Appeal number: EA/2020/0065/V

FIRST-TIER TRIBUNAL
GENERAL REGULATORY CHAMBER
(INFORMATION RIGHTS)

DOORSTEP DISPENSAREE LIMITED **Appellant**

- and -

THE INFORMATION COMMISSIONER

Respondent

Before:

JUDGE MOIRA MACMILLAN

Sitting remotely on 17 & 18 December 2020
Sitting in Chambers on 22 & 23 July 2021

Appearances:
Philip Coppel QC for the Appellant
Peter Lockley for the Respondent

DECISION

1 The appeal is allowed in part, in that the amount of the fine imposed by the Monetary Penalty Notice issued on 17 December 2019 is reduced to £92,000.

2 The Enforcement Notice issued on 17 December 2019 is upheld.

MODE OF HEARING

3 The hearing was convened by CVP. All parties joined remotely. The Tribunal was satisfied that it was fair and just to conduct the hearing in this way.

4 This determination was made by a Salaried Judge, sitting alone. The Tribunal was satisfied that it was appropriate to compose the panel in this way, having regard to paragraph 6(a) of the Senior President's Pilot Practice Direction dated 19 March 2020[1] and the desirability of determining all cases which are capable of determination by the most expeditious means possible during the pandemic.

5 The Tribunal held the hearing in public, within the meaning of rule 35A (3)(c) of the Chamber's Procedure Rules[2].

6 The Tribunal considered the following material:

a) An agreed electronic bundle of evidence comprising pages 1 to 1665;

ii) An additional 45 pages, consisting of the Notices under appeal;

iii) Documents produced by the Information Commissioner ('the Commissioner') during the hearing, comprising records relating to the registration of companies;

iv) Written submissions on discrete legal issues, provided by both Parties on 8 January 2021; and

---

[1] https://www.judiciary.uk/publications/pilot-practice-direction-panel-composition-in-the-first-tier-tribunal-and-the-upper-tribunal/

[2] http://www.legislation.gov.uk/uksi/2020/416/article/6/made

v) An authorities bundle comprising 348 pages.

REASONS

Background

10 Doorstep Dispensaree Limited ('DDL') is a pharmacy that operates as both a 'closed' online pharmacy and as retail pharmacy. The online pharmacy's business includes the supply of medicine to care homes.

11 In a Notice of Appeal dated 10 February 2020 DDL seeks to challenge a Monetary Penalty Notice ('MPN') imposing a fine of £275,000 and an Enforcement Notice ('EN'), both imposed on 17 December 2019. Both arise from circumstances brought to light following the execution of a search warrant by the Medicines and Healthcare Products Regulatory Agency ('MHRA') at 75 – 79 Masons Avenue, Harrow, Middlesex HA3 5AN ('the Property') on 24 July 2018.

12 The Information Commissioner was not present during the search but was contacted by the MHRA on 31 July 2018. The MHRA told the Commissioner that 47 stacked, unlocked crates had been recovered from the yard at the Property, and that these all contained personal data and special category personal data related to DDL's pharmacy business. The MHRA told the Commissioner that approximately 500,000 documents had been recovered. It described the personal data as being that of residents in care homes and as comprising names; addresses; dates of birth; NHS numbers; medical information; and details of prescriptions. Similar material was found in 2 disposal bags and in a cardboard box.

The Law

13 At the material time[3] 'GDPR' was the name commonly used to refer to Regulation (EU) 2016/679, which provides rights and protections to natural persons with regard to the processing of personal data.

14 Article 4 of GDPR provides the following definitions:

i) '*personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one*

[3] The EU GDPR was modified slightly in UK domestic law following EU Exit. Relevant sections of the Data Protection Act 2018 now refer to the 'UK GDPR', which is the modified Regulation.

or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

ii) *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

iii) *'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*

iv) *'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*

15 In addition, Article 9 prohibits the processing of 'special categories' of personal data unless certain conditions are met. One special category is data concerning health (Article 9(1)). Article 9(2)(h) provides a condition allowing processing special category personal data where it is necessary for the purposes of the provision of health or social care.

16 Chapter II of the GDPR sets out a number of Principles relating to the processing of personal data. The Principles contained in Article 5(1)(e) & (f) are that personal data shall be:

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); and

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

17 Paragraph 2, Article 5 stipulates that '*[t]he controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*'

18 Article 24 sets out further matters for which the controller is responsible. Article 24(1) & (2) create an obligation to put in place measures to ensure that data processing is performed in accordance with the Regulation:

> *1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*
>
> *2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.*

19 Article 25 requires the controller to consider and implement appropriate organisational measures, having regard to the likelihood and potential severity of risk posed by the processing, both when determining the means of processing and at the time the processing takes place.

20 Article 32 sets out requirements in relation to the security of processing. These include:

> *1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> > *(a) the pseudonymisation and encryption of personal data;*
> >
> > *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
> >
> > *(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
> >
> > *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*
>
> *2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*

21 Chapter III of the GDPR provides data subjects with various rights. Article 13 provides a right to information which the controller is required to provide to a data subject where their personal data are collected. This includes information about the identity and contact details of the controller; the purposes and legal basis for processing the data; the recipients of the personal data; the length of time for which the personal data will be stored and the existence of the right to request from the controller access to and rectification or erasure of personal data.

22 Article 14 requires the same information to be made available by the controller to the data subject as in Article 13, in circumstances where the personal data have not been collected from the data subject.

23 The Commissioner is a domestic supervisory authority for the purposes of the GDPR. Pursuant to Article 57(1) she must monitor and enforce compliance with the Regulation, and when doing so may exercise a range of powers created by Article 58. These include:

i) The power to order the controller or processor to provide information (Article 58(1)(a));

ii) The power to notify the controller or processor of an alleged infringement (Article 58(1)(d));

iii) The power to order the controller or processor to bring processing operations into compliance with the GDPR (Article 58(2)(d)); and

iv) The power to impose an administrative fine pursuant to Article 83 (Article 58(2)(i)).

24 Article 83 set out the general conditions for imposing fines. The relevant provisions are as follows:

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as

well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10000000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20000000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

25 The Data Protection Act 2018 ('DPA') implements and gives effect to the GDPR. Part 6 contains enforcement provision that are exercisable by the Commissioner.

26 S. 155 deals with the imposition of Penalty Notices. At the material time the relevant provisions were as follows:

(1) If the Commissioner is satisfied that a person –

(a) has failed or is failing as described in section 149(2), […]

the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.

(2) Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant –

(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the GDPR;

(b) to the extent that the notice concerns another matter, the matters listed in subsection (3).

(5) Schedule 16 makes further provision about penalty notices, including provision requiring the Commissioner to give a notice of intent to impose a penalty and provision about payment, variation, cancellation and enforcement.

27 The 'failings' described in s. 149(2) were, at the material time:

(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following –

(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);

(b) a provision of Articles 12 to 22 of the GDPR or Part 3 or 4 of this Act conferring rights on a data subject;

(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors);

28 S. 149 also empowers the Commissioner to issue an EN when she is satisfied that a person is failing to comply with GDPR in a manner described in s. 149(2)-(5).

