Lazarus Alliance
Proactive Cyber Security©

Data Rights, Consent and Operations for U.S. Businesses Under GDPR Regulations

Consumers and businesses in the United States are used to a particular model of data-driven commerce: businesses can collect and use data as they see fit, and consumers can, generally, opt-out of certain activities.

As global, data-driven corporations continue to operate worldwide, however, they are quickly running into the strict protective measures of the European Union's GDPR regulations. For example, Facebook was recently handed a ~$270M fine from Irish authorities for obfuscating data collection efforts contrary to GDPR rules.

While this might seem like an EU regulation isn't a huge concern for smaller companies without global reach, the reality is that many organizations are, knowingly or not, working in the EU in a way that requires them to adjust their data collection practices. One of the major areas where this is true is in consent protections.

In this whitepaper, we will discuss the concept of consent under GDPR and how it may impact your operations.

Consent and Terminology in GDPR Compliance

Since GDPR is a framework with jurisdiction over EU-participating countries, many U.S. companies aren't familiar with its regulations or even its philosophical approach to security and data rights.

Under GDPR, the primary focus of regulations and security are the rights of the "data subject." The data subject is the consumer or individual from whom an organization intends to collect data from for whatever purpose. GDPR regulations are therefore an extensive system of rights and protections for this individual such that they have as much control over their data as possible.

What sort of rights are included for the data subject under GDPR? Briefly, data subjects are given the ability to:

1. **Receive clear and unambiguous information** regarding how any data collected for business purposes will be used. This includes data processing, marketing applications and the sale of data to third parties (data subjects have the right to prevent companies from selling data).

2. **Gain access, upon request, to all data an organization has collected** from them directly or through third parties.

3. **Demand the deletion of any personal data** the organization has collected from them or third parties (the right to be forgotten).

Another important aspect of GDPR, and something that is markedly different from U.S. regulations, is the legal obligation of businesses and organizations to gain the consent of a data subject prior to data collection or marketing activities.

Unlike most regulations in the U.S., GDPR requires consent before any business activities. In the United States, activities like email marketing will often include an "opt-out" disclaimer where a consumer can forego receiving communication like emails or texts. The implication of this arrangement is that businesses can collect data and begin marketing activities without the consumer knowing it. Conversely, business processing and marketing activities cannot begin prior to this consent--the data subject must have consented beforehand, and the organization must have compliant documentation of that consent.

This includes requirements for consent to collect data and send marketing materials (particularly emails), the expectation of the security and privacy of that data, and the right to demand complete knowledge of that data and, if necessary, demand its deletion.

The Criteria for Consent Under GDPR

There are some key passages in the letter of GDPR law that define the criteria for consent under GDPR:

> *Article 4(11): Consent of the data subject means freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action signified agreement to the processing of personal data relating to him or her.*

Article 7:

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

While this is a seemingly clear set of requirements for gaining consent under GDPR, it can be a bit confusing as to what this means in day-to-day practice.

Concretely, compliance with GDPR calls for your organization to follow these criteria for consent:

- **Consent Must Be Informed:** A data subject cannot provide consent under ambiguous circumstances. That is, if you gain consent from a data subject it must be with a clear description of the data collected, why that data is collected and what could be done with that information. Furthermore, the mechanism for collecting data, including the disclaimer to inform the data subject of what they are consenting to, must have clear documentation in your IT systems.

- **Consent Must Be Specific:** Gaining consent isn't a place to cut corners with explanations and descriptions. GDPR requires that the use of consumer data be

limited only to business processes necessary for the relationship between the consumer and the business. For example, you cannot collect data for an email list and then sell that data to a third party without specifically gaining consent for both practices. Under GDPR, you should provide a specific description of what the data is for and isn't acceptable to have large and vague umbrella consent requests.

- **Consent Must be Freely Given:** You cannot implement any coercion or pressure to gain consent. That is, the consumer cannot suffer financial or business consequences because they did not give a certain kind of consent, nor should they have less access to services or products because of their response to consent requests.

- **Consent Can Be Revoked:** At any time, for any reason, the data subject can revoke consent for any process or practice. Your organization cannot circumvent this, there is no way to claim that you may keep data outside of the consumer's wishes, and, upon receiving a revocation of consent, you must immediately cease any related activities.

What Does This Mean for American Businesses?

If you are an organization doing business in the EU a digital or data-driven business collecting data for analytics or marketing purposes, you are operating under GDPR jurisdiction, and consent is a major concern for you.

To begin with, you must gain consent for specific activities that collect user data. Currently, many of us may have started to notice the increased use of consent forms from major websites asking for permission to use cookies. Cookies are small bits of information that websites use to retrieve information about users between sessions, including user settings and browsing history. Since some of this information falls under the definition of personal information, and since many of these websites offer services to consumers in the U.S. and the EU, they are using clear consent forms to stay compliant with GDPR.

Additionally, if you're using data collection forms on your site for any reason, you must include some form of consent-gathering. This mechanism doesn't need to be complex--it can be as simple as a disclaimer with a checkbox that shows that a user has consented to whatever you're asking for.

In terms of actual IT compliance, however, it's critical that you have technologies and practices in place to show that you are meeting the requirements for clear, freely given consent. This includes logs and records of consent given by users. This includes anything from consent to send emails for product updates to cookies for websites.

Furthermore, you must also keep records of any requests revoking consent that also include your response and evidence that you have ceased communications or activities related to that consent.

Compliance efforts must include technical and operational measures. Your people must understand what it means to respond to consent revocation requests in a timely matter, and they should also understand how to gain consent freely and unambiguously during consumer interactions.

Conclusion

Some marketing and analytics platforms will include GDPR security measures as part of their operation. Recently, HubSpot has implemented updates to automatically start GDPR measures for accounts working with customers in the EU. These measures seem strict at first: immediately blocking mass emails for any consumer (EU-based or not) who hasn't given consent and starting pop-up disclaimers for cookies on websites. But this move is a clear indicator that, as U.S. businesses continue to operate digitally in the EU, they will have to contend with GDPR.

If you are a small business or enterprise-grade corporate that wants to know that they are prepared for GDPR requirements, from cybersecurity and administration to consent and documentation, then it serves you to work with a partner that has extensive experience with GDPR and compliance more broadly. Lazarus Alliance is a veteran-owned company with decades of experience in the cybersecurity and compliance industry, including the management and implementation of compliance strategies in industries like healthcare, government and defense contracting, manufacturing and retail.

Lazarus Alliance is Proactive Cyber Security©

In any jurisdiction, and in all industries, we are your global partner in compliance, risk, policy, security testing, financial audit and Cybervisor© services.