Is Your IR Website GDPR Compliant?

13 Tips to Help You Understand GDPR

What You Must Do with Your IR Website Vendor

IR Website GDPR Whitepaper

Tom Runzo, Equisolve

EQUISOLVE

Introduction

Your IR website collects personally identifiable information from website visitors and shareholders, including such things as names, email addresses, phone numbers, IP addresses, data from cookies, and the contents of site visitors' web browser address bar.

If any of your shareholders or other visitors to your IR website are located within the European Union (EU), the new General Data Protection Regulation (GDPR) now governs how you collect, store, and use personally identifiable data of those people and anyone in the EU.

Fines for GDPR non-compliance may be €20,000,000 or up to 4% of revenue— whichever is larger. In the first 30 days of GDPR, which started on May 25th, 2018, U.S. companies have been sued for more than eight billion dollars. And a variety of data protection authorities have begun their enforcement activities by doing such things as organizational surveys, rather than simply waiting for consumer complaints or data breaches to bring compliance failures to the attention of regulators.

What is GDPR?

GDPR is the commonly used acronym for the General Data Protection Regulation adopted by the European Parliament in April 2016, and that allowed a two-year grace period for affected organizations to develop their compliance programs prior to the GDPR taking full effect on May 25, 2018.

The GDPR governs how organizations collect, process, use, and protect personal data and the privacy of individuals in the EU within all 28 EU member states. GDPR data processing includes anything related to collection, recording, organization, structuring, storage, modification, retrieval, use, disclosure, restriction, erasure, or destruction.

The GDPR applies both to organizations operating within the EU and to organizations that offer goods and services to people in the EU no matter where such organizations are located. Additionally, GDPR regulates the processing of personal data that is transmitted outside the EU for processing.

Who is Responsible for GDPR Compliance?

The GDPR defines three distinct entities that are key to understanding GDPR compliance obligations.

Data Subjects

Under the GDPR, a data subject is the identified or identifiable natural person that personal data is about. The data subject is any individual, whether that person is functioning as an individual consumer or in an employee role, or is interacting for business-to-business commercial purposes.

Data subjects are the individuals who are considered the owners of personal data and who are given specific rights under the GDPR related to their personal data.

In terms of your IR website, site visitors and your shareholders represent the majority of your data subjects.

Data Controllers

You, as the owner of your IR website, are the data controller for personal data collected from your IR data subjects.

Data controllers are the natural or legal persons or organizations that determine the purposes and means of the processing of personal data, and as a result, data controllers have the most complicated GDPR compliance requirements.

A data controller is responsible for deciding how they collect, transmit, store, and use data subjects' personal data even in situations where the data controller relies on data processors to handle those activities. In such cases, the data controller must provide clear and complete instructions for the work the data processor is to perform.

The data controller is ultimately responsible to the individual data subject whose data was collected and used.

Although data subjects may only be individual natural persons, a data controller may be a natural person but is more commonly an organization (whether business, government, or other type of organization).

Data Processors

Data processors are the natural persons or legal entities that provide services to data controllers related to personal data processing.

Data controllers may process data for themselves instead of, or in addition to using, external data processors; however, doing so does not make the data controller also a data processor. Data processors are those whose core business activities include such data processing provided as a service to data controllers.

Like data controllers, data processors may be natural persons or legal entities, but they are most commonly outside service provider organizations.

In terms of your IR website, Equisolve would be a data processor working on your instructions for various types of processing necessary to fulfill your purposes for the website.

What's the Risk if I Don't Comply?

Companies found in violation may be fined €20 million or 4% of revenue - whichever is greater. On the first day the regulation took affect, two U.S. tech giants were sued for over $3 billion each.

Can I Choose to Not Do Business with Residents of the EU and Skip GDPR?

