WHITE PAPER

Be Prepared for the GDPR

Data protection and privacy

twilio

Contents

The below information is Twilio's interpretation of GDPR requirements as of the date of publication. Please note that not all interpretations or requirements of the GDPR are well-settled and its application is fact- and context-specific. The information contained in this whitepaper should not be relied upon as legal advice or to determine how GDPR applies to your business or organization. We encourage you to seek guidance from your legal counsel with regard to how GDPR applies specifically to your business or organization and how to ensure compliance. This information is provided "as-is" and may be updated or changed without notice. You may copy and use this content for your internal, reference purposes only.

Introduction

Compliance with data protection laws is a hot topic for many of our customers. And, for any customer that processes personal data in the European Union (EU) or originating from individuals in the EU, the acronym GDPR is (or should be) top of mind.

> GDPR stands for General Data Protection Regulation—a major piece of legislation passed by the European Union (EU) that could significantly impact your business whether your organization is based in the EU or not. With fines up to 20 million or 4% of global revenue for violating GDPR, it's a piece of legislation that no one can afford to ignore.

GDPR replaces the 1995 EU Data Protection Directive, and its purpose is to ensure appropriate protection of personal data in our digital society. Like the Directive before it, GDPR is founded on the idea that everyone has the right to protection of personal data. GDPR treats personal data like an asset that belongs to the individual, so the individual has rights regarding how his or her personal data is used.

However, unlike the Directive before it, GDPR expands its reach beyond the borders of the EU. Not only does it apply to companies that process personal data in the EU, it also applies to companies that process EU personal data outside of the EU. The rationale is that data protection is a fundamental human right, so it simply won't do for companies to be allowed to violate that right just because their operations are overseas.

So, if you are an EU-based company or just have EU-based users, GDPR applies to you.

The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data.

RECITAL (2)
GENERAL DATA PROTECTION REGULATION

TWILIO IS YOUR PARTNER FOR DATA PRIVACY

Twilio welcomes GDPR as an opportunity to build a stronger data protection foundation for the benefit of all. Data privacy is an important human right, and in this data-driven world, more than ever, data protection is something that all companies should be paying close attention to.

In addition, we are keenly aware that organizations that process personal data of individuals in the EU need to be sure their service providers support compliance with GDPR.

> Twilio is committed to ensuring our platform is GDPR-compliant by May 25, 2018, when GDPR becomes enforceable.

Our first leadership principle at Twilio is to "wear the customer's shoes." We know that if our platform doesn't support your compliance needs, you can't enjoy all of the useful products and features we build.
We also understand that data protection and compliance with GDPR is a shared responsibility—some aspects of compliance will be covered by Twilio and some other aspects will necessarily fall to you. Because we are committed to supporting you in your journey towards GDPR compliance, we created this whitepaper as a resource.

> Keep in mind, we aren't your lawyers, so we aren't at liberty to give you or your organization legal advice.

TIP

GDPR compliance is a cross-functional effort and requires input and cooperation from legal, HR, security, IT, and product teams. That's why the very first step on the GDPR compliance journey is to build awareness and support among your company leadership. At Twilio, once we had support from our senior leadership, we started by forming a core team consisting of a data compliance program manager and senior members of our legal, security, data, and architecture teams to help steer and drive the program.

What is Data Processing, Who are Data Subjects, and What is Personal Data?

GDPR is all about protecting the rights of data subjects in connection with processing their personal data.

Data Processing

Data processing is really just anything you can do with or to data. It includes accessing it, collecting it, reading it, storing it, analyzing it, retrieving it, organizing it, transferring it, disclosing it, and deleting it.

Data Subjects

Under GDPR, data subjects are just people — human beings.

Personal Data

Personal data is data that relates to "identified" or "identifiable" data subjects. An "identifiable" data subject is someone who can be identified, directly or indirectly, such as by reference to an identifier like a name, ID number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Note how broad the definition of personal data is. It can include data such as the IP address of an individual's personal device, a device ID, or phone number. It doesn't matter that the identifier could change (e.g., that the user could change their phone number or device ID).

It's also important to note that the definition of personal data is not tied to concerns about identity theft the way that definitions of personally identifying information (PII) are under many U.S. data breach laws. For example, even if it seems like there would be little privacy harm if someone improperly gained an individual's device IP address, that doesn't mean that the IP address is not personal data. Instead, this data may not require the same level of protection as more sensitive personal data, such as a passport number, credit card number, or health information.