29 S. 162(1) provides a person who has been given an MPN or EN with a right of appeal to the Tribunal:

162 Rights of appeal

(1) A person who is given any of the following notices may appeal to the Tribunal –

(a) an information notice;

(b) an assessment notice;

(c) an enforcement notice;

(d) a penalty notice;

(e) a penalty variation notice.

(2) […]

(3) A person who is given a penalty notice or a penalty variation notice may appeal to the Tribunal against the amount of the penalty specified in the notice, whether or not the person appeals against the notice.

(4) […]

30 The powers of the Tribunal in relation to such an appeal are set out in ss. 163(1) – (4):

163 Determination of appeals

(1) Subsections (2) to (4) apply where a person appeals to the Tribunal under section 162(1) or (3).

(2) The Tribunal may review any determination of fact on which the notice or decision against which the appeal is brought was based.

(3) If the Tribunal considers –

(a) that the notice or decision against which the appeal is brought is not in accordance with the law, or

(b) to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently,

The Tribunal must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.

(4) Otherwise, the Tribunal must dismiss the appeal.

Additional legal issues

31 In a skeleton argument served shortly before the oral hearing, DDL raised an additional legal issue relating to the applicable burden and standard of proof in these proceedings. I drew the Parties attention to the decision of the Upper Tribunal in *Hackett v HMRC* [2020] UKUT 0212 (TCC). As the Commissioner was not in a position to deal with this matter I invited the Parties to provide written submissions following the oral hearing. In closing submissions Mr Coppel raised an additional matter relating to the application of the law of agency to these proceedings. I am grateful to both Parties for their written submissions on both issues.

Burden of proof

32 Mr Coppel submits that the Commissioner bears the burden of proof in relation to both the MPN and the EN. His central argument is that an appeal against an MPN is essentially criminal in nature. He relies as authority on *Khan v HMRC* [2006] EWCA Civ 89 [59] in which the Court of Appeal decided, in the context of an appeal against both a VAT assessment decision and a penalty notice, that the burden lay on the Appellant in the former, in that he had to show that the assessment was wrong, and on HMRC in the latter.

33 In relation to the EN, Mr Coppel submits that requiring an appellant to disprove a matter in relation to which the Commissioner asserts a failure is 'an unattractive legal approach'.

34 Mr Lockley submits that the burden of proof is 'neutral'. He notes that under the DPA the Commissioner need only be 'satisfied' of relevant

matters before issuing an MPN. He submits in addition that the full merits review carried out by the Tribunal on appeal, with attendant new findings of fact, has the effect of rendering the burden of proof as being of secondary importance.

Conclusion on burden of proof

35 The Parties agree that an appeal under s. 163 gives rise to a full merits review of the decision under appeal. The language of s. 163(2) is replicated in s. 58 FOIA, in which context the relevant language was interpreted by Upper Tribunal Judge Jacobs in *Information Commissioner v Home Office* (2011) UKUT 17 (AAC):

"57. As to the function of the section, the First-tier Tribunal hears appeals under a variety of legislation. There are various formulations in different legislation, but generally they have in common that the tribunal is required to undertake a fresh consideration of the case on the evidence and arguments put to it. That is what I expect to find in the case of an initial appeal from a decision-maker in a public body, as the tribunal will give the case the first judicial consideration. It is the nature of such an appeal that there is generally no restriction on the issues, evidence or argument that the tribunal can consider. This is, of course, subject to any express or implied limitation.

58. [ ]*…the section imposes the 'in accordance with the law' test on the tribunal to decide independently and afresh. It is inherent in that task that the tribunal must consider any relevant issue put it by any of the parties...*[ ]

59. I note that under subsection (1)(a) the test is whether the Commissioner's decision notice is in accordance with the law, not whether it was. That emphasises that the test is undertaken afresh at the time of the hearing. The date as at which it has to be applied was not before me.

60. In summary, the nature of the appeal before the First-tier Tribunal requires it to consider the response that the public authority should have made afresh. It must apply the law afresh to the request taking account of the issues presented at the hearing or identified by the First-tier Tribunal."

36 Therefore, when taking a fresh decision, the Tribunal is not required to undertake a reasonableness review of the Respondent's decision, but instead must decide whether it would itself reach the same decision based on the evidence now before it. The Tribunal has no supervisory jurisdiction – see *HMRC v Abdul Noor* [2013] UKUT 071 (TCC).

37 In *R (Hope and Glory Public House Ltd v City of Westminster Magistrates' Court* [2011] EWCA Civ 31 , the Court of Appeal decided that "*careful attention*" should be paid to the reasons given by an original decision-maker, bearing

in mind that Parliament had entrusted it with making such decisions. However, the weight to be attached to the original decision when hearing an appeal is a matter of judgment for the Tribunal, "*taking into account the fullness and clarity of the reasons, the nature of the issues and the evidence given in the appeal*". The approach recommended in *Hope and Glory* was approved by the Supreme Court in *Hesham Ali (Iraq) v Secretary of State for the Home Department* [2016] 1 WLR 4799.

38 I conclude from these authorities that Mr Lockley's submission is broadly correct, in that to a limited extent the burden of proof is of secondary importance in the context of a full merits review. However, when the appeal is against a penalty imposed in response to perceived infringements, I am satisfied that there must also be an initial evidential burden imposed upon the decision maker who is required to prove that the infringement has taken place. As a matter of common sense, this evidential burden must shift to the other party once evidence of the infringements has been introduced.

Standard of proof

39 Mr Coppel submits that a different standard of proof applies in each of the notices under appeal, in that the civil standard applies to an EN appealed under s. 162(1)(c), whereas the criminal standard applies to an MPN appealed under s. 162(1)(d). The standard of proof in relation to an EN is not in dispute.

40 In relation to an MPN, Mr Coppel submits that a penalty issued under s. 155(1) has attributes and consequences consistent with it being a penal sanction for the following reasons:

i) The purpose of the monetary penalty is punishment rather than seeking compliance. This is because s. 155(1)(b) makes clear that an MPN can be imposed in addition to an information, assessment or enforcement notice. It is therefore indistinguishable from other regulatory regimes in which a fine is imposed for non-compliance with an enforcement notice.

ii) The criteria set out in s. 155(3), to which the Commissioner must have regard when determining the amount of an MPN, are akin to sentencing guidelines issued in relation to regulatory offences. Unlike other regulatory regimes, these criteria are not set by reference to offsetting any benefit obtained through non-compliance.

iii) The maximum penalties permitted by s. 157 and Article 83 marks the MPN as a punitive regime, and are non-comparable to other monetary penalty regimes.

iv) The imposition of a MPN does not affect the right of a data subject to compensation, this being the natural civil consequence of non-compliance. The financial penalty is paid into the Consolidated Revenue rather than used to compensate the data subject or to offset the cost of enforcement, which is also consistent with the imposition of a penal sanction.

v) Enforcement of the MPN is achieved using the same procedure as enforcement of a fine imposed under the Magistrates Court 1980 (ie through proceedings in the County Court or High Court).

