IN THE UPPER TRIBUNAL
ADMINISTRATIVE APPEALS CHAMBER

UT Ref: UA-2022-001380-GIA
NCN [2024] UKUT 287 (AAC)

Appellant: DSG Retail Limited
Respondent: The Information Commissioner

DECISION OF THE UPPER TRIBUNAL

THE HON. MRS JUSTICE HEATHER WILLIAMS DBE

UPPER TRIBUNAL JUDGE WRIGHT

UPPER TRIBUNAL JUDGE STOUT

Decision date: 23 September 2024

ON APPEAL FROM:

Tribunal: **First-tier Tribunal (General Regulatory Chamber)**
Tribunal Case No: **EA/2020/0048**
Tribunal Venue: **Field House, London**
Hearing Dates: **15-23 November 2021**
Decision date: **5 July 2022**

IN THE UPPER TRIBUNAL **UA-2022-001380-GIA**
ADMINISTRATIVE APPEALS CHAMBER **NCN [2024] UKUT 287 (AAC)**

On appeal from the First-tier Tribunal (General Regulatory Chamber)

Between:

DSG Retail Limited

Appellant

– v –

The Information Commissioner

Respondent

Before: **The Hon. Mrs Justice Heather Williams DBE**
Upper Tribunal Judge Wright
Upper Tribunal Judge Stout

Decision date: 23 September 2024
Decided after a hearing on: 11 and 12 June 2024

Representation:

Appellant: Mr Timothy Pitt-Payne KC and Mr Rupert Paines of counsel, instructed by Pinsent Masons.
Respondent: Mr Peter Lockley of counsel, instructed by the Information Commissioner

DECISION

The decision of the Upper Tribunal is to allow the appeal by DSG Retail Limited.

As a consequence of our decision, and pursuant to section 12(2)(a) and 12(2)(b)(i) of the Tribunals, Courts and Enforcement Act 2007, we set aside the words "and is substituted by this Decision" in paragraph 1 and the whole of paragraph 2 of the First-tier Tribunal's decision in EA/2020/0048, dated 5 July 2022. We remit the appeal to be redecided by an entirely freshly constituted First-tier Tribunal in accordance with the law in this decision and on the basis of the uncontested matters as set out in this decision.

REASONS FOR DECISION

Introduction

1. This appeal concerns the lawful basis for the Information Commissioner ("ICO") imposing a monetary penalty notice ("MPN") on a data controller under section 55A of the Data Protection Act 1998 ("DPA 1998"). A key issue on the appeal is the correct construction of the phrase "personal data" as it appears within the seventh data protection principle in Schedule 1 of the DPA 1998 ("DPP7"), which

is concerned with data security. A three-judge panel of the Upper Tribunal was convened to hear the appeal because this issue of construction raises a question of law of special difficulty.

2. The structure of this decision is as follows:-

A summary of the relevant background

3. The appeal arises from a cyber-attack on the appellant's in-store payment systems and the information the attackers obtained from the appellant's payment systems as a result of that attack. We will refer to the appellant as "DSG" (although it is now Currys Group Limited). The attack, which took place between 24 July 2017 and 25April 2018, targeted its Currys PC World and Dixons Travel stores and resulted in the attackers obtaining the payment card data from the memory of the point of sale ("POS") terminals in those stores.

4. Most relevantly for the purposes of this appeal, over five million payment cards were affected by the attack. Most of those cards had what is termed "EMV" protection. A common example of such protection is the use of chip and pin. No chip and pin data was obtained by the attackers from the payment terminals in DSG's stores. However, the attackers did obtain from the EMV protected payment cards the unique 16-digit numbers on each credit or debit card (the "PAN") and the card expiry dates. In addition to these EMV protected cards, the attackers also exfiltrated over 52,000 other payment cards which did not have EMV protections. In respect of 8,628 of these non-EMV protected cards the attackers obtained not only the PAN and expiry date of each card but also the cardholder's name.

5. A substantial quantity of non-financial personal data was also obtained by the attackers, outwith the POS terminals. We address this further when we consider the First-tier Tribunal's ("FTT") decision.

6. As the FTT noted at paragraph 13 of its decision, forensic experts have not been able to identify the exact point of entry exploited by the attackers. However, once they gained access to the DSG environment, the attackers were able to compromise a number of internal systems and accounts, including multiple domain administrator accounts which provided the attackers with significant access privileges.

7. The ICO served a MPN on DSG on 7 January 2020. It was served under section 55A of the DPA 1998 "because of a serious contravention" of DPP7. The monetary penalty imposed by that MPN was £500,000 (the then maximum penalty).

8. DSG appealed against the MPN and its appeal was heard by the FTT over seven days in November 2021. The FTT in its decision of 5 July 2022 held that the ICO's MPN of £500,000 was wrong in law and substituted an MPN in the sum £250,000.

9. Permission to appeal was granted by Upper Tribunal Judge Wright on 9 June 2023 in respect of two of DSG's six proposed grounds of appeal (Grounds 1 and 3). As we explain in more detail below, there is an issue as to scope of the grant of permission in relation to Ground 1. Pursuant to Judge Wright's order, the effect of the FTT's decision is suspended until this appeal to the Upper Tribunal has been finally determined.

The ICO's MPN

10. Although the MPN served by the ICO has been superseded by the FTT's decision, it provides an important context for the FTT's decision and we therefore highlight some relevant parts of it.

11. Presaging a key issue in this appeal to the Upper Tribunal, the ICO rejected DSG's argument that the PAN did not constitute personal data in the hands of the attackers in those cases where the cardholder's name was absent from the data obtained by the attackers. The ICO maintained that "the PAN alone does constitute personal data" and therefore considered "that the total number of affected cards (5,646,417) contained personal data at risk of being compromised by the attack".

12. The ICO's MPN set out her "preliminary view" that DSG contravened DPP7 in relation to its computer system and organisational measures because: (i) DSG's network segregation was not sufficient; (ii) there was no local firewall configured on the POS terminals; (iii) DSG's approach to software patching of its domain controllers and the systems used to administer them was inadequate; (iv) vulnerability scanning of the compromised environment was not performed on a regular basis; (v) DSG failed to correctly manage application whitelisting across its full fleet of POS terminals; (vi) DSG did not have an effective system of logging and monitoring in place to identify and respond to incidents in a timely manner; (vii) it did not effectively manage the security of its POS systems because elements of its POS software was outdated; (viii) furthermore, DSG's POS system did not support point to point encryption; (ix) DSG failed effectively to manage the security of its domain administrator account in that it did not risk assess the addition of user accounts and failed to adhere to its own policies in respect of access permissions and passwords; and (x) it failed to implement standard builds for all system components based on industry standard hardening guidance.

13. The ICO, having had regard to the state of technological development, the cost of implementing any measures and the nature of the personal data and harm that could arise from its misuse, determined that there were multiple inadequacies in DSG's technical and organisational measures for ensuring the security of personal data on its system. The ICO stated that she was mindful that DPP7 and the requirements of section 55A of the DPA 1998 were concerned with measures and the kind of contravention, rather than with any actual data breach, but the attack had exposed the contents of DSG's systems to serious risks. It was the ICO's view that each of the ten inadequacies would have constituted a contravention of DPP7. However, she assessed DSG's arrangements in the round and on that basis took the preliminary view that there had been a multi-faceted breach of DPP7 by DSG.

14. Having found a contravention of DPP7, the ICO's MPN went on to explain why the conditions for issuing a MPN had, in her view, been met.

15. The ICO considered the contravention was serious because there were a number of distinct and fundamental inadequacies in DSG's security systems which appeared to have persisted over a relatively long period of time. Moreover, the attack had been ongoing for 9 months before it was detected, giving the attackers ample opportunity to view and extract data. A number of the inadequacies related to basic and commonplace measures which, in the ICO's view, were needed for any such system: for example, the absence of network segregation and inadequate software patching. Furthermore, there was a significant amount of personal data on DSG's systems, and the volume and breadth of financial personal data, and non-financial data, which had been affected was sufficient to increase the seriousness of the contraventions. Moreover, the nature of this

personal data heightened the seriousness of the contravention because it rendered the affected individuals susceptible to financial theft and identify fraud. In addition, the ICO had received a significant number of complaints about the attack, and the ICO considered these evidenced both the distress the attack had caused and the worry of increased fraud. Finally, the ICO considered that the general public would expect DSG to "lead by example" and to be sufficiently protected so as to avoid such systemic non-compliance.

16. Turning next to explain why the contravention was of a kind likely to cause substantial distress or substantial damage, the ICO's MPN set out, inter alia, that a contravention involving personal data, and in particular payment data, was likely to be useful in terms of identity theft and fraud. Furthermore, the contravention exposed personal data to the risk of cyberattack. And even if the damage or distress likely to have been suffered by each affected individual was less than considerable, the totality could nevertheless be substantial. Given the large number of affected individuals, whether in terms of financial or non-financial personal data, the "substantial distress" threshold was clearly met.

17. The ICO further determined in the MPN that DSG knew or ought reasonably to have known that there was a risk that the contravention would occur and be of a kind likely to cause substantial damage or substantial distress.

18. The ICO's MPN also found that DSG had failed to take reasonable steps to prevent such a contravention. This finding was based, inter alia, on DSG being a large, well-resourced and experienced data controller, which was processing payment card data and non-financial data for a large number of data subjects, and who therefore should have been aware of the potential consequences of cyber breaches where robust cyber security measures were absent. DSG, moreover, was well placed to assess weaknesses in its data security arrangements and take appropriate action. This was particularly so given a number of the inadequacies related to commonplace measures (e.g. network segregation and adequate patching) which should have been obvious to any data controller working with such IT systems. Further, given DSG's size and prominence, it should have appreciated that that the misuse of personal data held on its systems was likely to cause substantial distress and damage, including risks of identity fraud and theft. By failing to fully implement basic good practice measures prior to the attack, DSG failed to take appropriate steps to prevent the contravention.

19. It was on the basis of all of the above that the ICO decided it was appropriate to issue an MPN notice against DSG.

The FTT's decision

20. Given the breadth of the issues arising on this appeal, it is necessary to set out the FTT's decision in some detail.

21. Under the heading "Factual Background", the FTT set out that the attackers had "scraped" payment card data from the memory of the POS terminals before it entered DSG's encrypted system. 5,646,417 payment cards had been affected, of which 5,592,349 had EMV protection. Of the remaining 54,068 cards, DSG had been unable to determine whether 1,280 had EMV protection. However, 52,788 of those remaining cards were known not to have EMV protection, and of those in relation to 44,160 cards the attackers obtained only the PAN and the

card expiry dates. In the case of the remaining 8,628 cards without EMV protection, the attackers had obtained the cardholder name in addition to the PAN and expiry date. This scraped payment card data was referred to before the FTT as Batch 1 data.

22. The attack, however, also accessed a substantial quantity of non-financial data, which was accessed by the attackers other than from the POS terminals. This non-financial data comprised:

    (i) 1,181,839 records containing a combination of employee data, customer data and supplier information, described as having been obtained from different sources within DSG's domain. This was referred to as Batch 2 data. This data included customer email addresses, postcodes, postal addresses, and telephone numbers;

    (ii) approximately 10 million records of personal data had been extracted from a marketing database. This was referred to as Batch 3 data. This potentially included data such as customer names, postal addresses, phone numbers, email addresses, dates of birth, and data related to failed credit check details;

    (iii) approximately 2.9 million records from a database used by DSG for internal fraud investigations. This was called Batch 4.1 data in the FTT proceedings. This was personal data broadly similar to that in Batch 3, but also included payment card data in a masked format (i.e. details of the card expiry date, issue date and PAN with the middle eight digits replaced by XXXXXXXX); and

    (iv) approximately 4.7 million records from a second database related to internal fraud investigations. This was referred to as Batch 4.2 data. This data included bank account details and sort codes.

    The FTT noted that there was no definitive evidence whether any of Batches 1-4.2 had been successfully exfiltrated. However, it was not disputed that the attackers possessed the technological skills to have done so.

23. Having set out the relevant law at paragraphs 22 - 36, the FTT addressed the ICO's MPN. In particular, at paragraph 40 of its decision the FTT set out the "inadequate security measures ('contraventions') identified in the MPN". In summary, these were described by the FTT as: inadequate network segregation between the POS environment and the wider DSG network ("contravention 1"); the lack of a local firewall on the POS terminals ("contravention 2"); inadequate software patching ("contravention 3"); a failure to perform vulnerability scanning of the compromised environment on a regular basis ("contravention 4"); failure consistently to manage application whitelisting across all POS terminals ("contravention 5"); the lack of an effective system for logging and monitoring IT incidents in a timely manner ("contravention 6"); running software on the POS terminals that was outdated by several years and no longer maintained by the provider ("contravention 7"); as a consequence of contravention 6, running an out of date system on the POS terminals that did not support point to point encryption ("contravention 8"); failing to manage effectively the security of domain administrator accounts ("contravention 9"); and failing to implement standard builds for all components based on industry standard hardening guidance ("contravention 10").

24. Between paragraphs 50 – 74 the FTT summarised the evidence it had heard. It is unnecessary for us to refer to this in detail. The FTT heard oral evidence from

three non-expert witnesses: Mr Naveed Islam, the Head of Security Strategy for the Dixons Carphone Plc group until 31 December 2020; Mr Elliott Frazer, the Head of Business Standards and Data Protection Officer at Dixons Carphone Plc; and Mr Romeen Partovnia, a member of the ICO's Cyber Investigations and Incident Response Team. The FTT also heard evidence from three expert witnesses: Professor Paul Dorey, an expert in cyber and information security; Professor Steven Murdoch, an expert in the security of payment card data; and Mr Benn Morris, an expert on cyber security.