If the GDPR does not apply to your business, and you wish to minimize the risk that EU persons or regulators might think that you are governed by the GDPR, here are some things you can do to help protect your position:

1. Make sure your website content and your means of interacting with site visitors do not create the impression that you are seeking interactions from individuals in the EU. This can include:
    a. Making sure that your site is not offered in a language specific to any EU country beyond your site's native language, presumably English.
    b. Making sure that your site does not offer uses of currencies other than your own, presumably the U.S. dollar.
2. Including wording in your IR website notice of privacy practices that clearly states that your website is not intended for use by people in the EU, or at the very least, that states your business is governed by U.S. law and that your website's intended audience is limited to people in the U.S.
3. Provide an initial website landing page warning that states the intended audience for your site and links to the full details of your privacy notice. This landing page could be displayed to all visitors or limited to site visitors from EU IP addresses.
4. In lieu of the landing page notice just described, you could choose to block all IP addresses in the EU to prevent access to your website by anyone in the EU.

Please note that these are just some generally accepted current practices to help clarify for people when the GDPR does not apply to your business, and to avoid the risk of GDPR applying to your business inadvertently. None of these things have been put to the test of enforcement actions by any EU data protection authorities yet.

13 Tips to Help You Understand GDPR Compliance

1 Create a data inventory that describes all the data you collect.

The data inventory would include identifying what data you collect about your customers, shareholders, prospects, vendors, and employees, as well as about shareholders and visitors to your IR website.

This data inventory can be documented in a simple spreadsheet that identifies each type or category of personal information you collect, and that answers the following questions for each type or category:

I. Where do you get the information?

II. Who else has access to it?

III. What do you do with it?

IV. How long must you keep it?

2 Create a record of your data processing activities.

The GDPR requires data controllers and data processors to document their processing activities from data creation to data destruction. Your data processing record is different from a data inventory. The data processing record would identify each type of data processing and then for each type of processing, document answers to the following questions:

I. What specific data is included in that processing type?

II. How do you perform the processing, including what data processor(s) you use for that type of processing?

III. Why is that processing necessary?

IV. What is your lawful basis for that type of processing? (The GDPR provides 6 lawful bases for processing and data controllers must identify the basis that applies to each type of processing. Consent is one of that lawful base and it has a number of requirements)

3 *Make sure data is secure, both in transit and at rest.*

The GDPR doesn't provide a lot of new, specific security requirements, but your security policies and procedures are key parts of your GDPR data protection program, so you should make sure they are appropriate for the types of data you process.

4 *Make sure your security incident management and data breach response process is able to handle the GDPR 72-hour data breach notice requirement.*

One purpose of the GDPR and sound information security practices is to avoid data breaches in the first place. But the best plans can fail, and the GDPR requires that you have procedures in place to promptly detect and report breaches of personal data related to EU persons. Determine who you will need to report security failures to and be prepared to act quickly: Companies will have at most 72 hours to report breaches that threaten personal data security, and fines for failing to timely report are assessed on top of fines for allowing the breach to occur at all.

5 *Write a clear and fair notice of privacy practices to be placed on your IR website.*

This notice is commonly labeled as a "privacy policy" in the U.S., but since a privacy policy would more commonly be considered an internal document and the public-facing notice is targeted externally, the privacy practices notice is more appropriate.

You should avoid "legalese" and overly technical jargon in the privacy notice. Under the GDPR, this type of notice should be easy for your site visitors to navigate and understand.

6 *Make sure you have valid consent for your data processing, where you rely on consent as the basis for doing the processing.*

The issue of consent, especially for marketing purposes, is one area of preparation for the GDPR that has been confusing for many companies, and has led to a lot of activity, some of it

unnecessary and some of it not adequate to solve the problem.

If you are not certain your existing consent meets GDPR requirements, you can always seek new consent while observing the GDPR criteria for valid consent. Taking this approach can give you a fresh, better quality of consent and show that you are aware of your obligations, as well as interested in doing the right thing for your data subjects.

Here are some key consent considerations. Valid consent must be:

I. Freely given.

II. Specific to each limited, clearly defined purpose.

III. Informed.

IV. Given through an unambiguous indication.

V. Given through an affirmative act (opting in) rather than negation (opting out).

VI. Distinguishable from other matters.

The request for consent needs to be written in clear and plain language, intelligible and easily accessible.

For consent related to your IR website activities, do not entangle consent expectations within your website's terms of service.

