate simply to extrapolate from the one context to the other.

68. Thirdly, if the domestic and EU case law has any single unifying theme it is that the ordinary and natural meaning of the legislative language gives the concept of "personal data" an inherently broad reach that may have to be shaped and moulded to suit particular contexts, with sometimes heavy reliance on the tools of contextual and purposive interpretation.

69. Fourthly, I see no sound basis for inferring that the legislature intended the interpretation or outcome for which DSG contends. For one thing, a key consideration underlying the decision in *CSA* is that the public release of a data set so fully anonymised that nobody (or at least nobody other than the data controller) could identify any individual to whom it relates can have no adverse implications for any such individual. For the reasons I have given, the same cannot be said of the security duty. On the interpretation favoured by the UT and DSG, the duty would be limited in such a way as to expose individuals to real and substantial risks of harm, without significantly reducing the burden on the data controller as compared with the interpretation that commends itself to me.

Conclusions

70. My main conclusions can be stated in this way. Information is "personal data" if it falls within the statutory definition of that term. One of the statutory criteria, and the key criterion for present purposes, is that the individual to whom the information relates is identifiable to the data controller. The security duty requires any data controller of any such information to safeguard it – to the extent laid down in the 1998 Act - against any unauthorised or unlawful processing (as well as against its accidental loss, destruction or damage), whether or not the person carrying out that processing (or causing the loss, destruction or damage) would be able to identify the individual(s) to whom the data relate. If the data are "personal" from the perspective of the data controller, it will be unnecessary to pose the further question of whether they are personal data "in the hands of" or "from the perspective" of any other person. Again, these observations relate to the 1998 Act. In my judgment, the FtT reached the right conclusion and its reasoning was essentially correct. This appeal should be allowed and the matter remitted to the FtT to be determined in accordance with this judgment.

LADY JUSTICE ELISABETH LAING:

71. I agree.

LORD JUSTICE MOYLAN:

72. I also agree.