25. In its "Findings of fact and reasons" the FTT first noted that key aspects of the contraventions of DPP7 were no longer relied on by the ICO. Given the extent to which the contraventions identified in the ICO's MPN were no longer supported, the FTT was satisfied that not all the shortfalls identified in that MPN were contraventions of DPP7. It therefore found that the ICO's MPN was not in accordance with the law and that the FTT should substitute its own MPN.

26. The FTT found that approximately 18.5 million records of largely non-financial personal data records under Batches 2, 3, 4.1 and 4.2 were accessed by the attackers. This data comprised names, addresses, postcodes, email addresses, dates of birth, telephone numbers, details of failed credit checks, partially concealed PAN in a context where the PAN was linked with other personal data and bank account details. This total was approximately two million more than that found in the ICO's MPN, but the FTT based its higher finding on DSG's evidence before it, which the FTT took to represent the most current assessment of the attackers' activities. The FTT had regard to the fact that all figures before it were approximate and may have involved some duplication between the various Batches. However, it was "nevertheless…satisfied that a very substantial volume of non-financial personal data was unlawfully accessed as a consequence of the attack".

Personal data

27. As for the PAN scraped by the attackers from the POS terminals, the FTT said the following:

> "92. We conclude that, in the context of these proceedings, any PAN that identifies the bank account held solely by a living individual are personal data for the purposes of DPP7. This is because we are satisfied, on the balance of probabilities, that a living individual can 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.
>
> 93. The reasons for these conclusions are as follows:
>
> > a. 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, distilled from the relevant legislation and Upper Tribunal Judge Jacob's approach in *NHS BA*, 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.

b. The Parties' submissions concerning the PAN have focussed mainly on limbs (i) and (iii). They disagree as to whether the PAN directly identifies a living individual (the 'cloakroom ticket' argument in relation to identification of an account); or, in the alternative, whether a living individual could be identified indirectly from the PAN when combined with other information that is [reasonably] likely to come into the possession of a third party such as the Attackers. Less attention has been paid to limb (ii).

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.

e. It appears to be uncontroversial that the Batch 1 data was scraped from the POS terminals. Mr Islam's evidence is that the PAN processed by the POS terminals was separated from other transaction data, including presumably the name on the payment card, and was transmitted outside DSG's IT domain for processing. He described this as a security measure introduced in part due to concerns about the risks inherent in the POS terminals' internet gateway.

f. However, it has not been suggested that DSG could not thereafter combine the PAN with other data from the transaction should the need arise. In our view and as a matter of common sense, there must be a range of business needs that might require the PAN of a card used in

> a transaction to be linked to other data in DSG's IT estate, for example when processing a refund to the payment card. Therefore, whilst we accept that there may be some PAN stored on some parts of DSG's IT estate that may have been incapable of being linked to other data records, we are satisfied that a significant proportion of the PAN being processed must have been capable for being linked to other data, if only to the other data from the payment card (which would necessarily include the cardholder's name) or with partial PAN. We note in this regard that Batch 4.1 data comprised 2.9 million records that included masked PAN stored in combination with records that are unarguably personal data and that Batch 1 also included data from 8,628 payment cards in relation to which the records comprised PAN, expiry date and card holder name.

94. We are therefore 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. However, we cannot say definitively on the evidence before us how many of the PAN processed by DSG, or by the Attackers, could be combined with other information in such a manner. We therefore find only that some were so capable and make no findings as to quantity.

95. To clarify, our findings in this regard are not limited to a conclusion that the data in Batch 1 could have been combined with information from other Batches in order to achieve indirect identification. Mr Pitt-Payne objected in closing submissions to Mr Lockley putting such a case in cross examination, which he described as being a significant amendment to the Information Commissioner's case. We note that the Information Commissioner has previously raised as an issue in these proceedings the extent to which PAN could be matched to data from other Batches, primarily to data that contain partial PAN. More recently, 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.

97. Having concluded that at least some of the PAN processed by DSG were personal data pursuant to limb (ii), we have not gone on to consider whether, as a matter of principle, the PAN also met the limb (i) definition of personal data. We note that this is the approach relied upon by the Information Commissioner in paragraph 16 of the MPN. Our preliminary

> view is that data comprising a unique identifier of a financial account is capable of meeting the limb (i) definition but that, in the context of this case, the limb (ii) definition is much more obviously appropriate and applicable. Similarly, we have not gone on to determine whether the limb (iii) definition also applies. Although we appreciate the submissions made with considerable force by both Parties and have considered with care the evidence of the expert witnesses, we are satisfied that no further findings are required. The central question we were asked to determine was whether DSG had obligations under DPP7 in relation to the PAN it processed. We have concluded that it did, for the reasons given."

The contravention of DPP7

28. The FTT's findings and reasons then turned to DPP7 and, per paragraph 99:

> "99….whether the security measures in place at the time of the Attack were appropriate technical and organisational measures against the unlawful or unauthorised processing of personal data, having regard to the state of technological development at the time, the cost of implementing security measures and issues of proportionality".

29. The FTT noted that the ICO, on paper, appeared at times to have approached the matter as if the attack itself was a contravention; the FTT established that was not the ICO's view in practice (paragraph 107). It was clear that the attack itself was not a contravention (paragraph 107). Given the extent to which the ICO's case before it had changed, for reasons of fairness, the FTT made findings (at paragraph 110 of its decision) only in relation to the MPN contraventions upon which the ICO was still relying. The FTT found only two of the contraventions relied on by the ICO were contraventions of DPP7. These are contraventions 3 and 9, and we deal with them in greater detail below.

30. Before doing so, however, we touch briefly on the alleged contraventions the FTT did not find breached DPP7. Alleged contravention 1 was not made out because there was generally low take up of network segregation measures by industry due to the expense and complexity of doing so, and therefore DSG did not breach DPP7 in not putting in place such measures. As for alleged contraventions 2 and 5, the FTT found that DSG's POS terminals had adequate firewalls installed and whitelisting functions. Alleged contravention 4 concerned DSG's failure to vulnerability scan the POS terminals, but the FTT accepted it was rational for DSG to prioritise work on the data centre. Given Professor Dorey's evidence that the standard of DSG's logging and monitoring was meeting or better than expected standards in the retail sector in 2017, alleged contravention 6 was not a breach of DPP7 either. Nor was alleged contravention 8, as DSG's approach to the upgrade of security was rational. As for alleged contravention 7, the FTT found that "[g]iven the consultation with an IT security expert and the reliance on mitigations,… the continued reliance on outdated software was not a contravention of DPP7 *per se*", but it was a relevant factor when assessing the appropriateness of DSG's technical and organisational measures globally.

31. Contraventions 3 and 9 concerned DSG's having been made aware (by a report prepared by an information security consultancy in May 2017, referred to as "the B Report") that the DSG domain had not been updated with a number of software security patches, some of which had been identified as critical. One such patch

was from 2014 and required a two stage process in which the second stage, after the patch had been applied, required the pre-existing administrator passwords to be deleted from the Group Policy account. This had not been done by the time of the B Report in May 2017, which identified this failure as a recurring issue, and the administrator passwords had still not been deleted by November 2017. The FTT accepted that the responsibility for these software security patching actions lay at the time with DSG's external IT security contractor, but DSG remained accountable for its IT security. The FTT further gave weight to evidence of Professor Dorey that maintaining up to date security patches was an important security requirement, that the number of critical patches which were still to be applied in May 2017 would have been a source of concern for him and that this indicated an erratic approach to patch solution within DSG's domain. In addition, once the attackers had gained access to DSG's domain, they took advantage of the inadequate management of administrator passwords for the Group Policy account, and it was very likely that the failure to delete the administrator passwords became one of the vectors of the attack. There was, moreover, no evidence before the FTT of any risk assessment or decisions made by or on behalf of DSG relating to the critical risks of security patch management and password practices after it had had concerns about these matters drawn to its attention in 2017 and 2018.

32. Despite its use of external IT consultants, the FTT was satisfied that senior managers at DSG had been made aware at least twice that DSG's IT system had a critical security vulnerability in relation to its approach to patch management, and at least once that there was an issue with their password policy. Further, DSG had been notified of the critical risk arising from the failure to complete the required second stage (deleting the administrator passwords) in relation to the 2014 software patch.

33. The FTT therefore concluded that, having commissioned the B Report for the purpose of identifying security vulnerabilities of this nature, there was a reasonable expectation that DSG should have taken positive steps to address as a priority any critical risks or systemic weakness that had been identified. It further concluded that:

> "110. (m)…notwithstanding the complexity of the DSG IT domain and the challenges described of rolling out security patches across the entire estate, the approach within DSG to software patching and to the management of passwords/domain administrator password accounts amounted to a failure to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data…..Further, and in the absence of evidence of any risk assessment, we are satisfied that any decision made by DSG in relation to adopting appropriate technical and organisational measures in this regard ought not to be viewed as an exercise of judgement of the nature anticipated in ***Morrisons***, whether or not that decision was taken positively or default. We are satisfied that DSG's failure to take appropriate measures in relation to this risk was a contravention of DPP7 for which it is appropriate to hold DSG to account.
>
> (n) When reaching this conclusion, we have approached any evidence of use by the Attackers of the vulnerability created by the contravention as being solely confirmation of the potential risks. We are satisfied from the evidence before us that the Attackers were sophisticated criminals and that

> their ability to gain access to DSG's domain should not be taken as an indication that DPP7 obligations cannot have been met."

Seriousness of the contravention

34. The FTT then addressed whether the contravention of section 4(4) DPA 1998 that it had found made out in respect of DPP7 was serious. It concluded that it was serious having regards to:

> "111….
>
> a. The fact that the personal data of approximately 25 million individuals were stored on DSG's IT system at the relevant time;
>
> b. The nature of this personal data, which comprised names, postal addresses, email addresses, dates of birth, and credit check information, as well as an unknown quantity of PAN capable of being used to indirectly identify a living individual, and
>
> c. The reasonable expectation of individuals and society that a body of personal data of this nature would be adequately protected, given the potential consequences of unauthorised or unlawful processing."

Substantial damage and distress and knowledge

35. In respect of the "substantial damage or distress" requirement, the FTT directed itself that the test it was required to apply was whether the contravention was of a kind likely to cause substantial distress, not whether the attack did so. It concluded that contravention was of such nature, having regard to the range and volume of personal data held by DSG and the considerable worry and concerns throughout modern society about the risks of identity fraud. Its reasons for so concluding are in paragraph 113 of its decision, which reads:

> "113. In contrast to the approach taken in the MPN, we are not persuaded that the most significant risk arising from contravention was that of the fraudulent use of payment cards. We note from expert evidence that the use of PAN and expiry date alone provides only limited opportunity for unauthorised use. This appears to be reflected in the limited extent to which such data may have been used by the Attackers in this case. However, we find it more likely than not that individuals, whether customers or employees, who became aware that their names, dates of birth, addresses and email addresses had been accessed by a sophisticated criminal group would be caused substantial distress. As previously stated, we find in addition that, in relation to an unknown number of individuals, these records of personal data could potentially be linked to their payment card PAN, a circumstance we are satisfied is likely to compound feelings of distress. We therefore conclude that the personal data in relation to which this contravention occurred was of a kind likely to cause substantial distress both qualitatively and quantitatively."

36. The FTT also concluded that DSG knew or ought to have known about the contravention and failed to take reasonable steps to ensure that the external IT security consultant was prioritising this critical risk.

The substituted MPN

37. The last issue the FTT had to decide was whether to impose a MPN. It considered it was appropriate to do so because the contravention was particularly serious given the nature of the personal data involved in the contravention and the number of people affected, the length of time the inconsistent patch management was allowed to continue and the obvious risk that the large volume of personal data held by DSG was of a kind likely to be targeted by a criminal attack. The FTT balanced this against the fact that at the time of the attack DSG was directing substantial resources to long-term security transformation and had employed external security consultants to address the position in the interim. However, in the FTT's view this did not abrogate DSG of responsibility. In imposing an MPN the FTT also considered the resources of DSG, and took into account that the contraventions it had identified were fewer than those that had led to the ICO's MPN.

38. Having decided that it was appropriate to impose an MPN, the FTT then considered relevant aggravating and mitigating features. The FTT's analysis included the following passage:

> "120. We note again that the identified contravention is serious for reasons already given relating to the nature and volume of data processed by DSG and the number of individuals whose data was put at risk.
>
> 121. We are not persuaded that the number of PAN accessed by the Attackers is an additional, relevant consideration for the purpose of identifying the quantum of any MPN imposed in this context. As previously stated, we have concluded that the exact number of PAN meeting the definition of personal data remains unknown. Rather, we consider the overall volume of personal data, both financial and non-financial, which is known to have been unlawfully processed to be a more relevant consideration."

39. In terms of the quantum of the MPN, the FTT noted that the highest penalty was generally reserved for multiple contraventions of DPPs and/or contraventions of DPP7 comprising several inadequacies. Neither consideration applied in this case. It concluded that the appropriate figure in this case was £250,000.

The issues on this appeal

40. As the grant of permission was restricted to two of DSG's proposed six grounds (Grounds 1 and 3), a number of the FTT's findings were not the subject of free-standing challenges in this appeal. This included: the failings identified in relation to contraventions 3 and 9; that the contravention was of a kind likely to cause substantial distress; that DSG had the requisite knowledge in respect of the contravention; and the quantum of the penalty. Ground 1 concerns the FTT's conclusion that the data obtained from the 5,592,349 cards with EMV protection (the PAN and the card expiry date data) was "personal data" for the purposes of DPP7. We refer to this data as the "EMV Data". DSG accepted that the non-financial data that was exfiltrated and the cardholder plus PAN and expiry date data obtained from 8,628 of the cards that did not have EMV protection constituted "personal data". Ground 3 challenges the FTT's finding that there had

been a "serious" contravention of DSG's data responsibilities, within the meaning of section 55A DPA 1998.

