

DATA PROTECTION ACT 2018 (PART 6, SECTION 149)

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

ENFORCEMENT NOTICE

TO: Doorstep Dispensaree Ltd

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

1. Doorstep Dispensaree Limited ("**Doorstep Dispensaree**") is a "controller" as variously defined in sections 3(6), 5 and of the Data Protection Act 2018 ("the DPA") and Article 4(7) of the General Data Protection Regulation ("the GDPR").
2. The Information Commissioner ("**the Commissioner**") has decided to issue Doorstep Dispensaree with an Enforcement Notice under section 149 DPA. The Notice is in relation to contraventions of the (i) data protection principles set out in Article 5 GDPR; (ii) the data subject's rights set out in Articles 13 and 14 GDPR; and (iii) the obligations of the controller in Articles 24(1) and 32. This Notice is accordingly issued under section 149(2)(a), (b) and (c) DPA.
3. This Enforcement Notice explains the Commissioner's decision, including the account the Commissioner has taken of the representations made by Doorstep Dispensaree on 11 September 2019, in response to the Preliminary Enforcement Notice issued on 25 June 2019.

Legal framework for this Notice

4. The DPA contains enforcement provisions in Part 6 which are exercisable by the Commissioner.

5. Section 149 DPA materially provides:

“(1) Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an “enforcement notice”) which requires the person—

(a) to take steps specified in the notice, or

(b) to refrain from taking steps specified in the notice,

or both (and see also sections 150 and 151).

(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);

(d) a requirement to communicate a personal data breach to the Commissioner or a data subject under section 67, 68 or 108 of this Act;

(e) the principles for transfers of personal data to third countries, non-Convention countries and international organisations in Articles 44 to 49 of the GDPR or in sections 73 to 78 or 109 of this Act.

...

(6) An enforcement notice given in reliance on subsection (2), (3) or (5) may only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failure.”

6. Section 150 DPA materially provides:

"(1) An enforcement notice must—

- (a) state what the person has failed or is failing to do, and
- (b) give the Commissioner's reasons for reaching that opinion.

(2) In deciding whether to give an enforcement notice in reliance on section 149(2), the Commissioner must consider whether the failure has caused or is likely to cause any person damage or distress.

(3) In relation to an enforcement notice given in reliance on section 149(2), the Commissioner's power under section 149(1)(b) to require a person to refrain from taking specified steps includes power—

- (a) to impose a ban relating to all processing of personal data, or
- (b) to impose a ban relating only to a specified description of processing of personal data, including by specifying one or more of the following—
 - (i) a description of personal data;
 - (ii) the purpose or manner of the processing;
 - (iii) the time when the processing takes place.

(4) An enforcement notice may specify the time or times at which, or period or periods within which, a requirement imposed by the notice must be complied with (but see the restrictions in subsections (6) to (8))."

7. The data protection principles are now set out in Article 5(1) GDPR. Compliance with the principles is the responsibility of the controller: Article 5(2).

8. In particular, controllers are required to implement appropriate technical and organisational measures to ensure that their processing of personal data 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

9. 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.

10. 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.

11. Chapter III of the GDPR makes provision for the rights afforded to data subjects. These include, by Articles 13 and 14, the rights to

receive from the controller certain information about the processing of their personal data.

Doorstep Dispensaree's Processing of Personal Data

12. 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 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.
13. 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
14. 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.

15. The Commissioner investigated this issue and obtained copies of a number of Doorstep Dispensaree's data protection policies. These gave her further cause for concern, as they did not comply with the requirements of GDPR. 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 outline staff responsibilities, the practical advice provided to staff in relation to data protection is vague. The few procedures and guidelines which do make reference to the GDPR (the Data Protection Officer Guidance and Checklist, and the Definitions and Quick Reference Guide) are templates from the National Pharmacy Association and they do not appear to have been incorporated by Doorstep Dispensaree.
16. 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);

17. Furthermore, the Privacy Notice makes no mention of automated decision-making, or any further processing for a purpose other than that for which the data were collected. If these activities are undertaken by Doorstep Dispensaree, they must be specified in the Privacy Notice, in accordance with Articles 13(2)(f)/(14(2)(g) and 13(3) and 14(4) respectively.

18. With its representations in response to the Commissioner's Preliminary Enforcement Notice, Doorstep Dispensaree provided a witness statement from its Director, together with exhibits. Doorstep Dispensaree explained the ways in which it was seeking

to improve its data protection policies, by adopting more comprehensive documentation, improving the data protection information given to customers, and by better training of staff. The Commissioner welcomes the positive steps that Doorstep Dispensaree has taken. However, she notes that some of the policy documents provided remain in template form, and furthermore that Doorstep Dispensaree's director states that the actions outlined in the Preliminary Enforcement Notice are ones which Doorstep Dispensaree 'either have taken or will in the near future be taking'. She therefore considers Doorstep Dispensaree's programme of data protection improvements to be a work in progress.

