

DATA PROTECTION ACT 2018 (PART 6, SECTION 155)

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

PENALTY NOTICE

TO: Doorstep Dispensaree Ltd

OF: 263 Burnt Oak Broadway, Edgware, HA8 5EP

1. The Information Commissioner ("the Commissioner") has decided to issue Doorstep Dispensaree Limited ("Doorstep Dispensaree") with a penalty notice under s.155 Data Protection Act 2018 ("DPA 2018"). This penalty notice imposes an administrative fine on Doorstep Dispensaree, in accordance with the Commissioner's powers under Article 83 of the General Data Protection Regulation 2016 ("GDPR"). The amount of the fine is £275,000 (two hundred and seventy five thousand pounds).
2. The penalty is being issued because of contraventions by Doorstep Dispensaree of:
 - a. Articles 5(1)(f), 24(1) and 32 of the GDPR, in that Doorstep Dispensaree has failed to implement the appropriate organisational measures to ensure the appropriate security of the personal data it processes and has processed personal data in an insecure manner. It is also noted that Article 5(1)(e), which states that data be kept in a form that permits identification of data subjects

- for no longer than is necessary for the purposes for which they are processed, is likely to have been infringed;
- b. Articles 13 and/or 14 GDPR, in that Doorstep Dispensaree has failed to provide data subjects with the information required by those Articles.
3. This Penalty Notice explains the Commissioner's reasons for imposing such a penalty, and for the amount of the penalty. The Commissioner has carefully considered the representations made to her by Doorstep Dispensaree on 11 September 2019 and where appropriate this Notice explains what account she has taken of those submissions.

Legal Framework

Obligations of the controller

4. Doorstep Dispensaree is a controller for the purposes of the GDPR and DPA 2018, because it determines the purposes and means of processing of personal data (GDPR Article 4(7)).
5. 'Personal data' is defined by Article 4(1) GDPR to mean

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

6. Article 9 GDPR prohibits the processing of 'special categories of personal data' unless certain conditions are met. The special categories of personal data subject to Article 9 include 'personal data [...] concerning health'
7. 'Processing' is defined by Article 4(2) GDPR to mean

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
8. Controllers are subject to various obligations in relation to the processing of personal data, as set out in the GDPR and DPA 2018. They are obliged by Article 5(2) to adhere to the data processing principles set out in Article 5(1) GDPR. Article 5(1)(e) requires that personal data not be retained for unduly long periods of time:

(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')

9. In particular, controllers are required to implement appropriate technical and organisational measures to ensure that their processing of personal data is secure, and to enable them to demonstrate that their processing is secure. Article 5(1)(f) stipulates that

Personal data shall be [...] 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

10. Article 24 ("**Responsibility of the controller**") provides, in material part that:

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.*

11. Article 25 ("**Data protection by design and by default**") emphasises that controllers must consider appropriate security measures at the outset, when planning their data processing activities:

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures [...]

12. Article 32 ("**Security of processing**") provides, in material part:

- 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.

13. Chapter III of the GDPR makes provision for the rights afforded to data subjects. These include, by Articles 13 and 14, the right to receive from the controller certain information about the processing of their personal data.

The Commissioner's powers of enforcement

14. The Commissioner is the supervisory authority for the United Kingdom, as provided for by Article 51 GDPR.
15. By Article 57(1) GDPR, it is the Commissioner's task to monitor and enforce the application of GDPR.
16. By Article 58(2)(d) GDPR the Commissioner has the power to notify controllers of alleged infringements of GDPR. By Article 58(2)(i) she has the power to impose an administrative fine, in accordance with Article 83, in addition to or instead of the other corrective measures

referred to in Article 58(2), depending on the circumstances of each individual case.

17. By Article 83(1), the Commissioner is required to ensure that administrative fines issued in accordance with Article 83 are effective, proportionate and dissuasive in each individual case. Article 83(2) goes on to provide that:

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.*
18. The DPA 2018 contains enforcement provisions in Part 6 which are exercisable by the Commissioner. Section 155 DPA 2018 ("Penalty Notices") provides that

(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.

19. The failures identified in s.149(2) DPA 2018 are, insofar as relevant here:

(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) [...]