41. Five issues were argued before us. We shall use the same numbering and nomenclature as was used by DSG to identify those issues.

42. **Issue 1** is the **EMV Data Issue**. Did the FTT err in law in deciding that there had been a contravention of the DPA 1998, in relation to the EMV Data which was personal data in DSG's hands, without determining whether that data would be personal data in the hands of a third party such as the attackers? DSG argued that in so far as the EMV Data was not personal data in itself (Issue 4, below), it was a necessary quality of a contravention, on the facts of this case, that the data should be personal data in the hands of a third party such as the attackers and that the FTT wrongly directed itself that it did not need to determine this.

43. **Issue 2** is the **Consistency Issue.** Did the FTT err in: (i) failing to determine whether that data was personal data in the attackers' hands, in circumstances in which the FTT had (rightly) identified that that question "must be relevant" to other statutory preconditions; and/or (ii) then asserting, in relation to seriousness, distress, and quantum, that the fact that the data was personal data in DSG's hands was relevant to those issues? A logically prior issue arises here of whether DSG has permission to appeal on Issue 2.

44. **Issue 3** is the **Procedural Fairness Issue.** Did the FTT act unlawfully by reaching its conclusions on the EMV Data Issue on a basis that was not argued before it (that the EMV Data was personal data in DSG's hands), without giving the parties an opportunity to make representations and/or lead evidence on the FTT's newly-raised issue?

45. **Issue 4** is the **Implications Issue**. If the FTT did err in law in relation to its personal data finding, DSG submits that the Upper Tribunal should itself decide whether the EMV Data on its own constituted "personal data" (with all other questions remitted to the FTT)**.**

46. **Issue 5** is the **Seriousness Issue**. Did the FTT err in law in its determination of the question whether the contravention identified was serious? There are three elements to this ground of appeal. First, did the FTT err in law in conflating the consequences of the contravention with the seriousness of the contravention? Second, did the FTT err in law in taking into account the "expectations of individuals and society"? Third, did the FTT err in law in relying on an "unknown quantity of PAN capable of being used to indirectly identify a living individual"?

The grant of permission to appeal

47. Upper Tribunal Judge Wright's order granting permission to appeal said:

> "I give the DSG Retail Limited permission to appeal. The grant of permission to appeal is limited to grounds one and three as identified and explained below."

48. Paragraph 1 of his accompanying Reasons included the following:

> "Permission to appeal is given because I consider that it is arguable with a realistic prospect of success that First-tier Tribunal erred in law in the decision it made on 5 July 2022 on the grounds set out below. These are

> grounds one and three (but as identified and explained below – see, for example, paragraphs 23 and 37 below).[…]"

49. Judge Wright discussed Ground 1 between paragraphs 15 – 21. At paragraph 15 he described the question in terms that reflect the issue that we have referred to as Issue 1. He then said:

> "22. …I have concluded that DSG's argument here is not unarguable. I therefore give permission to appeal on ground 1. The ground should be the subject of full(er) argument and would benefit from a binding decision of the Upper Tribunal on an appeal.
>
> 23. Ground 1 also has a sub-ground within it or associated with it, on which I give DSG permission to appeal as well. The argument here, as I understood it, is that even if the First-tier Tribunal was right as a matter of law about in whose hands the information must constitute personal data for the purposes of the DPA 1998, the late basis on which it did so meant that DSG was not in a position to properly address this case against it…It appears conceded by the Information Commissioner that at no stage in the First-tier Tribunal proceedings was he arguing for the approach the First-tier Tribunal settled on in its decision in relation to the PANs.
>
> 24. DSG's argument under this associated aspect of ground 1 is that it had no, or no sufficient opportunity to put before the First-tier Tribunal (a) evidence about the systems it had in place at the time of the attack to protect the PANs alone from exfiltration, and/or (b)…evidence about the other information it held which when linked to the PAN could identify a living individual, and how that other information was protected." [Emphasis in the original.]

50. A dispute arose subsequently as to the scope of the grant of permission to appeal in respect of Ground 1. By letter dated 29 November 2023, the ICO sought clarification. The ICO's position was that the grant of permission was limited to what we have referred to as Issues 1 and 3 (the latter was Ground 1(b) in the application for permission). DSG disputed this proposition, contending in a letter dated 6 December 2023 that the grant included what we have identified as Issue 2, on the basis that this was set out at sub-paragraphs 19(3) and (4) as part of Ground 1 in the grounds of appeal.

51. On 12 December 2023 Judge Wright provided a ruling on the request for clarification. At paragraph 7 he indicated that, "[t]his ultimately may be a matter for the three-judge panel to determine in hearing and deciding the appeal". However, he included the following observations:

> "12. I plainly intended to give permission to appeal on the 'issue of principle' (and on Ground 1(b)). Whether the first ground of appeal was otherwise limited to that 'issue of principle' (and Ground 1(b)) may, trying to read the grant of permission as objectively as I can, require the word "here"…to do some heavy lifting.
>
> 13. **Second**, the grant of permission of appeal, save for the words "as identified and explained below" did not expressly limit the grant of permission to appeal under the first ground of appeal and did not expressly exclude sub-paragraphs (3) and (4) of paragraph 19 in DSG's grounds of appeal.

> 14. **Third**, the arguments which fall properly within the scope of the grant of permission to appeal in respect of the first ground of appeal cannot involve arguments for which permission has been refused under the second, fourth, fifth and sixth grounds of appeal." [Emphasis in the original.]

The legal framework

The Upper Tribunal's approach on appeal

52. This appeal is brought under section 11 of the Tribunals, Courts and Enforcement Act 2007 (TCEA 2007), so the task for the Upper Tribunal is to determine whether the decision of the First-tier Tribunal involved a (material) error of law (section 12(1)). What constitutes a material error of law has been discussed in many cases; a convenient list of common errors is to be found in *R (Iran) v SSHD* [2005] EWCA Civ 982 at paragraphs 9 - 10. Challenges to the FTT's findings of facts do not amount to errors of law unless they reach the high threshold for perversity: ibid at paragraph 11.

53. In scrutinising the judgment of the FTT, the Upper Tribunal must exercise restraint. The Upper Tribunal in *Information Commissioner v Experian Limited* [2024] UKUT 105 (AAC) summarised the principles as follows:-

> "64. As is well-known, the authorities counsel judicial "restraint" when the reasons that a tribunal gives for its decision are being examined. In *R (Jones) v FTT (Social Entitlement Chamber)* [2013] UKSC 19 at [25] Lord Hope observed that the appellate court should not assume too readily that the tribunal below misdirected itself just because it had not fully set out every step in its reasoning. Similarly, "the concern of the court ought to be substance not semantics": per Sir James Munby P in *Re F (Children)* at [23]. Lord Hope said this of an industrial tribunal's reasoning in *Shamoon v Chief Constable of the Royal Ulster Constabulary* [2003] UKHL 11 at [59]:
>
> > " … It has also been recognised that a generous interpretation ought to be given to a tribunal's reasoning. It is to be expected, of course, that the decision will set out the facts. That is the raw material on which any review of its decision must be based. But the quality which is to be expected of its reasoning is not that to be expected of a High Court judge. Its reasoning ought to be explained, but the circumstances in which a tribunal works should be respected. The reasoning ought not to be subjected to an unduly critical analysis."
>
> 65. The reasons of the tribunal below must be considered as a whole. Furthermore, the appellate court should not limit itself to what is explicitly shown on the face of the decision; it should also have regard to that which is implicit in the decision. *R v Immigration Appeal Tribunal, ex parte Khan* [1983] QB 790 (per Lord Lane CJ at page 794) was cited by Floyd LJ in *UT (Sri Lanka) v SSHD* [2019] EWCA Civ 1095 at [27] as explaining that the issues which a tribunal decides and the basis on which the tribunal reaches its decision may be set out directly or by inference."

Scope of grants of permission

54. Under rule 22 of the Tribunal Procedure (Upper Tribunal) Rules 2008 (SI No 2698) ("the Rules") the Upper Tribunal may grant or refuse permission to appeal. By rule 22(1) if permission is refused, "it must send written notice of the refusal and of the reasons for the refusal to the appellant". If permission is granted on some grounds, but not on all, or subject to some other condition, then (by rule 22(2)(a)) the Upper Tribunal "must send written notice of the permission, and of the reasons for any limitations or conditions on such permission, to each party". If permission is granted on an unlimited or unconditional basis, the Rules contain no express requirement for reasons to be given, only a requirement that each party be sent a written notice of the grant of permission (rule 22(2)(a)). By rule 22(2)(b), "subject to any direction by the Upper Tribunal, the application for permission to appeal stands as the notice of appeal …".

55. As we have indicated, there is a dispute in this case as to the scope of the grant of permission. A similar issue arose in the Court of Appeal in *Secretary of State for the Home Department v Rodriguez* [2014] EWCA Civ 2, where the question was whether the point sought to be run in the Court of Appeal had in fact been the subject of a refusal of permission before the Upper Tribunal (and thus a decision in respect of which no appeal could be made to the Court of Appeal). The order recording the grant of permission in that case had been unlimited, but the respondent argued that the grant of permission was in fact limited by the reasons for granting permission that followed. Davis LJ at paragraph 77 held that:

> "if there is ambiguity arising from the language of the Reasons given then […] such ambiguity is to be resolved in favour of the applicant: particularly where the opening part of the Order concerning the actual grant of permission was unqualified"

56. However, there is no rule that the reasons cannot limit the grant of permission, even where the determination is in unqualified terms. In *Sarkar v Secretary of State for the Home Department* [2014] EWCA Civ 195, Moore-Bick LJ at paragraph 17 held that:

> "In the present case the apparently unqualified grant of permission to appeal must be read in the context of the reasons which Judge Spencer gave for his decision, which make it quite clear that he intended to limit it to the ground that he had identified based on section 47 of the Immigration, Asylum and Nationality Act 2006."

Relevant provisions of the DPA 1998

57. This case is concerned with the 'old' data protection regime under the DPA 1998. Both parties to this appeal suggest that the relevant provisions of the 'new' regime under the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR) are materially the same, but we make clear that we have not considered the provisions of the new regime in this case.

58. Section 1 of the DPA 1998 defines "personal data" as follows:-

> "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,
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;"

59. Whilst the statutory wording only refers to the two possibilities of a living individual who can be identified from the data itself or from the data and other information in the possession of or likely to come into the possession of the data controller, it is apparent from Directive 95/46/EC (which the DPA 1998 implements) and the caselaw that we discuss below, that whether data amounts to "personal data" for these purposes may entail consideration of whether a living individual can be identified from the data itself in combination with additional information that is in the possession of, or reasonably likely to be in the possession of, a third party.

60. Section 1(1) of the DPA 1998 also contains the definition of "data controller" as follows:-

> "data controller" means, subject to subsection (4), 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;"

61. The DPA 1998 refers to seven "data protection principles". These data protection principles are set out in Part I of Schedule 1 (section 4(1)). The data protection principles are to interpreted in accordance with Part II of Schedule 1 (section 4(2)). By section 4(4):

> "… 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"

62. This case concerns DPP7, which is set out at paragraph 7 of Part I of Schedule 1 as follows:

> "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."

63. Part II of Schedule 1 makes provision as to the interpretation of DPP7 including, paragraph 9 which is relevant to this appeal:

> "9. 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 such 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."

64. By section 40 of the DPA 1998, where a data controller contravenes any of the data protection principles, the ICO may serve him with an enforcement notice requiring the data controller to take (or refrain from taking) certain specified steps. In deciding whether to serve an enforcement notice, the ICO must take into account "whether the contravention has caused or is likely to cause any person damage or distress" (section 40(2)) (but is not limited to issuing an enforcement notice only in such cases). There is also provision under section 13 for an individual who suffers damage or distress by reason of any contravention by a data controller of the data protection principles to make a claim for compensation (and we note that a number of such claims have been brought by individuals in the courts in relation to the same matters as led to the imposition of the MPN in this case).

65. This case, however, is concerned with an MPN issued under section 55A, which is a provision that applies only where the ICO is satisfied that there has been a *serious* contravention *likely to cause substantial damage or distress*. We need to consider the full text of the section, which is as follows:

> "**55A Power of Commissioner to impose monetary penalty**
>
> (1) The Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that—
> (a) there has been a serious contravention of section 4(4) by the data controller,
> (b) the contravention was of a kind likely to cause substantial damage or substantial distress, and
> (c) subsection (2) or (3) applies.
>
> (2) This subsection applies if the contravention was deliberate.
>
> (3) This subsection applies if the data controller—
> (a) knew or ought to have known—
> (i) that there was a risk that the contravention would occur, and
> (ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but
> (b) failed to take reasonable steps to prevent the contravention.
>
> …
>
> (4) A monetary penalty notice is a notice requiring the data controller to pay to the Commissioner a monetary penalty of an amount determined by the Commissioner and specified in the notice.
>
> (5) The amount determined by the Commissioner must not exceed the prescribed amount.

> (6) The monetary penalty must be paid to the Commissioner within the period specified in the notice.
>
> (7) The notice must contain such information as may be prescribed."

66. A right of appeal lies to the Tribunal under section 48(1). By section 49(1) the Tribunal must allow the appeal or substitute an alternative decision notice, if it considers that the enforcement notice was not in accordance with the law or that, to the extent that the notice involved an exercise of discretion by the ICO, that the discretion ought to have been exercised differently. In any other case, the Tribunal must dismiss the appeal. By section 49(2) the Tribunal has power to review any determination of fact on which the notice in question was based.