This leads to the next topic, which is that GDPR defines certain categories of personal data as extra sensitive. These special categories are personal data revealing race, ethnicity, political opinion, religious or philosophical beliefs, trade union membership, and also genetic data, biometric data, health data, or data concerning the data subjects' sex life or sexual orientation.

The rule under GDPR is that these types of data should not be processed unless a special exception applies such as the data subject providing explicit consent, or the processing being necessary to protect the life of the data subject and the data subject is incapable of giving consent. In addition to special categories of personal data,

GDPR also has special rules for processing children's data (data of data subjects under age 16) and data relating to criminal convictions or offenses.

TIP

When tackling GDPR compliance, an early step is to assess the types of personal data you process, paying particular attention to any special categories of personal data that has special processing restrictions. Then, map out which systems and processes are involved in that processing. GDPR does not specify the right or wrong way to do a data map. Instead, it just requires that you document your data processing activities. As long as your data map provides the information you need to understand how personal data flows through your system, it doesn't matter what tools you use.

Data Controllers and Data Processors

GDPR carries over the concepts of data controllers and data processors from the Directive. Similarl to the Directive, data controllers and data processors have different obligations under GDPR. Therefore, it's important to understand whether you're acting as a data controller or a data processor in relation to the various categories of personal data you process.

WHO IS A DATA CONTROLLER?

GDPR defines a data controller as **"the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data."** In other words, if your organization processes personal data for your own organization's purposes and needs—not merely as a service provider acting on behalf of another organization—then you are likely to be a data controller.

For example, Twilio, like all organizations, is a controller of our employees' personal data that it processes as part of our human resources operations. Similarly, like other organizations, we are a controller of the personal data that we collect in connection with our customer relationship management functions, such as billing information or telephone numbers and email addresses of users that open a Twilio account.

Perhaps less obviously, Twilio is also a controller of communications metadata, such as the metadata of phone calls or text messages transmitted or received via our products and services. These records often constitute personal data because they contain data subjects' phone numbers, for example. We need this data for our own business operations, like billing, routing, tax, and audit purposes. We colloquially refer to this data at Twilio as

"outside the envelope." If you think of an electronic communication as being a letter sent through the mail, the metadata is like the information you write on the outside of the envelope. Similar to how the postal service needs to read and use that information to operate its business, we need to read and use electronic communication metadata to operate our business. So, for a certain period of time, Twilio must retain this data even if a customer were to request that we delete it.

Of course, some customers may want Twilio to retain this data for their own business purposes, even after Twilio no longer needs it for its own purposes. Once Twilio no longer needs this data for its own business purposes, to the extent that our customers wish to retain this data on Twilio's systems, we shift from being a data controller to a data processor.

WHO IS A DATA PROCESSOR?

Businesses or organizations that process personal data solely on behalf of, and as directed by, data controllers are data processors. In other words, when a data controller outsources a data processing function to another entity, that other entity is generally a data processor.

Twilio is a processor of your communications content, like message bodies or voice or video media. We don't do anything with that content unless you, the customer, tell us to. So, if you want to delete it, we'll delete it. It doesn't impact our ability to run our business. We refer to this data as "inside the envelope." We don't need to know what your support agent said to your customer over your application built on Twilio Programmable Voice to operate our business.

TIP

When tackling GDPR compliance, an early step is to assess the types of personal data you process, paying particular attention to any special categories of personal data that has special processing restrictions. Then, map out which systems and processes are involved in that processing. GDPR does not specify the right or wrong way to do a data map. Instead, it just requires that you document your data processing activities. As long as your data map provides the information you need to understand how personal data flows through your system, it doesn't matter what tools you use.

Data Processing Obligations

Now that you understand who data subjects are, what personal data is, and whether you are a controller or processor of that personal data, let's discuss what are you supposed to do (or not do) with data subjects' personal data under GDPR.

THE PRINCIPLES OF DATA PROTECTION

Article 5 of GDPR outlines the seven principles of data protection under GDPR. The upside is that these principles are generally consistent with the EU Data Protection Directive and data protection principles worldwide.

TIP

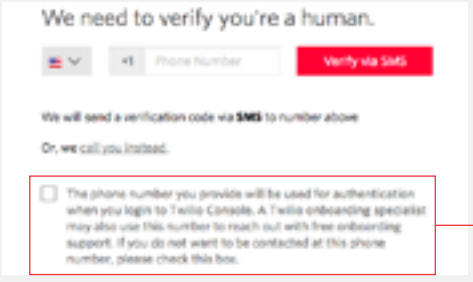
Because data protection principles are relatively consistent worldwide, if you apply GDPR's data protection principles to all personal data—not just EU personal data—you will be well-positioned for compliance with data protection regulatory frameworks around the world.