Background to the case

20. On 31 July 2018 the Commissioner received an email from the Medicines and Healthcare products Regulatory Agency ("MHRA"). MHRA told the Commissioner that it was conducting its own investigation into the alleged unlicensed and unregulated storage and distribution of medicines by Doorstep Dispensaree. On 24 July 2018 the MHRA had executed a search warrant at the premises of Doorstep Dispensaree under the Human Medicines Regulations. In the course of its search, the MHRA discovered, stored in a rear courtyard, 47 unlocked crates, 2 disposal bags and 1 cardboard box full of documents containing personal data. MHRA estimated approximately 500,000 documents but cannot estimate the number of data subjects.
21. MHRA have inspected the crates and the information contains:
 - a. Names
 - b. Addresses
 - c. Dates of Birth
 - d. NHS Numbers
 - e. Medical Information
 - f. Prescriptions

22. The dates on the documents range from January 2016 – June 2018. The documents were not secure and they were not marked as confidential waste. Some of the documents were soaking wet, indicating that they had been stored in this way for some time.
23. This gave the Commissioner cause to be concerned that sensitive personal data had been processed insecurely, in a manner that infringed the GDPR. On 15 August 2018 the Commissioner wrote to Doorstep Dispensaree outlining her concerns and asking a number of questions about its compliance with the GDPR. The Commissioner explained that she was investigating compliance with data protection legislation and that Doorstep Dispensaree had an obligation to cooperate with the investigation. The Commissioner requested:
 - a. Clarification of the categories of information that Doorstep Dispensaree regularly processes;
 - b. Information on Doorstep Dispensaree's processing, including the number of clients it supplies medicines to, and copies of its contracts with the care settings;
 - c. Clarification of whether Doorstep Dispensaree processes data on behalf of any other organisations;
 - d. A copy of Doorstep Dispensaree's privacy notice;
 - e. A description of the technical and organisational measures the Appellant has in place to ensure security of personal data;

- f. An explanation of why information was stored in the manner discovered by MHRA during its search;
 - g. An explanation of why some of the information appeared to have been retained since January 2016;
 - h. A copy of Doorstep Dispensaree's retention policy or equivalent guidance; and
 - i. A copy of Doorstep Dispensaree's policy or guidance relating to the secure disposal of personal data.
24. Doorstep Dispensaree responded on 22 August 2018 via its solicitor. It did not answer any of the Commissioner's questions. Instead, it seemed to deny that Doorstep Dispensaree had any knowledge of the matter.
25. The Commissioner wrote to Doorstep Dispensaree again on 11 September 2018, providing further information about the matter and repeating her questions about Doorstep Dispensaree's compliance with the GDPR. Doorstep Dispensaree responded on 28 September 2018 refusing to answer the questions. It appeared to conflate the Commissioner's investigation with the MHRA's separate investigation.
26. In light of Doorstep Dispensaree's continued refusal to answer the Commissioner's questions, the Commissioner decided to issue an Information Notice under section 142(1)(a) DPA 2018 on 25 October 2018, requiring Doorstep Dispensaree to provide the information summarised above.

27. Doorstep Dispensaree chose to appeal the Information Notice. Its appeal was dismissed by the First-Tier Tribunal (Information Rights) on 28 January: see *Doorstep Dispensaree Ltd v Information Commissioner* [2019] UKFTT 2018_0265 (GRC).
28. Despite the Information Notice having been upheld by the Tribunal, Doorstep Dispensaree did not then comply with it in a timely fashion. The Commissioner sent a chasing e-mail on 11 February 2019 and a further chasing e-mail on 21 February 2019, threatening to pursue an Information Order and/or issue a penalty.
29. Eventually, Doorstep Dispensaree responded to the Information Notice on 1 March 2019. It declined to provide information listed in (b), (c), (f) and (g) of paragraph 23 above, stating

My client invokes the protection under s. 143(6) DPA 2018 as there is a risk that in providing the information requested, my client will be exposing itself to prosecution in the MHRA's existing criminal proceedings against it...

30. In response to the remaining questions, Doorstep Dispensaree provided a number of procedures and guideline documents:
 - a. Code of Conduct;
 - b. Data Handling Procedure;
 - c. Information Governance Policy;
 - d. GDPR – Data Protection Officer Guidance and Checklist and Definitions and Quick Reference Guide (National Pharmacy Association template);
 - e. Doorstep Dispensaree Standard Operating Procedures – Disposal of Medicines;

31. Of these, most had not been updated since April 2015, and therefore dated from before the adoption, let alone the entry into force, of the GDPR. Furthermore, although they outlined staff responsibilities, the practical advice provided to staff in relation to data protection is vague. The few procedures and guidelines which did make reference to the GDPR (the Data Protection Officer Guidance and Checklist, and the Definitions and Quick Reference Guide) were templates from the National Pharmacy Association and they did not appear to have been incorporated by Doorstep Dispensaree.

