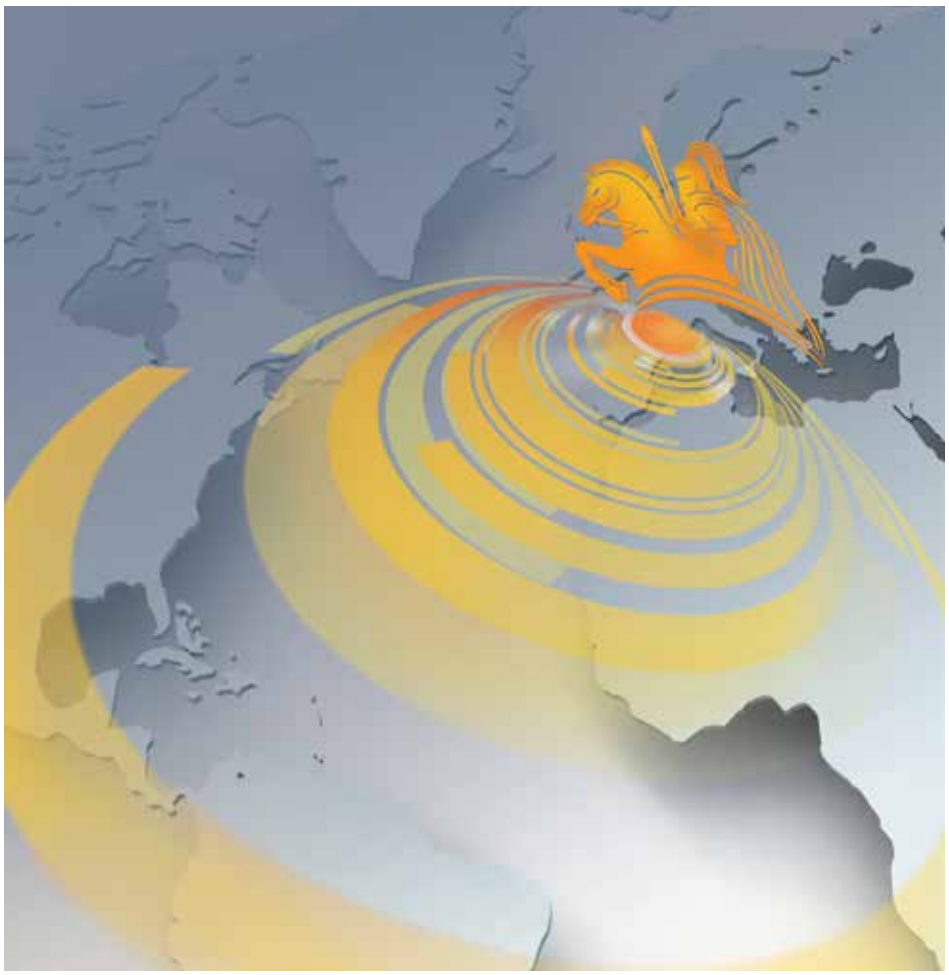
A Privacy Law Heard Around the World

Mortgage companies should take seriously new data-protection efforts spawned by EU

By Kathryne (Kate) M. Morris and Stacey Geringer



In the mortgage industry, compliance issues usually involve protections for borrowers in terms of equal housing opportunities, as well as loan quality or profitability. Typically, the industry focuses on compliance issues regarding privacy and data protection only when there is a data breach.

A new European Union (EU) law could and probably will change that. The EU's General Data Protection Regulation (GDPR), as well as similarly inspired legislative efforts in the U.S., are aiming to ensure businesses are transparent and accountable for how they collect, process, disperse and use personal data.

Companies across the globe have changed their business practices to offer privacy by default — and data protection by design — in response to GDPR, which went into effect May 25, 2018.

The regulation covers, among other things, borrowers' rights such as the right of data access, erasure and portability. Failure to comply with GDPR could result in fines of up to 20 million euros or 4 percent of the offending company's annual global revenue, whichever is higher.

These threats seem to have captured the attention of many industries, but the mortgage industry appears to be lagging behind, perhaps because many mortgage businesses have failed to see the need or are simply unaware of the regulation.

But it can have a real impact on mortgage companies in the U.S. What happens when

Continued >>

Kathryne (Kate) M. Morris is a privacy and technology lawyer in Dallas, Texas. Her practice focuses on data deals, technology transactions, e-commerce, and compliance with privacy and data-protection laws. Morris is a member of Clark Hill Strasburger's privacy, data and cybersecurity practice. She is certified by the International Association of Privacy Professionals as a certified information privacy professional in the United States (CIPP/US) and Europe (CIPP/E), and as a Certified Information Privacy Manager (CIPM). Reach Morris at kate.morris@clarkhillstrasburger.com.

