SLAUGHTER AND MAY/

November 2022

LESSONS FOR CONTROLLERS FROM DSG V INFORMATION COMMISSIONER

THE SCOPE OF DISCRETION WHEN IMPLEMENTING DATA SECURITY PRIORITIES

A version of this article first appeared in the Privacy Laws & Business UK Report, Issue 124 (November 2022)

In a world of headline-grabbing mega-fines against tech giants, it might seem that a £500,000 pre-GDPR fine would be of limited interest. However, a recent decision from the UK's First Tier Tribunal (FTT) provides important and valuable lessons for any organisation dealing with large amounts of personal data (or, indeed, a Data Protection Authority). The lessons include the scope for judgment organisations are allowed to exercise in relation to the appropriateness of technical and organisational measures and how to respond when these are called into question by a regulator.

The case relates to a January 2020 penalty handed down by the Information Commissioner's Office (ICO) to the retailer DSG Retail Limited (DSG) for data security failings under the Data Protection Act 1998 (DP Act 1998). The security failings were exposed by a sophisticated and extensive cyber-attack on DSG that occurred between July 2017 and April 2018. Cyber criminals initially targeted point-of-sale (POS) terminals (i.e. card machines) in DSG's bricks-and-mortar retail stores in July 2017 and installed malicious software to scrape payment card details from the POS terminal's memory. They also gained access to DSG's wider IT systems, including marketing and antifraud databases, and accessed employee data, customer data and supplier information (including names and contact details). Some of the details remain unclear as the attackers covered their digital tracks but DSG's investigation indicated that they are likely to have extracted at least some data. During this time DSG were carrying out a major upgrade to their IT security.

The penalty was the maximum permitted under the DP Act 1998 and the ICO stated that the fine would have been much higher under the GDPR. The ICO's penalty notice listed ten aspects of DSG's technical and organisational measures as inadequate for the purposes of data security under the DP Act 1998's seventh data protection principle. DSG challenged the ICO's fine and substantive decision. In its July 2022 decision the FTT took a different view on the extent of DSG's compliance with data protection law. Whereas the ICO found systemic failings, the FTT found DSG's faults to be more limited, substantially upholding only two of the ten security failings identified in the ICO's penalty notice and reduced DSG's fine by half.

In a number of instances, the FTT directly disputed the ICO's technical understanding of the facts as well as its interpretation of data protection law. Critical to reaching this conclusion was that the FTT exercised its discretion to admit new evidence even though that evidence was not available to a previous decision-maker. While the ICO amended their case substantially in light of new evidence, indicating that the regulator recognised that they learnt more about the technical details of the incident from the appeal proceedings than from their initial investigation, the FTT's decision notes that the extent to which the ICO's case was refined was "unusual and significant". The FTT's extensive analysis that now substitutes the ICO's entire ruling[1] provides organisations with important clarity in a number of areas, both procedural and technical, that are likely to be relevant to ongoing enforcement actions (or, indeed, information security compliance).

Meaning of 'personal data'

A key point of focus for the FTT was whether the 16 digit-long payment card number (i.e. PAN) together with a card expiry date, but without other accompanying information, would amount to personal data. The ICO's fine had determined that such PAN were personal data but did not elaborate on why.

During the course of the appeal, the ICO argued that PAN either: (i) directly identify an individual via their bank account which is a unique identifier of them and singles them out; or (ii) combine with other information reasonably likely to be available to a third party as part of a 'mosaic' to identify the individual.

DSG rejected both these arguments. DSG's counsel, Tim Pitt Payne KC, argued that PAN did not directly identify an

[1] The FTT decision runs to nearly 15,000 words whereas the ICO's initial decision is half that.

individual - only a bank account, much like a cloakroom ticket identifies the coat but not the owner. DSG also rejected the possibility of 'mosaic identification' of PAN as highly speculative and without evidential support in this case.

The FTT rejected the approach taken by both the ICO and DSG. It reasoned that the relevant question was whether PAN were personal data in the hands of the controller, rather than in isolation or in the hands of a third party. DSG held other data to match up to the PAN, such as transaction records needed to give refunds, and could therefore link them to a living individual indirectly. As such, a significant number of the PAN were personal data for DSG. Whether the PAN would amount to personal data in the hands of a third party was held to be relevant only to the extent that it affected the risks posed by the data and the extent of security it required. Although the FTT did not rule on the point, it suggested (as an obiter comment) that PAN could directly identify a living individual, and therefore could be personal data in the hands of a third party.

This analysis is an important reminder of the challenges for organisations in determining whether information they hold is personal data or not. The FTT's position suggests that organisations should adopt a fact-specific approach to what constitutes personal data, taking into account how the various types of information they hold at any given time could combine together to identify an individual. Further help on this analysis is in the pipeline, with the ICO currently **consulting** on updated anonymisation guidance and the Government putting forward a new definition of personal data in the July 2022 draft of the **Data Protection and Digital Information Bill** (DPDI Bill) which seeks to clarify the personal/anonymous data distinction.