Relevant case law and guidance on the meaning of "personal data"

67. The FTT in this case adopted as its starting point the three limbs to the definition of personal data distilled from the legislation and Upper Tribunal Judge Jacobs' analysis in *NHS Business Services Authority v Information Commissioner and Spivack* [2021] UKUT 192 (AAC):

> "Limb (i): data which identifies a living individual directly;
>
> Limb (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
>
> Limb (iii): As limb (ii), but where the additional information is or is likely reasonably to be in the possession of a third party."

68. The DPA 1998 was introduced to implement in domestic law Directive 95/46/EC and its provisions must be interpreted, insofar as possible, in a manner consistent with the Directive, including the recitals: per Cranston J in *Department of Health v Information Commissioner* [2011] EWHC 1430 (Admin) at paragraph 17 ("*Department of Health*").

69. Recital 26 of the Directive gives the following guidance relevant to the definition of personal data:

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

70. Article 2(a) of the Directive provides that for the purposes of the Directive:

> "'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;"

71. Accordingly, the Directive's concept of "personal data" takes account of the material that is reasonably likely to be accessed by others, as well as the data

controller, for identification purposes. Recital 26 also refers to the concept of anonymisation, as a process whereby personal data could cease to be personal data (under any limb) if it would no longer be possible, by all reasonably likely means, for a person to be identified from the data.

72. A number of cases have considered issues as to the dividing line between personal data and anonymised data, or what the authorities refer to as "plain vanilla" data or just "information". We return to the case law below. Some of the developments in that case law are reflected in the 'new' DPA 2018 regime in the equivalent recital to the UK GDPR (also recital 26) as follows:

> "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

73. The new recital 26 thus refers to the concept of 'pseudonymisation' whereby (unlike true anonymisation) data remains personal data because the individual remains identifiable by some reasonably likely means. The Article 29 Working Party, in its Opinion 05/2014 on Anonymisation Techniques warned about the dangers of conflating anonymisation and pseudonymisation (at 2.2.3):

> "A specific pitfall is to consider pseudonymised data to be equivalent to anonymised data. The Technical Analysis section will explain that pseudonymised data cannot be equated to anonymised information as they continue to allow an individual data subject to be singled out and linkable across different data sets. Pseudonymity is likely to allow for identifiability, and therefore stays inside the scope of the legal regime of data protection."

74. This issue as to the dividing line between personal data and plain vanilla data, which is relevant to both the limb (ii) and limb (iii) definitions of personal data, has been considered in a number of domestic and European authorities. Those authorities have considered the issue in two contexts: (a) controlled release of data under the Freedom of Information Act 2000 ("FOIA"); and (b) alleged unlawful disclosure cases under the data protection regime. The focus in those contexts has generally been the limb (iii) definition of personal data and the question of whether the information would be personal data in the hands of a third party. The case law also illustrates that data may be personal data in the hands

of one entity, but not personal data in the hands of another, if the former holds or can access additional information that enables identification to take place, but the latter does not.

75. As to the relevant case law, the starting point is in principle the decision of the House of Lords in *Common Services Agency v Scottish Information Commissioner* [2008] 1 WLR 1550 ("*CSA*"). However, the parties in this case agreed that there is no need for us to go back to the judgments of their Lordships in that case as, on the issue with which we are concerned, subsequent decisions of the courts and this Upper Tribunal have analysed the effect and implications of the House of Lords' decision, and it is sufficient to refer to those subsequent cases for the purposes of determining this appeal.

76. *The Information Commissioner v Miller* [2018] UKUT 229 (AAC) provides the most convenient summary of the principles to be applied when considering limb (iii) issues. This was a decision of Upper Tribunal Judge Markus QC concerned with a request made under FOIA for data on homelessness from each local authority. For data relating to five or fewer individuals or households, the Department for Communities and Local Government (DCLG) had relied on the exemption for personal data in section 40(2) of FOIA to withhold disclosure. The FTT held that the data was not personal data and ordered release of the data. Judge Markus dismissed the appeal, but set out the relevant legal principles by reference to the case law as follows:

> "10. The correct approach to the application of section 1(1)(b) to disclosure of anonymised data was addressed by the House of Lords in *Common Services Agency v Scottish Information Commissioner* [2008] 1 WLR 1550. That decision was discussed by the Administrative Court in *R (Department of Health) v Information Commissioner* [2011] EWHC1430 (Admin). Cranston J explained that the House of Lords had decided that, even though the data controller holds the key to identification of individuals to which the data relates, whether it is personal information when disclosed depends on "whether any living individuals can be identified by the public following disclosure of the information" (paragraph 52). In *Information Commissioner v Magherafelt District Council* [2013] AACR 14 the Upper Tribunal said that the decision in *Department of Health* meant that the proper approach to whether anonymised information is personal data within section 1(1)(b), for the purposes of a disclosure request, is to consider whether an individual or individuals could be identified from it and other information which is in the possession of, or likely to come into the possession of a person other than the data controller after disclosure.
>
> 11. In the *Department of Health* case Cranston J said at paragraph 66 that the assessment of the likelihood of identification included "assessing a range of every day factors, such as the likelihood that particular groups, such as campaigners, and the press, will seek out information of identity and the types of other information, already in the public domain, which could inform the search."
>
> 12. As for the likelihood of identification, Recital 26 of the preamble to the Directive provides that "account should be taken of all the means likely

reasonably to be used". In *Magherafelt* the Upper Tribunal acknowledged the "motivated intruder" test advanced by the Information Commissioner:

> "37 …A 'motivated intruder' was '…a person who starts without any prior knowledge but who wishes to identify the individual or individuals referred to in the purportedly anonymised information and will take all reasonable steps to do so.'. The question was then one of assessment by a public authority as to '… whether, taking account of the nature of the information, there would be likely to be a motivated intruder within the public at large who would be able to identify the individuals to whom the disclosed information relates."

13. While not expressly adopting that test, the approach of the Upper Tribunal in that case was consistent with it. A similar approach was taken by the Court of Session (Inner House) in *Craigdale Housing Association v The Scottish Information Commissioner* [2010] CSIH 43 at paragraph 24:

> "…it is not just the means reasonably likely to be used by the ordinary man on the street to identify a person, but also the means which are likely to be used by a determined person with a particular reason to want to identify the individual…using the touchstone of, say, an investigative journalist…"

14. The Information Commissioner's Code of Practice on "Anonymisation: managing data protection risk" provides guidance at page 22/23 on the application of the "motivated intruder" test:

> "The approach assumes that the 'motivated intruder' is reasonably competent, has access to resources such as the internet, libraries, and all public documents, and would employ investigative techniques such as making enquiries of people who may have additional knowledge of the identity of the data subject or advertising for anyone with information to come forward. The 'motivated intruder' is not assumed to have any specialist knowledge such as computer hacking skills, or to have access to specialist equipment or to resort to criminality such as burglary, to gain access to data that is kept securely."

15. The guidance also addresses the risk of re-identification where one individual or group of individuals already knows a great deal about another individual, such as a family member, colleague or doctor, and says at page 26:

> "The starting point for assessing re-identification risk should be recorded information and established fact. It is easier to establish that particular recorded information is available, than to establish that an individual – or group of individuals - has the knowledge necessary to allow re-identification. However, there is no doubt that non-recorded personal knowledge, in combination with

> anonymised data, can lead to identification. It can be harder though to substantiate or argue convincingly. **There must be a plausible and reasonable basis for non-recorded personal knowledge to be considered to present a significant re-identification risk**." (my emphasis)

16. The guidance also distinguishes between identification and an educated guess:

> "[Identification] implies a degree of certainty that information is about one person and not another. Identification involves more than making an educated guess that information is about someone; the guess could be wrong. The possibility of making an educated guess about an individual's identity may present a privacy risk but not a data protection one because no personal data has been disclosed to the guesser. Even where a guess based on anonymised data turns out to be correct, this does not mean that a disclosure of personal data has taken place."

77. In the present case, DSG relies on a number of other decisions where it was emphasised that disclosure of data that is personal data in the hands of the data controller (on the limb (ii) test), but only plain vanilla data in the hands of a third party (on the limb (iii) test), is not unlawful as, once released, the data in such cases is no longer subject to the data protection regime.

78. Thus in *APPGER v Information Commissioner* [2011] UKUT 153 (AAC) ("*APPGER*"), the Upper Tribunal considered information requested from the MOD under FOIA. The MOD relied on section 40 of FOIA to resist disclosure of information on the numbers of individuals transferred to particular detention facilities or particular kinds of detention facilities. The Commissioner determined this was not personal data. On appeal, the First-tier Tribunal and Upper Tribunal agreed. The Upper Tribunal in its judgment considered the implications of the House of Lords' decision in the *CSA* case. Having determined at paragraph 125 that the reasoning of their Lordships on this issue contained three different approaches and no majority decision, the Upper Tribunal went on to express its own view at paragraphs 126 - 128 as follows. The Upper Tribunal's conclusion at paragraph 128 has a particular resonance for the present case, indicated by our emphasis below:

> "126. We consider there is force in Baroness Hale's analysis, which Mr Hickman strongly urged us to adopt. It is difficult to imagine any situation where disclosure of anonymised information about living individuals, whose identities were known to the data controller, would not be regarded as disclosure of personal data, if one were required to take into account, in determining whether individuals were identifiable, the data controller's own knowledge of their identity. At first sight, that cannot be right, since it would have the result of retaining protection for anodyne information not affecting anyone's privacy (what Lord Rodger called "plain vanilla data"). The Commissioner similarly urged on us that the MOD's construction would give rise to absurdities. Mr Hooper submitted that on the MOD's construction, the number of individuals who had died

> of heart disease in the UK over the last decade would amount to "personal data" if this number were in the hands of a data controller that held the underlying records identifying each individual concerned, however large that number might be, but it would plainly not be a sensible construction of the DPA to require all processing of such a wholly general piece of information to comply with the data protection principles.
>
> 127. We cannot accept the Commissioner's argument in full. As we understand the reasoning of Lord Hope, it is important to remember in this context that the definition of 'processing' does not only cover disclosure. Information or data are also processed when they are merely held, or indeed when they are destroyed (so that no one can any longer be identified). Anonymisation by redaction is itself a form of processing. If the data controller carries out such anonymisation, but also retains the unredacted data, or retains the key by which the living individuals can be identified, the anonymised data remains "personal data" within the meaning of paragraph (b) of the definition and the data controller remains under a duty to process it only in compliance with the data protection principles. On this basis, therefore, and contrary to the submissions of the Commissioner, we consider that the analysis of the essence of Lord Hope's reasoning by the Information Tribunal in *Department of Health v Information Commissioner and Prolife Alliance* EA/2008/0074 (15 October 2009) at paragraphs 30-43 was probably correct.
>
> 128. **However, we remain concerned at the use of this analysis in such a way as would have the effect of treating truly anonymised information as if it required the protection of the DPA, in circumstances where that is plainly not the case and indeed would be absurd. Lord Hope's reasoning appears to lead to the result that, in a case where the data controller retains the ability to identify the individuals, the processing of the data by disseminating it in a fully anonymised form, from which no recipient can identify individuals, can only be justified by showing that it is effected in compliance with the data protection principles. Certainly the whole of the information still needs the protection of the DPA in the hands of the data controller, for as long as the data controller retains the other information which makes individuals identifiable by him. But outside the hands of the data controller the information is no longer personal data, because no individual can be identified. We therefore think, with diffidence given the difficulties of interpretation which led to such divergent reasoning among their Lordships, the best analysis is that disclosure of fully anonymised information is not a breach of the protection of the Act because at the moment of disclosure the information loses its character as personal data. It remains personal data in the hands of the data controller because the controller holds the key, but it is not personal data in the hands of the recipients, because the public cannot identify any individual from it. That which escapes from the data controller to the outside world is only plain vanilla data.** We think this was the reasoning that Baroness Hale had in mind, when she said at [92]:

> "For the purpose of this particular act of processing, therefore, which is disclosure of these data in this form to these people, no living individual to whom they relate is identifiable"."

79. Cranston J in *Department of Health* disagreed with the Upper Tribunal's analysis of *CSA* in *APPGER*, considering that it was not open to a lower court or Tribunal to rely on the speech of Baroness Hale when "our system of precedent demands that the High Court treat Lord Hope's speech as determinative" (paragraph 45). For what it is worth, we agree with Cranston J's analysis of the application of the doctrine of precedent, but we do not consider that anything turns on this particular point of divergence between *APPGER* and *Department of Health*. In the course of argument, Mr Lockley for the Information Commissioner referred us to paragraphs 46 - 47 of Cranston J's judgment, emphasising Lord Hope's view that even "barnardised" personal data (barnardisation is a means of anonymising statistical data) would remain personal data in the hands of the data controller, up to and including the point of disclosure to a third party when the lawfulness of its disclosure would need to be judged by reference to the data protection principles. Cranston J's analysis of Lord Hope's reasoning was as follows (emphasis added; the parties are in agreement about the "not" missing from the first paragraph):

> "46. Lord Hope's reasoning began by pointing out that disclosure is only one of the ways in which a data controller can process information. **The data controller must comply generally with data protection principles. It could [not] exclude personal data from the duty to comply with the data protection principles simply by editing the data so that a third party would not find it possible from that part alone, without the assistance of other information, to identify a living individual: [22].** If the definition of personal data could be read in a way that excluded information that had been rendered fully anonymous, putting it into that form would take it outside the scope of the agency's duty as data controller: [23]. Lord Hope continued that the relevant part of the definition was limb B, since a living individual could not be identified from those data, ie the barnardised statistics themselves (limb A). Data would not be personal data if the other information was incapable of adding anything, and the data itself could not lead to identification, or if the data had been put into a form from which individuals to whom they related could not be identified at all, even with the assistance of the "other information" from which they were derived: [24]. In the latter situation, a person who had access to anonymised data and "other information" held by the data controller would find nothing in the anonymised data that would enable identification. It would be the "other information" only, and not anything in the anonymised data, which would result in the identification: [24].
>
> 47. Lord Hope then referred to the wording of recital 26 of the preamble to Directive 95/46/EC, noting that the definition of personal data contained in Section 1(1) of the DPA gives effect to it. The first two parts of the recital refer to situations set out expressly in Section 1(1), the third part casting further light on what member states were expected to

achieve when implementing the directive: [25]. Lord Hope's analysis is then completed at paragraphs 26 to 27, which deserve quoting in extensio.

