GDPR: The General Data Protection Regulation

June 2018

bai.org

You've probably noticed your inbox filling up with new privacy policies to read and companies asking for you to interact with them, so they can continue to send you emails. Sadly, it seems many organizations have fundamentally misunderstood the obligations placed upon them by new EU privacy laws. This white paper provides an overview of the EU General Data Protection Regulation (GDPR) and associated EU privacy laws for the U.S. financial services market, in the hope of providing a better way of working with our consumers going forward. Protecting privacy is a way of showing your consumers respect and care, and will engender better trust and return on investment into the future.

From the past, into the future

Information privacy (or data protection) is not new. Privacy management has been around since after World War II, when people understood in real terms what it meant to have your name written down on a list: you could be discriminated against, targeted, profiled, and potentially tortured and killed because of your race, religion, sexual preference or other characteristics. Of course, the information collected about us now by companies and governments vastly outweighs the personal information collected in earlier times, and the potential for harm is magnified exponentially.

The GDPR (Regulation 16/679) replaces the previous EU Directive on data privacy from 1995. Since then, the world has changed. We have developed cloud computing, mobile smart phones, social media, AI, the Internet of Things, drones and blockchain as just some examples. By the time the GDPR is replaced in another 20 years, what will the world look like?

As a learning point, financial institutions should be looking to invest in evolving privacy management in the longer term, rather than GDPR compliance in the short term. The question is not how do I respond to GDPR, but how do I deal with privacy risk in the longer term? Just as you cannot be 100% secure with information security management. You can only give appropriate assurance over time, evolving your approach as the laws, regulations, technology and processes evolve.

EU vs U.S. models

The EU looks at privacy as a basic human right. In the United States, privacy has traditionally been treated as a consumer rights issue. This is a fundamental difference between the two. The traditional internet models of "free if you accept marketing and profiling" and "paid for if you want privacy" result in a standard of privacy for the rich. This is fundamentally unacceptable to EU thought processes, where privacy should be free to all.

Another difference is that the United States takes a "sectoral approach". There are differing laws at state and federal levels. There are industry-specific laws, such as Sarbanes-Oxley, HIPPA and FERPA.

In contrast, the EU approach is to have a single general law to cover all eventualities. This means the law is principle-based, using words like "adequate", "necessary" or "appropriate". There are few specific yes-or-no answers, with many compliance obligations dealt with as risk management provisions. For financial institutions to comply, they must show their work, or "do their homework," and establish and document for themselves what the risks to individuals are. They must take appropriate measures, ensuring data processing is necessary, justified and proportionate to their aims.

Finally, in the United States, the FTC is the privacy regulator alongside its other functions, while in the EU each country has its own privacy regulator, harmonized by the newly incorporated European Data Protection Board. In theory, while individuals will go to their national supervisory authority for remedy, companies should only be dealing with a "lead" authority based on their main locations in the EU.

Does this apply to me?

The GDPR applies to financial institutions in three circumstances:

1. Where the financial institution is established in the EEA (28 EU member states plus Norway, Iceland and Liechtenstein)
2. Where the financial institution is targeting goods and services to people in the EEA
3. Where the financial institution is monitoring individuals in the EEA

Clearly, the EU cannot legislate for the United States. However, some U.S. tech firms have used their U.S. incorporation to try to hide from their responsibilities. The GDPR was written to try and catch these organizations.

As an example, the EU cannot legislate for a U.S. mom-and-pop online store selling handcrafted furniture in Idaho. The store was meant for U.S. buyers. An EU individual might find the store on the internet and purchase something, but that person was never part of the intended market. GDPR does not apply.

But consider that same store gaining traction in the EU. It realizes it has a lucrative new market, and perhaps takes out advertisements in the EU, opens a production office in the EEA or actively promotes its products to the EU market. Clearly, its customers should now be covered by EU privacy law because the EU citizen is a clear target of its services.

Citizenship is not important, but physical location is. If an EU citizen moves to the United States, he or she is subject to U.S. law. If a U.S. citizen moves to the EU, he or she becomes subject to EU law, including the rights and privileges afforded to them by the GDPR.

