General Osteopathic Council

17

Council
31 January 2018
Preparing for the General Data Protection Regulation

Classification	Public
Purpose	For noting
Issue	The paper presents an update on the approach to updating the GOsC Information Governance Framework to meet the new requirements of the General Data Protection Regulation (GDPR).
Recommendation	To note the approach outlined in this paper for ensuring compliance with the GDPR
Financial and resourcing implications	Budget provision has been made for consultancy costs for this work.
Equality and diversity implications	None identified.
Communications implications	The Information Governance Framework is a public document published on the GOsC website.
Annexes	None.
Author	Sheleen McCormack

Background

1. The Information Governance Framework was considered by the Audit Committee in July 2014. Its purpose was to set out a comprehensive information governance assurance framework for preserving the confidentiality, integrity, security and accessibility of data processing systems and information held by the GOsC. The framework ensures that the GOsC complies with existing relevant legislative and regulatory requirements relating to the handling of information by preserving the confidentiality, integrity, security and accessibility of data held by the organisation. It also details the requirements placed on staff and non-executives.

2. EU Data Protection Directive 95/46 required all EU member states to implement data protection legislation which led to the UK enacting the Data Protection Act 1998 which came into force in March 2000.

3. However, the EU Directive was drafted prior to the exponential growth of the Internet and is now widely regarded as no longer fit for purpose, for example: personal data is now being used in ways that were not envisaged at the time through the use of 'big data', online advertising and social media. There has also been a public led, political impetus for stronger protection in the post-Snowden climate.

4. The new General Data Protection Regulation (GDPR) entered into force in May 2016 and has a two-year transition period, becoming applicable on 25 May 2018. This is the most significant change to data protection law in almost 20 years. In terms of scope, the GDPR will potentially repeal and replace the Data Protection Act 1998. The UK government has confirmed that the UK's decision to leave the EU will not affect the enforcement date.

Discussion

5. Article 1 of the regulation sets out two key objectives:

    - Protection of the fundamental rights and freedoms of individual persons, in particular, the protection of personal data
    - Protection of the principle of free movement of personal data within the EU.

6. Principles under the GDPR are very similar to the existing EU Data Protection Directive. However, the GDPR contains a number of changes including:

    - Enhanced documentation to be kept by data controllers
    - Enhanced Privacy Notices
    - More prescriptive rules on what constitutes consent
    - Mandatory data breach notification requirement
    - Enhanced Data Subject Rights
    - New obligations on Data Processors

- Appointment of Data Protection Officers
- Significant increase in the size of fines and penalties

7. The new law requires significant preparatory work and a full review of the GOsC Information Governance Framework from a GDPR compliance perspective is required. This is because while the GOsC is low on the risk scale, it is high risk given the type and amount of data we hold.

8. While the current Information Governance Framework means the GOsC is in a good position, it is currently not fully compliant and will require amending. Because of the scope and complexity of the work, WardHadaway law firm have been engaged to work with the Executive team on a consultancy basis to assist with preparations.

9. A preliminary meeting took place with Phil Tompkins, a partner at WardHadaway, on 7 November 2017. At this meeting the details for the project were finalised, including projected timelines for the interviews with staff. It was agreed that the first step is to build a comprehensive data map of all the data we hold (although the existing Information Asset Risk Register forms a good basis for this work). As an overview, the project encompasses:

    - Understanding of all the personal data GOsC holds

    - Mapping where such personal data is held, how it is used, why and by who

    - reviewing how data is kept accurate and up to date including how long data is held for

    - Reviewing existing data protection documentation

    - Reviewing the data protection provisions within key data processing contracts

    - Identifying any data protection risks and

    - Drafting a report and identifying good and bad data protection practice and drafting a gap analysis to identify the actions that need to be taken to get GOsC substantially compliant with data protection laws.

10. Pre-audit questionnaires on data use and practice, circulated to every employee in December 2017, have now been reviewed internally and by auditors at Wardhadaway. Follow up interviews based upon these responses were then carried out with individuals in the Communication team, Registration, Regulation, HR and IT in the week commencing 8 January 2018.

11. An audit report is now in the process of being drafted (due to be completed by end of January 2018) which will include a gap analysis identifying the compliance gaps and providing a route map with recommendations as to how

those gaps can be closed. Concurrent with this, an audit of existing documentation (including the Information Governance Assurance Framework and the Information Asset Risk Register) is being undertaken.

12. Staff and non-executives will require a programme of training to ensure awareness of their individual and collective responsibilities in respect of all the information held by the GOsC.

13. The whole process is expected to take 2-3 months up to the end of March 2018.

Recommendation: to note the approach outlined in this paper for ensuring compliance with the GDPR.