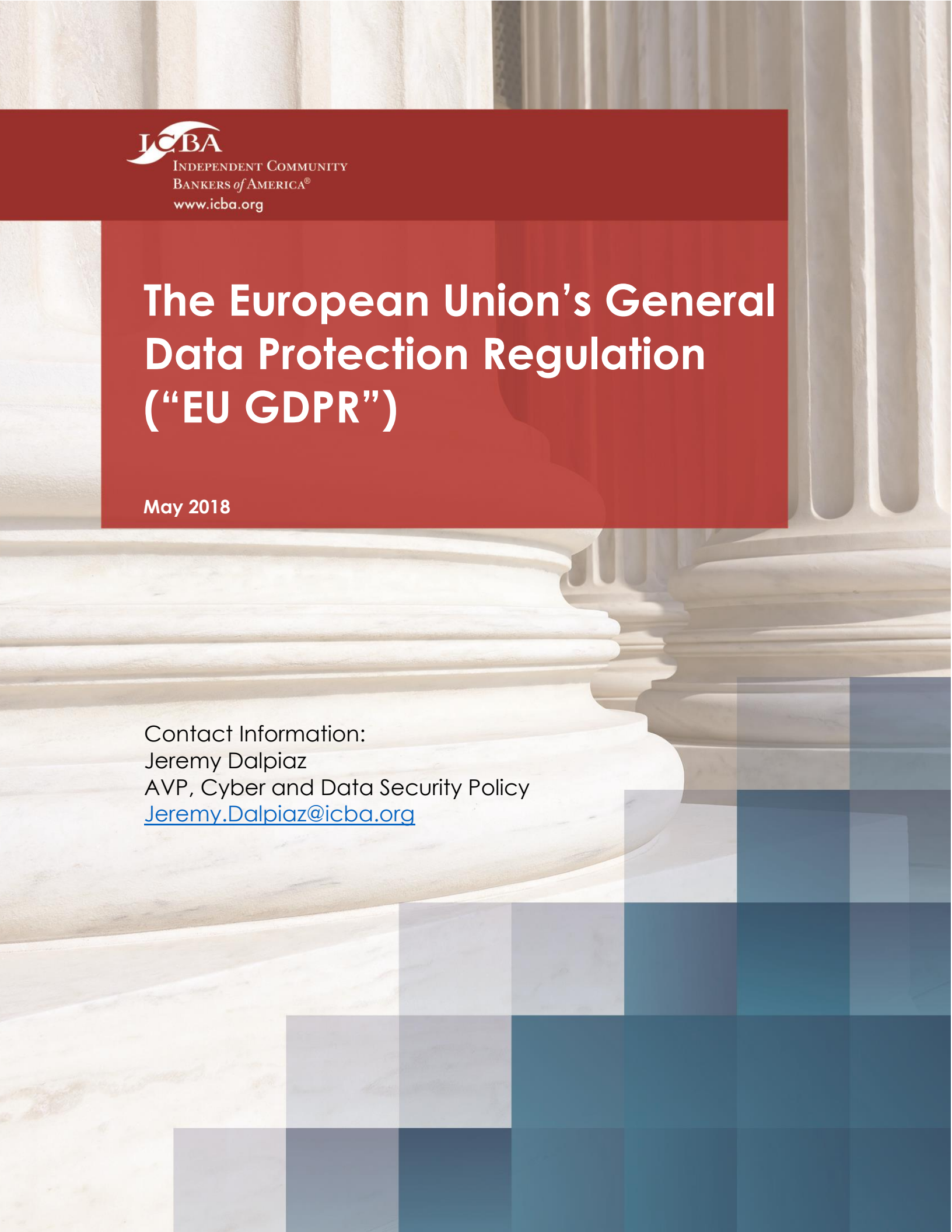

ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®
www.icba.org

The European Union's General Data Protection Regulation ("EU GDPR")

May 2018

Contact Information:
Jeremy Dalpiaz
AVP, Cyber and Data Security Policy
Jeremy.Dalpiaz@icba.org

EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION

I. BACKGROUND

The European Union ("EU") implements the General Data Protection Regulation ("GDPR" or "Regulation") on May 25, 2018, which dictates how businesses handle personal data of EU citizens and data subjects. In the EU, a regulation that is passed by the European Parliament and European Commission has direct legal effect throughout the EU. This Regulation replaces the 1995 "Data Protection Directive" (Directive 95/46/EC).[1]

II. OVERVIEW

Paramount to the GDPR is the EU legislative bodies' firm belief that data about an individual belongs to the individual and not to the business that collects the data about the individual. The individual has a right to the data and the individual, through control and deletion of their data, has a "right to be forgotten" (i.e., the individual has a right to privacy). That individual also has a right to obtain their data and take their data to another business. GDPR is wide-ranging and applies to companies within EU member states *and businesses across the globe*. While the application of EU GDPR for community banks may be limited, it is important to understand what GDPR is, why it is being implemented and some key elements of the Regulation.