When data leaves the EEA and goes into other countries that do not have "adequate" privacy laws, this fact must be identified, affected individuals must be notified and appropriate mechanisms must be put in place to ensure privacy rights will be respected when the data is processed in such a location. This will include transfers between the EEA and the United States, where appropriate safeguards must be put in place, such as the EU-U.S. Privacy Shield as an example.

Businesses seeking to operate consistently on a global basis often use the GDPR as a template for a "global gold standard" of data handling, accounting for regional variations in the law where applicable.

Personal Data vs Personally Identifiable Information (PII)

We have established who is covered. Now the question is *what* is covered. The GDPR introduces four categories of personal data:

1. Anonymous data - no individual can be identified from it

2. Pseudo anonymous data - data that is anonymized only at certain times, so it can be re-identified where necessary

3. Personal data - any information relating to an identified or identifiable individual

4. Special Category data - data relating to race, ethnicity, health, criminal record, sex life or orientation, trade union membership or biometric/genetic information

The GDPR does not apply to category 1. Any information that is incapable of identifying individuals is not covered, and therefore financial institutions can look to data minimization and removal of identifiers to reduce their risk and the risk to individuals. However, they should also be careful of data aggregation, or small statistical groups, where combinations of data render people re-identifiable, even in larger data sets.

Categories 2 to 4 are all covered by GDPR.

Pseudonymization will be a useful technique to ensure that data can be kept non-identifiable to reduce risks but can be re-identified where required. A good example of this could be for reporting and monitoring of financial fraud, where it may be good practice to remove identifiable data for monitoring purposes but also be able to re-identify the data where fraud is discovered.

Personal data is regardless of format, so everything recorded and structured, such as audio, video, paper or computerized data, is covered. Personal data should also pertain to the individuals you have a relationship with. For example, where you have collected contact details for a staff member's partner for emergency contact purposes, this forms part of the staff member's record. It does not mean you have established a relationship with the partner as a new data subject, as you have not created a record on him or her specifically.

Note this definition of personal data is very different from the U.S. definition of PII, which can be considered a subset of personal data, as the interpretation by EU courts and regulators is far wider. IP addresses, cookies, advertising IDs, device IDs and other information that might be thought of as specific to a device or computer are considered personal data in the EU, and relatable to the individual rather than just the device. Also, the U.S. definition of "sensitive" personal information (SPI) differs from the EU version, as it focuses on national identifiers such as Social Security numbers, rather than the sorts of information that the special categories in the GDPR represent. Again, this comes from the EU's human rights backdrop to privacy.

The EU special category data does not include financial records.

Legal basis - Why do you have the data?

Privacy law requires financial institutions to "do their homework." This means having a legal justification to process data, as well as a second reason to process special category data. Considering why you need data and minimizing data to strictly the amount necessary to achieve your aim are key to minimizing risk exposure.

Institutions often focus on consent as a legal basis for processing data. However, in practice this is rarely the basis that should be chosen. Within the GDPR, the definition for consent is very specific and difficult to meet. Also, relying on consent gives individuals many more rights (most obviously the right to withdraw it) and is often inappropriate. (As an analogy, try telling the IRS they don't have your consent to tax you!) Instead of consent, other legal bases, such as necessity for contract or for a legal obligation, are often much more concrete reasons to process the data. Reasons such as "legitimate interest" or "public interest" are more arguable because they involve the institution having to state what its interest is and how this overcomes the right to privacy.

Most financial service institutions will be relying on contractual relationships rather than consent-based relationships. However, it is worth noting that there are some purposes of processing data that may be consent related, and individuals in general should be given as much granular control over their preferences as possible and at all points be informed of the consequences of their choices.

In truth, delivering a process often depends on many legal bases in combination. For example, with employees you will primarily be processing on the basis of a necessity for the employment contract, monitoring your networks on a legitimate interest basis, passing data on health and safety on for legal obligations, and you may even ask for their (freely given) consent for appearances in the company PR photographs!

