Privacy Considerations For US Fintech When Going Global

By Jeewon Serrato, Oliver Linch and Kyle Koh

Law360, New York (July 11, 2017, 12:11 PM EDT) --
Driven by the internet and smartphone revolutions, the fintech industry has soared rapidly in the past decade, with global investment in fintech firms amounting to $24.7 billion last year. Many fintech firms are built on a foundation of data: After all, the unique selling proposition of many fintech firms lies in their ability to generate actionable insight from data that has been collected from customers, businesses and other stakeholders. Customers entrust firms with the protection of this data, and yet data breaches and cyberattacks, especially in the financial sector, have been on the rise. As such, cybersecurity, privacy and data protection have become increasingly important to fintech firms.

Jeewon Serrato

In addition to the cyberthreats from malicious actors, regulatory compliance issues have also become increasingly significant as privacy and data protection laws have proliferated in the post-Snowden, data-driven world, continually adding to the patchwork of laws that aim to restrict how data may be processed and used in various cross-border settings. The European General Data Protection Regulation, which goes into effect in May 2018, is most emblematic of this contemporary zeitgeist. For U.S. firms that either have a global presence or are looking to expand globally, going across the pond often means being subjected to European or other non-U.S. laws that address privacy and data protection issues very differently. This article focuses on the U.K. and European data privacy frameworks, but the lessons illustrated here highlight global trends.

Oliver Linch

Current U.K. Data Protection Framework

Unlike in the U.S., where the use of personal data by fintech firms is regulated by a mix of state and federal laws, the processing of personal data in the U.K. is regulated by an overarching piece of legislation, the Data Protection Act 1998 (DPA), which implements the European Data Protection Directive. The DPA focuses on data controllers — organizations that determine the purpose and means of data processing — that are established in the U.K., and those outside the European Economic Area that use equipment in the U.K. to process personal data (other than for transit). “Processing” is widely defined and is intended to cover any conceivable operation on data, such as obtaining, disclosing or destroying data. “Personal data” is data relating to a living individual who can be identified from such data or from a combination of such data with other information in the possession of, or likely to come into the possession of, the data controller.

Kyle Koh

Fintech firms most likely are processing personal data. For example, a typical mobile payments company may collect names, date of birth, addresses, phone numbers, email addresses and bank account details. As such, U.S. fintech firms that set up a subsidiary or an office in the U.K. will likely lie within the remit of the DPA. Even without a brick and mortar presence in the U.K., such firms may be subject to the DPA if equipment in the U.K. is used to process personal data.

Once subjected to the DPA, data controllers must notify the Information Commissioner's Office annually and must abide by eight data protection principles, such as to process data fairly and lawfully, adequately and not excessively, and in accordance with personal data subjects' rights.

Whereas U.S. law does not restrict data transfers beyond the U.S., the DPA mandates that data controllers may not transfer personal data outside the EEA unless the destination country ensures an adequate level of data protection for individuals, or one or more preconditions are met. One of the ways to meet this adequacy requirement is for the U.S. firms to certify to the EU-U.S. Privacy Shield program, a framework designed to facilitate the receipt of personal data by U.S. companies from the EU. U.S. companies that self-certify a commitment to protect personal data in accordance with standards deemed to meet European requirements can receive personal data from the EU.

Other ways of satisfying the EU adequacy requirements include the model contractual clauses or the binding corporate rules. Without having in place one of these data transfer mechanisms, U.S. fintech firms may run afoul of laws that prohibit the transfer of EU residents data out of the EU.

European Union General Data Protection Regulation

In addition to being aware of non-U.S. laws that might be applicable, it is important to note that in the world of privacy and data protection, those laws are still evolving and requires vigilance on the part of the firms to continually update its understanding of what laws might have an impact on the business.

In the EU, the GDPR will replace the European Data Protection Directive on May 25, 2018. As a regulation, it will have direct effect in all EU countries and represents a significant move to harmonize privacy and data protection practices across the EU under a more prescriptive and restrictive regime. For example, it regulates not only controllers but data processors too (those who process data on behalf of controllers) and institutes mandatory breach notifications and significant sanctions. More importantly, to ensure that EU citizens' data is protected globally, the scope of the GDPR extends to controllers and processors established outside the EU who process EU individuals' personal data and offer goods or services to them, or monitor their behavior. This differs from the U.S. regime, where data privacy laws generally apply only to data collected by American organizations and stored in the U.S.

In June 2017, the U.K. government announced that it would implement the GDPR and replace the DPA with a new Data Protection Bill to ensure that, post-Brexit, the U.K. would maintain the ability to share data with the EU. As such, it is critical that even U.S. fintech firms that do not have an EU presence, but which target or monitor EU individuals, whether they are employees, customers or otherwise, understand the impact of the GDPR. Below, we identify the GDPR's most important implications for fintech firms.

Sanctions

Hefty penalties can be imposed for breaches. For infringements of core obligations, such as those relating to the basic principles for processing, including conditions for consent, data subjects' rights and international transfers, companies can be fined a maximum of €20 million or 4 percent of annual global revenue, whichever is greater. Other breaches fall under a lower category and entail penalties amounting to the higher of €20 million or 2 percent of annual global revenue.

