Data Protection Officer for Ephedra Healthcare Ltd Policy

Table of contents

1 Introduction 2
1.1 Policy statement 2
1.2 Status 2
1.3 Training and support 2

2 Scope 2
2.1 Who it applies to 2
2.2 Why and how it applies to them 2

3 Definition of terms 3
3.1 Data protection officer 3
3.2 Data Protection Authority 3
3.3 Data controller 3
3.4 Data processor 3
3.5 Data subject 3
3.6 Personal data 3
3.7 Processing 3
3.8 Recipient 4

4 Data protection officer 4
4.1 Requirement 4
4.2 Designation 4
4.3 Requirements 4
4.4 DPO tasks 4
4.5 DPO position 5
4.6 DPO involvement 6
4.7 DPO protected time 6
4.8 DPO dismissal 6

5 Summary 6

6 Agreement 7

1 Introduction

1.1 Policy statement

The General Data Protection Regulation (GDPR herein) came into effect on 25 May 2018 and was applicable by law in the UK as of this date. The GDPR is supplemented by the Data Protection Act 2018 (DPA18 herein); both the GDPR and DPA18 replace the Data Protection Act 1998 with the emphasis being on harmonising data privacy laws throughout the European Union (EU). This policy will outline the contractual obligations of the data protection officer (DPO).

1.2 Status

Ephedra Healthcare aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have in regard to the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

1.3 Training and support

Ephedra Healthcare will provide guidance and support to help those to whom it applies understand their rights and responsibilities under this policy. Additional support will be provided to The new Data Protection Officer to enable them to deal more effectively with matters arising from this policy. External training courses will be booked and attended within 2 months of this policy being produced

2 Scope

2.1 Who it applies to

This document applies to the nominated DPO and all directors of Ephedra Healthcare. Other individuals performing functions in relation to data protection within services of Ephedra Healthcare, are encouraged to use it. All admin staff and Clinicians working for Ephedra must be aware of the new laws and their implications to the general processes within the practice. All staff will now have to complete the GDPR module on Bluestream as mandatory.

2.2 Why and how it applies to them

Ephedra Healthcare Ltd has a responsibility to protect the information that is processed on behalf of its data subjects. This document has been produced to enable all staff to understand the role of the DPO in conjunction with the roles of data controllers and data processors in relation to the GDPR.

3 Definition of terms

3.1 General Data Protection Regulation

The EU GDPR replaces the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe.[1]

3.2 Data protection officer

This should be "an expert on data privacy", working independently to ensure compliance with policies and procedure. The law does not currently state what form the expertise needs to be but the DPO will be encouraged to qualify with the CIPP(E) course offered in London.

The Data Protection Officer for Ephedra is currently Corinne Nightingale an Associate Director of Ephedra Healthcare Ltd. She has undertaken training in July 18 for the anticipated certification under CIPP(e) and has also attended the annual NHS Information Governance Summit covering GDPR with the Caldicott Guardian for Spring House Medical Centre. She now plans to find an up to date course to attend to ensure her knowledge is up to date.

3.3 Data Protection Authority

National authorities tasked with the protection of data and privacy.

3.4 Data controller

The entity that determines the purposes, conditions and means of the processing of personal data. This should be the Caldicott Guardian for the data. This is currently Dr Royce Abrahams Ephedra Healthcare.

3.5 Data processor

The entity that processes data on behalf of the data controller. This would apply to all employees of Ephedra Healthcare Ltd currently with the exception of the cleaners. Our cleaners have all signed confidentiality agreements. It would also apply to all locums and agency workers.

3.6 Data subject

A natural person whose personal data is processed by a controller or processor.

3.7 Personal data

Any information related to a natural person or 'data subject'. This would apply to all patients

[1] EU GDPR

3.8 Processing

Any operation performed on personal data, whether automated or not.

3.9 Recipient

The entity to which personal data is disclosed. Consent must be gained for any third parties. Capacity must be established for under 16yr olds from a Clinician despite the new age of consent under GDPR being 13yrs

4 Data protection officer

4.1 Requirement

In accordance with Article 37 of the GDPR, a DPO is to be designated where:[2]

- The processing is carried out by a public authority or body, except for courts acting in their judicial capacity
- The core activities of the controller and processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes require regular and systematic monitoring of data subjects on a large scale
- The core activities of the controller or the processor consist of processing on a large scale special categories of data

4.2 Designation

The Freedom of Information Act 2000 states that the National Health Service (NHS) is a public authority and as a result it is a mandatory requirement for Ephedra Healthcare Ltd, to designate a DPO.