Notice of Intent

32. On 25 June 2019, in accordance with s.155(5) and paragraphs 2 and 3 of Schedule 16 DPA 2018, the Commissioner issued Doorstep Dispensaree with a Notice of Intent to impose a penalty under s.155 DPA 2018. The Notice of Intent described the circumstances and the nature of the personal data in question, explained the Commissioner's reasons for the proposed penalty of £400,000, including what she regarded as the aggravating and mitigating factors of the case, and invited written representations from Doorstep Dispensaree.
33. On the same date, the Commissioner also issued Doorstep Dispensaree with a Preliminary Enforcement Notice, setting out her intention to issue Doorstep Dispensaree with an Enforcement Notice under section 149 DPA
34. On 11 September 2019, Doorstep Dispensaree provided written representations in respect of both Notices, together with a witness statement from its Director, and supporting documents.

35. On 26 November 2019, MHRA informed Doorstep Dispensaree that it was taking no further action, because there was insufficient evidence to support a reasonable prospect of conviction.

The Contraventions

Contraventions of Articles 5(1)(f), 24(1) and 32 of the GDPR

36. The Commissioner considers that Doorstep Dispensaree is the controller processing the personal data found in crates on its premises and seized by MHRA. In its representations, Doorstep Dispensaree suggested that any penalty should be issued against Joogee Pharma Limited ("**Joogee**"), a licenced waste disposal company operating under contract to Doorstep Dispensaree. However, from the evidence provided, the Commissioner is satisfied that Joogee is a data processor, acting on the instructions of Doorstep Dispensaree and carrying out data processing on its behalf. It is Doorstep Dispensaree that determines the purpose and means of the processing. It is therefore appropriate to issue the penalty against the controller, Doorstep Dispensaree.
37. It is clear that the data were not processed securely: the documents were left outside, in unlocked containers ("**the Breach**"). The Commissioner does not accept the suggestion made by Doorstep Dispensaree in its representations that the data were stored securely because the yard was locked: Doorstep Dispensaree admits that there is access from residential flats down the fire escape to the courtyard. Furthermore, Art. 5(1)(f) requires more than just protection against 'unauthorised or unlawful processing' by third parties: it also requires protection against 'accidental loss, destruction or damage' and the use of appropriate technical or

organisational measures. The ingress of water into the documents demonstrates that they could be accidentally damaged or destroyed, and the careless way in which they were stored fails to protect against accidental loss.

38. Nor were the documents shredded, contrary to Doorstep Dispensaree's then-current 'Data Handling Procedures' which required (appropriately) 'that all waste containing patient identifiable information [...] is cross shredded before disposal'. Doorstep Dispensaree has explained that it employed the services of a company to collect medical data and shred it on its behalf. However, no contract between Doorstep Dispensaree and the company has been provided. Some of the personal data dates back to 2016 and has remained unshredded since then. The Commissioner therefore considers that whatever shredding policies or contract Doorstep Dispensaree may have had in place at the time of the Breach, they were not being correctly implemented.
39. As noted above, several of the data protection policies that Doorstep Dispensaree initially provided to the Commissioner were out of date and/or inadequate and/or generic templates. Although Doorstep Dispensaree has, with its representations, provided a more comprehensive suite of policy documents, many of these remain in template form and in any event it is clear that they were acquired after the Breach, indeed, in response to the Commissioner's investigation into Doorstep Dispensaree's data protection practices.
40. The Commissioner therefore considers that Doorstep Dispensaree has contravened Article 5(1)(f) of the GDPR. At the time of the Breach, it had failed to adopt and/or implement appropriate technical measures, such as physically secure storage and/or shredding, that

would ensure the secure processing of personal data. Likewise, it has failed to adopt and/or implement appropriate organisational measures, such as adequate data protection policies, to ensure secure processing of personal data. The manner in which the data were stored gave rise to an unacceptable risk of unauthorised access. There was also an unacceptable risk of accidental loss, damage or destruction of such data.

