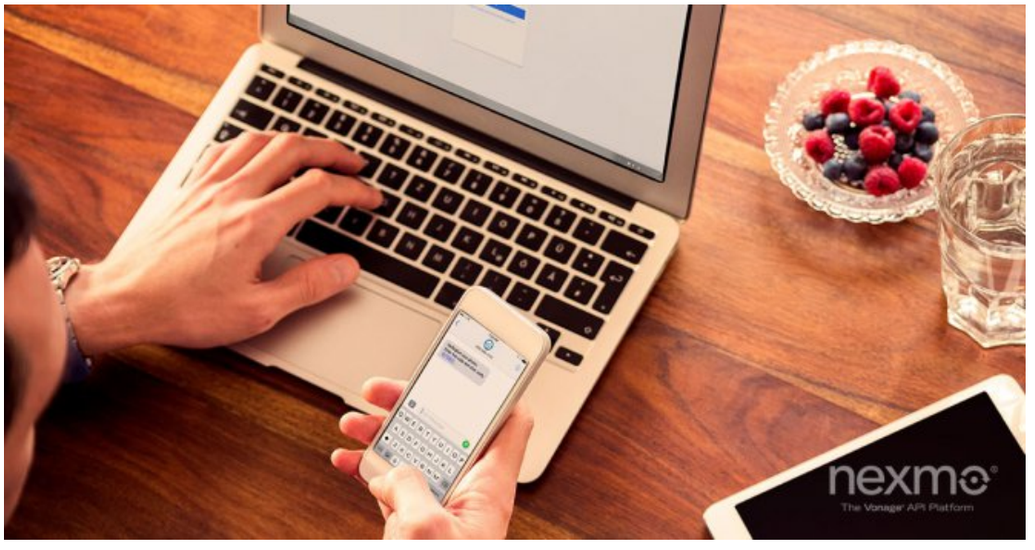
The GDPR: What It Means for Customer Communication

By GLEN KUNENE - Editor-in-Chief

Everything in customer communication changes on May 25, 2018. That's the day the European Union's new General Data Protection Regulation (GDPR) goes into effect, and it has serious implications for how companies communicate with their customers.



How serious? Up to €20 million or 4% of your company's global turnover (i.e. revenue) for non-compliance.

Read on to find out what the GDPR means for customer communication.

What is the GDPR?

For 20 years, the European Union has been a leader in setting clear legal expectations for how organizations must handle personal data. Its 1995 Data Protection Directive obliged each member state to create its own legislation and infrastructure for regulating the collection, storage and access to data held on individual citizens.

For as much data protection as the directive has provided, it has two significant weaknesses:

- **Each EU state implemented the directive in its own way.** Satisfying one member state's data protection requirements does not guarantee compliance with the equivalent laws in other states.
- **It applies only to EU-based organizations.** Organizations operating outside the European Union aren't held to the directive.

The GDPR is a new regulation that addresses these issues and makes a number of other changes to account for how the world has changed since 1995.

Perhaps the most impactful change is in who must now comply with the EU's data protection laws.

Does the GDPR affect my business?

If you collect, store or otherwise manage the data of individuals who live in the European Union, the GDPR affects you. It doesn't matter where in the world you are located. Even if you have no entity or presence in the EU, the GDPR applies to your company if you process the personal data of people who live there. So, if you operate a contact center that maintains customer relationships with EU residents, for example, it's safe to assume that your business falls under the new regulation.

To further understand how GDPR affects you, you need to determine whether your business is a controller or a processor. A controller is a company that collects personal data and then decides what to do with it. A processor is a supplier that handles the data on behalf of the controller. As an example, a bank would be a controller and their direct mail agency would be a processor.

The primary responsibility for GDPR compliance lies mainly with the controller, particularly when it comes to securing user consent. However, processors are equally liable for how they handle data.

A data bill of rights

Whether you're a controller or processor, the GDPR obliges you to prioritize the data-related rights of EU residents. As such, you can think of the GDPR as a bill of rights for EU citizens in relation to their data. Just as the US Constitution's Bill of Rights is uncompromisingly in

favor of the individual, so are the rights cited in the GDPR.

According to the UK's Information Commissioner's Office, those rights are:

1. The right to be informed.
2. The right of access: organizations must provide individuals access to the data they hold on them without any charge.
3. The right of rectification: if the data you hold on someone is incorrect, you must correct it and send that correction to any third parties with whom you shared the incorrect data.
4. The right to erasure.
5. The right to restrict processing: individuals control how and where organizations use their data.
6. The right to data portability: individuals must be able to export their data in an open format, such as CSV.
7. The right to object.
8. rights regarding automated decision making.