Under GDPR:

1. **Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject ("lawfulness, fairness, and transparency").**

TIP

In addition to an overall privacy notice, consider putting mini privacy notices in other places where you collect personal data to help your user understand what you'll be doing with the specific personal data you're gathering. For example, Twilio customers see this notice when they're asked to provide their phone number during the signup process:



GDPR aims to put data subjects in the driver's seat in relation to their personal data. Data subjects should not be forced to "drive" blind. Therefore, GDPR requires that you communicate to data subjects in a clear and understandable way describing what you are going to be doing with their personal data and how they can exercise their rights in relation to the personal data you collect. This is why having a clear and comprehensive privacy notice (sometimes referred to as a privacy policy) is important.

This privacy notice provides our customers with transparency regarding how and why their telephone number might be used by Twilio, and it also gives them information on how to exercise their rights.

GDPR also requires that processing be lawful. What constitutes lawful processing is stated in Article 6 of GDPR. Two commonly used bases for lawful processing are (a) consent from the data subject, and (b) the legitimate interests of the business that is processing the personal data.

Consent-Based Processing

If you process personal data based on consent, beware that under GDPR, this consent must be freely given by an affirmative act that is specific, informed, and unambiguous. "Pre-checked" boxes, items buried in long legal documents, and silence will not count as consent. Also, the data subject has to be able to withdraw his or her consent at any time and this withdrawal must be made easy. (See GDPR Article 7)

Legitimate Interest-Based Processing

If you process personal data based on a legitimate business interest, then you must be careful that you balance those interests against the right of the data subject to not have you process their personal data. If the data subject's privacy interests override your legitimate business interests, then your business interests must yield to the data subject's privacy interests. In the example provided in the Tip above, note that Twilio's legitimate business interest in contacting new users to help them with onboarding is overridden by an individual user's desire not to be contacted by us at that phone number.

2. Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes ("purpose limitation").

The purpose limitation principle requires that you say what you do (be specific and explicit about how you process personal data) and do what you say (only process personal data in the way and for the reasons that you said you would). So, tread carefully if someone suggests a new purpose for old data. You need to go back and double check that the "new purpose" is compatible with what you originally told data subjects you would be using their personal data for. In the world of data protection, surprises are bad.

3. Personal data must be adequate, relevant, and limited to what is necessary to achieve those purposes ("data minimization").

The data minimization principle is pretty straightforward on paper. If you don't need it, don't collect it. Don't just collect personal data with the hope that you'll decide what you need it for later. This may seem obvious on the front end (i.e., at the point where you collect data from your user).

Less obviously, the same principle should be applied throughout your operations, even internally. For example, let's say that you log certain system activity for troubleshooting purposes. Be thoughtful before collecting

information that could constitute personal data in those logs; make sure that any personal data that gets logged is really necessary. Don't just log everything and assume you will sort it out later. Not only does that violate the data minimization principle, it's also likely to cause you operational headaches down the road. If you log personal data, then you have to figure out how to delete it from those logs when it's no longer needed (see #5 below). And, you have to make sure your logs are secured at the level required in light of the personal data now being stored in them (see #6 below).

4. Personal data must be accurate and kept up to date ("accuracy").

It's hard for a data subject to be in control of their personal data if an organization is working off "bad data" about them. It probably doesn't do your organization much good either to be working off inaccurate or out-of-date data.

For example, customers who use Twilio Notify to communicate with their end users should be sure to keep their users' contact information (i.e., Address(es)) updated and accurate. If the user changes their contact information, their Address(es) should be updated accordingly because it will be used to contact the user in the future.

5. Personal data must be stored no longer than necessary to achieve the purposes for which it was collected ("storage limitation").

The "storage limitation" principle is similar to the "data minimization" principle above. Just as the data minimisation principle counsels that you should not collect or use personal data you don't really need in the first place, the storage limitation principle says you should securely get rid of personal data you no longer need in the future. Securely getting rid of personal data can mean properly deleting it (don't just toss it in the trash!) or anonymizing it (converting it to a form that no longer permits identification of the data subject, such as aggregating it).

TIP

Customers that want to delete communications content from Twilio's systems, such as voice recordings or message bodies, can make use of the HTTP DELETE functionality. In addition, customers can request access to Twilio's message body and phone number redaction tools for Programmable SMS. Using these tools.the message bodies and the last four digits of an end users' phone number, respectively, are simply not retained after delivery of a message sent or received using Programmable SMS.