41. Furthermore, the age of some of the data raises a concern about the retention of data. Doorstep Dispensaree has confirmed that it did not have a retention policy at the time. If there was no legitimate reason for the continued processing, that would constitute an infringement of Article 5(1)(e) GDPR, which requires that data shall be 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. For the avoidance of doubt, the Commissioner has considered only the on-going infringement occurring from 25 May 2018.
42. For the same reasons that Doorstep Dispensaree has infringed Article 5(1)(f) GDPR, the processing is also a contravention of Article 24(1) GDPR. The volume and sensitivity of the data plainly gave rise to a high risk to the rights and freedoms of the data subjects, warranting significantly more stringent data security measures than Doorstep Dispensaree applied.
43. For the same reasons, the processing is also a contravention of Article 32(1) GDPR. Given the degree of risk to data subjects, it would plainly have been appropriate to adopt additional simple, cost effective security measures such as shredding and storage in a secure location.

44. It follows that Doorstep Dispensaree failed to take account of the risks that were presented by the processing, in particular from accidental or unlawful destruction, loss, unauthorised disclosure of or access to the personal data stored, when assessing the appropriate level of security, in contravention of Article 32(2) GDPR.
45. In addition, because it has adopted inadequate data protection policies, and kept inadequate records of its data processing activities and security measures, Doorstep Dispensaree is unable to demonstrate that its processing is performed in accordance with GDPR: a further infringement of Article 24(1) GDPR.

Contraventions of Articles 13 and 14 GDPR

46. The Privacy Notice provided by Doorstep Dispensaree to the Commissioner did not contain all of the information required by Articles 13 and/or 14 GDPR. In particular, the Privacy Notice:
 - a. Implies but does not state explicitly that Doorstep Dispensaree is the controller, and gives no contact details (contrary to Article 13(1)(a) / 14(1)(a));
 - b. States in general terms the nature of the processing, but does not state the Article 6 legal basis, or Article 9 condition for processing special category data (contrary to Article 13(1)(c) / 14(1)(c));
 - c. Does not outline the categories of personal data concerned (contrary to Article 14(1)(d), where data are collected from third parties);
 - d. Does not specify the legitimate interest relied on, if it is the case that Article 6(1)(f) is the condition for processing (contrary to Article 13(1)(d) / 14(2)(f));

- e. Does not explain the recipients or categories of recipients of the personal data (contrary to Article 13(1)(e) / 14(1)(e));
- f. Does not state the retention period for personal data, or criteria for determining the retention period (contrary to Article 13(2)(a) / 14(2)(a))
- g. Does not inform the data subject of his/her rights of access, erasure, rectification and restriction (contrary to Article 13(2)(b) / 14(2)(c));
- h. Does not inform the data subject of his/her right to withdraw consent to processing, to the extent that this is the condition relied on (contrary to Article 13(2)(c) / 14(2)(d));
- i. Does not inform the data subject of his/her right to lodge a complaint with the supervisory authority (contrary to Article 13(2)(d) / 14(2)(e))
- j. Does not outline the sources from which personal data originate (contrary to Article 14(2)(f), where data are collected from third parties);
- k. Does not state whether the provision of personal data is a statutory or contractual requirement (contrary to Article 13(2)(e), where data are obtained from the data subjects).

Factors relevant to whether a penalty is appropriate, and if so, the amount of the penalty

47. The Commissioner has considered the factors set out in Article 83(2) GDPR in deciding whether to issue a penalty. For the reasons given below, she is satisfied that (i) the contraventions are sufficiently serious to justify issuing a penalty in addition to exercising her

corrective powers; and (ii) the contraventions are serious enough to justify a significant fine.

48. Doorstep Dispensaree has sought to downplay the seriousness of the contraventions other than the Breach; that is, those relating to its practices and procedures. Contrary to its representations, the Commissioner considers that these breaches are both repeated, and negligent in character. They would, taken on their own, be serious; taken with the Breach, the Commissioner considers that they are clearly sufficiently serious to warrant a penalty. Insofar as Doorstep Dispensaree prays in aid the changes it has since made to its practices and procedures: these are not relevant to how seriously defective the practices were at the date of the Breach. The Commissioner has, however, had regard to this factor in relation to the PEN, and as a potential mitigating factor when considering the appropriate amount of the fine, as explained further below.

