FASTEN YOUR BELTS FOR GDPR

DATA COMPLIANCE PENALTIES COULD COST YOU 4% OF GLOBAL REVENUES!

REGULATORY PERSPECTIVES
January 10th, 2018
Volume - 1
Series - 2

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

What is GDPR?

General Data Protection Regulation (GDPR)[1] is the new, overarching regulation governing the security of personal data that applies to all companies doing business in the European Union (EU). GDPR grants EU citizens both the Right of Access[2] to their personal data, as well as the Right to be Forgotten[3].

With **penalties of up to 4% of global revenues for any company conducting business within the EU**, the impact of GDPR will be felt far beyond Europe. All companies doing business in the EU will be impacted by GDPR. Financial institutions, already saddled with burdensome regulation on personal data retention, will bear the added burden of knowing what data must be destroyed. This will include the requirement for an auditable record for every spreadsheet, email, Word and PDF documents containing personal data on EU citizens. Within those files, each piece of data will need to be tagged for mandatory retention or disposal.

The process for tagging will need to be designed to continually resolve conflicts between GDPR and other regulations. Further, these processes will need to capture each iteration of documents drafted across all parts of each data collection process. The number of draft documents are generally multiples of the final ones used for compliance with Anti-Money Laundering (AML), Know-Your-Customer (KYC), Base Erosion and Profit Shifting (BEPS) and other financial regulations. In our estimation, the complexity of these

sanjay@greenpoint.financial
jeb@greenpoint.financial

GreenPoint> Financial
www.greenpoint.financial

already burdensome tasks will more than double under GDPR.

Why Non-European Companies Should Care

GDPR imposes rules and restrictions on the personal data of all EU citizens regardless of where that data resides, how it is used, or how it was originated. The penalty for non-compliance also applies to companies that have **only a small part of their business but fines are assessed on global revenues and can be substantial (upto 4%)**. Examples of companies which could fall under the GDPR purview include a U.S. broker-dealer distributing bonds through a European platform, a Japanese bank issuing retail notes to European investors, a Canadian wealth management platform servicing European clients, or a U.S. private equity firm with EU citizens as investors. Even banks without a European presence but servicing the correspondent banking needs of their European clients could be ensnared in the GDPR regulation.

The Need for Centralized Control

For most financial institutions, centralization of GDPR compliance should be mandatory. The regulation itself requires the appointment for a centralized **Data Protection Officer (DPO)** if a company is a:

1) Public authority, or an
2) Organization that engages in large scale systematic monitoring, or an
3) Organization that engages in large scale processing of sensitive personal data.[4]

AML/KYC regulation in most jurisdictions currently requires financial institutions to engage in "systemic monitoring" of personal data, thus causing most financial institutions to be classified under category 2 above. Even if that were that not the case, the penalties potentially imposed on the global enterprise for the regional non-compliance of a single business dictate that centralized data management and reporting is necessary.

Penalties for Non-Compliance

Thankfully, first infractions will generally receive only a written warning, particularly for unintentional offenses. Repeated non-compliance will be subject to harsher penalties. The guidelines prescribed for assessment of fines fall into two categories:

1) **Less Severe Infractions:** Up to the greater of €10MM or 2% of gross revenues for:
   a. Violations of the generic Data Controller obligations[5]
   b. Violations of the generic Certification Body obligations[6]
   c. Violations of the generic Monitoring Body obligations[7].

2) **More Severe Infractions:** Up to the greater of €20MM or 4% of gross revenues for:
   a. Violations of basic principles, in particular, those relating to Consent (see below)[8]
   b. Violations of Data Subject's rights of access and to be forgotten[9]
   c. Transfer of personal data to a recipient in a foreign country or an international organization[10]
   d. Valuations of any Member State law[11]
   e. Non-compliance with an order from a Supervisory Authority[12].

Other Key Facts

- **Effective Date**: May 25th, 2018

- **Regulation vs. Directive**: Under EU law, directives must be implemented regionally by the local jurisdictions within the EU. Regulations, on the other hand, carry the weight of law at the outset. On May 25th, the GDPR regulation will replace the prior directive. There will be no additional implementation required.

