Judiciary of England and Wales

19 February 2026

S U M M A R Y

DSG Retail Ltd v The Information Commissioner

[2026] EWCA Civ 140

Lord Justice Moylan, Lady Justice Elisabeth Laing and Lord Justice Warby

NOTE: This summary is provided to help in understanding the Court's decision. It does not form part of the reasons for the decision. The full judgment of the Court is the only authoritative document. Judgments are public documents and are available at:

https://caselaw.nationalarchives.gov.uk/

Introduction

1. This was an appeal 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", or "ATOMs". This is commonly known as the security duty.

2. The question raised by the appeal, simply stated, was whether the law required a data controller to guard against the risk that data which relate to individuals who could be identified by the data controller would be subject to unauthorised or unlawful processing by a third party who could not identify those individuals. The law in force at the relevant time was the Data Protection Act 1998 ("the 1998 Act"), specifically section 4(4) and the seventh data protection principle ("DPP7") contained in paragraph 7 of Schedule 1 Part I.

3. The factual context was that in 2017-2018 there was a cyber-attack on the systems of DSG Retail Limited ("DSG"). The attackers obtained millions of items of data by "scraping" transaction details as transactions were made, storing the data on DSG's servers, and attempting to exfiltrate the scraped data. In some cases the attackers obtained the card number or "PAN", the expiry date and the cardholder's name. But most of the cards were protected by "chip-and-pin" or "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.

4. The Information Commissioner found DSG in breach of DPP7 and served a monetary penalty notice. DSG appealed to the First-tier Tribunal ("FtT"), arguing that DPP7 did not require them to take ATOMs against third-party acquisition of the EMV data as this would not be "personal data" in the "hands" of the third parties. The appeal was dismissed but on a further appeal the Upper Tribunal ("UT") accepted DSG's arguments. It held that the question 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" 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. The Commissioner appealed.

The court's decision

5. The Court of Appeal allows the appeal, concluding that where the individual to whom information relates is identifiable to a data controller the security duty requires the data controller to safeguard that information – to the extent laid down in the 1998 Act – against any unauthorised or unlawful processing, whether or not the person carrying out the processing would be able to identify the individual to whom the data relate. The court remits the matter to the FtT for determination in accordance with its judgment. The lead judgment is given by Lord Justice Warby, with whom the other members of the court agree.

6. The judgment introduces the appeal **[1]-[8]** and defines the issue more closely **[9]**. At **[10]-[26]** it identifies the legal context, comprising the relevant provisions of the 1998 Act and of the Data Protection Directive (95/46/EC), which the 1998 Act was intended to implement, and some relevant UK and EU case law. The judgment summarises the reasoning of the FtT (**[27]-[29]**) the reasoning of the UT (**[30]-[32]**) and the submissions of the parties (**[33]-[34]**), before setting out its own analysis at **[35]-[69].**

7. The court holds 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 identified above: **[37].**

   (1) *The legislative language and its immediate context*.

8. The court analyses the language of the 1998 Act: **[38]-[41]**. At **[42]-[49]** it reviews its conclusions in the light of the Directive and the decisions of the Court of Justice of the European Union ("CJEU") in *Gesamtverband Autoleile-Handel EV v Scania CV AB,* C-319/22, [2024] 2 CMLR 40 ("*Scania*") and *Single Resolution Board v European Data Protection Supervisor*, C-413/23 ("*SRB v EDPS")*. The court finds that on the face of the Directive data are "personal data" if and for as long as the individual to whom they relate are indirectly identifiable to the data controller; the broader definition of "personal data" in the Directive does not

logically lead to a narrower interpretation of the security duty; *Scania* and *SRB v EDPS* support that view; and there is nothing else in the Directive that supports a narrower view of the security duty. At **[50]** the court concludes that the broader context buttresses its conclusions.

(2) *The purposes of the Directive*

9. The court finds a degree of additional, general, support for its conclusions in the Recitals to the Directive: **[51]**.

(3) *Consequences and practicalities*

10. At **[52]-[54]** the court explains that the UT's interpretation has consequences that would be surprising in the light of the express purposes and overall scheme of the Directive. There would, in particular, be no obligation to take measures against the risk of deliberate third-party interference with data held by the data controller, such as ransomware attacks, which do not depend for their impact on the attacker's ability to identify the data subjects. Such activities are self-evidently capable of causing significant harm to data subjects. Contrary to DSG's case, guarding against these risks would not add significantly to the burden of the security duty.

(4) *Authority*

11. At **[55]-[59]** the court considers the decision in *SRB v EDPS,* that "the relevant perspective for assessing whether the data subject is identifiable depends … on the circumstances of the processing", and that in the context of the "transparency duty" imposed by the GDPR the relevant perspective was that of the data subject. The court finds that the same approach should be adopted to the security duty under the 1998 Act. 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 - that is to say, the individual to whom they relate is indirectly identifiable to the data controller.

12. At **[60]-[69]** the court explains why these conclusions are unaffected by UK authorities about the freedom of information legislation: the House of Lords' decision in *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47, [2008] 1 WLR 1550 *("CSA")* and cases in England and Wales in which *CSA* has been considered.

Conclusions

13. At **[70]** the court sets out its main findings, holding that the FtT reached the right conclusion and its reasoning was essentially correct.