(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;

49. **Nature:** the Breach relates to the security of special category data that should have been treated with the utmost care. Any controller in the kind of business carried on by Doorstep Dispensaree ought to be well aware of its data protection obligations and be taking them far more seriously. The Commissioner therefore considers that the Breach resulted from a highly culpable degree of negligence on the part of Doorstep Dispensaree.

50. Equally, because of the sensitivity of the data, the Commissioner considers that it was particularly important to ensure that data subjects were provided with all of the information required by Article 13 and 14 GDPR, but Doorstep Dispensaree paid little or no attention to its regulatory obligations in this respect.
51. **Gravity:** the Commissioner considers that the Breach is very serious as it concerns highly sensitive information that was left unsecured in a cavalier fashion. The data subjects can be very readily identified and linked to data concerning their health. Given the nature of Doorstep Dispensaree's business supplying medicines to care homes, it appears likely that a high proportion of the affected data subjects are elderly or otherwise vulnerable.
52. Likewise, there are very serious shortcomings in the information provided to data subjects through the privacy policy. This is a significant infringement of the data subjects' right to transparency about the processing of their personal data, and is made more serious by the sensitive nature of the data. The data subjects had a right to know exactly what Doorstep Dispensaree was doing with their data, but Doorstep Dispensaree failed to tell them in anything like enough detail. Furthermore, no data subject would reasonably expect that personal data relating to their health would be handled in the manner that it was handled by Doorstep Dispensaree.
53. **Duration:** The Commissioner has been unable to confirm the exact duration of the Breach. However, given the age of some of the data, she is satisfied that it has been occurring, to some extent, since at least 25 May 2018, and she has not considered any contravention prior to this date, which would be considered under the previous data protection regime.

54. For the purposes of considering the infringement of Articles 13 and 14 GDPR, the Commissioner has likewise taken account only of the inadequacies of the privacy notices as relied on by Doorstep Dispensaree since 25 May 2018, when the GDPR entered into force.
55. **Number of data subjects affected:** The number of affected data subjects affected by the Breach cannot be confirmed but there were 47 crates, 2 disposal bags and one box containing personal data. In total there were approximately 500,000 documents. The MHRA suggested to the Commissioner that the documents related to around 78 care homes; however in its representations Doorstep Dispensaree stated that it currently has dispensing contracts with 15 care homes, although previously it was 27. Regardless of the exact number of care homes involved, given the volume of documentation and size of Doorstep Dispensaree's business it appears likely that hundreds, and possibly even thousands of data subjects have been affected. The failings in relation to Arts. 13 and 14 are also likely to have affected large numbers of individuals.
56. **Damage:** The Commissioner understands that the data subjects are not aware of the Breach, but were they to become aware it could cause high levels of distress, although financial damage is unlikely. The infringements of Articles 13 and 14 may have caused distress in the form of confusion or uncertainty about Doorstep Dispensaree's processing of sensitive personal data.

(b) the intentional or negligent character of the infringement

57. The Commissioner has treated both the Breach and Article 13 and 14 infringements as a case of a negligent rather than a deliberate infringement. However, she stresses that in both cases there is considerable evidence of extremely poor data protection practice, amounting to significantly negligent conduct.

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

58. The Commissioner is unaware of any mitigation measure that Doorstep Dispensaree may have taken, although there is no suggestion that the infringement is ongoing as the documents have been seized by the MHRA and are being stored securely.
59. The Commissioner has taken into account the improvements to its data protection practices which Doorstep Dispensaree states in its representations that it is currently making, or intends to make. The Commissioner acknowledges that Doorstep Dispensaree is now taking steps to improve both its written policies and contractual arrangements, and the level of training provided to its staff. These changes, if properly implemented, are likely to mitigate the on-going infringement of data subjects' privacy rights arising from breaches of Articles 13 and 14. The Commissioner has given some credit for this factor when considering the appropriate amount of the penalty, but she notes that some of the policy documents provided remain in template form.

(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

60. As set out above, there is little to no evidence that measures to ensure data protection by design and default were in place, as required by Article 25, nor that any technical or organisational measures were in place to protect the affected data as required by Article 32. This is a major failing for a controller that routinely processes large quantities of highly sensitive health data and accordingly the Commissioner considers that Doorstep Dispensaree bears full responsibility for these infringements. Likewise, it bears full responsibility for the shortcomings of its privacy notice. The requirements of the GDPR were extensively publicised in the period before it entered into force and it was incumbent on Doorstep Dispensaree to ensure that it complied. The Commissioner does not accept that the role of Joogee absolves Doorstep Dispensaree of responsibility. As the controller Doorstep Dispensaree was required to ensure the security of any processing undertaken by it or on its behalf.