> "26. The effect of barnardisation would be to conceal, or disguise, information about the number of incidences of leukaemia among children in each census ward. 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 then be 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. If he is unable to say that it would in that form be fully anonymised he will then need to consider whether disclosure of this information by the agency would be in accordance with the data protection principles and in particular would meet any of the conditions in Schedule 2.** This is the more difficult of the two routes I have mentioned. As the issues were fully argued I shall say what I think about them. But there is no doubt that the commissioner's task will be greatly simplified if he is able to satisfy himself that the process of barnardisation will enable the data to be sufficiently anonymised."

80. On Cranston J's analysis, therefore, Lord Hope's view was that if the CSA held a 'key' to the barnardised data that would enable it as data controller to re-identify individuals, then the CSA would need to comply with the data protection principles at the point of disclosure, even if, once disclosed, the data would not be personal data in the hands of a third party. Cranston J in *Department of Health* went on, however, to consider Lord Hope's reasoning in the light of the order that Lord Hope proposed, and the Supreme Court made, in that case and concluded as follows in the paragraphs relied on by *DSG* in this case (again, we add emphasis):

> "51. In my view, **the only interpretation open of Lord Hope's order is that it recognised that although the Agency 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. All members of the House of Lords agreed with Lord Hope's order demonstrating, in my view, their shared understanding that anonymised data which does not lead to the identification of a living individual does not constitute personal data**.
>
> 52. In my judgment, this conclusion maintains faith with Lord Hope's reasoning. […]
>
> 53. Secondly, the conclusion reflects the legal backdrop to the definition of personal data in the DPA, which is recital 26 of Directive, with the ambit of protection drawn in the third part of the recital so as not to apply to data rendered anonymous in such a way that the data subject is no longer identifiable…
>
> 54. Finally, any other conclusion seems to me to be divorced from reality. The Department of Health's interpretation is that any statistical information derived from reporting forms or patient records constitutes personal data. If that were the case, any publication would amount to the processing of sensitive personal data. That would be so notwithstanding the statistical exemption in Section 33, since that exemption does not exclude the requirement to satisfy Schedule 3 of the DPA. Thus, the statistic that 100,000 women had an abortion in a particular year would constitute personal data about each of those women, provided that the body that publishes this statistic has access to information which would enable it to identify each of them. That is not a sensible result and would seriously inhibit the ability of healthcare organisations and other bodies to publish medical statistics."

81. Cranston J went on to hold that it had been open to the Tribunal to conclude that disclosure of the statistics requested in that case would not constitute a disclosure of personal data as they had been "fully anonymised". Cranston J thus ultimately arrived at the same conclusion about the relevant legal principles as the Upper Tribunal did in *APPGER*, albeit by a different route.

82. In the present appeal, DSG also relies on the Information Commissioner's Anonymisation Code of Practice (ACOP) which restates the principles from the above cases as follows:

> "There is clear legal authority for the view that where an organisation converts personal data into an anonymised form and discloses it, this will not amount to a disclosure of personal data. This is the case even though the organisation disclosing the data still holds the data that would allow re-identification to take place. This means that the DPA no longer applies to the disclosed data …"

83. The parties also referred us to two decisions of the European Courts which take a consistent approach to the domestic jurisprudence.

84. First, T-557/20 *Single Resolution Board v European Data Protection Supervisor* ("*SRB*"). This case concerned personal data held by the Single Resolution Board ("SRB") consisting of comments from shareholders of Banco Popular about whether they should receive compensation under a resolution scheme. The SRB pseudonymised the data by giving each comment a unique alphanumeric code and then sent the comments to a third party (Deloitte). Five shareholders complained, asserting that as this was what we have categorised above as "limb (ii)" personal data SRB had acted unlawfully (paragraph 81). The General Court disagreed holding (at paragraphs 97 - 98) that it did not matter that the data was still personal data in the hands of SRB (on a limb (ii) basis), as it was not personal data in the hands of Deloitte (on a limb (iii) basis), there had been no unlawful disclosure.

85. Secondly, C-319/22 *Gesamthverband Autoteile-Handel eV v Scania* ("*Scania*"). This case was primarily concerned with compliance with a European Regulation on the approval and market surveillance of motor vehicles, but it included an issue about personal data. The personal data issue concerned the provision of vehicle identification numbers ("VIN") by vehicle manufacturers to vehicle repairers (paragraph 17). The VIN is an alphanumeric code assigned to a vehicle by the manufacturer to ensure proper identification of every vehicle. It is not the same thing as the vehicle registration number (paragraph 8). The Court of Justice examined whether the VIN fell within the concept of "personal data" in article 4(1) of the GDPR, concluding:

> "45 That definition is applicable where, by reason of its content, purpose and effect, the information in question is linked to a particular natural person (judgment of 8 December 2022, *Inspektor v Inspektorata kam Visshia sadeben savet* (Purposes of the processing of personal data – Criminal investigation), C-180/21, EU:C:2022:967, paragraph 70). In order to determine whether a natural person is identifiable, directly or indirectly, account should be taken of all the means likely reasonably to be used either by the controller, within the meaning of Article 4(7) of the GDPR, or by any other person, to identify that person, without, however, requiring that all the information enabling that person to be identified should be in the hands of a single entity (see, to that effect, judgment of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraphs 42 and 43).
>
> 46 As the Advocate General observed in points 34 and 39 of his Opinion, a datum such as the VIN – which is defined by Article 2(2) of Regulation No 19/2011 as an alphanumeric code assigned to the vehicle by its manufacturer in order to ensure that the vehicle is properly identified and which, as such, is not 'personal' – becomes personal as regards someone who reasonably has means enabling that datum to be associated with a specific person.
>
> 47 It follows from point II.5 of Annex I to Directive 1999/37 that the VIN must appear on the registration certificate for a vehicle, as must the name and address of the holder of that certificate. In addition, under points II.5

> and II.6 of that annex, a natural person may be designated in that certificate as the owner of the vehicle, or as a person who can use the vehicle on a legal basis other than that of owner.
>
> 48 In those circumstances, the VIN constitutes personal data, within the meaning of Article 4(1) of the GDPR, of the natural person referred to in that certificate, in so far as the person who has access to it may have means enabling him to use it to identify the owner of the vehicle to which it relates or the person who may use that vehicle on a legal basis other than that of owner.
>
> 49 As the Advocate General observed in points 34 and 41 of his Opinion, where independent operators may reasonably have at their disposal the means enabling them to link a VIN to an identified or identifiable natural person, which it is for the referring court to determine, that VIN constitutes personal data for them, within the meaning of Article 4(1) of the GDPR, and, indirectly, for the vehicle manufacturers making it available, even if the VIN is not, in itself, personal data for them, and is not personal data for them in particular where the vehicle to which the VIN has been assigned does not belong to a natural person."

Security of processing

86. We have already set out the material provisions on security of processing in the DPA 1998. Recital 46 of Directive 95/46/EC states:

> "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 it is incumbent on the Member States to ensure that controllers comply with these measures; 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;"

87. Article 17.1 of the Directive provides:

> "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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."

88. DPP7 was considered by Langstaff J in *Various Claimants v Wm Morrison Supermarkets plc* [2017] EWHC 3113 (QB), [2019] QB 772 ("*Morrisons*"). (The further appeals to the Court of Appeal and the Supreme Court in that case were focused on other issues.) An internal auditor employed by the defendant

company had copied personal information relating to its employees and had published them on a file-sharing website to which links were published on the internet. Amongst the claims brought by data subjects, it was alleged that Morrisons had breached its duties under the DPA 1998. Langstaff J held that the short answer in relation to the other data protection principles that were relied upon was that the acts in question were those of a third party (the internal auditor) rather than those of Morrisons (paragraph 65). However, he explained that DPP7 stood apart from the first, second and third data protection principles, in that Morrisons was undoubtedly the data controller in respect of the relevant information at the time when the duty fell to be discharged. If appropriate technical and organisational measures ("ATOMS") were not taken by Morrisons against unauthorised or unlawful processing of personal data then, provided the claimants could show that the breach of duty had caused the disclosure that was central to their complaints, liability would be made out (paragraph 71).

89. At paragraph 68 Langstaff J made some observations on the nature of the DPP7 duty:

> "The seventh principle does not impose a duty to take "reasonable care" as such. Those words do not appear in the statute. This might suggest that the draftsman was aiming at a rather different target when he required that "appropriate" measures be taken. The word comes from the Directive: it is likely therefore to bear an autonomous meaning, which will apply in each member state of the European Union…to whom it is addressed. However, it is clear that the principle is a qualified one. The mere fact of disclosure or loss of data is not sufficient for there to be a breach. Rather, "appropriate" sets a minimum standard as to the security which is to be achieved. This is expressly subject to both the state of the technological development and the cost of measures. Thus the fact that a degree of security may technologically be achievable, which has not been implemented, does not of itself amount to a failure to reach an appropriate standard…the following words in DPP7 indicate that a balance has to be struck between the significance of the cost of preventative measures and the significance of the harm that might arise if they are not taken."

90. In that case there was no dispute that the exfiltrated data was personal data both in the hands of Morrisons and when it was released, given the personal information that was included. We were told by counsel that there has been no authority so far on the meaning of "personal data" in the context of DPP7.

Relevant principle of judicial decision-making

91. The grounds of appeal in this case require us also to consider issues of procedural fairness and judicial notice, as to which we have directed ourselves as follows.

92. As to procedural fairness, it is well established, as Lord Mustill put it in *Re D* [1996] AC 593 at 603:

> "it is a first principle of fairness that each party to a judicial process shall have an opportunity to answer by evidence and argument any adverse material which the tribunal may take into account when forming its opinion."

93. As to judicial notice, in *Scott v Attorney General* [2017] UKPC 15 ("*Scott*") the Privy Council held:

> "40. Judicial notice is the acceptance by the courts of facts or a state of affairs which are so notorious, or so clearly established, that evidence of their existence is deemed unnecessary. As Cross and Tapper on Evidence 12th ed (2010), p 76 state:
>
> > "Judicial notice refers to facts which a judge can be called upon to receive and to act upon either from his general knowledge of them, or from inquiries to be made by himself for his own information from sources to which it is proper for him to refer."
>
> 41. Moreover, the party seeking judicial notice of a fact "has the burden of convincing the judge (a) that the matter is so notorious as not to be the subject of dispute among reasonable men, or (b) the matter is capable of immediate accurate demonstration by resort to readily accessible sources of indisputable accuracy" - Morgan, Some Problems of Proof under the Anglo-American System of Litigation 36."

94. The Privy Council in that case considered it "plainly impossible" to take judicial notice of the difference in cost of living between the Bahamas and England.

Issue 1: the EMV Data Issue: the parties' submissions

The appellant's submissions

95. Mr Pitt-Payne KC submitted that the FTT had erred in focusing on the information available to DSG in determining whether appropriate security measures had been taken "against unauthorised or unlawful processing of personal data" for the purposes of DPP7. He contended that, rather than adopting a limb (ii) approach to the question of whether the EMV Data constituted "personal data", the FTT should have taken a limb (iii) approach, addressing whether this data was personal data in the hands of the third party attackers. He said that it was clear from paragraph 97 of the FTT's decision that, having concluded that at least some of the EMV Data processed by DSG was personal data in terms of the information to which it held the key, it did not go on to determine whether this data was also personal data from the attackers' perspective. Mr Pitt-Payne emphasised that both parties addressed the FTT on the basis that if the EMV Data was not personal data in itself (Issue 4, below), then the limb (iii) definition of personal data had to be met for there to be a contravention of DPP7.

96. Mr Pitt-Payne confirmed that DSG had accepted before the FTT that the EMV Data was personal data in its hands. This was not on the basis that it had the ability to combine Batch 1 and Batch 4.1 data (as the FTT apparently thought), but because it had the means to combine the EMV Data with data that it held in a secure server which had not been accessed and was not accessible by others. However, that was irrelevant to whether there had been a contravention of DPP7 as a result of the Batch 1 and Batch 4.1 data being compromised.

97. Mr Pitt-Payne's original submission to us was based on the proposition that at the point of exfiltration the third party attacker became the data controller for the purposes of the DPA 1998 definition of "personal data" and thus it was incumbent

on the FTT to determine whether their actions amounted to the processing of "personal data" in their hands, by reference to any ability on their part to identify living individuals from combining the data with other information likely to be available to them (which DSG denied the attackers were able to do). He submitted that the caselaw we have summarised at paragraphs 78 – 85 above, showed that, where it is not possible for a third party to identify one or more individuals from the information in question, that information lost its character as personal data and was not personal data vis-à-vis third parties. Mr Pitt-Payne suggested that there was no reason in principle to distinguish the FOIA case law from the present circumstances; it mattered not whether there was an intended disclosure of data or an escape of data.

98. Mr Pitt-Payne said that it was necessary to know what it was that DSG had failed to protect and what data had got out into the world in consequence, in order to determine whether there had been a failure to protect personal data. If DSG had simply failed to protect information that would be anonymous data if it was attacked and released to the outside world, then there would have been no failure to take appropriate measures against "unauthorised or unlawful processing of personal data".

