



AiA Art News-service

artnet[®]

Worried About What GDPR Means for the Art World? Lawyers Answer 11 Questions About the Hair-Raising New Legislation

Art lawyers Thomas and Charles Danziger answer the most frequently asked questions about the EU's new privacy legislation.

Thomas Danziger & Charles Danziger, July 17, 2018



U.S. Air Force Staff Sgt. Jerome Duhan prepares for a command cyber readiness inspection. DoD photo by Senior Airman Franklin R. Ramos, U.S. Air Force/Released.

As art lawyers, we are no strangers to tricky legal issues. But the questions our clients have been raising lately about the new European data protection legislation—the General Data Protection Regulation (GDPR, for short)—have been harder than teaching calculus to a cat.

In an effort to keep things simple, we have put together answers to a few frequently asked questions from our art-world clients and others on this far-reaching new law.



The EU & GDPR. Image courtesy of Flickr.

1. What the heck is the GDPR?

The GDPR, which took effect on May 25, 2018, is a law that establishes expansive requirements for all European Union businesses and—significantly for our American clients—any business that processes the personal data of individuals in the EU in the course of providing goods and services or monitoring behavior that occurs in the EU.

2. I run an art gallery on Madison Avenue. Why should I care about the GDPR?

Because it applies to anyone who processes the personal data of EU residents, whether or not that person or business is physically located in the EU. If your gallery buys or sells art in the EU, you most likely need to comply with this law. And if you send out mass emails to EU residents or have financial information sent to you via email by EU clients, you most definitely need to comply with this law.

3. What personal data is covered under the GDPR?

The law applies to a broad range of data, from sensitive personal financial information (banking details, for example) to what many would consider less

sensitive information (an individual's name, email address, and IP address). It gives consumers enhanced rights to their own data, such as the right to access personal data that companies may have collected and stored, the right to delete personal data from the Internet (called, snappily, the "right to be forgotten"), and the right to correct inaccuracies in personal data.

The GDPR also raises the standard for consent to use personal data. This means that a business that intends to process an individual's personal data must be able to show that it has received permission from that individual. Gone are the days of pre-ticked checkboxes automatically signing you up for a newsletter or regular promotional emails.

Moreover, a business may only collect data for which it has a legitimate business purpose and may keep the data only for as long as is necessary to fulfill that purpose. That means you can't hold on to clients' information forever on the off chance that you might want to use it again in the future.

Lastly, the GDPR regulates the transfer of personal data from the EU to other countries, including those in the US, where data protection laws are less strict, and sets forth specific requirements for how companies must respond in the event of a data breach.



Visitors in front of Ron Terada's "TL; DR1," which addresses issues of cyber security. Photo by Harold Cunningham/Getty Images.

4. Our gallery only keeps the personal data of collectors who have bought art in the past and we don't use our customer lists for marketing or advertising. Do we need to take any action under the new law?

Yes—you need to keep records of exactly what kind of personal data (such as clients' names, credit card information, email addresses, etc.) you hold, and you need to be able to explain why you need the data to do your job and how long you have kept it. This is because the GDPR gives individuals a right to access, modify, and delete personal data whenever they wish.

5. If my client buys the work of an artist I represent, do I need that client's permission before I transfer any of his personal data to the artist?

Not surprisingly, the answer is yes.

6. I'm an artist and I sell only a few works directly to buyers. I'm exempt from this, right?

Wrong. The GDPR also applies to solo merchants, such as artists, not to mention larger companies and organizations. If you sell your art to an EU resident and collect or process the personal data of your buyers, the law applies to you.

7. We run a small auction house in France. Do we need consent when we collect personal data from bidders at a live auction as opposed to online auctions?

Bien sûr! The GDPR applies to any business that processes the personal data of EU residents when the business offers them goods or services. Although you might assume data protection is more important for an online business, there is no difference between a live auction and an online auction as far as the scope of the GDPR is concerned.

8. Our online auction house already has a terms and conditions page and a privacy policy that describe how we handle personal data. Is this sufficient?

Probably not. Again, not surprisingly, the GDPR establishes a high standard for consent and provides users with broad rights related to the collection and use of their personal data. If you intend to process personal data, you need to be able to show that you have received valid consent from your customers. Consent must be clear, unambiguous, and in plain language. It also must be spelled out separately from other terms and conditions. This means that your privacy policy probably needs to be updated to clarify the rights of your users.



Art galleries on Madison Avenue in New York City. Image courtesy of wikimedia commons.

9. What happens if I don't comply with the law?

The penalties are substantial. The maximum fine for significant breaches of the GDPR is either €20 million or four percent of the business's annual worldwide turnover from the preceding financial year, whichever is greater.

10. Those penalties sound horrible. What does compliance involve?

Unfortunately, compliance with the GDPR is not easy—or cheap.

For instance, you may need to enhance your existing consent forms and have your customers re-sign them to comply with the tougher requirements. You may also need to provide individuals with information about the reasons you collect and process their personal data, who would receive it if it were transferred, and how long you retain it. And if you are like many of our clients, you will probably need to enhance your cyber-security as well. The GDPR does not lay out a specific standard for data security, but it does require businesses to “ensure appropriate security of the personal data, including protection against unauthorized and unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures.”

11. What is the cost to comply?

Probably more than you would like to spend. Compliance may involve investing in both technology and training, including an upgrade of your IT infrastructure to strengthen your network or server security. The total cost will vary depending on the size of your business and whether you are currently in compliance with GDPR requirements—which means that understanding the rules of the GDPR is the first step. In any case, whatever you pay to comply may end up being just a fraction of the fine that you could face for violating the law.

In short, despite provisions like the “right to be forgotten,” the GDPR is one law you might actually want to remember. One thing is clear: This new legislation is already catnip for lawyers and IT professionals.

Nothing in this article is intended to provide specific legal advice. Thomas and Charles Danziger are partners in the New York firm Danziger, Danziger & Muro, LLP, which specializes in art law. Go to danziger.com for more information. The

authors gratefully acknowledge the assistance of Takuya Ishimura, Esq. and Danielle Gaier, Esq. in the preparation of this article.

