SOLVING THE GDPR TANGLE, WITHOUT COSTING A FORTUNE

OUR SECOND PUBLICATION IN THE GDPR SERIES

REGULATORY PERSPECTIVES
January 30th, 2018
Volume - 2
Series - 2

By **Jeb Beckwith – Managing Director, GreenPoint Financial**
and **Sanjay Sharma, Ph.D. – Chairman, GreenPoint Financial**

GDPR Refresher

The General Data Protection Regulation (GDPR)[1] is the new, overarching regulation governing the security of personal data across all companies doing business in Europe or with Europeans. GDPR grants EU citizens eight specific personal data rights[2] including the Right of Access[3] to their personal data, the Right to be Forgotten,[4] and the Right of Data Portability. Organizations must be able to respond to requests within seventy-two hours, and penalties can amount to 4 percent of global revenues.

Three Steps to Solving the GDPR Challenge

1. **Initial Risk Assessment**. If you have no interaction with European Union (EU) citizens, then you have no GDPR exposure, but consider this question broadly. Even if you have no direct business operations in Europe, or your businesses are all business-to-business, you could still be exposed through incidental contact to **Personal Data (PD)**.[5] PD under GDPR include not only basic identity information such as name, address, and identification numbers,[6] but also personally indefinable data on **biometrics, political opinions, race, ethnicity, sexual orientation, and genetics**. Consider the following questions prior to ruling out the need for a GDPR remediation plan:
   a. Do any of your businesses sell or market to EU citizens?
   b. Is there a possibility you might employ any EU citizen?
   c. Do you have any investors who might reside in the EU or be citizens of the EU?

sanjay@greenpoint.financial
jeb@greenpoint.financial

GreenPoint> Financial
www.greenpoint.financial

d. Do you gather any personal data under requirements of other regulations such as anti-money laundering (AML), know your customer (KYC), HIPAA,[7] or other regulatory mandates?
e. Is it possible that any employee uses social media sites at work which could incidentally capture PD on E.U. citizens. Examples could include FaceBook, LinkedIn, Instagram, and Snapchat, as well as communications apps such as WhatsApp and Bloomberg Messenger.
f. Is it possible that any computer on your network might incidentally capture the political opinions or "personally identifiable web data"[8] of any EU citizen?

Incidental data ingestion at the corporate level can be insidious and costly under GDPR. If you answer yes to any of the questions above, then you'll need to establish a GDPR assessment and governance strategy. Even if you answer no to all these questions, you should establish a governance control that addresses any new initiative.

2. **Establish a Written, Transparent, Data Governance Structure**. GDPR defines three mandatory roles for compliance. These roles can be vested within stand-alone full-time equivalents (FTEs) or can be added responsibilities and authorities vested with existing staff. Attribution of these roles will vary based on the size of a company and the size of its potential overlap with EU PD. The important point is that companies must ensure there is an accountable person assigned to each of the roles below.
    a. **Data Controller (DC).** The DC defines and controls the processing of PD, both internally and through third-party vendors. This includes how PD are processed as well as the purpose for collecting, storing, and disposing of PD.
    b. **Data Processor (DP)**. DPs engage in the daily processing of PD. DPs may be internal to the company or may exist as third-party vendors.
    c. **Data Protection Officer (DPO).** The DPO is the principally responsible party for overall GDPR compliance. Specific responsibilities under Article 39[9] are to:
        i. **Inform and advise** the DC and DPs of their obligations;
        ii. **Monitor compliance** with this and other EU or Member State regulations related to PD;
        iii. **Provide advice and education** to other areas of the company regarding PD compliance;
        iv. **Cooperate** with supervisory authorities;
        v. **Act as the contact point for supervisory authorities** and consult with supervisors where appropriate.

Roles, responsibilities, and authorities for each of these positions should be communicated to and acknowledged by the responsible party or parties in writing at least annually. Revised acknowledgments should also accompany any change in responsible party. These records should be retained and available for audit or supervisory review at any time.