41 Mr Coppel cites extensive authority for the proposition that, in any event, civil monetary penalties have long been classified as a penal sanction, in relation to which common law protections arise unless specifically displaced by parliament. He identifies these protections as (i) imposing the burden of proof upon the party seeking the sanction and (ii) requiring proof of a matter beyond a reasonable doubt. He submits in addition that, if the imposition of a monetary penalty is penal in nature, this implies a criminal offence within the meaning of Article 6 ECHR with consequent procedural requirements. His contention is that, as a consequence, any appeal against any monetary penalty, regardless of amount, must be viewed as a denial of a criminal offence with all attendant protections.

42 Mr Coppel submits that to approach an MPN issued under s. 155(1) as anything other than penal in nature would be to remove from the person concerned the protection of *autre fois convict*, resulting in a risk that the person concerned could be punished both an MPN and criminal prosecution in relation to the same data breach.

43 In relation to *Hackett v HMRC*, Mr Coppel points out that the Upper Tribunal followed the analysis of Mann J in *HMRC v Khawaja* [2020] EWHC 1687, in which it was recognised that there is presumption in appeals against tax penalties that a civil standard of proof will apply, but that this is only a starting point that may be departed from in circumstances where the consequences are so serious that the imposition of the criminal standard of proof is required.

44 Mr Coppel distinguishes the facts of the present case from those of *Hannam v FCA* [2014] UKUT 0233 (TCC) which was also reviewed by the Upper Tribunal in *Hackett* and used as authority for the conclusion that the civil standard applied. He submits firstly that the regime under consideration in *Hannam* is not strictly comparable since it concerns the application of a financial penalty as part of a suite of disciplinary provisions, and secondly that *Hannam* supports adoption of a variable approach to whether the

criminal standard applies based upon the facts of each case, which Mr Coppel submits risks inconsistency and uncertainty.

45 Mr Lockley's position is that the civil standard of proof applies in the context of an appeal against both the MPN and the EN. He submits as follows:

i) This Tribunal confirmed in *Scottish Border Council v Information Commissioner* [EA/2012/0212) that the civil standard of proof applies in an appeal against an MPN issued under the DPA 1998. This conclusion was reached on the basis that Parliament had intended that legislation to introduce both a civil and a criminal penalty scheme and had entrusted the former to the Commissioner, who has traditionally applied the balance of probabilities to her decisions.

ii) Further, the Tribunal does not have jurisdiction to determine its own constitution, an approach adopted in *Boost Finance Limited v Information Commissioner* (EA/2018/0235), in which the Tribunal decided that it did not have competence to determine whether the criminal standard of proof applied to proceedings before it due to the legislative and procedural schemes under which it operates.

iii) In the alternative, Mr Lockley submits that application of the principles identified by the Upper Tribunal in *Hackett v HMRC* confirms that the civil standard applies to these proceedings for the following reasons:

a. The wording of the DPA indicates a uniform civil enforcement system of MPNs in relation to which the Commissioner need only be 'satisfied' of the relevant matters. Appeals thereafter are to a civil tribunal which is empowered to 'review any determination of fact'.

b. This must be contrasted with the language of ss. 196 – 200 DPA which deals with prosecution for criminal offences, and which uses language such as 'investigation' and 'charge'.

c. The amount of the penalty imposed in this case cannot dictate that the criminal standard applies, since in both *Hackett* and *Hannam*, where the Upper Tribunal held that the civil standard applied, the quantum of the penalty was larger.

d. No deprivation of liberty or additional statutory consequences flow from the imposition of an MPN for either DDL or for Mr Budhdeo.

e. This appeal is concerned with negligent, rather than intentional, breaches of GDPR. However, both are capable of considered within a civil penalty regime, as reflected by the fact that the central issue in the case of *Hackett* was dishonesty.

Conclusion on standard of proof

46 I am not bound by the approach taken by this Tribunal in *Boost Finance Ltd* since First-tier Tribunal decisions are only binding on the parties to those proceedings. Neither am I persuaded that the First-tier Tribunal lacks jurisdiction to determine the applicable standard of proof, nor that the Tribunal's Procedure Rules are designed solely for application of the civil standard. I have reached this conclusion because not every regulatory regime with a right of appeal to the Tribunal relies upon a presumption that the civil standard of proof will apply.[4] Further, as alluded to by Mr Coppel, the Tribunal applies the criminal standard of proof when assessing whether to certify contempt to the Upper Tribunal pursuant to rule 7A in other Information Rights proceedings. I conclude accordingly that the Tribunal must be competent to determine at least the nature of the jurisdiction is has been given by Parliament.

47 Having considered both Parties' submissions, I am satisfied that the civil standard of proof applies in an appeal against an MPN brought under s. 162(1)(d) DPA for the following reasons:

i) I have reminded myself of the principles relevant to determining the applicable standard of proof as summarised by the Upper Tribunal in *Hackett*, to which the paragraphs cited below refer. In particular:

a. As identified by Lord Hoffman in *In re B (Children) (FC)* [2008] UKHL 35, there are three categories of civil cases in which it has been suggested that the standard of proof may vary according to the gravity of the misconduct alleged or the severity of the consequences, the first of which is a case classified as civil for the purposes of Article 6 but where the criminal standard should apply due to the serious consequences of the proceedings [59];

b. A number of authorities, including *McCann v Crown Court at Manchester* (2003) 1 AC 787, support the view that a serious consequence which imposes restrictions upon a person's liberty may require the criminal standard to be applied even though the

[4] See, for example, Regulation 87(2) of the Green Deal Framework (Disclosure, Acknowledgment, Redress etc.) Regulations 2012 which states that: "*The Tribunal must determine the standard of proof in any case".*

proceedings are civil in nature [60 – 61], although a deprivation of fundamental liberties is not always a necessary ingredient [76];

c. In *HMRC v Khawaja* [2008] EWHC 1687 (Ch) 2008 Mann J concluded that the civil standard of proof applied to civil penalty proceedings in the tax context having identified the existence of parallel criminal proceedings, while noting as Mr Coppel points out that this is only a starting point because, in some cases, the seriousness of the consequences or the nature of the claim is such that the criminal standard of proof is required [67];

d. The civil standard may apply in civil proceedings even when these involve allegations of civil fraud and dishonesty, and assistance in identifying the applicable standard may be found in the language of the legislation [70];

e. As determined by the Upper Tribunal in a subsequent hearing in *Khawaja,* the application of Article 6 to proceedings does not prevent the civil standard of proof from applying [74]; and

f. As found by the Upper Tribunal in *Hannam*, an allegation in relation to which a person faces an unlimited financial penalty and reputational damage but in which fundamental liberties were not at risk does not necessarily fall within Lord Hoffman's first category of cases [78].

ii) I have considered whether assistance may be found in the language of the DPA. This creates two distinct penalty regimes. The first is the s. 155(1) MPN regime, enacted in compliance with the UK's obligations under the GDPR. An appeal against an MPN is to a civil tribunal, and is brought under same statutory provisions as appeals against others. 155(1) notices, in relation to which it is agreed that the civil standard applies.