6. Personal data must be properly secured against accidental loss, destruction, or damage ("integrity and confidentiality").

Data protection is about a lot more than data security, but you can't have data protection without data security. If you can't keep personal data secure, it's hard to assure a data subject that you're following all the other GDPR processing principles.

GDPR is not terribly prescriptive when it comes to what security measures are required. Instead it requires security to be "appropriate." To be fair, not all forms of personal data require the same level of security. When deciding what is appropriate security, you need to conduct a risk-based analysis. Special categories or children's data, for example, warrant greater security, than "run of the mill" personal data. But even then, you must consider context.

For example, consider a database of phone numbers. If those phone numbers are for donors to a controversial political organization, they are likely to be considered higher risk than if they are for parent volunteers for a local school. Even though both involve phone numbers, the context of those phone numbers matters—it would be higher risk to reveal the phone numbers of the donors, because it would also reveal their political beliefs.

Nonetheless, while GDPR leaves it to the organization to conduct a risk-based determination of what is appropriate security, it does recommend in Article 32:

TIP

Twilio offers various tools that you can use to make your account more secure or the resources in your account more secure. For example, in addition to basic security options, you may want to check that you've enabled two-factor authentication on your account. Further, did you know that not only are voice recordings encrypted at rest on Twilio automatically, but you can also choose to use your own keys to encrypt recordings on Twilio for an added layer of protection? For customers who are looking for a broader suite of security tools, including access management tools like SSO, you should consider the Enterprise Plan.

- Pseudonymization and encryption
- The ability to ensure ongoing confidentiality, availability, and resilience of processing systems and services
- The ability to restore availability and access in a timely manner in the case of an incident
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisation measures for ensuring the security of processing.

7. Data controllers are responsible for and must be able to demonstrate compliance with the above stated principles ("accountability").

The accountability principle represents a shift in GDPR from the Directive before it. GDPR places more emphasis on accountability by data controllers processing personal data. It is not enough to "do" compliance—organizations now need to be able to "prove" compliance.

While data controllers are responsible for compliance with the data processing principles, as the service providers, data processors cannot afford to ignore them. Processors will be expected to appropriately support their controller customers' GDPR compliance, including ensuring that if they in turn outsource aspects of processing to sub-processors, applicable responsibilities and obligations flow through to those sub-processors (Article 28).

GDPR requires both controllers and processors to implement appropriate security (see Article 32) as demanded under the principle of integrity and confidentiality, and both controllers and processors must keep records of their processing activities (see Article 30).

TIP

Vendor management is an important part of GDPR compliance. If you have not already, you should make a list of all your vendors and service providers that process personal data on your behalf and put in place proper contractual protections to ensure that your vendors and service providers provide sufficient guarantees that personal data will continue to be adequately protected while in their custody. As your service provider, Twilio now offers a data protection addendum updated for GDPR.

TIP

As you go through the process of evaluating and bringing your business into compliance with GDPR, document your processing activities, how you're complying with GDPR, and, if you find gaps, how you plan to comply. This way you can address the "accountability" principle as you go through the process of addressing the other principles.

DATA SUBJECTS' RIGHTS

As a corollary to the above principles, data subjects have certain rights regarding their personal data. In fact,GDPR puts the onus on controllers to facilitate the exercise of these rights (see Article 12). Controllers must only use processors that can reasonably ensure protection of these rights, and processors, for their part, are expected to reasonably assist controllers in responding to data subjects' requests to exercise their rights (see Article 28).

Right of Access

As noted above under the principle of "lawfulness, fairness, and transparency," data processing must be transparent. Hand in hand with that, data subjects have a "right of access" to obtain from a controller a copy of their personal data being processed, as well as information about that processing, such as how and why their personal data is processed, how long it will be processed, and whom it has been shared with (see Article 15).

Right to Rectification

Data subjects have a right to ask a controller to rectify inaccurate personal data about them being processed by an organization. And, in appropriate circumstances, data subjects have a right to complete any incomplete personal data about them (see Article 16).

Right to Be Forgotten

The right to be forgotten, though implied under the Directive, is now clearly codified in GDPR in Article 17. Data subjects generally have a right to request that a controller erase their personal data.

Right to Restriction of Processing

Similar to the right to be forgotten, data subjects have a right to request that a controller restrict processing of their personal data (see Article 18).