7 *Keep a record of consent, such as who, when, and where.*

Under the GDPR data controllers must be able to prove that consent was given. Having a standing process and available record of consent provides an indicator of compliance and allows you to respond to requests with minimal business disruptions.

8 *Make it easy for data subjects to withdraw consent to their data being used or stored.*

Preferences dashboards are a good way to manage consent you have already obtained and communications preference going forward.

9 *Have a process for providing a copy of the personal data you possess or process to the data subject.*

This data subject access right, as well as others, create the likelihood that U.S. companies need to create procedures and tools related to the personal data they control that were never envisioned by their original systems designers. You need to proactively have a process in place that allows you to produce copies of the data you possess on a data subject when you get a valid data subject access request.

10 *Don't hold onto data unnecessarily.*

The concept of deleting data once it is no longer needed is one that sometimes puzzles U.S. companies, as this is not the normal practice. But in the GDPR model of data belonging to data subjects, and data subjects having the right to to be forgotten, data retention limitations should receive more focus by U.S. companies in the future.

11 *Have a process for deleting data.*

One of the data subject's rights is the right to deletion (also commonly referred to as "the right to be forgotten"). This right doesn't apply to all situations, but you need to have a way to remove data from your systems and storage.

12 *Make your team aware of and train them on the new GDPR and privacy principles in general.*

Information security awareness training has been a common element of U.S. business practice for more than a decade. But privacy-focused training, that covers concepts like data minimization and data subject rights, is still not common in the U.S. outside of key industries such as healthcare and financial services. GDPR has started to change that, and U.S. state laws will continue to affect the needs for basic privacy knowledge.

Data controllers should consider training their entire organization on GDPR basics, and consider providing additional training on key GDPR-driven policies and procedures specific to the organization.

13

Appoint someone to be responsible for privacy and security compliance.

You may be obligated under the GDPR to appoint a data protection officer, DPO, (and this is a role that has a very specific purpose and duties). But even if you are not required to appoint a DPO, you may benefit from having someone with explicit responsibility for data protection.

Tips for Working with Your IR Website Provider

If your company is subject to the GDPR, then any service provider who processes data of EU persons on your behalf is subject to the GDPR as data processor. Your IR website providers and associated information service providers who process data collected through your IR website would be included among those GDPR data processors, and you should expect that such data processors are fully aware of the GDPR and of what their roles as data processors mean for their operations and for your IR website.

Execute New Data Processing Agreements with Your IR Website Providers

In addition to your own internal GDPR compliance obligations, as a data controller, you must oversee your data processor relationships and make sure that your data processors follow your instructions and do not take unauthorized actions on your behalf. The contracts that you put in place with your data processors provide your primary means of instructing them and defining the limits of their role in your data processing, and you must have a data processing agreement or a data processing addendum to your existing contract or terms of service with your data processors. And these agreements need to be updated to meet the requirements of the GDPR.

Instruct Your IR Website Providers Regarding Use of Subprocessors

As a data controller, you will need to instruct your IR website provider regarding what data should be collected, how it will be used, and what the provider's role is in the data processing.

Your IR website provider is likely to be a primary data processor working for you related to your IR activities and is likely to be engaged with other data processors on your behalf. The GDPR does not draw distinctions between "subprocessors" as having any less responsibility than primary data processors, and you are still ultimately responsible for their work and for their non-compliance.

Be sure you know what third parties your IR website provider is already using. You will need to document them in your data processing record anyway. But you also need to make sure your primary IR website provider has executed valid data processing agreements with those subprocessors or determine whether you will need to execute a separate data processing agreement directly with the subprocessor (as would be the case with Google Analytics, for example).

And your controller-processor data processing agreement with your primary IR website provider should also provide specific instructions to the provider related to engaging subprocessors on your behalf.

Common Misconceptions

"Small businesses are exempt from the GDPR."

This is simply not true—no business is exempt when EU personal data is involved.

"Adding a notice that your website uses cookies makes your website GDPR-compliant."

Though a lot of websites have begun incorporating pop-over cookie warnings, there is no requirement in the GDPR to do this, and there is no consensus about whether such mechanisms adequately serve their intended purposes, such as gaining consent. As with so many other things at present, this kind of "solution" has not been tested in enforcement actions. And even if they fulfilled their intended purposes, they do nothing to address the bulk of GDPR responsibilities, especially around data subject rights.