Principle - based governance

The GDPR's main requirement is the adoption of good information management principles. This means that personal data must be processed in the following way:

- Transparently (by providing privacy notices to individuals)
- Lawfully (see the discussion of legal basis above)
- Limited in purpose (used only for the reasons individuals are told)
- Minimized to the just the amount needed to achieve your aim
- Accurately; where necessary, up to date
- Storage limitation (kept no longer than necessary for the purpose)
- Protected (with appropriate organizational and technical security measures)
- Accountably (see doing your homework below)

These principles are the heart of privacy law, and are what individual data flows and ground- level business processes should be reviewed against. They relate entirely to a specific purpose the financial institution chooses for the processing of data, such as staff administration, direct marketing, buying something online or providing a service such as a loan or a mortgage. Because of the omnibus nature of the law, regulators cannot legislate the detail, but instead must challenge the institution to prove that it has examined each of these principles and applied them correctly and appropriately to each of their purposes of processing. What is "appropriate" is up to the institution to research and inform the individual (or the regulator).

The heart of these privacy principles was established in the 1980 OECD Guidelines and has not changed over the past 40 years of privacy management. Compliance is not a yes-or-no answer in these cases, but a risk management decision by the institution involved; its reasoning and research would be the first things to be examined in the event of a regulatory investigation or customer complaint.

Nothing in these privacy principles says you *can't* do anything.

However, why would you want to hold inaccurate, excessive, irrelevant or out -of-date information? Keeping only what you need and managing it effectively create an information-efficient company. Holding out-of-date, excessive, irrelevant data insecurely and using it differently than consumers expect is clearly an undesirable place for a company to be. A good example of the failure to apply these principles is the Facebook and Cambridge Analytica scandal. This was not a question of data security, but of transparency and data use, where users who gave information for a fun psychological survey online ended up exposing themselves and their friends to political advertising from third parties through opaque and difficult-to-understand privacy settings.

Institutions that have followed the good governance principles and designed them into their systems, processes and technology should be well ahead of the pack in being compliant now and into the future.

Doing your homework

The GDPR introduces the idea of accountability, which is perhaps the biggest change from the previous 1995 legislation. This simply means making privacy a forethought rather than an afterthought, which includes having records ready to prove your compliance to your stakeholders, be they management, regulators or the individuals who have shared their personal information.

Being accountable for privacy means keeping records of what data you have as well as metadata, such as how data is secured, how long you will keep it, where and who it is disclosed to and the justifications for holding it. Some organizations will be legally required to have data protection officers to advocate for the individual and liaise with the regulator. Where processing of data is high risk you may have to conduct a privacy impact assessment (PIA) to determine appropriate risk mitigations, and incorporate Privacy by Design processes and Privacy by Default settings to ensure all your systems and processes respect individuals' rights and the privacy principles.

This is what elevates the GDPR above previous privacy laws: the requirement to do your homework on the data of the individuals you are serving and to prove that you are continually improving your services to them.

Supplier management

Protecting data also means regulating your suppliers. The GDPR recognizes **data controllers** (those who determine the means and purpose of processing) and **data processors** (those who act on their instruction). It's also possible that you might engage in processing activities jointly (such as a group of enterprises or businesses). In all cases, it is important to communicate to the individual who is the ultimate data controller. Controllers must establish robust contracts delivering instructions to their processors (often difficult in the case of large cloud providers who won't tailor their services per controller) and monitor compliance across any entity to which they pass personal data.

Article 28 of the GDPR includes a list of mandatory (but common-sense) contract requirements such as only acting on instruction, confidentiality, appropriate security, data breach assistance, passing on of requirements to sub-processors, right of audit, justifying transfer of data internationally, and assisting controllers in doing their homework or if a regulator/individual gets in touch.

For the first time, processors do have limited responsibilities under the GDPR, such as keeping records of processing, possibly maintaining a data protection officer and applying appropriate security. They can also be found liable both by the regulator and to the controllers where they have breached their contracts.

Does this mean I can't email my consumers?

Not at all. The sending of email, phone, ad tech and fax marketing is covered in a separate law called the ePrivacy Directive of 2003. This is due to be updated to a binding regulation in 2018 and is being negotiated in the EU right now. The GDPR updates the definition of consent in the ePrivacy directive, which is the reason for the re-consenting campaigns we have started to see from entities who hold our data. However, the ePrivacy directive also provides an exemption called soft opt-in. Essentially, this states that rather than relying on consent, you can rely on legitimate interest as a legal basis if someone has handed you a business card, attended an event, shown an interest by making an inquiry, or bought something from you. The exemption is fairly limited as on first and all subsequent contact you must provide opt-out for it to apply. But in most cases, it means that institutions may not have to rely on consent and are not required to carry out re-consenting campaigns.