iii) The second penalty regime is framed by reference to a criminal process, set out in ss. 196 – 200. This uses the language of criminal offences, including indictable offences, of convictions before the criminal courts, the appropriate sanction for which may also be a penalty. The criminal offences created by the DPA are contained within a number of provisions. Prosecutions may be brought either by the Commissioner after 'investigation', or by or with the consent of the DPP. The behaviours to which the offences relate are described in terms of deliberate acts taken in relation to personal data rather than by reference to breaches of the GDPR.

iv) The language used in s. 155(1)(a) requires the Commissioner to be 'satisfied' that a breach of the GDPR has occurred. I accept Mr Lockley's submission that this is reflective of the application of the civil standard of proof. I have noted the contrast between this language and that in s.200 that refers to the Commissioner's investigation.

v) I conclude from this analysis a clear intention by Parliament to create two distinct penalty regimes, only one of which is overtly criminal in nature. Accordingly I conclude that an MPN issued pursuant to s. 155(1) is a civil penalty for domestic law purposes.

vi) I have also considered whether, notwithstanding this, an MPN issued under s. 155(1) ought to be treated as a criminal offence, at least to the extent that the criminal standard of proof must apply.

vii) I am not persuaded by Mr Coppel's submission that any appeal against a monetary penalty is a denial of a criminal offence for the purposes of Article 6, such that it should be afforded enhanced procedural protections. Even if I was so persuaded, Article 6 does not assist in relation to the applicable standard of proof (see *Hackett* [72-74]). I am satisfied that, in any event, the domestic common law requirements of a fair hearing apply to, and have been applied in, these proceedings, and that these meet Article 6 requirements of procedural protection in any event.

viii) I note that the provisions of s. 155(1)(b) allow an MPN to be imposed in addition to an information, assessment or enforcement notice, and that this reflects the provisions of Article 83 in which such a penalty is described as an 'administrative fine'. I find that the use of this language in a European context is inconsistent with an intention to create a penal sanction amounting to a criminal offence. Moreover, the Commissioner may only impose an MPN under s. 155(1)(b) in circumstances where the person has failed to comply with the earlier notice. This means that an MPN may only be imposed:

a. where the Commissioner is satisfied that a breach of relevant parts of GDPR has taken place (s. 155(1)(a)); or

b. where a person served with an information, assessment or enforcement notice has failed to satisfy the Commissioner that no such breach of the GDPR subsists.

In either case the MPN is served in connection with established or suspected breaches of specified obligations under the GDPR.

ix) The language of s. 155(1)(b) differs significantly from that of the other regulatory regimes cited by Mr Coppel as examples of legislation in which the criminal standard applies to a fine is imposed for non-compliance with an enforcement notice. This is because, in contrast to Mr Coppel's examples, s.155(1)(b) does not refer to the creation of 'an offence'.

x) The right of appeal created by s. 162(1)(d) & (3) essentially replicates the right created by s. 55B(5) DPA 1998 – i.e. an appeal may be brought against an MPN and/or the quantum of the penalty. The well-established practice of this Tribunal under the earlier legislation is to apply the civil standard of proof. There is nothing in the language of the DPA to suggest an intention by Parliament to change the applicable standard of proof.

xi) The criteria identified in ss. 155(2) & (3) as relevant to the assessment of the quantum of the penalty are taken from Article 83. These are necessarily expressed in terms unconnected to offsetting any 'benefit' of non-compliance with GDPR obligations because the purpose of this aspect of the Regulation is to prevent the infringement of individual rights. Therefore the 'cost' of breaches of the GDPR is necessarily assessed on a different basis.

xii) Although the levels of MPN that may be imposed under s. 155(1) are significant and when imposed at the higher level must meet the description of 'a serious consequence', there is no additional consequent deprivation of a fundamental liberty. As pointed out by Mr Lockley, DDL may continue to operate as an online pharmacy, the MPN under appeal notwithstanding. Applying the principles identified in *Hannam* and *Hackett* to the circumstances of this appeal, I find that the potential quantum of a s.155(1) MPN is not by itself a sufficiently serious consequence so as to bring an appeal within the first category of cases identified by Lord Hoffman, thereby requiring application of the criminal standard of proof on the basis of serious consequence alone.

xiii) I therefore conclude that the civil standard of proof applies to an appeal under s. 162(d).

Law of agency

48 Mr Coppel submits that the relationship between controller and processor mirrors the legal relationship between principal and agent, including to the extent that the processor is capable of affecting the controller's relationship with third parties, in this context the data subjects in relation to whom the controller retains responsibility.

49 He further submits that, pursuant to Article 28(1), if a processor arrogates the responsibility of the controller by determining the purposes and means of the processing, it should be treated as the controller in respect of that processing and may be subject to an administrative fine (Article 83(1) and s. 155(1)(a)).

50 Mr Coppel contends that DDL was only the controller in relation to some of personal data recovered by the MHRA and that, in relation to any such data, JPL had departed from the arrangement with DDL to the extent that JPL had assumed the role of controller. He submits that, in relation the other personal data recovered, this was contained in documents wrongly returned by DDL's care home customers, and that the care homes remained data controller of these, in relation to which JPL remained the processor.

51 Mr Lockley submits that the law of agency had no application to this appeal. He contends that the Commissioner's decision has been taken on the basis that DDL was the controller and JPL the processor, that the legislation sets out the relevant framework and that therefore the principle of vicarious liability does not assist and does not apply. He argues that the contractual arrangement between DDL and JPL does not automatically mean that the latter was acting as the agent of the former, and that relative liability is more properly determined through the prism of the DPA. Mr Lockley's position is that the controller-processor relationship exists where the definitions in the legislation statute are met, and that they are in this case.

52 He submits that the only relevant questions are:

i) Whether JPL processed personal data on behalf of DDL; and

ii) Whether DDL determined the purpose and meaning of the processing.

53 In Mr Lockley's view, the answer to both is 'yes'. He contends that any references in evidence to JPL being the 'agent' of DDL is merely confirmation that it processed personal data on DDL's behalf.

Conclusion on the law of agency

54 Having considered the submissions of both Parties, I am not persuaded that consideration of the law of agency assists with the determination of the central issue in this appeal, which is the extent to which DDL was controller of the data recovered and whether it bears responsibility for any data protection breaches arising from JPL's processing activities.

Agreed facts

55 The Parties have produced a Schedule of Agreed Facts which may be summarised as follows:

i) Mr Budhdeo is the sole Director and sole shareholder of both DDL and JPL.

ii) DDL is a pharmacy that operates both a 'closed', internet-based pharmacy ('the closed pharmacy') and a retail pharmacy in Cambridge. DDL's closed pharmacy received prescriptions directly from nursing homes and GP's surgeries.

iii) JPL is a licensed waste disposal company.

iv) Mr Budhdeo and his wife jointly own the Property. At the material time, the Property was used by JPL to carry out waste disposal activities on behalf of DDL. These included the destruction of personal data and special category personal data generated in the course of DDL's business.

v) JPL's activities on behalf of DDL constituted data processing, in relation to which DDL was the data controller and JPL was the data processor.

vi) On 24 July 2018 the MHRA executed a search warrant at the Property. It seized at least 73,000 pieces of paper stored in unlocked crates, boxes and bags. Some of these contained personal data and special category personal data.

vii) At the material time many of DDL's data protection policies and procedures were not up to date and did not comply with GDPR. In particular, DDL did not provide data subjects with the information required by Articles 13 and/or 14 GDPR.

viii) Having been contacted by the MHRA, on 15 August 2018 the Commissioner requested information from DDL in the context of an investigation into a possible breach of GDPR. When DDL failed to comply with the Commissioner's request, on 25 October 2018 she issued an Information Notice.

ix) On 30 January 2019 the Information Notice was upheld following an appeal by DDL to the Tribunal. On 1 March 2019 DDL responded in part to the Information Notice, invoking privilege against self-incrimination in response to some questions.

x) On 25 June 2019 the Commissioner issued a Notice of Intent ('NOI') and Preliminary Enforcement Notice ('PEN'). The NOI proposed a penalty of £400,000.

xi) On 26 November 2019 the MHRA informed DDL it was taking no further action against DDL, having concluded that that there was insufficient evidence to support a reasonable prospect of conviction.

xii) Having received written submissions from DDL and a witness statement from Mr Budhdeo in response to the NOI and PEN, on 17 December 2019 the Commissioner issued the Notices under appeal.