99. During the course of his oral submissions, Mr Pitt-Payne refined his position. He accepted that the section 4(4) DPA 1998 duty to comply with the data protection principles, was a duty that was placed on DSG as the data controller, including in respect of DPP7. However, he said that, in order to determine whether DSG had breached its DPP7 duty, it was necessary to consider the risks that DSG was required to guard against. The relevant risk for present purposes was the risk of an "unauthorised or unlawful processing of personal data"; and whether there was a breach would therefore depend upon the kind of data that was insufficiently protected. If that data was anonymous in the hands of third parties, the sheer fact that DSG had other data that it could combine with this data to identify living individuals was irrelevant if that other data was held securely and was not at risk of being accessed by third parties.

100. Mr Pitt-Payne also advanced an argument based on the terms of paragraph 9 of Part II of Schedule 1 DPA 1998. He emphasised that, pursuant to paragraph 9, DPP7 requires protective measures that are appropriate to the harm that might result from an unauthorised or unlawful processing of personal data. Accordingly, in order to set the applicable standard and to assess whether the data controller has achieved the appropriate level of security, it is necessary to assess the prospect of an unauthorised or unlawful processing of personal data taking place. DSG's case was that it had achieved an appropriate level of protection by effectively separating the EMV Data that it held from data that was capable of identifying the cardholders. However, by focusing on a limb (ii) approach, the FTT failed to engage with this.

The respondent's submissions

101. Whilst accepting that his submissions below had been based on a limb (iii) approach, Mr Lockley sought to persuade us that the FTT had been correct in focusing upon whether the data was personal data in the hands of DSG and that in light of its finding that it was, the FTT had been right to decide that it did not need to determine whether the EMV Data would be personal data in the hands of the attackers.

102. Mr Lockley emphasised that, unlike other data protection principles, DPP7 imposes a duty to protect data which is anticipatory in nature. The duty was on DSG as the data controller and the duty would be breached if and at the point the data controller had not taken ATOMS in respect of the personal data that it held, whether or not any exfiltration of data actually occurred. Accordingly, the focus was upon the prior failure of DSG's responsibilities in relation to the personal data that it held, rather than on the data that the attackers obtained in the particular attack or what they were able to combine it with. Accordingly, he said, the duty imposed by DPP7 applied to all data that was personal data in the data controller's hands.

103. Mr Lockley noted that the "personal data" in section 4(4) DPA 1998 was clearly a reference to data that was personal data in the hands of the data controller. He submitted that it was unlikely that "personal data" meant something different when it was then used in the phrase "unauthorised or unlawful processing of personal data" in DPP7. Furthermore, the second reference to "personal data" in DPP7 ("accidental loss or destruction of, or damage to, personal data") was plainly a reference to material that was personal data in the hands of the data controller and the same phrase could not have shifted its meaning within the same data protection principle. He also stressed that the DPP7 duty to protect data was a broad one, that required the data controller to guard against a multitude of risks, not only data exfiltration, but also deletion, malicious encryption or alteration of data. The focus was not upon what a particular attacker did in a particular situation; DSG's contentions impermissibly sought to reason backwards from the attackers' actions.

104. Mr Lockley also emphasised the nature of contraventions 3 and 9. The shortcomings upheld by the FTT were of a basic and sustained nature, which in a general sense failed to protect the DSG estate. They did not directly relate to particular data, whether the EMV Data or otherwise; they allowed for access to large amounts of data and what was actually accessed showed the minimum of what was at risk.

105. Mr Lockley contended that the authorities which Mr Pitt-Payne relied upon (those we have discussed at paragraphs 78 – 85 above) were not on point. They were concerned with the fundamentally different exercise of a controlled disclosure of a known set of data, not with DPP7 which impose a duty in advance of any attack or other release of data. Furthermore, these judgments recognised that pseudonymised data remained personal data in the hands of the data controller as it held the key to the identification of data subjects, even though at the moment of disclosure the anonymised information lost its character as personal data in terms of third parties.

106. Mr Lockley accepted that the FTT had not made findings as to whether the attackers could have combined the EMV Data with identifying data in respect of living individuals, but for the reasons we have summarised, he maintained that it was not required to make findings on a limb (iii) basis.

Issue 1: the EMV Data Issue: discussion and conclusions

107. As we have explained at paragraph 40 above, Issue 1 is solely concerned with whether the EMV Data (the 16-digit PAN, plus the expiry date on the 5,592,349 payment cards that had EMV protection) is "personal data" for the purposes of

DPP7. Mr Pitt-Payne confirmed that it was accepted that the non-financial data that was exfiltrated and the 8,628 instances where the attackers had obtained the cardholder's name as well as the PAN and the card expiry date did involve personal data (paragraph 40 above). As we understand it, the EMV Data was the focus of both parties' submissions below, because the ICO had been particularly concerned about the degree of access that was obtained to payment data and this had been a significant factor in the decision to issue the MPN (albeit the ICO did so on a limb (i) basis as we explained at paragraph 11 above). The EMV Data Issue is also relevant because the nature and extent of any contravention of DPP7 may be significant in deciding whether the section 55A DPA 1998 criteria is met and, if it is, to the consideration of whether to issue a MPN and, if so, in what sum.

108. As we have noted in summarising the submissions, Mr Pitt-Payne accepted that the EMV Data was personal data in DSG's hands (albeit not on the basis found by the FTT). However, he disputes the relevance of this to the question of whether there was a contravention of DPP7 in respect of this data. The question raised by Issue 1 is whether the FTT were correct to find that the DPP7 duty to take ATOMS against "unauthorised or unlawful processing of personal data" refers to data that was personal data in the hands of DSG (the limb (ii) definition) or whether this refers to data that would be personal data in the hands of potential third party attackers, either because the data itself is personal data or by virtue of their ability to link it with data that would identify the individuals whose payment card data had been obtained (the limb (i) and limb (iii) definitions). The FTT concluded at paragraph 97 of its decision that the limb (ii) definition was "much more obviously appropriate and applicable" and that in the circumstances it was not required to make findings in respect of the limb (i) or limb (iii) definitions.

The statutory provisions

109. Although this appeared to be in issue during the earlier part of his submissions, Mr Pitt-Payne subsequently clarified that he accepted that as regards DPP7, the section 4(4) DPA 1998 duty to comply with the data protection principles is placed on the data controller in respect of all data that is personal data in their hands. He was right to do so. This is clear from the statutory wording and it is reinforced by the terms of recital 46 and article 17.1 of the Directive and by Langstaff J's judgment in *Morrisons* (paragraphs 86 – 90 above). Accordingly, it follows that DSG was subject to the DPP7 duty at all material times and that it applied to all the data that was personal data in its hands.

110. It is clear from the statutory language that the duty is an anticipatory one. The obligation is to take precautionary steps, ATOMS, to guard against the risks that are referred to in DPP7, namely the risk of unauthorised or unlawful processing of personal data and the risk of accidental loss or destruction of, or damage to, personal data. The duty will be breached if the appropriate measures are not taken, whether or not these eventualities materialise and, indeed, if they do, the breach will have occurred prior to that time. Our understanding in this regard is reinforced by the language of paragraph 9 of Part II of Schedule 1 DPA 1998, which identifies the standard of security measures to be taken by reference to (amongst other factors) "the harm that might result" from the eventualities specified in DPP7. The position is, again, reinforced by the terms of the Directive; recital 46 refers to ATOMS that are to be taken "to prevent any unauthorized

processing" and article 17 to ATOMS that the controller must implement "to protect personal data against.[…]".

111. Accordingly, whether a contravention has occurred is to be determined by reference to whether the appropriate precautionary steps have been taken, not just by reference to what (if any) third party attack occurred in practice, albeit that may well be good evidence of an antecedent failure to take ATOMS. Applying that approach to the present case, the correct focus is upon the extent to which DSG failed to take appropriate steps to guard against the risks specified in DPP7, not simply upon what the attackers managed to achieve in the particular attack that took place upon DSG's data.

112. However, the fact that the DPP7 duty lies on the data controller and is an anticipatory one does not of itself answer the question we have to resolve as to the meaning of "personal data" in the context we have identified. As Mr Pitt-Payne emphasised in the refined version of his submission, 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). DSG was subject to the DPP7 duty in respect of all of the personal data that it held. However, in order to decide whether DSG breached that duty, it is necessary to determine whether it failed to take ATOMS to guard against a specified risk. 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.

113. We will take a hypothetical example which Mr Pitt-Payne raised in submissions in order to illustrate this point. As it accepts, DSG held information that was personal data; in relation to the EMV Data, it held information within its estate as to cardholders' identity. It was therefore obliged to take appropriate steps to protect the security of this personal data. However, if the only data that was accessible as a result of its security failings was vanilla data in data protection terms, for example, financial data relating to the performance of the company and none of the data that it held relating to identifiable individuals could be accessed, then there would be no contravention of DPP7, as in that scenario no personal data was put at risk of exposure. The sheer fact that the data controller also held personal data in another part of its estate that would make the data at risk of exposure limb (ii) personal data would be irrelevant. However, if data that became accessible as a result of security failings included material about identifiable living individuals (i.e. limb (i) personal data in anybody's hands) or material that enabled their identification when combined with other available information (limb (iii) personal data), then DSG would have failed to guard against the risk that DPP7 required it to protect against.

114. In other words, we conclude that it is not possible to know whether the data controller has failed to take ATOMS against "unauthorised or unlawful processing of personal data" without ascertaining whether personal data has been put at risk of exposure by the absence of those measures. 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". To take an example from a very different context, which does not provide a precise analogy, but serves to illustrate the point: if a householder goes out to work leaving the front door of their house unlocked, for DPP7 purposes, the failure to lock the door would not amount to a breach in itself, it would depend on the risks that this gave rise to, specifically upon what a potential intruder would be able to access if they took advantage of the unlocked door.

115. We do not accept Mr Lockley's suggestion that an alternative interpretation can be applied because DSG's failings were of a general kind that impacted broadly on the security of its data, rather than solely on particular sub-sets of data. For the reasons we have explained, it remains necessary to focus on the statutory wording and to determine whether the data controller has failed to take ATOMS in respect of the risks that are specified in DPP7. Whilst it does not alter the interpretation of DPP7, plainly the nature and scale of the failings are likely to be relevant to whether the duty has been complied with. We also observe that Mr Lockley's suggestion about the nature of DSG's failings is not rooted in the FTT's findings of fact in this case: the FTT has not made any finding about whether DSG's failings had exposed to risk not just the data it identified as Batch 1, Batch 4.1 and 4.2 (etc.), but also the other data held by DSG that it considered could be combined with that data in order to make it personal data on a limb (ii) basis (and thus which could if released render the data limb (iii) personal data in the hands of any third party).

116. This interpretation is reinforced by the terms of paragraph 9 of Part II of Schedule 1, which, as we have explained, informs the question of what is an "appropriate" measure for the data controller to take. Amongst other things, paragraph 9 requires that the measures must ensure a level of security appropriate to "the harm that might result from such unauthorised or unlawful processing…as are mentioned in the seventh principle" (emphasis added). In order to understand the harm that might result from the unauthorised or unlawful processing of personal data and thus the standard of security that is required, it is necessary to understand the data that stands to be exposed if such steps are not taken. Again, the fact that the data controller holds what amounts to personal data in its hands is only pertinent if that data is at risk of being exposed.

117. Contrary to Mr Lockley's submission, we do not consider that this interpretation is precluded or counter-indicated by the terms of section 4(4) or that it gives rise to problematic internal inconsistency within DPP7. As to the former, as we have explained, we accept that the DPP7 duty lies on the data controller in respect of all of the personal data that it holds. As to the latter, DPP7 imposes an obligation on the data controller to take appropriate steps to guard against two different kinds of risk. The first risk it covers is the one we have just discussed, namely the risk of third parties undertaking unauthorised or unlawful processing of personal data. However, the data controller is also required to take appropriate steps to guard against the distinct risk of "accidental loss or destruction of, or damage to, personal data". In this scenario, the risk to be guarded against is the inadvertent actions of the data controller, who accidently loses, damages or destroys personal data whilst it is in its possession. Accordingly, for the purposes of this

risk, the reference to "personal data" is inevitably a reference to data that amounts to personal data in the data controller's hands.

118. We consider that our interpretation of "personal data" in DPP7 is also supported by the terms of the Directive. Article 17.1 requires Member States to provide that data controllers implement ATOMS to protect personal data against a number of specified risks, including the risk of "all other unlawful forms of processing". Consistent with the caselaw that we return to below, in order to decide whether there is a risk of unlawful processing by a third party it is necessary to know whether the data in question would be personal data in their hands.

The case law

119. Our interpretation is also consistent with the domestic and European authorities that we have discussed at paragraphs 78 – 85 above. For the avoidance of doubt, we do not accept that this caselaw is determinative of the construction of DPP7 in the way that Mr Pitt-Payne initially suggested. We accept that there cannot be a direct read across; the context was different as we emphasise below. None of these cases were concerned with DPP7 or with analogous provisions. All of these cases involved a controlled disclosure of a known data set to identified third parties.

120. The domestic authorities (*APPGER*, *Department of Health* and *Miller*) were concerned with FOIA and whether requests for disclosure of specific data could be resisted on the section 40 ground that the data in question constituted "personal data". Unsurprisingly, in a context where data had been anonymised to all but the data controller, the courts determined that the question of whether the requested information amounted to "personal data" had to be looked at from the recipient's perspective (limb (iii)) and, as it could not lead to recipients identifying living individuals, it was not personal data from the point of disclosure (paragraphs 78 – 81 above). The alternative interpretation that the data was "personal data" for these purposes simply because the data controller alone retained the means of identification would have very substantially restricted the FOIA disclosure provisions; and was described by the Upper Tribunal at paragraph 128 in *APPGER* as "absurd" (paragraph 78 above).