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

61. The Commissioner is unaware of any previous data protection infringements by Doorstep Dispensaree.

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

62. Doorstep Dispensaree's level of co-operation with the Commissioner's investigation was poor. It did not engage with the Commissioner and multiple chasing e-mails have been required to achieve responses to enquiries. Doorstep Dispensaree tried unsuccessfully to appeal the Information Notice, when it was open to it simply to rely on s.143(6) to withhold any information that might be self-incriminating. However, the Commissioner accepts that these failings have not hampered either the remedying or the mitigating of the infringement, as the data are now secure (albeit due to the actions of the MHRA) and the data subjects unaware of the incident. The Commissioner also acknowledges and has given credit for the more co-operative approach demonstrated by Doorstep Dispensaree in its representations, and the action it is taking to improve its data protection practices.

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

63. These include information allowing very easy identification of individuals (name, address, date of birth) and sensitive, special category data relating to health (medical information, prescriptions).

(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

64. Doorstep Dispensaree did not notify the Commissioner. She was notified by another regulator carrying out a criminal investigation.

(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;

65. Not applicable.

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

66. Not applicable.

(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.

67. It is possible that there was a modest financial gain to Doorstep Dispensaree from saving the costs of secure destruction or appropriate storage for the documentation.

Summary and decided penalty

68. For the reasons above, the Commissioner considers that the Breach was extremely serious, and demonstrates a cavalier attitude to data protection. The systemic nature of Doorstep Dispensaree's data protection failures is underlined by the fact that its policies and procedures are outdated and inadequate. In particular, its Privacy Notice falls far short of the requirements of Article 13 and 14 GDPR.

69. The Commissioner has taken into account the size of Doorstep Dispensaree and the financial information that is available about the company on the Companies House website, as well as the representations that Doorstep Dispensaree has made to her about its financial position. She is mindful that the penalty must be effective, proportionate and dissuasive.
70. Taking all of the above factors into account, the Commissioner has decided to impose a penalty in the sum of £275,000 (two hundred and seventy five thousand pounds).

Payment of the penalty

71. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by **17 January 2020** at the latest. The penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.
72. There is a right of appeal to the First-tier Tribunal (Information Rights) against:
 - (a) the imposition of the penalty
and/or;
 - (b) the amount of the penalty specified in the penalty notice.
73. Any notice of appeal should be received by the Tribunal within 28 days of the date of this penalty notice.

74. The Commissioner will not take action to enforce a penalty unless:

- the period specified within the notice within which a penalty must be paid has expired and all or any of the penalty has not been paid;
- all relevant appeals against the penalty notice and any variation of it have either been decided or withdrawn; and
- the period for appealing against the penalty and any variation of it has expired.

75. In England, Wales and Northern Ireland, the penalty is recoverable by Order of the County Court or the High Court. In Scotland, the penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

76. Your attention is drawn to Annex 1 to this Notice, which sets out details of your rights of appeal under s.162 DPA 2018.

Dated the 17th Day of December 2019

Signed

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

Rights of appeal against decisions of the commissioner

1. Section 162 of the Data Protection Act 2018 gives any person upon whom a penalty notice or variation notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.
2. If you decide to appeal and if the Tribunal considers:-
 - a) that the notice against which the appeal is brought is not in accordance with the law; or
 - b) to the extent that the notice involved an exercise of discretion by the Commissioner, that she ought to have exercised her discretion differently,

the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

GRC & GRP Tribunals
PO Box 9300
Arnhem House
31 Waterloo Way
Leicester
LE1 8DJ

- a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.

- b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.
4. The notice of appeal should state:-
- a) your name and address/name and address of your representative (if any);
 - b) an address where documents may be sent or delivered to you;
 - c) the name and address of the Information Commissioner;
 - d) details of the decision to which the proceedings relate;
 - e) the result that you are seeking;
 - f) the grounds on which you rely;
 - g) you must provide with the notice of appeal a copy of the penalty notice or variation notice;
 - h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.
5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.
6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and Tribunal

Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules
2009 (Statutory Instrument 2009 No. 1976 (L.20)).