The overarching principle is that individuals have control of how their data is collected, processed and used in decision making. Let's look at some of the key rights in more detail.

The right to be informed

Half of Americans don't know what a privacy policy is, let alone take the time to understand the verbiage within one. Perhaps it's no surprise then that so many terms of service—including privacy policies—appear to be written as a form of lexical subterfuge.

The GDPR's right to be informed puts an end to that for EU citizens. Specifically, the GDPR obliges organizations to state clearly how they plan to use personal data. They must communicate that information in a way that is:

- concise, transparent, intelligible and easily accessible
- written in clear and plain language
- free of charge

There's no room for obfuscation or trickery.

The right to erasure

In 2014, the European Court ruled that individuals can have the right to ask search engines to remove links to content containing their personal information. Known then as the right to be forgotten, this has developed into the right to erasure and forms a key part of the GDPR.

EU residents can ask organizations to delete their data and prevent further processing of it, where:

- the purpose behind collecting the data is no longer necessary
- the individual withdraws consent
- processing the data breached one of the other rights granted by the GDPR

- another legal obligation requires erasure
- the data relates specifically to a child

Ultimately, if an EU resident requests that an organization delete their data, then the organization's default response should be deletion of that data.

However, there are scenarios in which an organization could refuse the request, but they must present their decision and the legal basis of their refusal within a month. Even then, it's not straightforward. It's about balancing the rights of the individual against certain defined needs of the organization (more to come on this). As each EU member state enacts the GDPR through its own legislation, there will likely be court cases over the next few years that put these ambiguities to the test.

The right to object

Along with the right to be informed, the right to object is, perhaps, the most impactful for contact center operators. It grants individuals a wide-ranging ability to ask organizations to stop processing their data. The following example demonstrates why this is particularly important for customer communication.

Let's say you run the contact center for a real estate listings website. You want to increase the number of information requests that your customers—i.e. realtors—receive from your website. So, you run a report on all of the people who recently requested information about a property, and you prepare an email for each person, offering details on similar properties.

Under the GDPR, you need to ensure that you have a legal basis to contact them. (We'll look at that in a moment.) However, you will also need to ensure that none of the people you contact has objected either to your processing of their data or, specifically, to receiving emails recommending similar properties.

Granularity of consent is an important concept in the GDPR. It's no longer enough to offer an opt-out from marketing communication. You need to give people the opportunity to consent or object to each way in which you want to use their data.

Just as with the right to erasure, an organization can deny such a request but they must have a legal basis to do so.

Rights around automated decisions

As AI becomes established in the contact centers of the near future, human lives will be affected more often by decisions made algorithmically. Such decisions, cloaked in proprietary technology not easily understood by most people, have the power to make significant changes to people's lives.

Like any bills of rights, the GDPR aims to protect citizens from such unchecked power and, as such, it addresses automated decision making. Specifically, it grants EU residents the right to know when a decision was made automatically regarding their personal data and:

- obtain human intervention
- express their point of view
- obtain an explanation of the decision and challenge it

There are exceptions. The right does not apply if an automated decision is:

- necessary for entering into or performance of a contract between you and the individual
- authorized by law (such as to prevent fraud)
- based on explicit consent (as defined elsewhere in the regulations)

The first exception seems ripe for conflicting interpretations. Thankfully, the Information Commissioner's Office in the UK offers some guidance. They say the rights here apply where two requirements are met:

- the decision is taken using personal data processed solely by automatic means
- it must have significant effect on the individual concerned

If a human is involved in making the decision, even if they do so on the basis of data collected by an automated system, then the rights do not apply. Similarly, if the decision has no significant impact on the individual—such as a Facebook personality quiz—then the rights do not apply.

Even with such guidance, there is room for debate. For example, an automated loan decision can be made entirely without human intervention and have a significant impact on the applicant. However, it would seem that the decision is also necessary for entering into the loan contract.

Lawful processing in the GDPR

We've seen what rights EU residents gain under the GDPR but what do those rights mean for data controlling and processing organizations?

Under the new regulations, it's up to the organization using the data to prove that they are doing so legally. Much discussion around the GDPR cites explicit consent as necessary for any use of personal data. However, as the UK's Information Commissioner says, "consent is one way to comply with the GDPR, but it's not the only way."

So, what are those other ways?

The GDPR provides several legal bases for processing data, with the five most important being:

- the individual gives their consent
- processing the data is necessary to fulfill or enter into a contract with the individual
- legal obligation makes it necessary
- task carried out in the public interest or through official authority makes it necessary
- processing the data is necessary to pursue the legitimate interests of the data controller

EU member states are free to add their own legal bases, and there are a number of other, special, categories. However, for most companies communicating with their customers, it's the first two and the last one of these bases that will have the most impact: either the individual has consented or you are not legally permitted to run your business without processing that data.