Stacey Geringer has more than 25 years of experience in the development, sales and marketing of software products and services in the U.S., Europe and Central America. Geringer founded software companies Collabrian Design & Technology in 2000 and Mortgage Bank Solutions in 2006, and continues to serve as president of both companies. She started her career as a software developer at LTV Aerospace after graduating from the University of Texas with a degree in computer science. Reach Geringer at stacey@mortgagebanksolutions.com or (214) 684-9959.

Scotsman Guide

Reprinted from *Scotsman Guide* Residential Edition and ScotsmanGuide.com, November 2018

<< Continued

a German purchases a vacation home in Florida, for instance? The scope of GDPR is to protect all EU citizens, even ones who are doing business abroad. GDPR may apply even if a U.S. mortgage company has no employees or offices in the EU.

Although this still needs to be sorted out, it's clear this is an issue that isn't going away and is likely to be further addressed. Several states are looking at similar privacy protections, most recently with the California Consumer Privacy Act of 2018, which was signed into law this past June and goes into effect on Jan. 1, 2020.

Involve management

Most mortgage companies delegate data protection to their information technology (IT) departments and often allow IT, human resources and marketing teams to contract for services and software on their own. But compliance with GDPR requires a comprehensive and holistic approach in which privacy and data protection are interwoven into everyday operations, not just as responses to data breaches.

If you are collecting personal data from EU residents on loan applications or for other purposes, have data-storage locations and service providers in the EU, or even have a website with cookies that can track EU residents, then you need to prioritize compliance with GDPR now.

It may no longer be enough to ask whether a borrower is a U.S. citizen or not. Under GDPR, EU citizens have fundamental rights with respect to the processing of their personal data. So, if you are processing the personal data of an EU citizen, you need to know the law. Ignorance of citizenship is not a defense.

Now is the time to review how your company is handling these matters. The easiest way to start your company's compliance efforts is to get management involved in order to command attention, knock down departmental silos, establish a budget if necessary and ensure follow-through. Document their decisions and actions.

Reasonable steps

If GDPR is only now appearing on your radar, then it may be time to reach out to a privacy lawyer or hire an in-house lawyer with expertise on this subject, not only to provide GDPR-related compliance advice, but also to help your business deal with the evolving compliance risks posed both by new legislation and by outsourced services.

Note that in certain limited circumstances, GDPR actually requires the appointment of a data-protection officer who is qualified with, among other things, "expert knowledge of data protection law and practices." Expertise and a holistic approach to privacy, data protection and cybersecurity are valuable.

Consider alternative organizational models and web or mobile presences, including EU-based entities and websites. Some companies, whose primary exposure to GDPR arises through their websites, have even chosen to "go dark" in the EU, for the time being.

Now also is the time for your company to review and update its cybersecurity measures. GDPR requires the implementation of appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Consider the use of encryption. Encryption is not mandatory, but it may provide many defenses and solutions to common problems. Also consider independent certification standards, such as the ISO 27000 series. This is not mandatory either, but it can help show challengers the seriousness of your resolve and the reasonability of your steps.

Prepare data maps, inventories and other records of all personal data pertaining to EU (and California) residents. GDPR requires that you understand what personal data you are collecting and processing. You also are required to keep a record of all processing activities under your responsibility.

It is strongly suggested that you consider borrower information as a living entity, and as such, you should implement onboarding and offboarding policies and procedures, just like you do (or should do) for staff.

Serious risks

Review contracts with service providers and employees to ensure that they are GDPR compliant. The law requires that "data controllers" and "data processors" contract appropriately to protect personal data. You are one or the other. If you aren't already addressing privacy and data protection as part of your procurement and contracting process, it is time to start.

Transparency under GDPR requires that a data controller "be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject." Re-examine your website to confirm you know how and who is processing such data, review the related contracts with your service providers and update the privacy notice on your website so that it is GDPR compliant.

Prepare for data-subject requests from consumers. GDPR empowers individuals to request information related to their data privacy. The mechanics of responding to these requests need to be worked out in order to facilitate timely responses.

Update your written data-protection policies and procedures. The GDPR principle of accountability also requires documentation (such as incident-response plans, document-retention policies and procedures for responding to a requests related to data-subject rights, etc.) to prove compliance with GDPR.

Data protection is an issue for your entire business. Your employees should be aware of data-protection issues and your organization's related policies and procedures. Think of loan officers transferring borrower data into their customer-relationship management software for drip-marketing campaigns.

Continued >>

<< Continued

How will your company hope to prevent this, or even control it, if loan officers aren't aware of the regulations?

GDPR is here and the risks are serious. Unless your company can mechanically ensure that it has no contact with individuals or service providers in the EU, then you're at risk.

■ ■ ■

Finally, even if you have nothing to do with Europe or Europeans, your company is probably doing business with California or Californians, and the new California Consumer Privacy Act of 2018 requires you to safeguard the privacy of California residents in ways that are very similar to the GDPR. Now is the time to re-evaluate privacy and data protection in your business ■

Reprinted from *Scotsman Guide* Residential Edition and **ScotsmanGuide.com**, November 2018