Scope for judgment in data security

In overturning some of the ICO's data security findings, the FTT confirmed the approach to data security obligations endorsed in *Morrisons*[2], (as discussed in our previous article here). The FTT held that a "holistic approach" should be taken to compliance with data security requirements, "allowing a degree of permissiveness in the exercise of judgement". As such, the FTT emphasised that DSG had scope for discretion in how they chose to comply with their data security duties – including balancing the cost of security measures and the risk of harm if these are not implemented. This will be welcome news to many controllers grappling with how to successfully counter fast evolving and increasing security threats, particularly for those with large organisations and legacy systems.

The FTT also emphasised that DSG's judgement in respect of data security measures had to be evaluated without the benefit of hindsight. The FTT suggested the ICO had wrongly substituted its own judgment for that of DSG, without the ICO being in possession of all the necessary contextual and technical information. For example, the ICO failed to take into sufficient account the resources spent by DSG on upgrading its IT security and the challenges of implementing some of the security measures identified as critical omissions in their fine. The FTT went as far as to tentatively suggest the ICO should have "sought external expert views given the technical complexity of the information provided by DSG". The decision again demonstrates the value of controllers investigating any incident themselves and proactively presenting the relevant facts and technical details to the ICO from the outset.

Relevance of payment standards

The FTT also endorsed the *Morrisons* approach when it dealt with the interaction of the payment card industry data security standard rules (PCI-DSS) - which are mandatory for organisations processing payment card data - and the data security requirements under the DP Act 1998. The FTT concluded that the PCI-DSS are prescriptive and compliance is binary, whereas organisations have more discretion in how they satisfy the data security rules. The FTT held that while satisfaction of PCI-DSS is a relevant consideration in relation to compliance with the data security rules, it is possible for an organisation to fail to meet the PCI-DSS standard, yet satisfy the data security requirements and vice-versa. On the facts, the FTT cited DSG's strong internal governance framework and reliance on external IT experts as supporting its judgement in prioritising certain other areas of its IT security upgrade (e.g. its e-commerce environment) ahead of introducing point-to-point encryption (P2Pe) on its POS terminals (as endorsed by PCI-DSS). The ICO's fine cited DSG's decision not to introduce P2Pe on its terminals as a standalone breach of its data security obligations, whereas in contrast, the FTT held that DSG's failure to do so "involved an exercise of judgement of the kind anticipated by the Court of Appeal in the Morrisons case".

Interestingly, the ICO also relied on the National Cyber Security Centre's Cyber Essentials Guidance as representing a minimum standard of acceptable IT in internet-facing areas – a standard which was not fully met by DSG's measures – but which had not been referenced in the penalty notice. However, while the FTT did not make any findings in relation to this specific point, the reference to objective, public standards by the ICO is one which data controllers should take note of and the ICO's current **data security guidance** makes clear that it considers Cyber Essential a 'base' set of controls that organisations can put in place relatively easily. [3]

The FTT's position suggests that organisations do have some discretion in making challenging choices in respect to their data security priorities (and budgets). However, defending those decisions will require evidence (and

[2] *Various Claimants v Wm Morrisons Supermarkets plc [2018] EWCA Civ 2339*

[3] The ICO's current **data security guidance** also addresses compliance with PCI-DSS and accords with the FTT's view that it is a relevant consideration but is not necessarily determinative.

awareness of the relevant information or cyber security standards), particularly if something does go wrong later.

Address risks – document them

While the FTT's analysis of DSG's data security compliance was more favourable than that of the ICO, it did highlight two serious failings that ultimately warranted the imposition of a fine - the failure to implement critical software security patches and defective password policies. The cyber attackers took advantage of both weaknesses, although notably, only once they had already gained access to DSG's systems.

Both issues had persisted over an extended period despite having been specifically flagged to DSG's Information Security Data Protection committee and highlighted by external and/or internal security tests, yet, the FTT emphasised, there was no evidence of that committee making any specific decisions in relation to them.

In justifying the imposition of a fine for these infringements, the FTT pointed out that Carphone Warehouse was subject to a **previous fine** from the ICO (of £400,000) for inadequate software patch management before it was acquired by DSG. The FTT held that this previous failure should have put DSG on notice of the specific risks presented by inadequate software patching (given patches highlight known vulnerabilities). However, the FTT did not find this previous fine to be an aggravating factor in the calculation of the final penalty amount due to the proactive steps DSG had taken to manage the risks posed by the Carphone Warehouse IT system (including by using external IT consultants to manage that system).

In contrast, the ICO's October 2022 fine against Interserve makes clear that it will take into account prior data incidents (and any unaddressed remediation efforts from such incidents) as aggravating factors when considering enforcement action. The Information Commissioner, John Edwards, has also flagged (somewhat forcefully) that he considers the biggest cyber risk to be complacency within an organisation and has warned that organisations will face fines if they fail to monitor for suspicious activity on an ongoing basis, act on warnings, update software and train their staff.