"GDPR is an information security issue, and our information security program makes us GDPR-compliant."

The GDPR says relatively little about information security beyond requiring appropriate protections for personal data. The GDPR is primarily about privacy rights and incorporating "privacy-by-design" proactively into business practices.

"GDPR is an IT problem."

Though technology is integral to nearly every aspect of communication and relating to customers, GDPR is not focused on the technologies themselves, but the decisions that are made in designing and carrying out data processing activities and may involve every department in any company that is working to comply with the GDPR.

"Companies that are not in the EU aren't subject to GDPR and to GDPR enforcement actions."

The law applies to the data of residents of the EU regardless of where the data is stored and processed. Companies that are in the U.S. may face enforcement actions from EU regulators and those could come through cooperation with U.S. regulators such as the FTC or from EU individuals pursuing their rights directly. In addition, reputation risk and risks of more local enforcement by U.S. states could be created by data breaches or complaints that come to light through EU efforts to enforce the GDPR with a U.S. company.

"GDPR only applies to data that has been provided by a user."

The GDPR applies to all personal data related to or collected about a data subject. And the GDPR defines personal data in much broader terms than U.S. companies may be used to from U.S. practices and state and federal compliance efforts.

"Consent is always required."

Consent is usually required for the types of processing that relate to functions of your IR website; however, there are a variety of processing circumstances that do not require consent, including things such as processing related to securing the data and protecting against fraud and processing related to your fulfillment of a contract that the data subject has entered with you.

“There is only one way to give consent.”

There are lots of ways that consent may be given. The key to valid consent is observing all the criteria needed in practice for the consent to be valid rather than it being dependent on the specific means for gaining consent. In addition, it is of critical importance that the consent process and specific instances of a data subject giving their consent be properly documented so that you can prove the consent is valid.

“If I rely on legitimate business interests as my lawful basis for processing information, I don’t need to get user consent.”

Data controller determination of a lawful basis for any given type of information processing is one of the more complicated privacy design requirements of the GDPR, and legitimate interests as a default basis is likely to be one area of extra scrutiny by regulators. Even if legitimate business interests allow for one type of processing, data collected in that processing cannot be freely used for other purposes.

“If your website is not SSL, it can still be GDPR-compliant.”

Though the GDPR doesn’t get very specific with technologies that must be employed, the transmission of data through your site must be sufficiently secured to protect from unauthorized access or use in transmission, so it would be difficult to defend this statement as true, and making such a statement would help indicate a lack of understanding to data subjects and regulators so it is a statement that is best avoided.

“Companies must maintain all data in its country of origin.”

GDPR specifically provides for the ability of data controllers to use cross-border transfers and data processors outside the country of data origin, provided there are adequate security measures and ways to affirm sufficient compliance related to the processing and the processors.

“I can certify my business and websites as being ‘GDPR-compliant’.”

Currently, there are no certification mechanisms that have received any kind of approval from EU regulators.

Conclusion

The impact of the GDPR on business practices worldwide has been huge, especially in the last several months leading up to the May 25, 2018 full compliance date. And since so many aspects of working to comply with such a sweeping regulatory framework include making decisions about things that have yet to be clarified, the GDPR impact on business practices will continue.

In the U.S. in particular, several elements of the GDPR's individual data subject rights are not familiar to businesses outside healthcare or financial services. And the concept of " privacy-by-design" and "privacy principles" is very new to most U.S. businesses. But U.S. states are already moving to create these same types of business requirements for U.S.-based operations that may only target U.S. residents.

So any effort you make for GDPR compliance now will help minimize the risk and impact of GDPR enforcement activities and individual data subjects exercising their rights from now on, as well as make your eventual need to address similar requirements in the U.S. be less costly and less disruptive of your normal business operations.

EQUISOLVE

Tom Runzo, CEO
2455 E. Sunrise Blvd., Suite 1201
Fort Lauderdale, FL 33304
954-858-8550
tom@equisolve.com
equisolve.com