Evidence

56 The Commissioner elected not to rely on witness evidence, but instead relies on the Notices under appeal, exhibits provided by the MHRA and a number of documents she describes as being relevant to her investigation and decision. Mr Coppel on behalf of DDL indicated during the oral hearing that he challenges the provenance of at least one exhibit. I am satisfied that the Commissioner's evidence should be admitted although interpretation is necessarily limited by the lack of witness testimony.

57 In relation to processing activities at the Property, the Commissioner relies almost wholly on evidence provided by the MHRA. This includes an email from the MHRA to the ICO which describes in broad terms the content of '50 crates of paperwork'. The MHRA subsequently sent the Commissioner a memory stick containing images and video footage of the Property at the date of the search warrant, as well as sample documents.

58 The Commissioner has only viewed a sample of the documents and relies on an audit carried out by the MHRA. This describes documents as originating from 78 care homes and as comprising:

i) Dispensing tokens (print outs of electronic prescriptions). These are described by the MRHA as documents that were sent to the pharmacies by the care homes and as comprising as the majority of the documents.

ii) Medical Administration Records ('MAR') bearing the name of DDL's pharmacies;

iii) Copies of prescriptions;

iv) Faxes from care homes ordering new prescriptions;

v) Patient medication review documents;

vi) Residents lists and photographs of residents;

vii) Patient management records;

viii) Medicines dispensing check lists;

ix) Pharmacy delivery manifests

x) Patient identifiable medicinal waste; and

xi) Pharmacy delivery driver records.

59 Many of these documents are described by the MHRA as containing personal data and special category data, mainly of that of care home residents. The MHRA describes three confidential waste bags that appeared to originate from each of DDL's pharmacies and 47 crates containing documents. It further describes 'tens of thousands' of documents, some of which are 'soaking wet' consistent with having been stored outside. MHRA estimates the total number of documents as being over 500,000, with dates ranging from December 2016 – June 2018.

60 On 24 September 2019 members of ICO staff attended MHRA's premises and inspected a sample of the seized material.

61 The CCTV seized by the MHRA shows JPL employees removing labels from medicines. For example, footage from 20 June 2018 shows employees placing labels taken from bottles in a 'TK Maxx' carrier bag. ICO staff noted on inspection that one of the seized crates contained a TK Maxx bag full of documents. Overall they noted that each crate contained a mix of documents, and those stored together did not originate from the same care home. Documents also varied in age, the earliest dating from September 2016. It was further noted that approximately 100 documents were still wet and had become mouldy in storage.

62 In relation to DDL's policies, the Commissioner relies on the deficiencies of material provided by DDL when asked to demonstrate GDPR compliance at the time of the search. Only two referred to the GDPR and these were provided as blank templates. There was no data retention policy. DDL's 'Standard Operating Procedure – Disposals of Medicines Policy had been backdated to August 2018 having been drawn up in February 2019. The other policy documents had not been updated to reflect GDPR.

63 Following the PEN issued on 25 June 2019, DDL sent further information to the Commissioner but included references to future intentions to improve data protection policies, rather than demonstrating current compliance.

64 DDL has produced as evidence a more detailed analysis of the documents recovered by the MHRA. Kavi Mayor, DDL's solicitor, audited the documents in January and July 2020. He calculates that there are fewer than 75,000 documents in total, not all of which contain personal data and only a

proportion of which contains special category data. He describes three of the 53 crates and bags provided by the MHRA as containing damp documents that exhibited mould. Mr Mayor further states that he was not provided with exactly the same crates and boxes as shown in the MHRA photographs taken at the Property.

65 Mr Budhdeo has provided three witness statements, which he has made on behalf of both DDL and JPL. His evidence is as follows:

i) He is highly critical of the MHRA and the Commissioner's standards of investigation.

ii) He relies on Mr Mayor's audit to assert only 73,719 documents were recovered from the Property. Of these:

- 7,351 contain no personal data;
- 6229 contain a name only;
- 6268 contain a name and address only; and
- Approximately 53,871 contain special category data.

iii) In July 2018 DDL had dispensing contracts with 27 care homes. By September 2019 this number had reduced to 15 cares homes to which it dispensed approximately 7000 items each month, plus another 2000 items to the general public.

iv) Mr Budhdeo is not himself a pharmacist. DDL employs superintendent pharmacists who are responsible for the DDL 's pharmacy activities.

v) The MAR charts recovered from the Property are produced by DDL and used by staff in the care homes to record when each medicine is given to a patient. Two copies are delivered to the care homes along with the medication, which is organised by DDL in reusable racks known as SUMS. The top copy of the MAR is signed when the medicine is administered to the patient. The bottom copy is returned to DDL each month where it is retained for a month then either securely destroyed or sent to the Property for destruction. Mr Budhdeo describes the care homes as habitually returning the top copy MAR charts in error, and that this is collected by JPL when collecting medicinal waste under contract to DDL.

vi) In his third statement Mr Budhdeo speculates that most or all the dispensing tokens recovered in the crates must also have been wrongly returned via JPL by the care homes. He accepts that some of the personal

data recovered at the Property had been sent there for destruction by DDL's pharmacies.

vii) As at July 2018 JPL's business activities included collecting and disposing of medicines from care homes and carrying and disposing of waste from the pharmacies. DDL is under contract with the care homes to provide medicine in and outside of SUMS and also provides a service whereby it collects and disposes of unused medication.

viii) Since March 2018 JPL has carried out this activity on DDL's behalf under contract, although Mr Budhdeo accepts that no written contract existed until after the MHRA search. Neither was JPL a registered waste carrier at the time of the search. He states that JPL was collecting approximately 400 boxes from care homes a month and that these included returned medicines. Part of JPL's role is to sort patient data from the returned material and securely dispose of it within 28 days.

ix) The Property is secure and all doors and gates are kept securely locked. Mr Budhdeo insists that the general public are unable to enter the yard area. Although he accepts that the yard can be accessed via fire escapes from three residential flats at the property, Mr Budhdeo sought to minimise this risk, describing the fire escapes as leading from 'small ventilation windows'. Neither company nor Mr Budhdeo has any connection with the tenants of these flats which Mr & Mrs Budhdeo sold several years ago, although they retain the freehold as well as the Property. Notably, in his second witness statement Mr Budhdeo describes the Property as being used by JPL pursuant to an agreement between DDL and JPL, rather than agreement between Mr & Mrs Budhdeo and JPL.