Right to Data Portability

GDPR introduces a new data subject right: the right to data portability. This right requires controllers to make it easy for data subjects to take their personal data with them to another organization. In other words, they should be able to take their personal data out of one business's system and move it to another business's system (see Article 20).

TIP

Twilio allows you to export your raw call and message logs into a commonly used format.

Right to Object

Controllers whose lawful grounds for processing personal data are legitimate business purposes (see the first principles of data protection, above) must allow data subjects a right to object to the processing of their data. The data subject's wishes must be respected, unless the business has a more compelling interest in processing the personal data than the data subject's interests in not having their data processed (see Article 21).

A common scenario where this comes up is in the context of marketing communications. When a data subject objects to their personal data being used for direct marketing purposes, their wishes must be respected. A data subject's interest in not being marketed to is more compelling than your interest in marketing to him or her. Further, no later than the very first marketing communication with a data subject, they must be made aware of their right to object to further use of their personal data for these purposes.

TIP

By default, Programmable SMS offers support for common opt-out keywords on long codes. If you request that this feature be disabled, be sure to build your own opt-out system that complies with GDPR (and any other laws that may apply to your messaging program). Failing to honor a data subject's request to no longer receive marketing communications from you is a very visible violation of GDPR and will likely leave you with an annoyed data subject on your hands. Annoyed data subjects tend to be more motivated to notify a data protection authority about your misstep.

Right to Object to Automated Decisionmaking

When it comes to decisions that could have a legal, or otherwise significant impact, GDPR gives data subjects the right to insist that a human be involved in that decision-making process. In particular, GDPR says data subjects have the right "not be subject to a decision based solely on an automated process, including profiling" (see Article 22). The data subject's wishes must be respected, unless the business has a more compelling interest in processing the personal data than the data subject's interests in not having their data processed (see Article 21).

It is worth noting that nearly all of the above data subject rights are not absolute. For example, there may be situations where your business may have a greater interest in not erasing certain personal data than a data subject has in asking you to erase it. Therefore, if any of the rights described above cause you concern, it is worth further investigation into the nuances of the law relating to that right to make sure you fully understand your obligations.

OTHER GDPR OBLIGATIONS

In addition to the above, it is worth noting some additional obligations under GDPR.

Data Protection by Design and by Default

As the data processing decisionmakers, controllers are expected to implement, data

protection by design and default.

Data protection by design (also referred to as "privacy by design") means taking data protection principles into account when designing a product or service.

While this has been considered best practice for a while, it is now legally mandated by GDPR.

TIP

Putting aside that this is an obligation under GDPR, it simply makes good operational sense to take data protection into consideration when designing a product or service. It's generally much easier to design a product that complies with data protection principles from the get-go rather than having to retrofit a product or service after it's in production.

Data protection by default means that controllers should process the minimum amount of personal data needed to achieve the purpose for which they are processing it.

In regard to data protection by default, GDPR states that "such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons." An easy example of this would be a social media platform making posts limited to "friends only" by default and the user of the platform would have to actively choose to make it "public" to everyone (see Article 25).

Data Protection Impact Assessments

Controllers that are considering engaging in personal data processing that poses a high risk to the privacy rights of data subjects are supposed to conduct a data protection impact assessment (DPIA). A DPIA should not only review the proposed processing activity, but also the purpose for it, the necessity and proportionality of it in light of the risk to the data subjects, and any measure that could be taken to mitigate any data protection risk (see article 35). Data processors are expected to reasonably assist controllers in conducting DPIAs.

Establishment of an EU Representative

Controllers and processors that process EU personal data on a more than merely incidental (and low risk) basis, must designate a representative established in an EU Member State (see Article 27). The Member State chosen must be one whose data subjects are impacted by the processing activities. For example, if you only process personal data from data subjects in Australia and France, then France is where you should designate an EU representative.

Appointment of a DPO

Certain organizations, that process personal data will be required to appoint a data protection officer (DPO) to oversee and monitor personal data processing activities. In particular, the organizations that must appoint a DPO are public authorities, organizations whose processing involves regular or systematic monitoring of data subjects on a large scale, or organizations whose core activities consist of large-scale processing of special categories of personal data or data relating to criminal convictions (see Article 25). The Article 29 Working Party, a group of EU data protection authorities, has provided guidance on what kinds of activities constitute regular and systematic monitoring on a large scale.