As well as being a reminder of some of the basics of cyber security, the FTT's decision shows the importance of organisations acknowledging the data security risks they face, appropriately mitigating them and documenting their decisions. In the context of mergers and acquisitions, this includes carrying out appropriate IT/data security diligence and then putting in place remediation measures post-deal to address any weaknesses identified, in the target or acquiring entities.

Calculation of the penalty

In determining the appropriate level of penalty, the FTT expressly benchmarked the appropriate fine for DSG against the fine issued to **Yahoo! UK Services Limited** (Yahoo) in 2018. The FTT reasoned that although the number of individuals affected in the DSG attack was significantly lower[4], the DSG attack involved financial data and the contravention persisted for longer. Both the incident duration and the inclusion of financial data were viewed by the FTT as specific aggravating factors, along with the volume of data and the number of affected individuals.[5] The FTT also referenced a number of mitigating factors, including:

- DSG's long running security upgrade programme;
- DSG notifying all its customers of the breach (rather than just an affected subset);
- DSG spending £9 million in response to the cyber-attack; and
- the security failings upheld by the FTT equating to a small subset of those originally identified by the ICO.

The FTT's comparison of the DSG fine with that of Yahoo gives a useful indication of some important aggravating and mitigating factors in the calculation of fines. However, unhelpfully, it is unclear from the Tribunal's reasoning how these factors (quantitative and qualitative) were applied to reach the £250,000 number that ultimately aligned with the Yahoo penalty. DSG has indicated that it plans to appeal the decision to the Upper Tribunal, so it is possible that more focus will yet fall on this penalty calculation.

In any case, organisations can expect greater clarity on how fines are calculated once the ICO finalises its new regulatory action policy (and accompanying statutory guidance). The **current draft** sets out a detailed nine step process it will follow ahead of recommending a penalty amount, including reference to both an organisation's turnover and a detailed calculation of a 'starting range' for the penalty depending on the level of seriousness of the breach, to which adjustments are made for aggravating or mitigating factors.

The new guidance suggests the ICO will "clearly record which aggravating and mitigating features we take into account and why and how [they] influence the proposed

[4] Only a portion of DSG's 25m customers were affected compared to 500m Yahoo users.

[5] The ICO's first GDPR-era penalty against Doorstep Dispensaree was reduced from £275,000 to £93,000 on appeal to the FTT, one of the reasons for which was that the ICO had over-estimated the number of documents containing personal data affected by the relevant breach. However, the FTT determined that the fine should not be reduced by a percentage based solely on the lower numbers of documents but should be considered alongside aggravating factors such as the type of personal data affected and the data subjects impacted.

administrative penalty" which should provide helpful clarity in due course.

What are the key takeaways?

The FTT's decision was clearly welcome news for DSG, but it is also relevant to controllers more generally as it demonstrates:

- an increasing appetite on the part of controllers to challenge the ICO (especially where there is a risk of follow-on claims by data subjects) and a willingness on the part of the FTT to hold the ICO to account;
- that controllers have scope for judgment in relation to the appropriateness of the technical and organisational measures they put in place – but they must be able to demonstrate they have considered (and documented) their decisions; and
- the importance of controllers' carrying out their own investigations into data incidents and proactively presenting clear facts from the outset - not only in relation to how the incident happened but what data has been affected (i.e. the personal / anonymous data distinction).

While offering these useful takeaways for controllers, the FTT's decision makes plain the challenges facing the ICO. The regulator must police an ever more complex and technically demanding environment as appetites to challenge fines increase. The ICO has increased the numbers in its cyber-investigations team from 8 in 2020 to 13 in 2021 but its capacity to carry out complex investigations remains constrained by the resources available to it and the FTT's suggestion that it should consider seeking external expert views appears to recognise as much. However, the ICO seems intent on facing these challenges head on. It has **secured** new funding earmarked for litigation and has set out fresh priorities, in its new draft **ICO25 strategy**, to "continuously develop the ICO's culture, capability and capacity". While the status of the current DPDI Bill is unclear, it is likely that its reforms of the ICO, including increasing transparency and accountability on its enforcement action, will persist in the Government's next iteration. Organisations should welcome these developments, as they should help the regulator provide greater certainty and clarity in its future fines

CONTACT

RICHARD JEENS
PARTNER
T: 020 7090 5281
E: Richard.Jeens@slaughterandmay.com

ROSS O'MAHONY
ASSOCIATE
T: 020 7090 3856
E: Ross.O'Mahony@Slaughterandmay.com

BRYONY BACON
PROFESSIONAL SUPPORT LAWYER
T: 020 7090 3512
E: Bryony.Bacon@slaughterandmay.com