LAW.COM

An ALM Website

May 2, 2018

Are U.S. Records Retention Requirements on a Collision Course with the GDPR's 'Right to Erasure?'

U.S. laws require companies to retain records for years, and sometimes forever, and violating U.S. records retention laws can result in domestic fines and penalties. How can U.S. companies comply with the GDPR's "right to erasure" while still fulfilling their U.S. records retention obligations?

By Stacey Garrett

On May 25, 2018, many United States companies will find themselves subject to the European Union's sweeping General Data Protection Regulation (GDPR). The GDPR creates new rights that do not exist under — and may even conflict with — U.S. laws. One of those rights is the "right to erasure," which entitles individuals to have their personal data "erased" from company records within one month in some circumstances.

Violating the GDPR exposes companies to hefty fines of up to 4% of the company's worldwide revenue. *See*, GDPR, Art. 83(5). At the same time, U.S. laws *require* companies to *retain* records for years, and sometimes forever, and violating U.S. records retention laws can result in domestic fines and penalties. How can U.S. companies comply with the GDPR's "right to erasure" while still fulfilling their U.S. records retention obligations?

The obvious answer is that U.S. companies are legally required to retain the data under U.S. law. But the problem is that the GDPR recognizes only legal obligations imposed by EU and Member State law as a basis for processing personal data. Legal obligations imposed by other countries or states do not qualify.

U.S. companies can, however, lawfully reject an individual's request for erasure on other, less obvious grounds: that is that the companies have a "legitimate interest" in storing personal data to comply with U.S. records retention laws. Although companies may be tempted to invoke other GDPR grounds to justify their records retention, each of the other grounds is subject to pitfalls and should be avoided.

GDPR Application to U.S. Companies

To start, it is important to understand how the GDPR applies to U.S. companies. The GDPR applies to any person or company who processes personal data in connection with an organization that is established in the EU, and, on a long-arm, extra-territorial basis, to organizations that offer the sale of goods or services to, or who monitor individuals in, the EU. *See,* GDPR, Art. 3(1) and (2).

A few key concepts can help here:

What does it mean to be "established" in the EU? "Establishment" implies the effective and real exercise of activity through stable arrangements. *See,* GDPR, Recital 22. The bar here is relatively low. A single representative in the EU may satisfy the establishment requirement. *See, Weltimmo s.r.o. v. Nemzeti*

Adatvédelmi és Információszabadság Hatóság (2015), Case C-230/14, 1 October 2015.

What if a U.S. company is not physically located in the EU but does have an Internet presence that it uses to collect personal data in connection with offering goods or services to people in the EU? One-off transactions will not subject a company to the GDPR, but if it appears the company intended to direct the website to people in the EU, the GDPR will apply. Factors to consider are: whether the website uses a local language or an EU-domain name, whether the website displays prices in or accepts transactions in EU currency, and whether the website mentions customers or users in the EU. *See*, GDPR, Recital 23.

What is "personal data?" The definition of "personal data" is extremely broad. It includes any information relating to an identified or identifiable natural person. *See,* GDPR, Art. 4(a). It includes obvious information such as an individual's name, address, e-mail address, telephone number, and account numbers, as well as not-so-obvious information such as internet protocol addresses, cookie identifiers, radio frequency identification tags and information recorded by fitness tracking devices.

What does it mean to "process data?" "Processing" means any operation that is performed on personal data, either wholly or partially by automated means or on personal data that is part of a filing system. It includes collecting, transmitting, retrieving, using and yes, even *storing* personal data. *See,* GDPR, Art. 4(2). The definition of "processing" is so broad that it is difficult to identify any action that would not be considered "processing" under the GDPR.

'Right to Erasure' Under the GDPR

The GDPR is premised on the principle that every person has the right to control the use of their own personal data. *See,* GDPR, Recital 1. Consistent with that premise, the GDPR gives individuals the right to request that their personal data be "erased" where it is no longer needed for its original purpose, or where the individual withdraws his consent to processing. *See,* GDPR, Art. 17(1)(a) and (b). Unless an exception applies, the company must erase all of the person's personal data *wherever it is stored* within one month. *See,* GDPR, Art. 17(1); Art. 12(3).

U.S. Records Retention Requirements

In contrast to the GDPR's utopian "right of erasure," U.S. laws *require* many companies to retain industry-related records for years. For instance, securities broker-dealers must retain customer account records reflecting the customer's name, tax identification number, address, telephone number and other information for at least six years after the account is closed. *See,* 17 C.F.R. §240.17a-4(c). Financial institutions, casinos and other businesses must retain records required by the Bank Secrecy Act for a period of five years. *See,* 31 C.F.R. §1010.430(d). And bank records that are not authorized for destruction after a specific period of time must be retained permanently. *See,* 12 C.F.R. §1235.2. Companies outside the financial services industry have similar obligations. Employers subject to the Fair Labor Standards Act (29 C.F.R. §516.5(a)) must retain payroll records for at least three years, and the Equal Employment Opportunity Commission (29 C.F.R. §1602(A)(1)) requires private employers to retain personnel records for one year after the employment ends.