4.3 Requirements

To be able to undertake the role of DPO, the individual must be a subject matter expert (SME) in data protection law and the GDPR. Furthermore, the designated individual must have an acceptable level of understanding of Ephedra Healthcare's structure and data-processing procedures.

4.4 DPO tasks

Within Ephedra Healthcare Ltd the following are the core tasks of the DPO, as stated in Article 39:

- To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions
- To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or

processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits
- To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35
- To cooperate with the supervisory authority (ICO)
- To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter
- The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing

Recital 97 of the GDPR states that DPOs "should be in a position to perform their duties and tasks in an independent manner" and are not to be instructed how to deal with any data protection matters with which they are presented. The Directors of Ephedra Healthcare Ltd, acknowledges this and will permit the DPO to operate independently.

4.5 DPO position

Within Ephedra the data controller (i.e. the Caldicott Guardian) will ensure that the DPO is involved in all matters pertaining to the protection of personal data. More specifically:[3] The Data Controllers for Ephedra Healthcare will also involve the appointed DPO in all matters.

- The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge
- The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.
- Data subjects may contact the data protection officer with regard to all issues related to the processing of their personal data and to the exercise of their rights under this Regulation
- The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law
- The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests

4.6 DPO involvement

[3] Article 38 GDPR

Pursuant to the referenced articles, Ephedra Healthcare Ltd, will ensure that the DPO:[4]

- Participates in meetings of senior and middle management
- Is involved in decisions which may have data protection implications, enabling the DPO to provide SME advice
- Is consulted in the event of a data breach or any other incident involving personal data

If the practice opts not to follow the guidance of the DPO, the reasons for this are to be recorded and retained for audit purposes.

4.7 DPO protected time

For the DPO to be effective for Ephedra Healthcare Ltd, they are to be afforded the necessary time and resources to enable them to carry out their tasks effectively. The DPO will be allocated 2 hours week, to fulfil the tasks associated with the role.

Furthermore, Ephedra Healthcare Ltd, will provide:

- Adequate support in terms of financial resources, infrastructure and staff where appropriate
- Inform all practice staff of the designation of the DPO to ensure that their existence and function is known within the organisation
- Necessary access to other services, such as human resources, legal, IT, security, etc., so that DPOs can receive essential support, input and information from those other services
- Funding and time to undertake training in order to stay up to date with regard to developments within data protection

4.8 DPO dismissal

Article 38 is quite clear in stating that a DPO cannot be dismissed or penalised for performing their tasks as a DPO. However, a DPO can be dismissed justifiably for reasons such as theft, bullying and harassment or other acts deemed as gross misconduct. Ephedra will adhere to the terms and conditions of their contract of employment and job description. Matters of a disciplinary nature will be dealt with in accordance with the practice discipline policy.

5 Summary

It is essential that data-processing activities within Ephedra Healthcare are carried out in accordance with the GDPR and DPA18. By introducing the role of DPO to the practice, it provides demonstrable reassurance to data subjects that the practice is intent on complying with the regulations and maintaining excellent data protection standards.

[4] Guidelines on Data Protection Officers

6 Agreement

For Ephedra Healthcare, the role of DPO will be undertaken by Corinne Nightingale – Practice Manager – Spring House Medical Centre. It is acknowledged that this is an additional responsibility and, as such, the practice has taken into consideration the role requirements and the level of support necessary to enable the designated individual to carry out the role effectively.

I, Dr Vivian Tangang in my role as Clinical Director of Ephedra Healthcare Ltd and Clinical Lead for Spring House Medical Centre, agree to the conditions set out in this policy and will ensure that the DPO for Ephedra Healthcare Ltd is afforded the time and resources as outlined in this policy to undertake the role of DPO.

Signed:

Name: Dr Vivian Tangang

Role: Clinical Director of Ephedra Healthcare Ltd

I, Corinne Nightingale, agree to undertake the role of DPO for Ephedra Healthcare Ltd, in addition to my current role as Practice Manager of Spring House and Asst Director of Ephedra Healthcare Ltd and will adhere to the guidance and referenced material stated within this policy.

Signed:

Name: Corinne Nightingale

Role: Practice Manager