DSG Retail Limited v Information Commissioner [2026] EWCA Civ 140

By Mariya Peykova

3PB Barristers

Introduction

In February 2026, the Court of Appeal handed down judgment in DSG Retail Limited v Information Commissioner [2026] EWCA Civ 140. The appeal concerned the scope of the duty imposed on data controllers to protect personal data in their possession and control by taking appropriate technical and organisational measures ('**ATOS'**).[1] The relevant duty is commonly known as the security duty, and as Warby LJ pointed out, it '*is a protective duty to take proportionate steps to guard against risk, not to guarantee a particular outcome'*. The security duty is particularly relevant when data controllers fall victim to cybersecurity attacks that result in hackers exfiltrating personal data.

Relevant facts

In or around 2017-2018, the systems of DSG Retail Limited ('DSG') were the subject of a cyber-attack. Over a period of nine months, the hackers were able to obtain personal data by 'scraping' transaction details from point-of-sale terminals or card readers, storing the data on DSG servers as transactions were being made, and attempting to then exfiltrate the stored data. In a number of instances, the hackers were able to exfiltrate the 16-digit card number or 'PAN', the expiry date of the relevant card, and the cardholder's name. The great majority of cards were protected by the so called 'chip-and-pin' system. In those instances, the hackers were only able to obtain the PAN and the expiry date ('the EMV data'). They were not able to obtain the cardholders' names or any other information that would enable the hackers to identify the cardholders.

[1] Today this duty is found in various forms in respect of data controllers in Articles 5 (1) (f), 24, 25 and 32 UK GDPR (the latter of which amounts to a protective duty against accidental or unlawful destruction or loss, among other things, and also applies to processors), and is commonly referred to as the security duty owed by data controllers to safeguard personal data in their control. The legal context in this case was provided by the previous data protection regime. The security duty was imposed by the seventh data protection principle ('DPP7') under the Data Protection Act 1998, enacted to give effect to the obligations imposed on the United Kingdom by the Data Protection Directive, 95/46/EC ('the Directive').

Following an investigation, the Information Commissioner found that DSG had breached the security duty and served DSG with a monetary penalty notice ('MPN'). DSG appealed to the First-tier Tribunal ('FtT') and argued that the security duty did not require DSG to take ATOMs against third party-acquisition of the EMV data, as this would not constitute 'personal data' in the hands of the hackers. The FtT rejected this argument and held that the security duty was triggered if the EMV data was 'personal data' in the hands of DSG (i.e. as long as the personal data constitutes information relating to an *identified or identifiable* natural person). The MPN was upheld, although it was reduced. DSG appealed to the Upper Tribunal ('UT') arguing 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. Applying this interpretation, third-party acquisition of data would not amount to 'unauthorised or unlawful processing of personal data' against which a data controller was obliged to undertake ATOMs, because the data did not identify the individuals to whom it pertained. The UT accepted DSG's case and reversed the findings of the FtT on this point. The Information Commissioner appealed to the Court of Appeal.

The issue on appeal

The single issue on appeal was one of legal principle - on the assumption that the cardholders were identifiable to DSG but not to the hackers: whether in those circumstances a data controller is under an obligation to take ATOMs, i.e. whether the security duty is triggered in these circumstances.

The Court's judgment

The Court of Appeal found that the security duty requires a data controller to take ATOMs against the risk of processing by a third party of data which relates to an individual who is identifiable to the controller, even if the personal data does not enable the third party to identify the data subject in question (DSG, at [37]). In summary, the Court of Appeal held that information is 'personal data' if it falls within the statutory definition of the relevant term. One of the statutory criteria is that the individual to whom the information relates is *identifiable* to the data controller. The security duty requires any data controller to safeguard personal data against any unauthorised or unlawful processing (as well as against accidental loss, destruction or damage) whether or not the person carrying out the processing (i.e. a third party) would be able to identify the individual(s) to whom the data relates. Finally, if the data are 'personal' from the perspective of the data controller, it will be unnecessary to pose

the further question of whether they also constitute 'personal data' in the hands or from the perspective of the third party (DSG, at [70]).

