CLARIFY

AGENCY

MEMO

To: Clarify Clients

From: Will Bunnett, Audrey Glaser

Date: April 18, 2018

Re: GDPR Compliance for U.S.-based organizations

Objective

This memo is intended to acquaint our clients with the General Data Protection Regulation (GDPR), outline the basics of GDPR compliance, and help you weigh the time and effort of GDPR compliance against the value of maintaining E.U. names on your list.

Note: We are not attorneys, and we highly recommend consulting with a licensed attorney who practices in this area to understand GDPR compliance and what strategy is right for your company. The guidance in this memo offers an overview of certain publicly discussed compliance criteria and is for informational purposes only, and not for the purpose of providing any legal advice or a legal strategy.

Background

On May 25, 2018, the European Union will implement a new law called the General Data Protection Regulation (GDPR). The GDPR places sweeping regulations on how businesses can collect, store, and use E.U. citizens' personal data. Even if you are a U.S.-based entity intended for a U.S.-only audience, you could be subject to the new law if you're storing any data from E.U. citizens -- even unintentionally.

While it's not yet clear if authorities could actually enforce the GDPR on American soil, no one will know for sure until the first test case gets prosecuted. And if the E.U. determines that your organization has violated GDPR, you may face an exorbitant fine – up to €20 million or 4% of global revenue, whichever is larger. The exact requirements of GDPR compliance depend on your organization's size and function, making qualified legal advice all the more important.

So we strongly recommend you move to understand what GDPR compliance entails, and weigh the time and effort of compliance against the value of keeping E.U. names on your list.

GDPR Compliance

Relevant GDPR principles

The GDPR aims to make sure that businesses treat peoples' data privacy and security as a primary concern rather than an afterthought. For U.S. companies, we see a handful of main principles in the hundreds of GDPR requirements:

- Right of consent: Consent to use someone's data must be "freely given, specific, informed, and unambiguous" – and also updated after a "reasonable" amount of time
- Right to access: A person's right to know what of their personal data a company is using, and how they're using it.
- Right to be "forgotten": The right to have one's data permanently deleted upon request
- Right to data portability: The right to have one's data transferred from one company to another company upon request
- Right to data security: Companies must provide a "reasonable" amount of protection and privacy to personal data, a standard which the GDPR governing body has not yet defined. Companies must report any data breaches to both supervisory authorities and the affected individuals within 72 hours of detection.
- Data assessments: Companies must regularly assess themselves to identify potential risks to data security and measures they are taking to mitigate risks.

Is it worth it for your organization to maintain E.U. names?

In all likelihood, no. Proper GDPR compliance will require taking on the costs of legal counsel as well as a labor-intensive audit of your organization's data facilities and processes. If E.U. names represent a minor segment of your list, you're probably better off removing them and foregoing GDPR compliance. If you choose this path, here are two important measures you could take:

1. Fully delete all E.U. citizen records from your CRM before 5/25/18, the day the GDPR goes into effect.
2. Update your opt-in forms to exclude E.U. citizens by requiring a validated U.S. zip code on each opt-in form. Legal summaries indicate that GDPR law

should not apply to U.S. companies that aren't targeting E.U. citizens. With this in mind, you should make sure your opt-in forms explicitly target U.S. citizens.

How do we comply with GDPR?

If you choose to continue storing or collecting E.U. names, prepare to re-evaluate how your organization acquires, stores, moves, and deletes user data. All of your data facilities and processes will need to meet GDPR's high standards around protecting individual privacy.

- Make sure your opt-in forms are GDPR-compliant:
    - Users need to actively consent by ticking a checkbox or radio button.
    - Pre-checked boxes or "By signing this you agree to sign up" disclaimers do not constitute consent.
    - Companies must obtain explicit consent for each intended use of an individual's data. For example, you have to obtain consent for each individual digital channel (i.e. email, SMS, calls) to use it for communications.
- Re-opt in your E.U. citizens before 5/25/18! (You most likely don't have record of their prior consent and/or cannot prove their consent was GDPR-compliant.)
- Check in with third-party providers who store and process your users' data. You'll need to make sure that they're set up to do the following:
    - Maintaining records of consent, from which you can retrieve granular details like when the consent happened and which uses of data the consumer consented to.
    - Regularly updating your consent records. The GDPR specifies that consent is time-limited, though it is up to each organization to decide the "appropriate" time to refresh users' consent. (The emerging rule of thumb is two years.) In practice, this means your data management service must be able to:
        - Notify you when a user's consent is nearing expiration
        - Send a (preferably automatic) request or series of requests to renew the user's consent
        - Unsubscribe and permanently delete the user's record if consent is not renewed in time, or the user requests a deletion
- Conduct a privacy impact assessment (PIA). If GDPR authorities investigate your organization for a privacy concern, they'll expect to see proof that you've conducted a PIA, or a documented self-audit in which you discuss, inventory, and mitigate the privacy risks inherent in the way you collect and store data through your web properties.

CLARIFY
AGENCY

Additional Resources

Here are a few additional resources if you'd like to learn more about the GDPR (which we highly encourage if you're thinking of attempting compliance!)

- Full text of the GDPR: https://gdpr-info.eu/
- The U.K. Information Commissioner's guide to the GDPR: https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/
- The "Privacy By Design" framework for GDPR-compliant developers: https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/

Again, we are not attorneys, and we highly recommend consulting with a licensed attorney who practices in this area to understand GDPR compliance and what strategy is best for your company. The guidance in this memo is meant to offer an overview of certain publicly discussed compliance criteria and is for informational purposes only, and not for the purpose of providing any legal advice or a legal strategy.