121. The European cases were concerned with the legality of disclosing particular information to particular third parties. *SRB* was concerned with an alleged infringement of article 15 of Regulation 2018/1725 in that the complainants had not been informed that their personal data might be disclosed to Deloitte. Accordingly, the focus was again on whether the data was anonymised from Deloitte's perspective; the General Court holding that "it is necessary to put oneself in Deloitte's position in order to determine whether the information transmitted to it relates to 'identifiable persons'" (paragraph 97). *Scania* was concerned with whether vehicle manufacturers were legally obliged to disclose certain information, including VINs, to independent operators; whether this material amounted to "personal data" within the meaning of GDPR was to be assessed by reference to the means of identification reasonably available to the independent operators.

122. As our above reasoning indicates, our focus has been on the terms of the relevant DPA 1998 provisions, read in the light of the Directive. However, the domestic and European caselaw is significant for a number of inter-related reasons. Firstly,

these authorities establish 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. Secondly, the cases show 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. (Whilst the terms of recital 26 of the Directive contemplate account being taken of the means of identification available to the controller and to other persons, this does not mean, as Mr Lockley suggested, that both perspectives are taken into account in every instance; it will depend upon the context.) Thirdly, the authorities indicate 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".

123. 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 FTT's reasoning and the FTT's error

124. Having set out what we consider to be the correct interpretation of DPP7, we can address quite briefly the FTT's reasons for concluding that for the purposes of determining whether DSG failed to take ATOMS against unauthorised or unlawful processing of personal data, it should take a limb (ii) approach, simply considering whether the data held by DSG amounted to personal data. At paragraphs 93c and 95 of its decision, the FTT emphasised that the DPP7 duty was imposed on DSG as the data controller in respect of the personal data that it held. As our reasoning indicates, we agree with this point. However, as we have explained, this simply indicates where the duty lies; interpreting the nature of the risk that is to be guarded against is a separate question. At paragraph 93d of its decision, the FTT pointed out that the meaning of "personal data" in DPP7 is not limited by the same contextual considerations that applied in the FOIA cases. Again, we agree that the contextual considerations are not the same. Nonetheless, we have explained why we consider that this caselaw is instructive. The point made in the opening sentence of the FTT's paragraph 94 overlooks the fact that DPP7 requires the data controller to protect against particular, specified risks. Furthermore, we see nothing inconsistent or surprising in the proposition that there would be no contravention of DPP7 if a data controller's security failing only enabled third parties to access anonymised data from which individuals could not be identified and that the data that it held which would enable identification to take place remained securely protected. The remainder of this part of the FTT's decision (particularly paragraphs 93e, 93f and 94) simply focused upon the wrong question, namely whether the limb (ii) test was made out on the facts.

125. The FTT did not address the majority of points that we have relied upon in arriving at our conclusion as to the correct interpretation of "personal data" in this context. Given the complexity of the law in this area, it is pertinent to observe that it was unfortunate that the FTT went off on a tangent of its own, when neither party had asked them to adopt a limb (ii) approach and they had not invited or heard submissions on this point.

126. As we have already indicated, in light of its decision that it should apply a limb (ii) approach, the FTT did not make any findings as to whether the security shortcomings that it had upheld (contraventions 3 and 9) entailed a failure to take ATOMS against unauthorised or unlawful processing of data that constituted personal data (limb (i)) or data that would identify a living individual when combined with other information in the possession of or likely reasonably to be in the possession of third parties (limb (iii)). In short, the FTT failed to make relevant findings as to the consequence of the shortcomings that it had identified. The sheer fact that DSG held personal data did not resolve this question. DSG's case was that neither the limb (i) nor the limb (iii) definitions were met in this instance. We address limb (i) under Issue 4. As regards limb (iii), as explained to us, DSG's case was that the security failings that were upheld in respect of contraventions 3 and 9 did not give rise to any risk of third party attackers obtaining personal data in respect of the EMV Data, as the information that would have enabled identification of the cardholders was held in an inaccessible secure storage area; and although the FTT appears to have found at paragraphs 93f and 94 that DSG could link Batch 1 and Batch 4.1 data (a proposition that DSG disputes), this could not have been done by third parties. Accordingly, the FTT needed to make findings on these relevant, disputed matters.

127. In the interests of clarity, we re-emphasise that the issues we have identified in the previous paragraph are to be answered by reference to the risks that shortcomings in security gave rise to, not simply by reference to what actually happened in the attack. This will involve consideration of what a motivated attacker could and could not have obtained data-wise from the DSG estate as a result of the shortcomings. The FTT's decision has not addressed this.

128. We also note for completeness that in finding that there was a contravention, the FTT did not apply paragraph 9 of Part II of Schedule 1 to determine what was the appropriate level of security required. In turn, this would have involved the FTT in making findings as to the harm that might result from unauthorised or unlawful processing of personal data, understood in the sense that we have referred to in the previous paragraph.

129. Accordingly, the FTT's decision involved a material error of law in deciding that there had been a contravention of the DPA 1998 in relation to the EMV Data without determining whether that data would be personal data in the hands of third parties who could access all the data put at risk by DSG's failings.

Issue 2: the Consistency Issue: the parties' submissions

The appellant's submissions

130. Mr Pitt-Payne submitted that the grant of permission included the points raised at paragraphs 19(3) and (4) of the grounds of appeal (now Issue 2). He emphasised that they were part of the Ground 1 complaint that the FTT had not determined

whether the EMV Data would be personal data in the hands of third parties and that there was nothing in the grant of permission in respect of Ground 1 that clearly excluded these contentions. Furthermore, in so far as there was any ambiguity, it was to be resolved in the appellant's favour. The Upper Tribunal's clarification ruling could have said that these points were not within the grant of permission if that was unambiguously the case, but it did not do so.

131. As to the substance of Issue 2, Mr Pitt-Payne contended that the FTT made two errors, even on its own approach to the personal data issue. Firstly, having accepted in paragraph 96 of its decision that when assessing the risk of consequential damage and distress, it was relevant to know whether data that constituted personal data in the hands of a data controller, was personal data or only vanilla data in the hands of a third party who unlawfully processed it, the FTT then failed to make this assessment altogether in respect of the EMV Data. Secondly, having expressly stated in paragraph 97 that it had not gone on to consider whether the limb (iii) definition of personal data applied to the EMV Data, when it came to assessing whether the section 55A criteria was met and the quantum of the MPN, either the FTT proceeded on the basis that some degree of indirect linkage by third parties was possible or it wrongly and irrelevantly confined its assessment at these stages too to the fact that, as DSG could link the data, it was personal data in its hands.

The respondent's submissions

132. Mr Lockley did not accept that the grant of permission included the points raised in paragraphs 19(3) and (4) of the grounds of appeal. He said that the terms of the Upper Tribunal's order specifically limited the permission in respect of Grounds 1 and 3 "as identified and explained below". This was reinforced by the terms of paragraph 1 of the Reasons. The body of the reasons made no reference to the paragraph 19(3) and (4) points. He also contended that for the grant of permission to embrace these points would be inconsistent with the refusal of permission on Ground 4, which concerned the FTT's "substantial distress" finding, as one of the points raised under this ground was that the FTT had erred in assuming for these purposes that the attackers could link records of personal information to the EMV Data.

133. In terms of the substantive dispute, Mr Lockley said that the FTT had sufficient material from its other findings in relation to the non-financial data, to be satisfied that the section 55A criteria was met, so that the alleged error was not material. He also suggested that at paragraph 113 of its decision, the FTT did make a "very tentative" finding that the third party attackers would be able to link records of personal data with the EMV Data. As regards quantum, he reminded us that there was no live ground of appeal in respect of the figure determined by the FTT.

Issue 2: the Consistency Issue: discussion and conclusions

134. The parties approached Issue 2 on the basis that it only arose if DSG failed on Issue 1, since success on Issue 1 would in any event lead to the setting aside of the FTT's finding that the EMV Data was personal data for the purposes of the alleged DPP7 contravention. Whilst we agree that, technically, this is the case, we have decided to address Issue 2 briefly, as it may assist the FTT on remission.

Scope of the grant of permission

135. First, we are satisfied that the points raised by Issue 2 are within the scope of the grant of permission. Consistent with the earlier caselaw, any ambiguity in the grant has to be resolved in favour of the applicant (paragraph 55 above). The points raised by paragraphs 19(3) and (4) of the Grounds of Appeal were part of Ground 1, they were not explicitly excluded from the grant and they were closely allied to what we are referring to as Issues 1 and 3, in respect of which permission was clearly given. When asked to clarify his ruling, Judge Wright did not consider that his grant of permission had unambiguously excluded these points and, to the contrary, suggested that the ICO was seeking to read a great deal into particular words that he had used during the course of the 39 paragraphs of his reasons.

136. Lastly, we do not consider that treating the grant of permission as encompassing these points gives rise to any inconsistency. Paragraphs 19(3) and (4) were, like the rest of Ground 1, focused on the FTT's failure to consider the alleged breach of DPP7 in respect of the EMV Data on a limb (i) or limb (iii) basis. Whilst one aspect of paragraph 19(4) referred to the FTT's reasoning at paragraph 113 of its decision on the "substantial distress" criterion, this was in the context of highlighting the Issue 1 error. The complaint in question under Ground 4 was that the FTT had erred in assuming that the attackers could link the EMV Data to personal cardholders' information. By contrast, the complaint at paragraph 19(4) of the grounds was put on the basis that at paragraph 113 the FTT was referring to the irrelevant fact of DSG's ability to link the information.

The FTT's errors

137. The first error that DSG relies upon is readily apparent from paragraphs 96 and 97 of the FTT's decision. On the one hand, the FTT said that it was unnecessary for it to determine whether EMV Data was personal data in a limb (i) or limb (iii) sense; at the same time it acknowledged that whether or not the data was "personal data" in the hands of the third party "must be relevant to any assessment of the risk of consequent damage and distress". Accordingly, there is a clear contradiction between the FTT's reasoning in these paragraphs.

138. We accept that this was a material error. We have already explained under Issue 1 why this determination was directly relevant to whether there had been a breach of DPP7 in respect of the EMV Data. We accept that it was also relevant to whether the section 55A criteria was satisfied, in particular as to whether there had been a "serious contravention" of section 4(4) by DSG and, if so, whether it was "of a kind likely to cause substantial damage or substantial distress". Whilst the FTT was in any event able to rely on its findings in respect of the non-financial data and the personal data obtained from the 8,628 cards (paragraphs 21 - 22 above), given the nature of the EMV Data, the very large number of payment cards involved and the ICO's emphasis upon this aspect, proper findings in respect of the EMV Data were required.

139. Mr Lockley sought to argue rather faintly that the FTT did in fact make some assessment as to the likelihood of third parties being able to combine the EMV Data with identifying details of the cardholders. However, we consider it clear that this was not addressed by the FTT. First, the FTT said itself at paragraph 97 that it had not made findings to this effect. Secondly, it is apparent that paragraphs 93f, 94 and 95 are solely focused upon whether DSG as the data controller was

able to combine the data in this way. Thirdly, there are no findings of fact or reasoning that address a limb (iii) analysis. Fourthly, whilst we agree that it was not directly relevant to the "substantial distress" issue, it is apparent that at paragraph 113 of its decision, the FTT placed significance upon DSG's ability to link its records of personal data with the EMV Data (rather than to a third party's ability to do so), as the FTT introduced this point by saying, "As previously stated…". That can only be a reference to its earlier limb (ii) conclusions at paragraphs 92 – 97.

140. We take the same view in relation to the FTT's reference at paragraph 111(b) of its decision. When considering if the contravention was "serious", the FTT said that it had regard to the EMV Data being "capable of being used to indirectly identify a living individual". The FTT introduced this paragraph by referring back to the contravention of DPP7 that it had "identified", thereby tethering its conclusion on the seriousness issue to its earlier finding that DSG was able to combine the EMV Data with personal records that it held (limb (ii)). Again, we do not see why the fact that the data controller was able to combine the data impacted on the seriousness of the failure to protect against unauthorised access by third parties. The data controller was able to do so, absent any DPP7 failings at all. The real question was whether personal data was put at risk of escaping as a result of the shortcomings identified.

141. Lastly, a similar error is apparent from paragraph 120 of its reasons, when the FTT came to consider quantum. It relied upon its earlier finding on seriousness "for reasons already given relating to the nature and volume of data processed by DSG". Accordingly, our previous comment applies.

142. We therefore conclude that the FTT's central error of law in respect of Issue 1 was compounded by the errors that we have accepted in respect of Issue 2.

Issue 3: the Procedural Fairness Issue

143. We can refer to this issue very briefly, since the parties were agreed that it only arose if we concluded that the FTT was correct in adopting a limb (ii) approach to the ability to combine the EMV Data with data that identified the cardholders. We have explained under Issue 1 why that was an error of law.

144. This part of Ground 1 was based on the proposition that it was unfair of the FTT to adopt the limb (ii) approach without giving the parties an indication that this was under consideration and without giving them an opportunity to address this. We have already noted that it is a fundamental principle of fairness that each party to a judicial process has an opportunity to answer by evidence and argument any adverse material which the tribunal may take into account when reaching its determination (paragraph 92 above). In this instance, contrary to that well-established principle, the parties were not made aware before receiving the FTT's decision that it was intending to take a limb (ii) approach. Although we do not need to address Ground 3 in detail, we consider it important to emphasise this.

Issue 4: the Implications Issue: the parties' submissions

The appellant's submissions

145. Mr Pitt-Payne submitted that if we were with him on Issue 1 and we accepted that the FTT erred in law in failing to assess whether the data that was put at risk of the shortcomings in security was personal data from a limb (i) or a limb (iii) perspective, then the former was a pure question of law which we should determine (whereas resolution of the limb (iii) question involved disputed evidence and further findings of facts, which inevitably would require remission to the FTT). Mr Lockley accepted that the Upper Tribunal was in a position to decide the limb (i) question.