The following points from the court's judgment are also relevant:

a. The general duty imposed on a data controller under the relevant legislation is a duty imposed in relation to 'all personal data in respect to which [he/she] is the data controller' (DSG, at [38]).

b. The definition of personal data has two categories: the first one is data which enables a living individual to be identified by anyone, i.e. data that is defined by direct identifiability. The second category is data relating to an individual who cannot be identified by the data themselves, but requires additional information which is, or is likely to come into the possession of the data controller, i.e. data that is defined by a criterion of indirect identifiability (DSG, at [38]). Thus, the general duty imposed on data controllers is imposed in respect of both categories of personal data, and there is nothing in the relevant statutory language which would suggest that indirect identifiability by a third party is in any way a factor that expands, limits, or in any way controls the scope of the duty (DSG, at [38]).

c. The object of the security duty in DPP7 is 'personal data'. Applying the usual principles of statutory interpretation, the term 'personal data' in the context of the security duty must bear the same meaning as its interpretation in the context of the general duty imposed on data controllers – thus, the duty applies in respect of all personal data (DSG, at [39]).

d. The risks against which a data controller is required to guard against in respect of category two data (i.e. data that is defined by the criterion of indirect identifiability) include the non-accidental processing by a third party that is unauthorised or unlawful, whether or not the individual is identifiable to a third party (DSG, at [41]).

e. The Court noted that the language of the Directive gives the concept of 'personal data' an expanded reach compared to the more restricted meaning in the DPA 1998 and further remarked that the definition of 'personal data' in the GDPR is materially identical to that of the Directive. On the face of both the DPA 1998 and the Directive, data are 'personal data' if and so long as the individual to whom they relate is indirectly identifiable to the data controller, and even though the concept of 'personal data' is broader in the Directive than it is in the DPA 1998, this does not logically lead to a narrower or different interpretation of the security duty (DSG, at [42] – [46]).

f. There was nothing in the Directive which would support a narrower view, given the wording of the relevant provisions and the purpose of the Directive (DSG, at [47] – [51]).

g. The interpretation adopted by the UT and supported by DSG has consequences which would be surprising given the express purpose and overall scheme of the Directive, especially in circumstances where hacking incidents and ransomware attacks are prevalent in modern society, with the impact of such attacks not being dependent on the attacker's ability to identify the data subjects, and particularly in the light of the very real risk of 'jigsaw identification' in many cases (DSG, at [52] – [54]).

h. Applying the principles from existing authorities to the security duty, the Court held that the duty is an incident of the legal relationship between the data subject and the data controller, and the latter owes the obligation in relation to all and any data entrusted to the data controller and are personal data. When determining whether data are 'personal data', it is sufficient that they qualify as such from the perspective of the data controller. The duty will continue to apply as long as the individual is indirectly identifiable by the data controller (DSG, at [59]).

i. The Court set out its main conclusions at [70] of its judgment and remitted the matter back to the FtT to be determined in accordance with its judgment.

Practical advice for data controllers

The judgment of the Court of Appeal in DSG is significant, as it clarifies the position regarding the scope of the security duty applicable to data controllers. It is clear that data controllers are under an obligation to take ATOMs in respect of *all* personal data being processed by them if the individuals to whom the data relates are directly or indirectly identifiable by the data controller. The following is relevant:

a. Data controllers should treat all controller-identifiable data as requiring full protection, whether the individuals in question are directly or indirectly identifiable. This may require data controllers to classify specific datasets and consider whether 'jigsaw identification' may be possible in respect of certain sets of data.

b. Partial or pseudonymised data may still require full protections where the individuals to whom it relates are identifiable to the data controller, for example if the data controller is able to link the data to the specific individual through information which is

available to the data controller or is likely to come into the possession of the data controller.

c. Data controllers should always keep a record of their internal security decision making, including the reasons for the implementation of specific security measures and why they were deemed appropriate at the time they were introduced. Periodic Data Protection Impact Assessments are also crucial, especially where the data controller is operating high risk systems and/or sensitive data.

d. Data controllers often outsource to external IT providers, who are responsible for the implementation of a data controller's cyber security measures. Where this is the case, data controllers need to have proper agreements in place with the relevant IT provider, which comply with data protection legislation, notably contractual arrangements specifically tailored for the relationship between a data controller and a data procesor. Equally, where personal data is being processed by third parties, the data controller in question needs to ensure that it complies with its transparency and other obligations under data protection legislation.

Mariya Peykova
Barrister
3PB Barristers
mariya.peykova@3pb.co.uk
0330 332 2633
3pb.co.uk