Issue of the Notice

19. The Commissioner considers that the past contraventions of GDPR by Doorstep Dispensaree are significant ones which warrant enforcement action. Her reasons for this conclusion include that:
 - Doorstep Dispensaree routinely processes sensitive, special category personal data relating to health;
 - It supplies medicines to numerous care homes, and so a large number of data subjects are affected, many of whom are likely to be elderly or otherwise vulnerable;
 - Doorstep Dispensaree's policies are inadequate and out of date;
 - Its poor data protection practices have already led to a very serious infringement in which large numbers of health records were left unsecured outside ("**the Breach**").
20. The Commissioner considered, as she is required to do under section 150(2) DPA when deciding whether to serve an

Enforcement Notice, whether any contravention has caused or is likely to cause any person damage or distress. Although the Commissioner understands that the data subjects are not yet aware of the Breach, were they to become aware it could cause high levels of distress, although financial damage is unlikely.

21. However, the Commissioner considers that compliance with the principles in Article 5, 13-14, 24 and 32 to be a matter of central importance to data protection law. Even if a failure to comply has not, or is not likely, to cause any person damage or distress, the issue of this Enforcement Notice to compel compliance would nonetheless be an appropriate exercise of the Commissioner's enforcement powers.
22. Having regard to the significant nature of the contravention, the scale of the personal data being processed and the context in which it is processed, the Commissioner considers that this Enforcement Notice is the proportionate regulatory step to bring Doorstep Dispensaree into compliance. As noted above, although Doorstep Dispensaree states that it intends to take many of the actions set out in this Enforcement Notice, it has not, even on its own case, yet carried out all of them. As the steps in this Enforcement Notice are all ones which should anyway be taken by any conscientious controller in the position of Doorstep Dispensaree in order to ensure compliance with its data protection obligations, the Commissioner does not consider that imposing the Enforcement Notice is unduly onerous. Moreover it is necessary, given the notable past failings of Doorstep Dispensaree in this regard.

Terms of the Notice and next steps

23. The Commissioner has therefore decided to exercise her powers under section 149 DPA to serve an Enforcement Notice requiring Doorstep Dispensaree to take specified steps to comply with the GDPR. The steps required are set out in Annex 1 of this Notice, which requires that they be completed **within three months of the date of this Notice**. Please also note the provisions in Annex 1 which require you to provide evidence to the Commissioner of your compliance with GDPR within the same timeframe.

Consequences of failing to comply with this Enforcement Notice

24. If a person fails to comply with an Enforcement Notice the Commissioner may serve a penalty notice on that person under section 155(1)(b) DPA requiring payment of an amount up to 20 million Euros, or 4% of an undertaking's total annual worldwide turnover whichever is the higher.
25. By virtue of section 162(1)(c) DPA, there is a right of appeal against this Notice to the First-tier Tribunal (Information Rights). If an appeal is brought this Notice need not be complied with pending determination or withdrawal of that appeal. Information about the appeals process may be obtained from:

First-tier Tribunal (Information Rights)
GRC & GRP Tribunals
PO Box 9300
Leicester
LE1 8DJ

Tel: 0300 1234504
Fax: 0870 739 5836
Email: GRC@justice.gov.uk
Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

26. Any Notice of Appeal should be served on the Tribunal within 28 calendar days of the date on which this Notice is sent.

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

TERMS OF THE PROPOSED ENFORCEMENT NOTICE

Doorstep Dispensaree shall, within three months following the date of this Notice (and following the permissible time for appealing this notice):

Policies

1. Update all policies, procedures and Standard Operating Procedures (SOPs) to ensure they are compliant with data protection legislation. Changes to current policies needed to ensure compliance include, but are not limited to:
 - Giving an overview of data protection legislation and how it has been incorporated by Doorstep Dispensaree.
 - Explaining your responsibilities as a controller.
 - Explaining staff responsibilities for protecting personal data.
 - Providing clear, detailed advice to staff on data handling and secure disposal. This could include 'step-by-step' guides and/or examples.
 - Providing guidance on what staff need to do in the event of a data breach.
2. Appointing a member of staff as 'Information Governance Lead' or Data Protection Officer and providing their contact details in the relevant policies. Outline when staff would be required to contact them and the information that would need to be provided. This

member of staff should also ensure that security measures are being adhered to and investigate security incidents.

Training

1. Mandatory data protection training should be given to all staff in the next 6 months.
2. There should be regular refresher training at least every two years.
3. Completion of such training must be monitored, properly documented and enforced.
4. Reiterate to staff the importance of protecting personal data and ensure they are familiar with Doorstep Dispensaree's policies and procedures.

Privacy Notice

1. Update privacy policy to include all information required under Article 13 and 14 of the GDPR ('The Right to be informed').

Providing Evidence of compliance

1. Provide to the Commissioner evidence that the steps set out above have been completed.