x) The Property came to be used for waste disposal by JPL in March 2018. Therefore any documents seized which predate this must, in Mr Budhdeo's view, have been wrongly retained by the care homes and thereafter passed by the care homes to JPL in error.

xi) Mr Budhdeo denies that any personal data was stored in the yard area of the Property. He accepts in his second statement that the CCTV shows crates being placed in the yard less than a week before the search warrant was executed, but disputes that there were 50 of these or that they were stacked up in the manner photographed by the MHRA. In cross examination he suggested that the mouldy documents seen by the Commissioner's staff may have become damp whilst being stored by the MHRA.

xii) The Commissioner produced two photographs of seized items not connected with DDL, one of which was a delivery note addressed to Mr Budhdeo at home and the other a bank card in his name. Mr Coppel disputes the provenance of the former. However, in the absence of any other explanation and given Mr Budhdeo's connection with the Property I conclude that it must have been seized when the search warrant was executed. I do not consider either exhibit to be evidentially significant for the purposes of these proceedings.

xiii) In cross examination Mr Budhdeo stated that both DDL and JPL were responsible for disposing of personal data. He describes JPL's primary job as collecting waste and destroying it, and said it was implied throughout that JPL would dispose of data when disposing of waste.

xiv) In oral evidence Mr Budhdeo described the yard at the Property as also being used for the storage of building materials, although he stated that he had no interest in the building trade. It was put to him in cross examination that he had been a director of Equitable Sustainable Housing Limited which Mr Budhdeo denied, stating that the 'S Budhdeo' listed on the Companies House website was his brother. Mr Lockley subsequently produced documents showing that Mr Budhdeo had been a director of the company. Mr Budhdeo stated that he had forgotten this information.

xv) Mr Budhdeo accepts that the data protection polices of both DDL and JPL required improvement in 24 July 2018. Since then Shred-it has been employed to carry out disposal of all confidential paper waste. It is not clear from Mr Budhdeo's statement whether this is on behalf of DDL or JPL. DDL has also engaged the services of The Informacist Ltd to improve compliance with data protection legislation.

xvi) In cross examination Mr Budhdeo inferred that his previous solicitors had not sent the Commissioner all of the data protection policy documents he had given them, stating that he had sent the solicitors everything required. He further stated that this must have included a privacy policy, notwithstanding the fact that no such document was submitted to the Commissioner, since it was a policy document DDL's pharmacists were required to have and that the policy documents sent to the Commissioner as blank templates had in fact been completed by DDL at that date. He did not know why blank templates had been submitted. Mr Budhdeo accepted that the GDPR guidance for data protection officers he had sent to the Commissioner with a signature dated August 2018 had in fact been signed in February 2019. He further accepted that the contractual agreement between DDL and JPL had been drawn up after the search warrant had been executed.

xvii) Mr Budhdeo stated that the pharmacists employed by DDL produced all necessary Standard Operating Procedures and that these met data protection requirements at the time, including retention requirements. He said that he did not have authority to interfere in these SOPs as they had to be drafted to meet the regulatory requirements of the Superintendent Pharmacist. He produced evidence to show that DDL's pharmacies had passed the required regulatory inspections.

xviii) In Mr Budhdeo's view, at the date of the alleged breach DDL's policies and contracts relating to medicinal waste extended to and included the destruction of related personal data. On that basis he stated that JPL's contract with DDL, which refers to collecting and disposing of medicines, also included the collection and destruction of personal data and that no distinction was made by JPL between data and non-data. He likened JPL to a courier company and said it had no knowledge of what it was collecting from care homes at any time.

xix) Mr Budhdeo's evidence is that both DDL and JPL were responsible for disposing of personal data. He relies on aspects of the contract between DDL and JPL in support of this view. He maintained that, even though DDL did not have written GDPR compliant policies in place in July 2018, the waste disposal processes followed met the requirements of the GDPR. He described JPL as being meticulous when ensuring that all personal data was securely destroyed. Mr Budhdeo accepted that the data destruction process employed by JPL on the relevant date did not reflect the process described in DDL's data handling document, in that personal data was being incinerated rather than cross-shredded.

Submissions

66 Both Parties have provided detailed and helpful submissions, for which I am grateful. I have considered these with care, although for reasons of brevity I have only summarised those that are central to the Tribunal's determination.

67 DDL submits that the evidence does not support the Commissioner's interpretation of events. It relies upon Mr Mayor's audit as evidence to contend that any breach of the GDPR was much less serious than the Commissioner assessed it to be, comprising only 66,404 documents containing personal data and special category data, rather than the 'over 500,000' figure upon which the MPN is based.

68 DDL contends that the standard of the Commissioner's evidence is deficient, noting in particular the absence of witness evidence and criticizing her unquestioning acceptance of the MHRA's assertion of facts.

DDL suggests that little reliance can be placed upon this evidence and submits that the processing in breach of the GDPR has been assumed purely on the basis of a lack of adequate data protection policies. DDL's position remains that all personal data was securely destroyed by JPL in accordance with data protection obligations and within 28 days of receipt.

69 DDL submits in that, in any event. it was not the controller of the personal data and special category data recovered. It asserts that these documents must have been wrongly passed to JPL by the care homes, and that therefore the care homes are the responsible data controllers. It submits in the alternative that JPL has assumed the role of controller, as it had determined the purposes and means of processing the care homes' data.

70 In the further alternative, and to the extent that DDL had been the controller of the seized personal data at one stage, DDL submits that by virtue of Article 28(1) JPL had become the controller because it was processing the data otherwise than in accordance with DDL's instructions. It relies in support upon the contractual arrangement between DDL and JPL, under which JPL was only authorised to destroy personal data in relation to DDL-sourced excess medication and equipment and must do so securely and in good time.

71 In relation to the quantum of the penalty, DDL submits that this is disproportionate to the seriousness of any proven breach and fails to consider DDL's position of financial hardship and ability to pay. It contends that the quantum has been calculated by reference to the Commissioner's erroneous acceptance of the MHRA's estimate of document numbers. More generally, it submits that the higher level of penalty imposed by the Commissioner for breaches of the GDPR are unfair and arbitrary when compared with penalties under the predecessor legislation.

72 In relation to the EN, DDL submits that it was inappropriate and unnecessary to issue a coercive notice in circumstances where the data protection policy breaches identified at an earlier stage had largely been remedied.

73 In response, the Commissioner submits that she will consider any additional evidence produced by DDL in relation to document numbers but maintains the analysis of relevant issues set out in the notices under appeal.

74 The Commissioner contends that, irrespective of the number of crates stored in the yard, some had clearly been stored in this manner since this is the only logical explanation for some of the documents becoming wet. She describes this as an inappropriate storage arrangement, in part because the yard area could be accessed by occupiers of the residential flats and by

visitors to the yard. Moreover, this manner of storage risks the accidental loss or destruction of data and rendered DDL unable to respond as required should any the data subjects affected exercise their rights under the GDPR. Further, the Commissioner submits that the jumbled way in which the documents were stored prevented DDL from knowing with any certainty what personal data was being stored and processed by JPL on DDL's behalf.