Data Breach Notice

GDPR requires that the controller notify appropriate government data protection authority within 72 hours after the organization has become aware of a personal data breach, and data processors must notify controllers "without undue delay" upon discovering a breach (see Article 33). Further, if the breach is "likely to result in high risk to the rights and freedoms" of data subjects, the controller must notify the data subjects without "undue delay" (see Article 34).

Transfers of Personal Data Outside the EU

GDPR, like the Directive before it, does not prohibit transfers of EU personal data out of the EU. However, it does carry forward the Directive's requirement that EU personal data may only be transferred outside the EU if the country to which it is transferred has been deemed by the EU Commission to have "adequate" data protection laws (see Articles 44-50). If the country has not been deemed "adequate", there must be some other approved mechanism that ensures "adequate" data protection, such as standard contractual clauses, binding corporate rules, or approved schemes such as the EU-US Privacy Shield.

In age of cloud computing, it can be difficult operationally to ensure that no EU data leaves the EU or that EU personal data is only transferred to countries deemed "adequate," of which there are not that many. And, as of the date of publication of this whitepaper, most personal data that Twilio processes in connection with its customers' use of our products and services will be transferred back to the U.S. where the bulk of Twilio's data processing operations are. The U.S., however, has not been deemed "adequate" by the EU Commission. Accordingly, as a Twilio customer or just as a user of cloud-based services, it's worth having a working knowledge of the mechanisms for transferring EU personal data to non-EU locations.

For U.S.-based data processing operations, such as Twilio's, two commonly-used mechanisms for personal data transfer from the EU to the U.S. are the EU-U.S. Privacy Shield and standard contractual clauses.

With regard to the EU-U.S. Privacy Shield, to quote the International Trade Administration within the U.S. Department of Commerce, it was "designed by the U.S. Department of Commerce and the European Commission…to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce." U.S. organizations may join the EU-U.S. Privacy Shield once they have satisfied a series of requirements designed to ensure that they will continue to provide a level of data protection deemed "adequate" by the EU Commission. Participants must provide an independent recourse mechanism to data subjects for investigation and resolution of individual complaints or disputes at no cost to the data subject. Further, the U.S. Department of Commerce and Federal Trade Commission also both have certain enforcement powers to ensure companies that sign up for the EU-U.S. Privacy Shield are abiding by its requirements.

The EU-U.S. Privacy Shield is particularly useful for U.S. organizations that are not in a position to enter into individual contracts with each of their customers, such as is the case with many consumer-facing businesses. Notably, however, the EU-U.S. Privacy Shield is a mechanism that is only available for transfers from the EU to the U.S. Further, the EU-US Privacy Shield program requirements, which were developed under the Directive, might have to be adjusted to meet GDPR standards.

An alternative mechanism for transfer to the U.S., or any other country not deemed "adequate" by the EU, is the use of standard contractual clauses.

Standard contractual clauses are basically just what their name would suggest – a set of contractual clauses added to a contract between two parties that will ensure the non-EU organization will nonetheless process EU personal data in a manner consistent with EU data protection principles. Under the Directive, there are two "flavors" of standard contractual clauses: one for transfers from an EU data controller to a non-EU data controller and one for transfer from an EU data controller to a non-EU data processor. As of the date of publication for this whitepaper, a GDPR-ready set of standard contractual clauses has not yet been generated by the EU commission.

In addition to the two mechanisms commonly used by U.S. data processing operations discussed above, GDPR also recognizes other mechanisms such as binding corporate rules, approved codes of conduct, and certain derogations (i.e., exceptions) for specific situations. One derogation that might be tempting to leverage is where the data subject has "explicitly consented to the proposed transfer." But, beware that it's generally understood that consent-based transfer is really only valid for one-off transfers, not for the ongoing transfers which are typical when using cloud-

TIP

Twilio currently offers two mechanisms for transfer of EU personal data to Twilio's U.S. processing operations. Twilio is a participant in the EU-U.S. Privacy Shield Framework. Further, Twilio offers standard contractual clauses as an addendum to its terms of service. Twilio is monitoring updates to the available mechanisms for transfer.

Conclusion

GDPR represents a significant update to the provisions of the Data Protection Directive in an effort to provide appropriate protections for data subjects with respect to how organizations process, transfer, store, and protect the enormous amount of personal data being processed in this new digital world. Therefore, it is important that when your organization selects a product or software, your selection entails consideration of these new compliance obligations.

While there is still some ambiguity as to how these provisions will be enforced and interpreted once this measure takes full effect in May 2018, data privacy considerations and conversations around processing of personal data should not be delayed.

We hope this whitepaper provides you with insights for taking a proactive approach to data protection.