How to Respond to GPDR Requests from Website Visitors

By Michael E. Young, J.D., LL.M.
Attorney & Counselor at Law

Date: May 3, 2018

What Is The GDPR?

The General Data Protection Regulation (GDPR)[1] is a new 88-page regulation designed to protect the privacy rights of European Union (EU) residents. This includes information collected from EU residents when they visit websites (whether or not they are customers of the business that owns the website).

When Does The Regulation Go Into Effect?

May 25, 2018

What Are The Penalties For Noncompliance?

For violations by small and medium-size enterprises (SMEs), there can be a fine of up to € 20 million euros (currently about U.S. $25 million).

In addition, you can expect there to be expensive legal proceedings costing six figures whether or not your business "wins" the dispute.

Does GDPR Cover Your Website?

There's not an easy answer to this question because the regulation is new. This means there aren't court cases to look at for guidance.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

In addition, if your home country is located outside of the European Union, there *may* also be a treaty or trade agreement that contains language requiring your nation to comply with the regulation.

Without the clear guidance of court decisions, a treaty, or trade agreement, here are three factors to consider.

1. Background.

The United States has been applying its laws globally for many years. For example, a man was arrested in Australia and sent to the United States to stand trial for sending out unsolicited commercial emails (spam). He was convicted and put in a U.S. federal prison.

Similarly, the U.S. federal government is currently trying to extradite Kim Dotcom (a Finnish and German citizen) from his residence in New Zealand to stand trial in the United States for allegedly violating U.S. copyright and other laws. His home was raided by a SWAT team, websites shut down, bank accounts frozen, and assets seized.

Because of this history of enforcing laws beyond borders, it should come as no surprise the EU claims the GDPR applies globally to protect the privacy rights of EU residents.

2. Do You Collect Data Covered By The GDPR?

The personal data the regulation seeks to protect is very broad. For example, an EU visitor to your website could have his IP address automatically logged by your server. If the visitor provided you an email address by subscribing to your e-newsletter, that would also be covered.

Even if you blacklisted all countries in the European Union using software (e.g. Wordfence), an EU resident surfing the Web using a virtual private network (VPN)

service could easily access your site and provide personal data covered by the regulation.

3. Where Is Your Business Based?

If your business is based in the European Union, the GDPR applies to your website if you're collecting personal data.

If your company is not based in the European Union, it may make sense to comply with the GDPR to the extent it isn't in conflict with your national and local laws.

After all, even *if* you don't have a legal obligation to comply, do you want to spend the time and a small fortune fighting the European Union on the issue if there's a complaint?

Can You Charge For Processing GDPR Requests?

If a GDPR request is reasonable, as a general rule, you typically can't charge for responding to the first request made by a person.

However, if a request is clearly unfounded *or* excessive, then you can charge a reasonable fee for processing the request if you don't reject it.

For example, it would likely be an *unfounded* request if a person wanted a copy of all the IP addresses they've used to visit your website during the past year from many locations but never provided you with any other personal data.

Similarly, it would be *excessive* to request copies of the exact same data you provided the month before to the person in response to a prior request.

So, what's a reasonable fee to charge under circumstances where you can do so? That's unclear.

However, you should be able to back up your fee based on standard business practices. For example, if it would cost you U.S. $50 in labor to process a request,

the expense could be a reasonable basis for justifying the fee charged. On the other hand, charging U.S. $10,000 to process a request would likely be unreasonable.

What Can Be Requested Under The GDPR?

EU visitors to your website can request: (1) access to their personal data you've collected; (2) deletion of their personal data you've collected; and (3) that you stop processing their personal data for marketing purposes.

They can also request (4) you transfer their personal data in a commonly use electronic format (e.g. CSV file) to a third party.[2]

For example, if your business has their medical records, there can be a request to transfer the records to a health insurer or medical service provider. If you've collected their financial information (e.g. an online loan application), they can request the information be transferred to a financial institution or other lender.

How Do You Handle Requests?

Within 30 days, you should respond to the request.

Approved Requests

Most requests will be easy to process. In fact, you should expect common requests to ask for typical information you collect on a customer, agreeing to delete such information, or promising to not use it for marketing purposes (e.g. unsubscribing them from marketing emails or text messages).

[2] If you're not tech savvy, you can have a Web developer compile personal data for your responses to GDPR requests.

Denied Requests

If you deny a request, you should explain why you denied it. For example, you may have a legal obligation to retain copies of certain personal data that prevents you from deleting it upon request.

As a general rule, you should also let the person know they can challenge the denial with the EU Data Protection Authority and seek a judicial remedy for your denial.

However, if your national laws, local laws, or some other legal authority controls instead of the GDPR, you may want to pursue an alternative dispute resolution process outside of the GDPR.

For example, the forms generated by Website Legal Forms Generator software provide the flexibility to demand arbitration of disputes in the County or Parish where your business is located based on national and local laws instead of the GDPR if there's a conflict.

Automated Processing

The GDPR also protects EU residents against solely using automated processing to make financial and other important decisions that are legally binding or significantly affect the person.

For example, if your website collects financial information and uses algorithms to screen loan applicants, you should obtain the applicant's express consent to do so as part of the application process.

Your automated decision can be based on a relevant law. For instance, if a minor tries to buy something from your website that's only legal to sell to an adult, an automated decision to reject the purchase is okay.

On the other hand, if your automated decision is based on something other than a legal requirement, you should explain to the person the logic behind the process and the significance of the automated decision.

Generally, you should tell the person they have the right to human intervention if they wish to contest the automated decision, i.e. a human being at your company will review the matter to determine whether or not the automated decision was the correct one.

Conclusion

Whether or not your business has a legal obligation to obey the GDPR, from an economic standpoint the benefits of compliance likely outweigh the risk of being assessed a huge fine and spending a lot of time and money dealing with international legal proceedings. If nothing else, consider it part of providing support to potential and existing European customers who visit your website.

ABOUT THE AUTHOR

Mike Young is a Business & Technology Lawyer who helps clients prevent and solve business problems. The current president of the Internet Attorneys Association, Mike prepared the forms generated by Website Legal Forms Generator software.

Disclaimer

This special report is for general educational purposes only. It does not contain legal advice or create an attorney-client relationship between the reader and the report's author. Consult with an experienced business and technology attorney if you have legal questions.

PLEASE SHARE THIS SPECIAL REPORT WITH OTHER WEBSITE OWNERS

BUT DO NOT MODIFY IT IN ANY WAY.