146. Mr Pitt-Payne contended that the EMV Data (the 16 digit number on the payment card (the PAN) and the expiry date) was not personal data. The PAN simply identified an item of property. He drew an analogy with the VINs in *Scania*, which the Court of Justice concluded were not personal data in themselves; they simply identified a unique item of property, namely a motor vehicle. Similarly, a PAN links to a particular bank account, but it does not provide information that identifies a particular individual. He said that even if the EMV Data enabled a third party attacker to extract funds from the bank account (which was not accepted), this did not make it data about an identifiable individual. In this regard he observed that a cloakroom ticket enabled the person who possessed it to present it and receive an item of property in return, but the ticket contained no data that identified an individual.

147. Mr Pitt-Payne emphasised that the limb (i) definition of personal data required that the data identified a living individual directly; it was quite clear that the PAN and the expiry date on a payment card did not do so.

The respondent's submissions

148. Mr Lockley referred us to paragraph 21 of Cranston J's judgment in *Department of Health*, where he referred to Opinion 4/2007 issued by the Article 29 Working Party, in particular that "the definition of personal data should be as general as possible so as to include all information concerning an identifiable individual". He submitted that whilst a PAN did not identify an individual by name, it did identify the holder of a particular bank account (assuming that there was a sole, living individual account holder). The function of the PAN was to single out the particular bank account in order to enable the relevant economic activity to occur and, in turn, this economic activity was fundamental to a particular person's identity. It was information that was much more fundamental to a person's identity than a coat or a car. He clarified that he was not suggesting that the EMV Data would enable an attacker to gain access to the financial information relating to the particular account, but he described the PAN as a proxy for the account.

Issue 4: the Implications Issue: discussion and conclusions

149. We accept that we are in a position to determine whether the EMV Data itself (as opposed to when combined with other data) constitutes personal data. We agree that this is a question of pure law and that it will assist the FTT on remission for us to decide it.

150. We clarified with the parties that there was no inter-relationship between the digits of a PAN and the digits comprising a particular bank account number; they were simply two separate unique identifiers of an account. The PAN gave no indication of the bank account number or sort code. Counsel drew an analogy with a motor vehicle that may be identified by its VIN or by its numberplate, but these identifiers are entirely separate from each other.

151. We concluded that the EMV Data does not amount to personal data in itself. It does not identify any individual directly. It does not enable financial information relating to the usage of the particular bank account to be accessed. The PAN simply provides a link to a unique bank account. Whether the EMV Data can be combined with other data to identify a living individual is neither here nor there from a limb (i) perspective; that is (depending on context) a limb (ii) or (iii) question.

152. We do not consider that the sheer fact that the PAN is a unique number identifying a particular account alters this position. Mr Pitt-Payne's analogy with the VIN in *Scania* is an apt one. The Court of Justice indicated that the unique alphanumeric code assigned to the vehicle by its manufacturer did not in itself constitute personal data; it was only personal data in so far as the person who had access to it had the means of enabling them to use it to identify the owner of the vehicle to which it related.

153. We were not persuaded by Mr Lockley's emphasis upon the purpose of the PAN being to enable economic activity in relation to the particular bank account. Whilst such activity would undoubtedly be of importance to the holder of the account, the fact remains that the EMV Data does not identify them.

154. Accordingly, the limb (i) definition of personal data does not apply to EMV Data for the purposes of the FTT considering on remission whether, pursuant to DPP7, DSG took ATOMS against unauthorised or unlawful processing of personal data.

Issue 5: the Seriousness Issue: the parties' submissions

The appellant's submissions

155. Mr Pitt-Payne relied upon three respects in which he submitted that the FTT erred in the conclusion it reached at paragraph 111 of its decision that there had been a serious contravention by DSG of its duty to comply with the data protection principles.

156. First, he submitted that the FTT had erred in conflating the consequences of the contravention with its seriousness. He submitted that these were distinct elements and that the consequences were relevant to the next section 55A criterion, namely whether the contravention "was of a kind likely to cause substantial damage or substantial distress". He said that seriousness was a quality of the contravention; it required that the contravention reached a certain standard of gravity or degree of departure from (in this case) the level of protection that the data controller was required to provide by DPP7. However, the FTT failed to make any finding in this regard and none of the three factors referred to by the FTT in its paragraph 111 addressed the seriousness of the contravention.

157. In response to our questions, Mr Pitt-Payne acknowledged that the consequences of a contravention could have some bearing on its seriousness (contrary to his original submission). He said, however, that the FTT had failed to ask and answer the right question; it had not made any finding as to how far short of the applicable standard DSG had fallen.

158. Secondly, he submitted that it was irrelevant for the FTT to have taken into account the "expectations of individuals and society", this was not pertinent to identifying the appropriate standard or how far below it DSG had fallen. Alternatively, if this was relevant, the FTT had erred because it had no evidence before it on this matter.

159. Thirdly, he contended that the FTT erred in respect of paragraph 111(b) in taking into account that there was "an unknown quantity of PAN capable of being used to indirectly identify a living individual". We have already considered this complaint, finding that the FTT erred, when we considered Issue 2 and so we do not need to address this further.

The respondent's submissions

160. Mr Lockley submitted that seriousness was a broad concept which did encompass the consequences of a contravention; the factors relevant to subsections (1)(a) and (1)(b) in section 55A overlapped. He contended that the FTT had made relevant findings as to the seriousness of the contravention, when it explained why it upheld contraventions 3 and 9 at paragraph 110(g) – (n) of its decision and that it was clear from those findings that it considered that DSG had fallen significantly below the expected standard. He also reminded us that we must focus on the substance of the FTT's reasoning, reading its decision as a whole, rather than considering paragraph 111 in isolation.

161. As regards the second alleged error, Mr Lockley contended that the expectations that were referred to were capable of being a relevant factor. He argued that the FTT did not require evidence on this point; it was a matter of commonsense and as a specialist tribunal it was fully entitled to take notice of this; the circumstances were very different to those in *Scott* which concerned a numerical matter on which specific evidence was required. Further or alternatively, he submitted that if this was an error on the part of the FTT, it was not a material error.

Issue 5: the Seriousness Issue: discussion and conclusions

162. In light of our conclusions on Issue 1, it follows that the FTT's conclusion on seriousness cannot stand in any event. However, we consider that it is likely to assist the FTT on remission if we address the Issue 5 points (in so far as we have not already addressed them under Issue 2).

163. As regards the first alleged error, we reject the proposition that the factors relevant to the seriousness of the contravention are entirely distinct from those that relate to whether the contravention was likely to cause substantial damage or substantial distress. Such an approach would be highly artificial. Seriousness is a broad concept and we see no reason why it cannot include the extent of the likely consequence of the failing. As we have already discussed, paragraph 9 of Part II of Schedule 1 indicates in terms that the consequences of an unauthorised or unlawful processing of personal data ("the harm that might result") are relevant to the applicable standard of security and thus, in turn, to whether there has been

a contravention. It would be illogical to then exclude consideration of the potential consequences from an assessment of the seriousness of that contravention.

164. Mr Lockley accepted during his submissions that an assessment of the seriousness of the contravention did require the FTT to determine how far DSG's contravention had fallen below the appropriate standard. We agree; this is inherent in the concept of a "serious" contravention.

165. Mr Lockley also accepted that there was no specific passage that he could point to in the FTT's decision where it had addressed the applicable standard or addressed how far below it DSG had fallen. We have considered the decision as a whole and it does not appear to us that these matters were addressed. We do not know how far the FTT thought that DSG had fallen below the applicable standard.

166. Whilst we have considered it carefully, we are not persuaded that the FTT addressed the seriousness of the contravention at any point within the contents of paragraph 110 of its decision, where it explained why it had found that there was a contravention of DPP7 (by virtue of contraventions 3 and 9).

167. The need for a distinct finding as to the seriousness of the contravention is underscored by the statutory scheme. As we have explained at paragraph 64 above, an enforcement notice may be served by the ICO in respect of a contravention that has caused or is likely to cause damage or distress; and pursuant to section 13 DPA 1998, an individual who suffers damage or distress by reason of a contravention may make a claim. Unlike section 55A, neither of these provisions requires there to have been a "serious" contravention of the section 4(4) duty to comply with the data protection principles. Accordingly, it is not appropriate to simply elide the question of whether there has been a "contravention" and, if so, whether it is a "serious" one.

168. The proposition that the FTT failed to address how far DSG's contravention had fallen below the applicable standard is also reinforced by the structure of the FTT's decision: after concluding at paragraph 110 that there had been a contravention, at paragraph 111 the FTT proceeded to consider the section 55A(1)(a) criterion, then at paragraphs 112 – 113 it addressed the section 55A(1)(b) criterion and at paragraph 114 the section 55A(3) criterion. Thus, although we have considered the decision as a whole, it is reasonable to infer that the FTT identified at paragraph 111 those matters that it considered relevant to its determination of whether the contravention was "serious". As we have already observed, there is no reference here to the FTT either asking or answering how far DSG had departed from the applicable standard.

169. We therefore conclude that the FTT erred in law in this respect as section 55A(1)(a) DPA 1998 required it to make this assessment.

170. We are not persuaded that there is force in Mr Pitt-Payne's second criticism. Whilst it appears to us to be peripheral, rather than central, to the determination of seriousness that the FTT had to make, we do not consider that the reasonable expectations of individuals and society that a body of personal data of this nature would be adequately protected is wholly irrelevant to the seriousness of the contravention. Furthermore, this is not a matter that would easily lend itself to specific evidence (unlike the respective costs of living in *Scott*). It is, in our judgment, something which ought to be an uncontentious matter of common

sense, given that the DPA 1998 seeks to ensure adequate protection of personal data and we do not accept that the FTT erred in taking this into account.

The outcome

171. For the reasons that we have set out above, we conclude that the FTT erred in law:

    (i) In concluding that there was a contravention of s. 4(4) Data Protection Act 1998 ("**DPA 1998**") by reason of third party access to payment card data comprising only (i) primary account numbers; and (ii) expiry dates ("**EMV Data**"), on the basis that the EMV Data was personal data in the hands of DSG. EMV Data is not "personal data" in itself as it does not directly identify a living individual (Issue 4);

    (ii) In determining that DSG had failed to comply with DPP7 in respect of the EMV Data on the basis that this was "personal data" in DSG's hands, rather than deciding whether the security shortcomings that it had upheld entailed a failure to take appropriate protective measures against "unauthorised or lawful processing of personal data", which required consideration of whether the data that was rendered vulnerable would be "personal data" in the hands of third parties who could access it (Issue 1);

    (iii) In taking an inconsistent approach to whether it was necessary to determine the Issue 1 point (albeit failing to do so); and in relying on the undisputed fact that the EMV Data was "personal data" in DSG's hands, rather than a finding on the Issue 1 point, when reaching its conclusions on the section 55A DPA 1998 criteria (in particular whether there had been a "serious contravention" and, if so, whether it was "of a kind likely to cause substantial damage or substantial distress") and on the quantum of the MPN (Issue 2);

    (iv) In finding that the contravention of the section 4(4) DPA 1998 duty was "serious", without having assessed the applicable standard or how far below it DSG's conduct had fallen (Issue 5).

172. As we also explained, we accept that Issue 2 is within the scope of the grant of permission to appeal; and in light of our conclusion on Issue 1, it was unnecessary for us to determine Issue 3, albeit we have thought it right to emphasise the departure from procedural fairness that occurred.

173. On remission, the FTT will need to decide whether the EMV Data is "personal data" in the hands of those who could access it as a result of security shortcomings on the part of DSG (the limb (iii) question). In this regard, the FTT will be assisted by:

    (i) Focusing on the risk of "unauthorised or unlawful processing of personal data" that DPP7 required DSG to take ATOMS to guard against;

    (ii) Assessing the data that was put at risk as a result of those shortcomings, in particular whether the EMV Data could be linked by a motivated attacker to other data put at risk by DSG that would identify the cardholders in question. It will also be necessary to consider the extent to which, if at all, it was possible to establish the identity of the cardholders by means of externally obtained information;

(iii) Keeping in mind that as the duty on DSG is of an anticipatory, protective nature, the answers to these questions involve assessing what was put at risk as a result of security shortcomings, as opposed to simply what was obtained in the attack that took place (albeit, that is likely to be good evidence of the vulnerabilities in the system); and,

(iv) The summary of the principles to be applied when considering limb (iii) issues provided in *Miller* (paragraph 76 above).

174. We give the decision, and direct the new FTT to redecide the appeal, in the terms set out at the beginning of this decision. It was not contested before us that the non-financial data which was exfiltrated and the 8,628 payment cards without EMV protection that were accessed by the Attackers both constituted personal data, and the new FTT should redecide the appeal on this basis. Nor were the FTT's findings of fact in relation to contraventions 3 and 9 in terms of the FTT's findings about the security shortfalls identified or DSG's state of knowledge disputed before us, and the new FTT should redecide the remitted appeal accordingly (although the new FTT Tribunal will need to consider afresh to what data those shortfalls related in order to decide whether there was in fact a contravention).

175. DSG invited us to be more specific as to the errors that we have found in the FTT's decision. We have taken their submissions into account, but have considered it appropriate to summarise our findings in the way we have done in paragraph 171 above. The ICO invited us specifically to direct that the findings at paragraphs 99-110 of the FTT's decision are not challenged by DSG and should not be re-opened at a remitted hearing. We record that it is our understanding that it should not be necessary for those findings to be re-opened, but we do not make such a specific direction lest it have an unintended consequence of restricting the FTT's freedom to decide the matters that need to be decided on remission in the way it considers appropriate in the light of our judgment.

Mrs Justice Heather Williams DBE

Chamber President

Stewart Wright

Judge of the Upper Tribunal

Holly Stout

Judge of the Upper Tribunal

Approved for issue on 23 September 2024