- **Definition of Personal Data**: Any information related to a natural person defined as a "Data Subject". This broad definition is not limited to name, address and phone number, but also includes email addresses, account numbers, photos, posts on social networking sites, medical records, and computer IP addresses. Information could be collected proactively, as with utility bills for KYC due diligence, or incidentally, as in an employee viewing the Facebook post of an EU citizen.

- **Data Breach Reporting**: Actual or potential data breaches must be reported within 72 hours, not only to the authorities, but also to the affected parties. Such breaches must include a description of the information at risk, which implies that the institution must have auditable records of all information they have on file.

- **Authority for Data Processing:** Companies may only lawfully process personal data if one of the following conditions exists:

  1) Consent has been obtained from the Data Subject (see consent definition below)
  2) Data Subject is party to or has requested a contract which requires processing
  3) **Data Controller** has a legal obligation to process data
  4) "Vital interests" of the Data subject or another natural person must be protected
  5) Data Controller must perform a task in the public interest or in the exercise of an official authority
  6) "Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, specifically where the data subject is a child"[13].

- **Consent**: GDPR defines two types of permissible consent.

  1) **Explicit Opt-In Consent**: Using clear and plain language, separate and apart from any other executed agreements, the Data Subject must give explicit consent for sensitive data to be processed by a company. A failure for such explicit consent defaults to an automatic "opt-out" of such consent.
  2) **Unambiguous Consent**: Unambiguous consent can be used for non-sensitive data, be must still be granted through a clear and transparent form understandable to a layperson

- **Pseudonymisation:** GDPR defines pseudonymisation as the process of transforming personal data into non-attributable, portfolio data through the use of encryption or by other means. Although GDPR encourages the use of pseudonymisation, this does NOT mitigate the need to track personal data transformed in this way. Not only does pseudonymisated data remain subject to GDPR requirements, but encryption keys must be separately stored and tracked from the transformed portfolio data with the original data reconstructable. Specific personal data must be destroyable upon request from the Data Subject.

Actions to Take Today

The field of End-User-Computing (EUC) can provide most companies with clear, transparent, and auditable views of their client data across multiple sources (XL, Word, email, databases, etc.) in a centralized format without interfering with the daily business of other activity. The process of implementing robust EUC procedures can be straightforward or complex, depending upon the organization and business structure, but in any event, it will be a necessary requirement for any financial institution operating in the E.U. or interacting with E.U. entities. By far, the most challenging obstacle for most companies is to define ownership and accountability for GDPR compliance. We provide the following guidelines that should be implemented across business lines and support functions.

- **Senior Management**:

  1) Appoint a **Chief Data Protection Officer (CDPO).** This may be a new position or additional duties for an existing employee. In either case, GDPR accountability should be assigned to a single management professional or a functional group. The CDPO function should be tasked with developing and implementing firm-wide technology, policies, and procedures which demonstrate GDPR compliance at a robust and granular level.
  2) **Educate** senior staff and business heads of the financial consequences for non-compliance to ensure robust cooperation with the CDPO.

3) Task the **audit** function with creating clear criteria for validation of policies and procedures developed by the CDPO.

- **CDPO:**

1) **Inform** the education process sponsored by senior management for the entire organization.
2) **Deploy** comprehensive and robust EUC software across the organization. GDPR requires centralized reporting which is only practical by using sophisticated EUC tools. This will also alleviate the need for regular intrusive interactions with business lines.
3) **Establish policies and procedures** for GDPR compliance which consider existing regulation and clearly articulate how potential conflicts should be handled.
4) **Vet** policies/procedures with experienced advisors and/or authorities and adjust based in recommendations prior to implementation.
5) **Monitor and report** variances and exceptions regularly and report to management on a quarterly basis at a minimum.

- **Audit:**

1) Create clear **criteria** for compliance with policies and procedures created by the CDPO
2) Conduct **audits at least annually** and consistent with other activities that are classified to entail **high operational risks.**

---

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April, 2016 found here➔ http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
2. Ibid, Article 15
3. Ibid, Article 17
4. Ibid, Article 37
5. Ibid, Articles 8, 11, 25-39, 42-43
6. Ibid, Articles 42-43
7. Ibid, Article 41(4)
8. Ibid, Articles 5-7, 9
9. Ibid, Article 12-22
10. Ibid, Article 44-49
11. Ibid, Chapter IX
12. Ibid, Article 58 (1)
13. Ibid