III. SUMMARY

GDPR applies to "a company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; or, **a company established outside the EU offering goods/services (paid or for free) or monitoring the behavior of individuals in the EU."**[2] The Regulation has a broad territorial scope. It applies to a controller or processor

- "established in the EU,
- not established in the EU but offering goods or services to subjects in the EU,
- not established in the EU but monitoring behavior of subjects in the EU."[3]

Under GDPR, "personal data" is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online

---

[1]Blackmer, W. Scott. Info Law Group, LLP. https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/. 5 May 2016.
[2] European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en.
[3] KL Gates, "The new General Data Protection Regulation: Global impact, more duties, higher sanctions". http://www.klgateshub.com/files/Uploads/Documents/ACC_Webinar_GDPR_Final.pdf. Page 8. 24 May 2017.

identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person."[4] Additionally, GDPR carefully defines data controllers and processors. Understanding these definitions are key to understanding the Regulation.

A data "controller," is the original owner of the data. In the Regulation, data controller is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data...".[5]

A data "processor" is the "legal person, public authority, agency or other body which processes personal data on behalf of the controller."[6]

While a community bank may be established to serve a small area, or a targeted area of consumers within the United States and likely without branches outside of U.S. borders, some of the community bank's customers may be EU citizens or travel, study, or vacation within the EU. If the bank tracks the data of the individual while they are in the EU (i.e. by tracking a customer using website cookies), the bank may also be subject to provisions of GDPR. If the bank does engage in this activity, the bank may want to consider reviewing its disclosures specific to these customers [see "Compliance with GDPR," below].

"ENVISAGE"

The Regulation is clear that natural persons, or what is commonly referred to in the Regulation as a "data subject" should not be deprived of the protection for which they are entitled under this Regulation. Determining whether persons are entitled to this protection can be a murky exploration into the community bank's offerings, especially if the bank has EU citizens or American customers with a presence in the EU (whether while studying, traveling, living temporarily, etc.). To determine whether a bank is offering goods and services to such persons, or data subjects in the EU, "it should be ascertained whether it is apparent that the controller or processor **envisages** offering services to a data subject in one or more Member States in the Union."[7]

Envisage is not defined within the Regulation. The Merriam Webster dictionary defines "envisage" as "to view or regard in a certain way; to have a mental picture of especially in advance of realization."[8] Additional parameters for determining whether a company envisages offering services to a subject in the EU would be the use of a language or currency generally used in one more Member States,[9] or mentioning of customers or users

[4] EUGPR, Article 4 (1), 111. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.
[5] Council of the European Union: *General Data Protection Regulation*. Chapter 1, Article 4 (7). http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf. Page 111.
[6] Ibid. Article 4(8). 111.
[7] Ibid. 14.
[8] See: https://www.merriam-webster.com/dictionary/envisage.
[9] To see a full listing of EU Member States, see https://europa.eu/european-union/about-eu/countries_en.

who reside in the Union.

COMPLYING WITH EU GDPR

A community bank with EU citizens or American customers with a presence in the EU should conduct a risk assessment determining whether the bank is offering services to customers in the EU. If the bank contemplates offering services to EU data subjects, then the bank may most likely subject to the provisions of the GDPR.

If a bank determines it is likely subject to EU GDPR following a risk assessment, the bank should review its privacy and data collection disclosures. GDPR requires that, rather than assuming customers consent to the bank's privacy policy, customers must actively agree to very specific data collection policies. GDPR is very clear on this point:

> *Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.*[10]

Additionally, if a bank determines it must comply with GDPR, the bank should consult with competent counsel as there are several other conditions required for compliance with the Regulation, such as adherence to the rights of the data subject, including, but not limited to: breach notification, the right to access whether data is being processed by a data controller, the right to be forgotten (data erasure), data portability (i.e. the ability of the data subject to receive personal data concerning them and the right to transmit that data to another controller), privacy by design (i.e. including data protection from the onset of designing systems rather than adding data protection after the system is designed). Data processors are required to maintain certain records and employ a data protection officer.

In the event of a data breach, the GDPR requires the entity to report a "personal data breach" within 72 hours of becoming aware of the breach. The GDPR defines personal data breach as "a breach of security leading to

[10] Council of the European Union: *General Data Protection Regulation*. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf. Page18.

the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data, transmitted, stored or otherwise processed."

Noncompliance with the Regulation can be costly. The supervisory authority in Europe (the Information Commissioner's Office) can impose sanctions and other corrective measures before assessing fines. However, administrative fines may also be imposed at two levels. The first is up to €10M, or 2% annual global turnover (whichever is greater) or up to €20M, or 4% of annual global turnover (whichever is greater).

THE U.S. REGULATORY PERSPECTIVE ON EU GDPR

To date, none of the prudential U.S. financial regulators have issued any guidance about the applicability of EU GDPR to U.S.-based institutions. While the agencies may not examine for EU GDPR compliance, community banks should anticipate examiners asking banks if they considered EU GDPR compliance and how a decision was reached regarding such compliance. Banks are encouraged to speak with their regulators about the applicability of EU GDPR to their specific institutions. Community banks should also be aware there has been some question as to the level of applicability of the EU's Regulation to U.S.-based institutions as well as questions of enforceability of an EU-based regulation in the U.S. court system.

Community banks are advised to consult with appropriate and knowledgeable counsel about this Regulation as this summary is not meant to provide, nor constitute, legal advice.