Privacy by Design (and by Default)

Whereas privacy by design is implicit in the Data Protection Directive and DPA, the GDPR explicitly recognizes privacy by design and by default and requires organizations to implement appropriate technical and organizational measures to protect privacy and personal data (e.g., pseudonymization is encouraged to protect the identity of individuals).

In certain cases, a detailed privacy impact assessment (PIA) is also required. If the PIA concludes that there are risks for the relevant individuals, controllers must consult the supervisory authority to determine appropriate measures to mitigate these risks.

Fintech firms that systematically monitor individuals on a large scale must also appoint a data protection officer to advise the organization of its GDPR obligations, monitor compliance with such obligations and other data protection laws, and be the first point of contact for supervisory authorities and data subjects.

Consent

The GDPR introduces stricter conditions for obtaining user consent than currently exist under the Data Protection Directive. Data subjects will have the right to withdraw consent at any time and omnibus consent mechanisms will be presumed invalid, meaning that separate consents must be obtained for each processing activity.

Fintech companies that rely on consent for justifying the processing of personal data will have to review existing consent procedures to ensure that genuine, unambiguous and granular consent is obtained and not assumed. For many companies, this might require the data protection notices to be amended, further requirements of which are found below.

Transparency Obligations

The GDPR requires extensive disclosure regarding the processing of personal data. In addition to existing Data Protection Directive requirements to provide the identity and contact details of the controller and the purpose of processing, the GDPR obliges data controllers to notify data subjects of the legal basis for processing, details of data transfers outside the EU, the retention period for the data, and their right to withdraw consent. Moreover, if personal data is not obtained directly from the data subject, the controller must inform the individual of the categories and sources of such information.

U.S. fintech firms should review their privacy notices, policies and other communications to ensure compliance with the expansive transparency requirements regarding information that must be provided to a data subject.

Notices for Data Breaches

The GDPR imposes a duty of notification on data controllers and processors in the event of personal data breaches. This type of data breach notification rule is not new as U.S. firms have had to comply with state laws that have such notification requirements, but under the GDPR, data breaches must be reported to the supervisory authority within 72 hours. Under certain circumstances, the supervisory authority can also compel notification of affected individual data subjects.

Fintech firms that process personal data, whether collected from a third-party provider or directly from customers, will need to review how data breaches are detected and how relevant parties can be notified within the prescribed timeframe.

Subject Rights to Access, Portability and Erasure

The GDPR grants data subjects a vast suite of rights that U.S. firms may not have encountered. Data subjects have a right to (1) request and receive a copy of their personal data in a commonly used electronic form, free of charge; (2) under certain conditions, request the transfer of relevant information to another data controller without hindrance (known as portability); and (3) request the erasure of their personal data. Controllers must comply with these requests without undue delay, and at the latest within a month.

Cross-Border Data Transfers

Much like under the Data Protection Directive and DPA, transfers of personal data beyond the EEA are restricted under the GDPR. Over 2,000 organizations participate in the EU-U.S. Privacy Shield to circumvent this restriction. Many others have chosen to use the EU model clauses and still others have decided to implement the binding corporate rules to overcome the data transfer restrictions.

It is worth noting that post-Brexit, the U.K.'s departure from the EU would likely mean that it would no longer benefit from the Privacy Shield and will have to develop an alternative arrangement with the U.S.

Implications for U.S. Fintech Firms

Given the far-reaching implications of the GDPR, U.S. fintech firms that anticipate having to process the personal data of EU citizens or seek to do business in the EU should familiarize themselves with its requirements and evaluate how to adapt their business processes accordingly. Organizations should establish clear internal reporting chains and guidelines to ensure proper oversight and accountability over data protection.

Other Relevant U.K. Laws

Firms will be regulated and must be authorized by the U.K. financial regulator, such as the Financial Conduct Authority if they engage in certain regulated activities and do not fall within the scope of an exemption. If a U.S. fintech firm becomes regulated in the U.K., it will be required to establish and maintain systems and controls to minimize risk, including with respect to information technology systems. It must also report any material cyberattacks to the regulator, such as those that result in a significant loss of data, or impact a large number of victims.

Fintech firms that intend to send electronic marketing messages or use cookies must also

comply with the Privacy and Electronic Communications Regulations, which complements the DPA by setting out privacy rules regarding electronic communications. The requirement includes obtaining user consent to and providing clear notices with respect to the use of cookies on an organization's website.

Conclusion

Ever-evolving regulations may have an impact on decisions that are made during a business expansion, such as where the business operates. For fintech firms going global, robust compliance mechanisms need to be in place to help guide business risk decisions. Firms that understand how to not only meet the changing consumer demands but are also able to adapt to the different regulatory landscapes will have a competitive advantage and go far across the pond and beyond.

Jeewon Kim Serrato is a counsel in the San Francisco office of Shearman & Sterling LLP and head of the firm's global privacy and data protection group. She was previously chief privacy officer of Fannie Mae.

Oliver Linch is an associate and Kyle Koh is a trainee in the firm's London office.