Of course, where you are relying on consent, and cannot rely on soft opt-in, consent will have to be to a GDPR standard (freely given, informed, specific, affirmative action etc.). Sending out an email asking for consent may indicate you never had permission to send it, thus you are violating the law by the very action of sending the re-consenting email! Rather, I'd separate the emails you are sending by purpose. Sending out direct marketing emails may rely on consent as a basis, whereas sending out a customer monthly statement or service-related email may be on the basis of contract necessity, meaning the individual has no choice but to receive the email as part of the service he or she has signed up for.

Finally, the rules are different for business-to-business than for business-to-consumer, with B2B having slightly less expectation to privacy than B2C. However, in each case you should respect individuals' preferences where they are expressed and always give options to opt out. Most importantly, just because you can *find* someone's contact details, doesn't give you permission to *use* them. Remember that notice requirements still apply, and covert surveillance should not be carried out, except by the appropriate authorities, without a significant, legitimate business interest.

What about individual rights?

The GDPR gives financial institutions responsibility, but it also gives individuals rights—a lot of them! These rights primarily include a 30-day window for the institution to respond when an individual is claiming their rights, and in general the institution cannot levy a charge for doing so. It is not hard to imagine that in the event of a data breach people will claim their right of access to a copy of their data, causing a significant administrative overhead on the business to respond. In a situation like this, understanding where you have stored data and being able to justify that it is managed properly and in accordance with the principles are extremely important.

The right of **access** underpins all the other rights the individual has, such as rights of **correction, objection, rectification, complaint, compensation, and rights regarding automated decision-making** (such as machine-made decisions for loans or insurance). Without knowing what information organizations have on them, consumers cannot pursue their later rights, so an access request is only the start of a longer journey with the complainant.

Much has also been made of the right of **erasure**, which will only apply if relying on consent or if you have failed the principles above. However, the media have educated people they have this, which may lead to some angry consumers who have been told they have rights that, in many cases, they do not.

Finally, the right of **portability** means that when relying on a contract or consent-based relationship, the individual can ask you to send *only the data they have given to you* (so, not your own data you have added to it) to one of your competitors electronically. This right is less privacy-law based, and more about competition law and allowing movement of consumers in the marketplace between companies.

I'm going to be fined millions!

The regulators are not monsters. Of course, they will appropriately and necessarily act where financial institutions have deliberately or willfully breached the law. They have a wide variety of actions they can take, from "naming and shaming" to audits, fines and even enforcement or stop notices. However, they also recognize that institutions must balance innovation, bring legacy systems and data into compliance given limited resources and conduct risk prioritization. For regulators, May 26th is the same as before that date, and they stand ready to advise as well as admonish.

Much has been made of the maximum fines of 4% of global annual turnover or E20m, whichever is bigger, but not much has been said about the payout for individual compensation for damage or distress that could occur from a large data breach. For example, if you have hurt a million customers for $200 each, that makes the regulator-applied fine maximum look small! Fines will be proportionate to the offense, so maximum fines are unlikely for all but the biggest players. The regulator will first ask you what you did to prevent a problem, and so again, doing your homework as per the accountability parts of the law will be your best defense.

As a note of caution, the regulator will only be in touch if you have consumer complaints against you, so your best defense remains to keep showing your consumers respect, facilitating their rights, and, if the worst does happen, being able to provide evidence of the hard work you have done to work out how the GDPR applies to you and the resulting preparation and ongoing monitoring of your privacy program.

Conclusion

The GDPR was passed in May 2016 and is enforceable from May 25, 2018. However, privacy is forever. Organizations will need to manage their customer expectations long into the future, and all these laws boil down to one essential principle: *manage other people's information as you would wish your own to be managed.* Managing people's personal information is a privileged responsibility, not a commodity to be monetized and exploited. Proper management of individuals' information can bring consumer trust and a competitive advantage in the marketplace. So, whether GDPR applies or not, public consciousness about our data use has never been higher, and global privacy laws are here to stay.