Audit Committee, 12 June 2018

GDPR preparedness activity

Executive summary

Introduction

The EU General Data Protection Regulations (GDPR) came into force from 25 May 2018. The GDPR replaces the Data Protection Act 1998 (DPA) in the UK.

Domestic legislation, the Data Protection Act 2018 received royal assent on 23 May. The Act reflects the GDPR and covers certain aspects of data protection law not within the remit of GDPR. The Act will remain in place post the UK's exit from the European Union when GDPR no longer directly applies.

The majority of the requirements of the GDPR were already required by the DPA 1998. Therefore, the HCPC's good standard of compliance with DPA makes the transition to GDPR easier. Our ISO27001 processes and documentation have also helped us in meeting the accountability and transparency aspects of GDPR.

However, there are new elements and enhancements required by GDPR that have required the HCPC to build on its compliance practice.

This paper provides a summary of the nature of GDPR changes and a summary of the work undertaken to date to ensure compliance.

GDPR what's new?

1. Personal Data

    1.1 Like the DPA 1998, the GDPR applies to personal data. However, the GDPR's definition is more detailed and includes a wide range of personal identifiers to constitute personal data, reflecting changes in technology and collection methods. For example an IP address is personal data under GDPR.

    1.2 Personal data that has been pseudonymised can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

1.3 The ICO has stated that for most organisations the change to the definition should make little practical difference.

2. Controllers and Processors

2.1 Unlike the DPA the GDPR applies to both data 'controllers' and 'processors'. The definitions are broadly the same as under the DPA, the controller says how and why personal data is processed and the processor acts on the controller's behalf. The HCPC is a controller, our print supplier for example, is classed as a processor when handling our data.

2.2 The GDPR places specific legal obligations on processors for example to maintain records of processing activities. Processors will also have more legal liability if they are responsible for a breach.

2.3 However, Controllers are still liable where a processor is involved in a breach. The GDPR places further obligations on Controllers to ensure contracts with processors comply with the GDPR and due diligence is carried out.

3. Data processing lawful basis

3.1 The most noticeable impact of GDPR changes is the use of consent as a basis for processing personal data. Under GDPR consent has to be explicit and opt in only. It should be granular and easy to withdraw at a future date.

3.2 This has led to many commercial organisations emailing out to their newsletter lists to obtain valid consent for ongoing marketing, as the original consent they obtained (if any) did not meet the new standards.

3.3 Lawful basis for public protection focused public bodies is actually simplified under GDPR. The HCPC is able to rely on its 'public task' as the basis for the vast majority of the processing we undertake. Those activities required by our legislation (the Order) are our public task.

4. Rights of Individuals

4.1 GDPR expands on the existing information rights of individuals (data subjects). Privacy notices require more information about the specifics of data processing.

4.2 A data subject may require the controller to erase their personal data on request, this is a 'right to erasure' often called the 'right to be forgotten'.

The right is not absolute and a number of specified grounds for refusal are available to controllers. Regulatory investigations are a basis for refusal.

4.3 The right to data portability allows a data subject to receive their personal data in a structured commonly used machine readable format to transmit to another data controller. For example to ease the switching of insurance providers or bank account.

4.4 Subject access under GDPR prohibits the use of a fee (DPA currently £10) and requires a response in 30 days (DPA 40).

5. Breach Notification

5.1 The GDPR places a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

5.2 A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. Only breaches that are likely to result in a risk to the rights and freedoms of individuals require notification. This has to be assessed on a case by case basis.

5.3 Failing to notify a reportable breach can result in a significant fine up to 10 million Euros or 2 per cent of global turnover.

6. Data Protection Officer

6.1 Under the GDPR a Data Protection Officer (DPO) must be appointed for public bodies and certain private companies. This can be an additional responsibility of an existing employee.

6.2 The DPO's minimum tasks are defined in GDPR:

- To advise the organisation and its employees about their obligations to comply with the GDPR
- To monitor compliance with the GDPR and manage internal data protection activities
- To be the first point of contact for ICO and data subjects

5.3 The GDPR also specifies the requirements of a DPO;

- Reports to the highest management level of organisation
- Operates independently and is not dismissed or penalised for performing their task
- Professional experience and knowledge of data protection law
- Adequate resources are provided to enable DPOs to meet their GDPR obligations

7. Accountability

7.1 The GDPR has a strong focus on accountability and governance. While the principles of accountability and transparency have previously been requirements of the DPA, the GDPR emphasises their significance.

