TerraTrue

The future of U.S. privacy:

3 things to learn from GDPR enforcement

TerraTrue

United States compliance law is entering a new phase, and businesses are rightfully nervous.

With new privacy laws going into effect in California, Colorado, Utah, Virginia, and Connecticut, companies are desperate to see how states will interpret and enforce the laws.

The CPRA is a particular source of uncertainty. The law gave the California Privacy Protection Agency extensive power over rulemaking and enforcement. However, the CPPA has faced multiple delays. At this point, it's unclear whether the rules will even be finalized, even though the law goes into effect on January 1, 2023.

On the federal level, things are just as hazy. After seven months of gridlock, Congress finally confirmed Alvaro Bedoya, breaking the FTC's 2-2 partisan split. FTC chair Lina Khan brought an ambitious agenda to the job, and recent actions show she is already pursuing antitrust and children's privacy measures, but how far the organization will be able to pursue its privacy agenda remains to be seen.

Fortunately, there are a wealth of lessons available already from European regulators.The GDPR has been in effect since 2018, and EU regulators have produced a wealth of compliance guidance. And while the details of the GDPR are different from U.S. laws, the basic concerns are the same, and underlying controls like DPIAs are very similar. Here are three lessons the GDPR can teach you about complying with U.S. privacy law.

TerraTrue

Make privacy controls straight-forward, accessible, and transparent

Both the U.S. and EU law require you to inform consumers about your data practices and give them significant control over what data you collect and how you use it. In both cases, that means disclosing what you're collecting, why you need it, and what you plan to do with it.

Your privacy UX should be as clear, accessible and transparent as possible so users can make informed decisions about their data. That also means avoiding so-called "dark patterns" — practices that are designed to manipulate users. The European Data Protection Board recently released a set of guidelines on "Dark patterns in social media platform interfaces," warning businesses to avoid misleading and deceptive methods to gain user consent.

According to the EDPB dark patterns include interfaces that:

- Overload users with too much information or too many options
- Skip privacy policies by misdirecting user attention
- Stir user emotions to encourage consent
- Hinder users from controlling their data by making the process difficult or impossible
- Use inconsistent design to make it hard to navigate privacy options, or;
- Leave users in the dark by hiding information or privacy controls

Multiple state laws and the FTC share the EDPB's concern over dark patterns, making them an important priority for your privacy and compliance program as a whole.

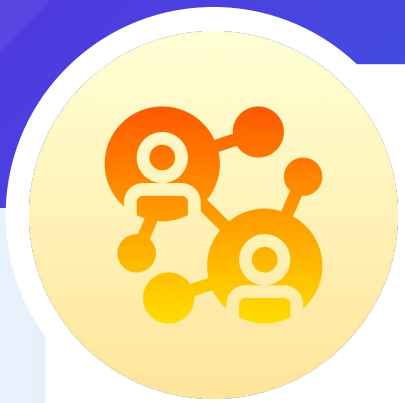
The easiest way to avoid dark patterns is to think like a consumer. If you were using your app's onboarding or privacy controls, how would you feel? Would it be easy to understand the company's data practices and control your own privacy? Or would you feel pressured, confused, or frustrated?

If you can build a good UX for your products and services, you can build a good UX for user privacy. With all the compliance challenges companies face, removing dark patterns should be an easy win for everyone.

TerraTrue

Be scrupulous about data mapping

The GDPR guarantees EU citizens certain privacy and security protections no matter where their data goes. If companies transfer data to another country or a third party, they need to be able to ensure that data is protected to the same standards. Companies must carefully account for where their data goes and, if necessary, put in place extra protections and/or process the data in a different location to ensure EU privacy rights are protected.



That means you have to be diligent about mapping your data flow and documenting your controls to comply with GDPR.

While U.S. laws don't have the same international data transfer rules, they do require you to secure your data against leaks and misuse. And unless you know where your data goes and what happens to it at every stage, you can't do that. So even though the legal rationale is different, the GDPR still serves as an outstanding model for US compliance.

In both cases, you should map out each stage of your data flow, including:

- Where the data is stored
- Who has access to it
- What protections are in place
- What risks the data faces in transit, during processing, and at rest

And in both cases, you should put in place extra controls if you can't ensure the data is adequately protected everywhere it goes. For more on this, see our recent webinar on DPIAs, GDPR compliance, and what you need to know to comply with U.S. state laws.

TerraTrue can help you stay on top of data protection and privacy compliance, wherever your data goes. We integrate DPIAs and other reviews into your development workflow, enabling you to verify, remediate, and document without bottlenecks. We also provide a complete window into your compliance operations, including a complete map of your data, and a repository of your DPIAs, onboarding, and privacy controls.

Not only does that help you meet all your compliance obligations; it also means that, if you do get audited, you'll be able to prove you've put in the work to protect your users.

Get a free demo, to learn just how much easier compliance can be.

TerraTrue

Understand when to implement a DPIA

There are differences between the GDPR and U.S. compliance requirements for data protection impact assessments (and between different state laws), but the underlying idea is the same: to protect consumers by documenting and mitigating any processes that could put their rights at risk.

The EU has extensive resources on DPIAs, including whitelists and blacklists with examples to show when you need a DPIA and when you don't. You can check out our blog for a breakdown of the whole DPIA process. But essentially, DPIAs are required any time data protection poses a significant risk to consumer privacy or data rights. That includes a range of use cases, from evaluating and scoring users (e.g. credit screenings) to innovative or new technology usage.

Several member states have also outlined when you don't need a DPIA. For example, if you're administering salaries for people who work for your company, or processing data exclusively for accounting purposes, the Belgium Privacy Commission does not require a DPIA. This guidance can help you focus your compliance efforts more effectively, without wasting resources on processes that don't require reviews.

About TerraTrue

TerraTrue empowers teams to build privacy and security into everything they do through a collaborative, intuitive, and scalable platform. Purpose-built to work with modern product development, TerraTrue seamlessly captures structured data about how teams plan to collect, use, store, and share data.

The platform then maps that digital blueprint to the world's privacy laws to automate guidance, risk-flagging, and downstream data maps and reports. Sitting as a hub between product teams and review teams, TerraTrue also smartly routes rule-based workflows throughout an organization, automatically detects and reports infrastructure changes in cloud environments, and drives vendor management — all from the same single source of truth.

Using TerraTrue, companies run a scalable, fast pre-deployment privacy program that eliminates spreadsheets, manual ad-hoc processes, and compliance bottlenecks.

Modern brands like Lyft, Robinhood, Roku, and Foursquare are shifting left to get privacy right.

TerraTrue

terratrue.com
#ShiftLeftPrivacy