75 In reply to DDL's submissions as to the identity of the controller, the Commissioner contends that this was DDL, as JPL was contracted to collect and dispose of waste medicines, including incidental personal data, on behalf of DDL. Further, she relies on the arrangement whereby JPL was also contracted to dispose of DDL's own pharmacy waste, which was being stored at the Property and subjected to the same inadequate data protection procedures.

76 The Commissioner submits that DDL retained responsibility for determining the purpose and means of processing data since the entire purpose of JPL's activities was the secure destruction of personal data for which DDL had responsibility. She contends that DDL was the controller both of care home waste collected by JPL and of DDL's own waste. The Commissioner relies in part upon DDL's SOP with JPL, under which DDL stipulates what JPL must do with returned medication and paper waste, without any distinction being made by JPL as to whether the matter it is disposing of is data or non-data.

77 The Commissioner further submits that DDL's failure to put in place adequate procedural and contractual arrangements was a contributory cause to any breaches of GDPR by JPL. The absence of adequate written policies is therefore cited in the MPN in addition to breaches arising from JPL's wrongful data processing.

78 In relation to the quantum of the MPN, the Commissioner refers to her statutory guidance and to the purpose of the GDPR. She submits that penalty decisions made under the DPA 1998 are not a suitable comparator, as the intention is that higher penalties are to be imposed for infringements of the GDPR. She contends that the MPN takes DDL's financial hardship into account, and that this and DDL's compliance improvements resulted in a reduction of the penalty proposed in the NOI.

79 The Commissioner submits that it would defeat the purpose of the GDPR if a person responsible for a serious infringement were exempted from the imposition of a penalty solely on the basis of their financial circumstances. She reiterates the legislative purpose of a s. 155(1) MPN, which is that it should be effective, proportionate, and dissuasive.

80 Finally, in relation to the EN the Commissioner submits that it was proportionate and appropriate to issue the EN in December 2019, notwithstanding improvements in compliance demonstrated by DDL in September 2019, since at that stage DDL had still failed to show that it had rectified all data protection compliance concerns, even though serious contraventions had already been identified in the context of a serious breach.

General conclusions

81 The Commissioner relies on evidence that was produced during an investigation carried out for a different purpose. It therefore lacks important details about the nature of the personal data concerned, not least an accurate calculation of the number of documents recovered. The Commissioner has also elected not to rely on witness evidence, nor to produce evidence of the origin of the personal data being processed by JPL. By contrast, DDL has audited all of the documents, and the evidence it has produced is necessarily a more reliable source of information. I have therefore proceeded on the basis that 73,719 documents were seized from the Property, of which 12,491 contained personal data and 53,871 contained special category data, and that these can have originated from no more than 27 care homes.

82 Mr Budhdeo, on behalf of DDL, suggests that most of the personal data recovered must have originated from care homes rather than DDL itself. I find this explanation improbable and have concluded that DDL was the controller of data processed by JPL for the following reasons:

i) Mr Budhdeo's evidence is that JPL took over responsibility for the collection and destruction of waste medicines from care homes in March 2019 and had been using the Property for that purpose from the same date.

ii) DL does not dispute that much of the data recovered is that of patients residing in different care homes. Neither does it dispute that the documents upon which the data are recorded are copies of documents generated by DDL's pharmacies, in relation to which DDL is data controller.

iii) If Mr Budhdeo's explanation is correct, several of DDL's care home clients must have potentially breached their own regulatory and data processing obligations between March and July 2019 in that by giving JPL documents containing data they were required to retain, without also taking steps to ensure that the data would be appropriately and securely processed. Further, if his explanation is correct, that when

doing so the care home provided JPL with historic documents dating back to 2016 or 2017 and, given Mr Budhdeo's assertion that JPL securely destroyed data within 28 days of receipt, that the care homes had largely returned this data over the preceding month.

iv) I find DDL's explanation to be improbable. I am satisfied that a more likely explanation for the presence of historic data, which on DDL's account should have already been securely destroyed, is that this is the result of data protection failures by DDL and/or JPL. I find in addition that DDL's suggestion relies on the highly improbably coincidence that several data controller care homes acting independently replicated the same error in a short period of time.

v) I note in addition that, other than Mr Budhdeo's witness testimony, there is no evidence to suggest that dispensing tokens, MAR charts, patient records etc recovered by the MHRA were the care homes' copies of these documents.

vi) I am satisfied that it is appropriate to look for corroboration of Mr Budhdeo's evidence on this point. This is because Mr Budhdeo's credibility as a witness has been diminished by his misleading answers concerning his directorship of Equitable Sustainable Housing Limited. I find Mr Budhdeo's explanation, when presented with contradictory evidence, also lacks credibility.

vii) No other evidence suggests that the documents recovered are the care homes' copies that should have been retained. Neither has evidence been produced supporting the view that the care homes are the data controllers of the recovered data.

viii) Even if some of the data were wrongly returned by the care homes to JPL, JPL's only purpose was to collect medicinal waste on behalf of DDL. DDL admits that JPL's activities on its behalf constitutes data processing in relation to which DDL is the controller and JPL the processor. Mr Budhdeo, who describes himself as giving evidence on behalf of both companies, describes the contractual arrangement between DDL and JPL in terms whereby DDL stipulates the processes JPL must follow, describing JPL's collection activities as robotic. He further confirms that JPL's waste disposal agreement with DDL did not distinguish between personal data and non-data. Accordingly, I conclude that DDL was determining the purposes and means by which any personal data collected by JPL would be processed.

ix) I have considered the extent to which JPL's activities may have departed from DDL's stipulated processes and, if so, whether as a consequence

JPL thereby assumed the role of controller. I conclude that JPL remained the processor rather than the controller of the data it processed for the following reasons:

a) The issue of whether a processor arrogated the role controller in this context must be considered by reference to the Article 5(2) accountability principle. This provides the controller with retained responsibility for ensuring compliance with the Article 5(1) data processing principles, including though the provision of comprehensive data processing policies. Although it is possible that a tipping point may be reached whereby the processor's departure from the agreed policies becomes an arrogation of the controller's role, I am satisfied that this does not apply to the facts of this case.

b) At the material time Mr Budhdeo was the sole director and shareholder of both companies. He appears to have been responsible for deciding which waste disposal processes JPL would adopt as DDL's agent. Since this arrangement was not reduced to writing until after the MHRA search warrant, and because even then the data processing policies were incomplete, I find no basis upon which to conclude that JPL departed to a material extent from any tangible data processing instructions it had received from DDL.

83 I am further satisfied that JPL allowed at least some of the data processed on behalf of DDL to be stored in unlocked crates, and at least some of these were stacked in an outside yard before the documents were recovered, as a result of which some of the documents became wet. I find in addition that the yard was not an appropriately secure area in which to store personal data, due to the fact that the yard could be accessed by the occupants of and visitors to three residential flats, via fire escapes that as a matter of common sense must be readily accessible. The unlocked crates in the yard could also potentially be accessed by business visitors to the Property. I conclude from this that JPL's methods of data storage was not appropriately secure and did not afford sufficient protection against accidental loss or destruction, and that this was a breach of the integrity and confidentiality requirements of Article 5(1)(f) for which DDL retained responsibility by virtue of Article 5(2).