7.2 Data controllers are expected to put into place comprehensive, but proportionate, governance measures. Good practice tools previously encouraged ICO, such as privacy impact assessments (renamed to Data Protection Impact Assessments DPIAs) and privacy by design will be legally required in certain circumstances.

7.3 The GDPR accountability principle requires data controllers to demonstrate compliance and state their responsibilities explicitly and publicly. Compliance can be demonstrated by;

- Implementing appropriate technical and organisational measures
- Maintaining relevant documentation on processing activities
- Appointing a Data Protection Officer
- Implementing measures that meet the principles of data protection by design and data protection by default.

8. Summary of HCPC GDPR preparedness activity

8.1 A gap analysis was reviewed by EMT in April 2017 and a number of work streams were agreed to achieve GDPR compliance. Activity undertaken in preparation for GDPR is summarised below.

8.2 The Executive has;

- Created a system of Data Protection Impact Assesment (DPIA) documents. The HCPC has used PIAs for some time, we built on the PIA process and formalised documentation to have one suite of compliant templates. Guidance to accompany the more formal process has been produced and internal communications activity undertaken to promote awareness.

- Created a new process within our QA system – Information rights.

- Revised our data protection policy to be more reader friendly, with a greater emphasis on transparency and the rights of an individual.

- Revised our privacy notices, included on our website and those issued through registration and FTP and registration data collection. The notices are

more focused on engagement type specific information and the information rights of individuals.

- Reviewed the use of consent within FTP, seeking to minimise this where possible and rely on our public task basis.

- Mapped out and documented the personal data the HCPC processes, including who, what, who gets it, where we get it from, why we collect it, our retention period and our legal basis in GDPR for processing. The HCPC is required to provide this information to any EU authority on request. For transparency we have included a version of this map as part of our privacy notice.

- Reviewed our newsletter sign up consent mechanisms, ensuring all are opt out and include an easy one click unsubscribe link in each mailing.

- Appointed the Governance Manager as DPO (a role that was already undertaken) and made this clear on our website and documentation.

- Scoped the additions required to our information security online training to cover GDPR changes, this includes the use of DPIAs for all employees.

- Undertaken focused internal communications on the main themes of GDPR and the key changes.

- Clarified the status of our Partners as data processors and amended our standard Partner contract.

- Amended our employee agreement for GDPR and revised our standard contract terms for suppliers, as well as agreeing a number of schedules to existing contracts where appropriate.

- Reviewed HCPC documentation and website content to replace references to DPA 1988 and the old principles and rights.

- Attended regular information sharing sessions with other regulators on GDPR and shared plans and approach where we can.

8.3 We are currently midway through a review of our retention policies. We are combining the FTP and organisational policies into one and reviewing our retention needs.

8.4 Our Policy team are also reviewing the Confidentiality Guidance for registrants, information has been published on our website about this review as well as signposting information about GDPR to registrants.

8.5 Our most recent (May 2018) ISO27001 audit touched on GDPR compliance preparation. The next audit in 2019 will be a full review of compliance.

9. Future areas for review

9.1 GDPR compliance will be an ongoing effort as best practise norms emerge, initially we have identified the following areas for future review;

9.2 Review of our powers to require information provision.

Article 25(1) of the Health and Social Work Professions Order 2001 gives us the power to make a person or organisation give us information or produce documents which are relevant to fitness to practise allegations.

Another regulator has recently undergone a campaign to re-frame this power in a more positive light, as a tool to smooth investigation requests with less concern from those providing data about lawful basis. While our legislation is different, as are our stakeholder links, we will establish if there is the scope (or a benefit) in making greater use of this power in investigations.

9.3 Data Minimisation

We will review our current practise to seek assurance that the data we request during investigations remains proportionate for our needs.

9.4 Comprehensive review of disclosure through FOI and Subject Access.

We want to ensure we remain in step with transparency best practise, reviewing recent case law and our own ICO decision notices. We also want to document our approach comprehensively for business continuity as this is a specialised skill.

Decision

The Committee is asked to note the paper.

Appendices

None

Background information

- ICO's guide to GDPR - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Date of paper
1 June 2018