What Do I Need to Do to Comply with GDPR?

In April 2016, the European Commission adopted the General Data Protection Regulation (GDPR), which will replace existing European Union data protection laws. Companies doing business in the EU or processing or controlling the personal data of EU citizens have until May 2018 to reach full compliance with the new requirements. Failure to comply with GDPR can result in substantial penalties, including fines up to 4% of annual revenue.

GDPR Readiness Assessment

### PRIVACY PROGRAM MANAGEMENT

**PRIVACY ACCOUNTABILITY AND GOVERNANCE**

Although GDPR does not explicitly require companies to establish a formal data privacy department or team, the new regulatory regime does require the implementation of governance measures to demonstrate compliance with the requirements.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>1. Do you have updated corporate privacy policies in place, including website privacy statements, privacy notices, and internal privacy policies?</td>
<td></td>
</tr>
<tr>
<td>2. Do you have an established internal audit process to monitor data privacy related activities and compliance?</td>
<td></td>
</tr>
<tr>
<td>3. Do you train employees on data privacy and their associated responsibilities?</td>
<td></td>
</tr>
<tr>
<td>4. Do you evaluate and incorporate privacy and data protection considerations into strategic decisions, particularly related to new data collection or use initiatives, technology investments, or product innovations (i.e., “privacy by design”)?</td>
<td></td>
</tr>
</tbody>
</table>

Total “YES” Answers

### DATA PROTECTION OFFICER

Companies regularly processing or handling EU personal data must hire or appoint a data protection officer (DPO) with sufficient knowledge of data protection laws and obligations, adequate resources and independence to perform their role, and direct reporting to senior management.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>1. Do you have an individual with clearly assigned responsibilities for managing privacy compliance?</td>
<td></td>
</tr>
<tr>
<td>2. Do you provide your DPO with sufficient independent authority to perform their duties and direct reporting to the most senior levels of management?</td>
<td></td>
</tr>
<tr>
<td>3. Do you provide dedicated budget dollars or resources for privacy compliance activities?</td>
<td></td>
</tr>
</tbody>
</table>

Total “YES” Answers
PRIVACY PROGRAM MANAGEMENT (continued)

PRIVACY IMPACT ASSESSMENTS
GDPR requires companies to conduct data protection impact assessments, also known as privacy impact assessments or PIAs, to assess and address privacy risks in new projects, data uses, technology investments, or other initiatives.

1. Do you have a formal process in place to assess the privacy risks in corporate initiatives? □ Yes □ No
2. Do you document the results of all privacy reviews of corporate initiatives, including associated remediation efforts? □ Yes □ No
3. Do you have standard controls in place to address risks identified through the review process in a consistent manner? □ Yes □ No

Total “YES” Answers

DATA BREACH RESPONSE PLAN
Companies will now need to provide notification to supervisory authorities and affected individuals of any data breaches of EU personal data within 72 hours of learning of the incident.

1. Do you have a process or safeguards in place for identifying possible data breaches? □ Yes □ No
2. Do you have an updated breach response plan in place? □ Yes □ No
3. Have you communicated data breach response duties to responsible parties both internally and externally? □ Yes □ No

Total “YES” Answers

DATA PROCESSING AND USE

CROSS-BORDER DATA TRANSFER MECHANISMS
GDPR continues to restrict the transfer of EU personal data to countries deemed “adequate” by the European Commission or under specific types of data transfer agreements. Such restrictions also apply to the transfer of EU personal data to a non-EU third party providing processing or handling services on behalf of the company.

1. Do you have an approved data transfer mechanism (e.g., binding corporate rules, standard contract clauses, or Privacy Shield) in place to govern the transfer of EU personal data to outside the EU? □ Yes □ No
2. Do you have an updated data map in place to understand where EU personal data resides and how it is transferred within your company? □ Yes □ No

Total “YES” Answers

DATA SUBJECT CONSENT
Companies must now obtain affirmative consent (e.g., clicking “accept”) from EU data subjects regarding the collection and use of their personal information and will need procedures in place to document and verify the consent.

1. Do you currently require EU data subjects to provide affirmative consent before collecting or using their data? □ Yes □ No
2. Do you have procedures in place to document and verify data subject consent? □ Yes □ No
3. Do you have procedures place to document and grant data subjects’ requests to withdraw their consent? □ Yes □ No

Total “YES” Answers
**DATA PROCESSING AND USE (continued)**

**INDIVIDUAL DATA SUBJECT RIGHTS**

The new EU data protection regime both strengthens existing data subject rights and introduces new ones. The central theme of these individual rights is to provide data subjects with more transparency into what personal information will be collected and how it will be used, as well as providing data subjects with more ownership and control once their information has been collected.

1. Do you provide EU data subjects with clear notice of what personal information will be collected and how it will be used?  
   - [ ] Yes  
   - [ ] No

2. Do you have mechanisms in place to provide EU data subjects with timely access to their personal information and the ability to correct inaccurate or incomplete data?  
   - [ ] Yes  
   - [ ] No

3. Do you have procedures in place to enable EU data subjects to control the use of their personal data, including requesting deletion, objecting to or restricting data use, or taking their data elsewhere?  
   - [ ] Yes  
   - [ ] No

**CUMULATIVE “YES” ANSWERS**

<table>
<thead>
<tr>
<th>Privacy Accountability and Governance</th>
<th>Data Protection Officer</th>
<th>Privacy Impact Assessments</th>
<th>Data Breach Response Plan</th>
<th>Cross-Border Data Transfer Mechanisms</th>
<th>Data Subject Consent</th>
<th>Individual Data Subject Rights</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**0 TO 7 “YES” ANSWERS**

With the compliance deadline fast approaching, putting your privacy program in order should be a top priority. The most important thing to do first is to take stock of what you do have and to tackle longer term projects (e.g., developing a PIA process) while simultaneously checking shorter term initiatives off your to do list (e.g., update policies).

**8 TO 14 “YES” ANSWERS**

You may already have the foundation of a privacy program. To bring current efforts into full compliance, identify both program gaps and underperforming processes. Assign clear ownership (and deadlines) to individuals responsible for GDPR compliance initiatives and meet regularly to assess progress and make program adjustments.

**15 TO 21 “YES” ANSWERS**

You are likely well on your way to full GDPR compliance and may only need to augment existing efforts. Take time to not only make any necessary updates to existing program elements but also to test and refine new processes or policy changes. This is also a good time to create a strategic plan for the long-term development of your privacy program.

---

**GENERAL DATA PROTECTION REGULATION READINESS ASSESSMENT**

**CYBERSECURITY AND PRIVACY**

**MICHAEL P. HINDELANG** CIPP/US, CIPM  
313.465.7412  
mhindelang@honigman.com

**KARL A. HOCHKAMMER** CIPP/US  
313.465.7582  
khochkammer@honigman.com