Let's look at consent first, because it's the easiest to pin down.

Gaining and losing informed consent

Consent is a big part of the GDPR and the text of the regulations is strongly opinionated on what counts as consent. Here's the text of article 4 of the GDPR, where consent is defined:

"consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Let's unpack that with some help from the UK's Information Commissioner's Office. To gain GDPR-compliant consent, you'll need to:

- give individuals genuine choice and control over whether they give consent
- gather positive opt-in: pre-ticked boxes and similar ruses do not count as consent whereas double opt-in will provide greater certainty
- be clear and very explicit in stating what the individual is consenting to
- keep your requests for consent separate from other terms of service
- be specific and granular: a blanket catch-all will not do
- be clear and concise: there's no room for deliberately hard-to-parse double negatives
- name any third party who will rely on the consent
- make it easy for the person to withdraw their consent, and tell them how they can do that
- keep evidence of the consent: who consented, when, how and what they were told at the time
- review the consent you have and refresh it if anything changes
- avoid making consent a precondition of using your service

This is a long way from typical signup processes. Be clear, leave no doubt and keep an evidence trail in case you need it later. Under the GDPR, consent is a moving target: if the situation changes, consent may no longer be valid.

Processing the data is necessary to your contract with the individual

Another legal basis for processing someone's data is that your contract with them makes it necessary. For example, an employer needs to process data about its employees.

The key word here, though, is "necessary." If there's another way to fulfill the contract without processing that personal data, then you can't claim that as a legal basis.

Legitimate interests

"Legitimate interests" is the vaguest of the legal bases. It's intended to allow for circumstances not foreseen by the drafters of the regulations. Existing European Union data protection laws already allow for this reason for processing data, so guidance exists, but it is

not specifically tuned to the GDPR.

The existing guidance makes it clear that it's not enough only to claim that your organization needs to process the data. You must also show how that need balances against the individual's rights.

Document everything

Whichever basis you choose, the GDPR requires an audit trail. The more you document, the greater chance you have of fighting a challenge brought by an individual.

GDPR personal data defined

So far, we've covered a great deal about how the GDPR will mandate that organizations handle the personal data of EU residents. However, we haven't looked at what data the GDPR considers to be personal.

In the US, what counts as personally identifiable information is defined by the NIST:

"any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

The GDPR definition is much broader:

"any information relating to an identified or identifiable natural person."

The definition adds further detail that confirms the breadth of the what the GDPR means by personal data:

"an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Guidance in the UK, and elsewhere, states that this would cover all manner of data, such as IP addresses, that previously would not have qualified as personal data.

There are also further "special categories of personal data", such as racial origin and religious beliefs, that are subject to additional regulations.

What all this means for customer communication

As of March 2018, the personal data of EU residents becomes a little like radioactive material: if handled properly, there's no problem. At every stage, careful thought must be put into why that data is needed, how it will be used, and why the organization is legally allowed to have it. And when something goes wrong, there must be a detailed log to prove that the law was followed.

Much customer communication today happens without an explicit thought about its legality. Other than for marketing communications, the business of storing and using customers' data to communicate with them is just another part of getting the job done. However, under

the GDPR, every item of personal data and every communication will require careful thought.

Do you have the correct permissions and reasons to send that SMS to that customer on that subject? Did this person give informed consent for you to store their IP address each time they log into your website? Are your security procedures strong enough to prevent a data breach?

GDPR requires a 180-degree turn in how your company regards and treats personal data. You must get used to thinking that you have no permission to collect, store or use that data, even if *you already have collected it*! GDPR regulations mandate a new level of rigor and permissions checking for customer communication, unlike anything we've seen before.

Since there's a great deal of room for error and misinterpretation, data controllers and processors need to be vigilant. The UK's Information Commissioner says that fines will be the last resort (how other member states approach infractions remains to be seen). However, the potentially enormous fines (up to 4% of global turnover or €20 million) should be cause for concern. Even if noncompliance doesn't result in an immediate fine, companies that are found in violation of GDPR regulations could face a loss of public and market confidence.

For companies running contact centers, or who otherwise engage in customer communication, new, more stringent review systems need to be implemented to ensure that citizen data rights are being upheld. May 25, 2018, will be here before we know it. If you haven't already, the time is now to learn about and prepare for these changes in customer communication.

Editor's Note: *nothing you read here is legal advice. Seek legal counsel for specific recommendations related to GDPR compliance. For more information on Nexmo's approach to GDPR, please click here.*

Message (optional)