Given that U.S. law requires companies to retain records containing personal data for years (and sometimes forever), how can companies comply with their obligations under U.S. law while still complying with the GDPR?

Consent Is Not the Answer

Theoretically, individuals could consent to the company retaining their personal data for the duration of the retention period. But under the GDPR, consent must be freely given, and the individual must have the right to withdraw consent at any time. *See,* GDPR, Art. 9; Recital 43. Consent is not freely given if the individual has no genuine free choice. In other words, if the company would still process the personal data without the individual's consent, asking for consent is misleading and inherently unfair because it presents the individual with only the illusion of control.

People in the U.S. cannot *choose* whether their brokerage firm, bank or employer complies with legally imposed records retention requirements. Companies must retain these records *irrespective* of whether the account holder or employee consents. For that reason, consent is not the answer.

Is Storing the Data Necessary to Perform a Contract?

Processing personal data also is lawful where it is necessary to perform a contract to which the individual is a party. *See*, GDPR, Art. 6(1)(b). Financial services firms already enter into account agreements with their clients. Can companies comply with the GDPR simply by adding a clause to the account agreement giving them the right to store clients' personal data for the duration of the retention period? Probably not. The phrase "necessary for the performance

of a contract" is interpreted narrowly and includes only what is necessary for the *performance* of the contract; it does not apply to every event associated with the transaction. *See,* Working Party 29 Opinion 06/2014, p. 17 (Apr. 9, 2014, analyzing Article 7 of Directive 95/46/EC).

In the securities brokerage account context, processing personal data would be necessary for the purchase and sale of securities, but storing the client's personal data for a period of six years after the account was closed probably would not be deemed "necessary for the performance of the contract." Even if retaining the data for a period of years was mentioned in the contract, that fact alone would not make retaining the data "necessary" for the performance of the contract.

What About 'Legal Obligation?' Not So Fast.

The GDPR also allows companies to reject erasure requests where processing the personal data is necessary to comply with a "legal obligation" to which the company is subject. *See,* GDPR, Art. 6(1)(c). This seems like a natural solution for financial services firms and employers, who are obligated to comply with records retention periods imposed by law. Not so fast. The GDPR expressly states that the "legal obligation" must be one imposed by *European Union law or Member State law*. *See,* GDPR, Art. 6(3)(a) and (b); Recitals 40, 41 and 45. And if that were not enough, GDPR interpretative guidance states that legal obligations imposed by the laws of third countries — such as the U.S. — do *not* fall within this exception. *See,* Working Party 29 Opinion 06/2014, p. 19. Now what?

'Legitimate Interest' Is the Solution

The GDPR allows private companies to reject an individual's request to erase personal data where the company has "compelling legitimate grounds" to continue processing (including storing) the individual's personal data. *See,* GDPR, Art. 6(1)(f); Art. 17(1)(c) and Art. 21(1). Significantly, unlike the "legal obligation" basis, the company's legitimate interest does *not* need to be based in EU or Member State law. Companies who invoke the legitimate interest ground to store personal data for records retention purposes should keep several things in mind:

- The company's legitimate interest in storing the personal data must be balanced against the individual's reasonable expectations, fundamental rights and freedoms. *See,* GDPR, Art. 6(1)(f) and 21(1). Fortunately, the GDPR offers some help here. A company's legitimate interest in continued processing of personal data can arise where the individual is a client or employee of the company. *See,* GDPR, Recital 47. But it is the company's burden to demonstrate that its legitimate interest overrides the rights of the individual. *See,* GDPR, Art. 69.
- The company must inform the individual (in writing is best) that it has rejected the individual's request for erasure based on the company's legitimate interest in complying with U.S. records retention laws.
- If the company rejects a request for erasure based on its legitimate interest of complying with U.S. records retention laws, the company should retain the data for records retention purposes only; the data should not be used for marketing or other purposes.
- After the retention period has expired, the personal data should be disposed of in a secure fashion (assuming no other legitimate interest warrants continued storing of the data).

Conclusion

The GDPR advocates a minimalist approach to data collection and retention. U.S. companies subject to the GDPR must carefully consider the correct basis on which they retain an individual's personal data if faced with a request for erasure. Consent, performance of a contract and legal obligation each has its shortcomings. But by invoking the company's "legitimate interest" in complying with U.S. records retention rules, U.S. companies should be able to comply with both the GDPR and U.S. law and avoid a head-on collision between these two statutory powerhouses.

Stacey Garrett *is a shareholder of Keesal, Young & Logan, P.C. For 26 years she has successfully represented financial institutions, securities broker-dealers and banks in jury trials, bench trials, class actions and arbitrations. Stacey is a member of KYL's cybersecurity and privacy law practice. She is certified by the International Association of Privacy Professionals in the area of U.S. privacy law (CIPP/US) and European Union privacy and data protection law (CIPP/E).* *This information has been prepared for informational purposes only and is not intended to be legal advice. Individuals and/or companies should not act upon this information without seeking professional counsel from an attorney.*