3. **Establish Clear Policies and Procedures to Prove High Data Hygiene Standards.** These should be openly communicated throughout your organization and should include:
    a. **A Culture of PD Minimization.** PD can be ingested in in many diverse ways. To protect the firm, consider the following protections:
        i. **Restrict the use of social media** sites using company infrastructure, particularly sites in which political opinions are regularly expressed;
        ii. **Establish clear policies** for the retention and processing of PD. These should include guidance on when PD must be retained for compliance with other regulations;
        iii. **Establish policies** and procedures for how and where required PD will be ingested, processed, stored, and removed. These should include time frames for retention and disposition;
        iv. **Establish policies** and procedures for regular scrubbing and removal of unneeded PD;
        v. **Establish annual internal audits** and compliance checks against policies and procedures. You should understand and remediate deficiencies prior to your supervisory audit.
    b. **End-User Computing (EUC) Tracking**. As discussed, PD can be ingested, processed, and stored in

multiple ways and locations within your organization. Clearly articulated and communicated EUC policies are your first line of defense for passing supervisory scrutiny. Comprehensive EUC policies should include direction to all employees on:

i. The definition of PD;
ii. Prohibited and allowed vehicles for PD ingestion;
iii. Procedures for reporting PD;
iv. Procedures for responding to and escalating PD requests on a timely (e.g., well within seventy-two-hour) basis;
v. Responsibilities and authorities of the DC, DPs, and DPO in monitoring and enforcing EUC policy compliance.

c. **Robust Data Compliance Technology.** Consistent GDPR compliance will not be possible without some assistance from EUC technology. Analysis of any internal or vendor solutions should include an assessment of the following capabilities:
   i. Tracking changes to critical XL, Word, PDF, email, and system files with similar or identical names stored in multiple locations;
   ii. Establishing reviewers and approvers for changes to critical files, particularly XL files;
   iii. Auditable reports and easy reconciliation creating reliable evidence for supervisory and internal audit review.
d. **A Culture of Responsiveness.** Consequences for GDPR noncompliance escalate dramatically with high-response latency. EU citizens have the right to request their PD be moved, destroyed, or revealed in a prompt and robust manner. Detailed policies and procedures that have considered the legitimate reasons for your company to retain data will expedite response times and mitigate the consequences of mistakes.

4. **Plan for Data Breaches.** It is estimated that only 4 percent of global data today is encrypted. Data breaches are now ubiquitous; it is no longer a matter of *if* your company will be breached, but *when*. Under GDPR, the consequences of a data breach are significant, but they can be greatly mitigated by rapid response. Consider taking the following steps before a breach.
   a. **Prepare a Written Plan**. The plan for a data breach must include roles and responsibilities for any employee who might encounter PD from an EU citizen. The plan should include specific details about identifying a potential breach, escalating the threat to the DPO, and the importance of rapid escalation. The plan should also include procedures for notifying the supervisor and any impacted individual.
   b. **Test the Plan**. GDPR requires that companies report breaches within seventy-two hours of an incident. You will only know if your processes and procedures can meet this test through periodic testing and evaluation. Results of these tests can be shared with your supervisor and/or compliance staff.
   c. **Limit Sharing**. PD must be carefully controlled. Restrictions should be put on sharing data with counter-parties or within jurisdictions that are known to have compromised data security protocols.

This is the second in our series regarding GDPR implementation. As we move closer to the May effective date, please look for further publications on lessons learned and best practices.

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, found at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.
2. Ibid., Chapter 3
3. Ibid., Article 15
4. Ibid., Article 17
5. Note that the EU definition of PD is significantly broader than other jurisdictions, such as the US definition of Personally Identifiable Information (PII). The EU definition of PD under the Data Protection Directive 95/46/EC is found at https://ec.europa.eu/health/data_collection/data_protection/in_eu_en.
6. Note that ID numbers include not only government issued IDs but may also include IP addresses, cookie data, and RFID tags that can be traced back to an individual.
7. Health Insurance Portability and Accountability Act of 1996, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/health-insurance-portability-and-accountability-act
8. Such as IP addresses, RFID tags, cookie data, or location tracking
9. https://gdpr-info.eu/art-39-gdpr/