84 I find in addition, on the balance of probabilities, that at the date of the search warrant JPL was storing personal data in a form that permitted identification of data subjects for longer than necessary. This is because the presence of personal data that was two or more years old indicates that not all data was destroyed when it was no longer required. DDL has confirmed that historic, hard copy documents were not required for record keeping purposes. Given the findings I have already made in relation to the

provenance of these documents, and the absence of any evidence that the historic records had only been passed to JPL for destruction recently, I am satisfied that the retention of this data by JPL was a breach of the storage limitation requirements of Article 5(1)(e,) for which DDL also retained responsibility by virtue of Article 5(2). I note in addition that, other than Mr Budhdeo's witness testimony, no contemporaneous evidence has been adduced to show when and how JPL securely destroyed personal data on DDL's behalf.

85 I find that DDL's failure to devise adequate data processing policies contributed to JPL's breaches of relevant data processing requirements. In particular, I find that the absence of a retention policy and of a clear explanation by DDL of the processes JPL must follow when destroying personal data incidental to the destruction of medicinal waste must have contributed to JPL's breaches as it was provided with no appropriate procedures to follow.

86 I conclude as a consequence that DDL's responsibility for JPL's breaches also amount to a breach of the requirements of Article 24(1), in that DL failed to implement appropriate and organisational measure to ensure that JPL's processing was performed in accordance with the GDPR, as well as a breach of the requirements of Article 32, in that DDL failed to implement appropriate measure to ensure a level of security appropriate to the risks.

87 I note in addition that DDL accepts that it breached the requirements of Articles 13 and/or 14 in relation to the provision information in its Privacy Notice.

Monetary Penalty Notice

88 In accordance with the principles identified in *Hope and Gory* I have afforded appropriate weight to the Commissioner's decision to issue an MPN but note that the level of penalty was predicated upon 500,000 documents having been seized. I have instead considered the appropriate level of penalty based on a finding that 66,638 documents containing personal data were recovered, 53,871 of which contained special category data.

89 I nevertheless reach the same conclusion as the Commissioner, in that the contraventions identified are sufficiently serious to justify issuing a penalty. However, in contrast to the approach taken by the Commissioner in the MPN, I do not consider a breach of Article 24(1) to be a contravention in relation to which an MPN may be imposed under s. 155(1), because it is not a breach of GDPR listed in s. 149(2).

90 I adopt the Commissioner's assessment of the factors set out in Article 83(2), other than her assessment of the number of data subjects affected by the contraventions which was based on the MHRA's estimated figure of 500,000 documents. I note in particular the Commissioner's conclusions as to the gravity of the breach and the risk of significant emotional distress being caused to a vulnerable group of data subjects were they to become aware of the contraventions. I also agree with the Commissioner's conclusion that the serious breaches of the data processing principles occasioned by JPL's activities were largely due to DDL's negligence in relation to its Article 24(1) and Article 32 obligations.

91 I conclude as a consequence that issuing an MPN is an effective, proportionate and dissuasive response to DDL's contraventions.

92 I note the statutory intention of both the GDPR and DPA is that a higher financial penalty should be imposed under this than other the predecessor legislation. Having considered the Commissioner's statutory guidance and the circumstances of this case, I am satisfied that the Commissioner's penalty assessment in the NOI of £400,000 was appropriate given the facts as she understood them to be. I am further satisfied that her subsequent decision to reduce the penalty to £275,000 was appropriate in light of DDL's financial position.

93 I agree that a person responsible for a serious contravention of the GDPR should not avoid a monetary penalty solely on the basis their financial position, since such a practice would undermine a key purpose of the legislation. However, financial hardship remains an important consideration in terms mitigation. I find that it has already been reflected in an appropriate manner in the MPN under appeal.

94 I am satisfied that the amount of the penalty imposed on DDL should be reduced further in light of the Tribunal's conclusion that substantially fewer than 500,000 documents were recovered. However, 12,491 documents containing personal data and 53,871 documents containing special category data are still very large numbers of documents, and the significant aggravating factor that majority contained the personal data of highly vulnerable data subjects remains.

95 Given the gravity of the contraventions, my additional finding that DDL is responsible for a breach of Article 5(1)(e) obligations, and the long list of aggravating criteria identified in the MPN, I am satisfied that the level of the penalty imposed should not be reduced by a percentage based on solely on the lower numbers of documents.

96 Having taken all of these matters into consideration I have decided that the amount of the MPN should be reduced to £92,000, which is a reduction of approximately two thirds.

Enforcement notice

97 I am satisfied that it was proportionate and reasonable to issue an EN on 17 December 2019 in relation to DDL's data protection policies for the following reasons:

i) DDL was put on notice in August 2018 that the Commissioner was investigating GDPR compliance arrangements in light of documents recovered during the MHRA search of the Property.

ii) DDL accepts that its data protection policies were inadequate at that date, particularly its privacy notice and the policies relating to the retention and destruction of personal data.

iii) The documents submitted by DDL to the Commissioner on 1 March 2019 were still inadequate for data protection purposes. At least one of these had not been drawn up until after the unsuccessful appeal against the Information Notice and had thereafter been backdated to August 2018.

iv) On 25 June 2019 the Commissioner issued a PEN, drawing DDL's attention to potential continued breaches of data protection requirements. The Commissioner did so having concluded that, since DDL continued to process special category data and given that poor data protection arrangements had already resulted in a serious breach, there remained a risk that any continued contraventions were likely to cause high levels of distress to those affected.

98 On 11 September 2019 DDL sent further data protection policy documents to the Commissioner, as well as a statement by Mr Budhdeo. These were still incomplete and referred to some changes that were yet to be implemented.

99 I am therefore satisfied on the evidence before the Tribunal that, as of September 2019, DDL's data protection polices still did not fully comply with legislative requirements. I am further satisfied that, the Commissioner having produced evidence of perceived deficiencies, it must be for DDL as data controller to demonstrate adequate compliance with legislative requirements. I conclude that DDL has failed to satisfy this evidential burden in the course of these proceedings because it has continued to rely on the documents sent to the Commissioner in September 2019, some of which are incomplete and unclear.

100 Given DDL's failure to demonstrate adequate data protection policies more than a year after serious concerns were drawn to its attention, I am satisfied that it was appropriate and proportionate for the Commissioner to issue an EN on 17 December 2019.

101 Because not all of DDL's current data protection policies are before the Tribunal, I am unable to determine whether an EN is still required in the same terms. This is a matter for the Commissioner to determine. Should she decide that DDL's deficiencies continue, she will no doubt consider the extent to which enforcement powers remain open to her, given the terms of the MPN.

(Signed)

TRIBUNAL JUDGE MOIRA MACMILLAN

DATE: 9 August 2021
PROMULGATED: 18 August 2021

Slip Rule amendment: 2 September 2021