Data Protection Act and GAPP Alignment

With the advent of increasing privacy laws and regulations, global data privacy risk has become one of the major drivers of spotlighting the role of IT auditors and how this role can help drive, through technological means, the protection of sensitive data. For private and public enterprises alike, their data are like gold. Key channel data can be generated—particularly in the pharmaceutical industry—through clinical trials, sales and marketing, information technology, human resources (HR), procurement, regulatory affairs, physical security and surveillance, and clinical service centers. Properly managing the compliance aspects of these data, once in the hands of the data controller, is essential for keeping the company in compliance with data authorities throughout the world.

This article will align the UK Data Protection Act of 1998 (DPA) and the American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP)1 in order to help global companies with a presence in both the US and the UK. The AICPA GAPP is aligned with the European Union (EU) Data Protection Directive (DPD) of 1995,2 which requires member states to protect people’s fundamental rights of freedoms. The DPA3 is derived from the EU Directive and, thus, by default, is a widely accepted framework that is applied specifically to companies operating in the UK.

EU AND UK DATA PROTECTION ACT

Companies that operate in the EU are required to follow basic principles that are set forth by the EU’s data protection commissioner. The data protection commissioner is responsible for upholding the rights of individuals as set out in the DPD and enforcing the obligations upon data controllers. The commissioner is appointed by the government and is independent in the exercise of his/her functions. Individuals who feel their rights are being infringed can complain to the commissioner, who will investigate the matter and take whatever steps may be necessary to resolve it.4 The DPD which defines personal data as information relating to an identified or identifiable natural person (Article 2(a) DPD).5

Similarly, the Information Commissioner’s Office (ICO) is the UK’s independent body set up to uphold information rights. The ICO mandates the DPA, which is based around eight principles of information handling best practices (figure 1) that are considered in good order by the Information Commissioner’s Office.

Figure 1—Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Harbor Privacy Principles. They also are recommended to follow the framework of the GAPP, which can be used as an operational framework to help multinational entities address privacy matters that take into consideration local, national or international requirements.

A FRAMEWORK FOR ASSESSMENT: DPA AND GAPP

One of the mechanisms that can be utilized to satisfactorily map out the DPA principles to the enterprise’s adapted privacy principles is to align the DPA with the AICPA GAPP. This is a foundational step to further the capability maturity model (CMM) of an enterprise from a data privacy compliance perspective. By going through the process of mapping out the DPA principles with the GAPP, the entity goes through the exercise of understanding which principles are pertinent, thus establishing current state versus future state. There are eight DPA principles that should be addressed in order to fulfill the ICO guidelines for managing personal data. Figure 2 offers an example of the DPA principles that were mapped to the GAPP. This is a starting point for one to

<table>
<thead>
<tr>
<th>Data Protection Principle/Guideline Control</th>
<th>Work Program</th>
<th>Entity A</th>
<th>Entity B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Personal data shall be processed fairly and lawfully.</strong></td>
<td>D.1.1.2 AICPA GAPP Alignment (Collection)</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>• Only collect and use personal information where it has lawful grounds and legitimate business reasons to do so.</td>
<td>D.1.1.2 AICPA GAPP Alignment (Collection)</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>• Be transparent in dealings with people as to what information about them it collects and how it will process their information.</td>
<td>D.1.1.14 Data Privacy Program—DPA</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.</strong></td>
<td>D.1.1.15 Data Privacy Program—EUDD/DPA Alignment</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>• If information is collected for a particular purpose, ensure that it will not be used for anything else until the individuals concerned have been informed and, where required, their permission obtained.</td>
<td>D.1.1.15 Data Privacy Program—EUDD/DPA Alignment</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td><strong>3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.</strong></td>
<td>D.1.1.5 AICPA GAPP Alignment (Monitoring and Enforcement)</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>• Do not ask for more information than needed for the purposes for which it is collected (even if the information would be useful to know).</td>
<td>D.1.1.5 AICPA GAPP Alignment (Monitoring and Enforcement)</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td><strong>4. Personal data shall be accurate and, where necessary, kept up to date.</strong></td>
<td>D.1.1.15 Data Privacy Program—EUDD/DPA Alignment</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>• Update records when informed by an individual that their details have changed.</td>
<td>D.1.1.15 Data Privacy Program—EUDD/DPA Alignment</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.</strong></td>
<td>D.1.1.15 Data Privacy Program—EUDD/DPA Alignment</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>• Comply with records retention policies and ensure the organization can justify why it need to retain each category of personal information.</td>
<td>D.1.1.15 Data Privacy Program—EUDD/DPA Alignment</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>• Ensure personal information is securely disposed of at the end of the appropriate period.</td>
<td>D.1.1.15 Data Privacy Program—EUDD/DPA Alignment</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>6. Personal data shall be processed in accordance with the rights of data subjects under this Act.</strong></td>
<td>D.1.1.15 Data Privacy Program—EUDD/DPA Alignment</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>• Ensure the right to opt out of receiving marketing communications.</td>
<td>D.1.1.15 Data Privacy Program—EUDD/DPA Alignment</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>• Ensure the right to have inaccurate information corrected.</td>
<td>D.1.1.15 Data Privacy Program—EUDD/DPA Alignment</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>• Ensure the right of access to data subject information.</td>
<td>D.1.1.15 Data Privacy Program—EUDD/DPA Alignment</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
begin to establish compliance with the DPA and the validation check of alignment with the GAPP.

The AICPA performed its own mapping of privacy concepts set out in domestic and international privacy regulations, laws and guidelines in relationship to the GAPP. Figure 3 lists the 10 Generally Accepted Privacy Principles.\(^6\)

**Figure 3—Generally Accepted Privacy Principles**

The following are the 10 *generally accepted privacy principles*:

1. **Management.** The entity defines, documents, communicates and assigns accountability for its privacy policies and procedures.
2. **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.
3. **Choice and consent.** The entity collects personal information only for the purposes identified in the notice.
4. **Collection.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.
5. **Use, retention and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual as provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. **Access.** The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality.** The entity maintains accurate, complete and relevant personal information for the purpose identified in the notice.
10. **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Source: American Institute of Certified Public Accountants Inc., and Canadian Institute of Chartered Accountants. Reprinted with permission.
CONCLUSION
Multinational companies that operate in the EU, and specifically in the UK, need to abide by an increasingly complex and regulated privacy landscape. The establishment of a proper framework is essential to assess the maturity level of the enterprise’s compliance as it pertains to protecting personal data of its customers, employees and partners. One of the best ways to conduct this is to establish the framework of the GAPP and tie it to the DPA. This will provide the enterprise with a sure way of mapping the frameworks and, more important, the transparency required to identify gaps, if any, that can be mitigated or addressed fully to comply with the privacy laws of the UK.

ENDNOTES
1 American Institute of Certified Public Accountants (AICPA), Generally Accepted Privacy Principles (GAPP), www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx

Enjoying this article?
• Read Personally Identifiable Information (PII) Audit/Assurance Program.
  www.isaca.org/auditprograms
• Learn more about, discuss and collaborate on privacy/data protection in the Knowledge Center.
  www.isaca.org/topic-privacy-data-protection