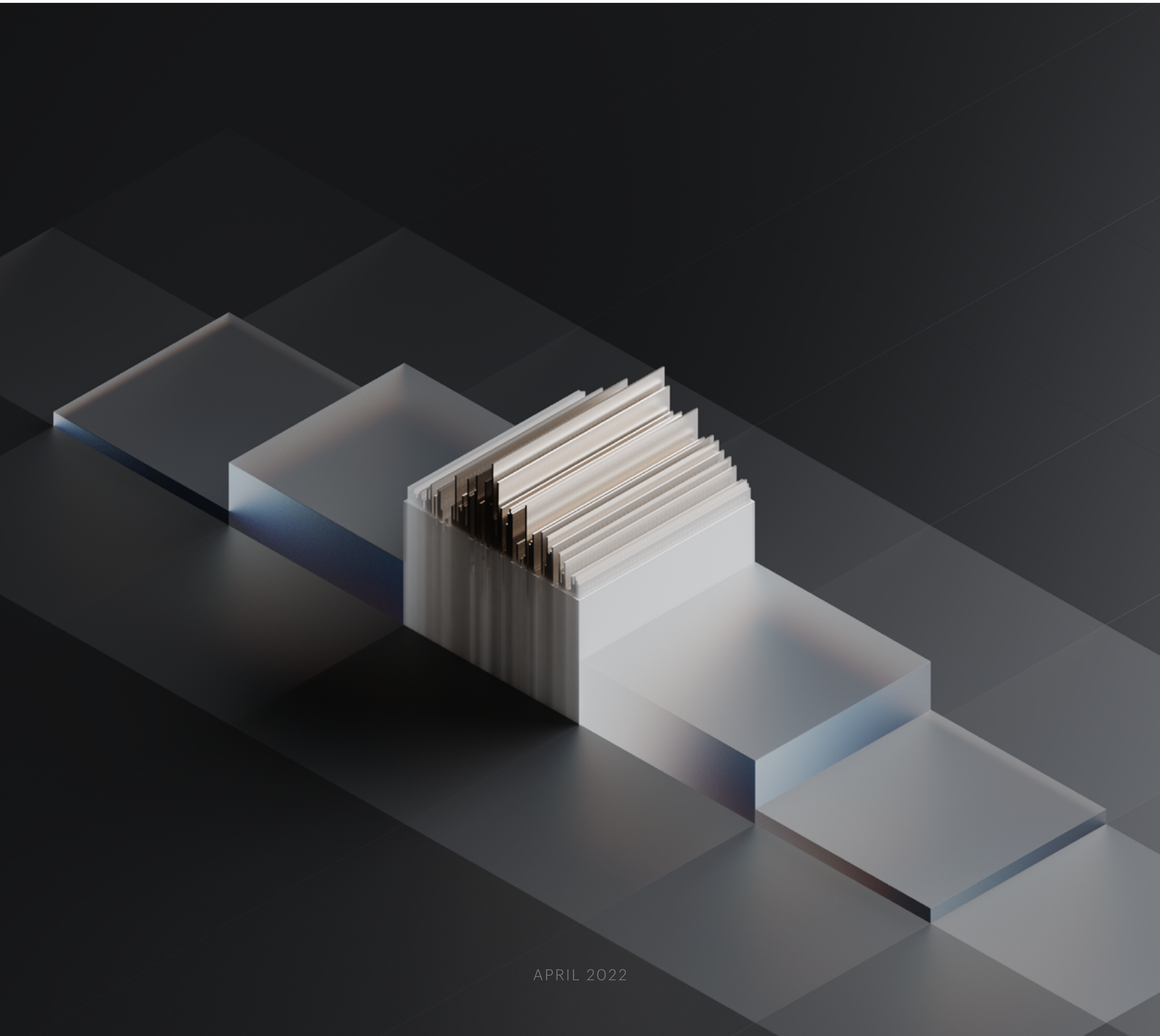
piano analytics

Putting Privacy First

Building a data analytics strategy that's compliant with EU privacy laws



APRIL 2022

Breaking down data privacy

The first real sign of change ahead came in December 2021.

That's when Datenschutzbehörde—the Austrian Data Protection Authority—ruled against medical news company NetDoktor. Its use of Google Analytics, the authority determined, was breaking the European Union's General Data Protection Regulation (GDPR).

Except NetDoktor wasn't using Google Analytics in any way that was unusual. Through the use of cookies, they tracked visitors across their website—getting a better understanding of which pages their customers went to, the amount of time they spent on site, and more. That data was linked to other data on the same user through an identification number, to get a fuller picture of each individual visitor. Companies everywhere use the tool in exactly the same way.

As if to prove exactly that, France's Commission Nationale de l'Informatique et des Libertés (CNIL) followed in February 2022 with a similar decision against a different company. Liechtenstein announced its own ruling in March 2022.

NetDoktor wasn't the problem, it was clear. Not exclusively, at least.

By allowing the transfer of European user data into the United States without appropriate guarantees, the data protection authorities all agreed, Google Analytics—and by association, every business that used it—was breaking the European Union's data privacy regulations. Rules against this type of data transfer claimed it could make European user data vulnerable to US law enforcement and spy agencies. But what does that even mean? And what are the repercussions to businesses employing digital analytics?

The far-reaching effects

For those who follow data privacy laws, the rulings happening across Europe didn't come as a complete surprise.

Just a year and a half prior, in July 2020, Privacy Shield—used by many to protect data as it moved between the European Union (EU) and the US—had itself been determined illegal by the Court of Justice of the European Union. When the rulings started coming down, no sound replacement had been agreed on yet. According to European officials, that left data insecure.

Now, any company using Google Analytics, is left at risk of noncompliance. And not just in France, Austria, and Liechtenstein, either. A ripple effect of decisions was predicted to follow.

"We expect similar decisions to now drop gradually in most EU member states," Max Schrems said in January 2022. Schrems is the Honorary Chair of noyb (None of Your Business), the data privacy advocacy group that initially brought the issue of data transfers to the European authorities. "We have filed 101 complaints in almost all Member States and the authorities coordinated the response."

And those rulings affect Google Analytics users not just in Europe, but worldwide, putting any tool or business that uses data in a similar way at risk of possible noncompliance.

"The GDPR applies to European companies as well as companies that deal with European data," explains Louis-Marie Guérif, Piano's Group Data Protection Officer and data specialist in France. "So more or less everyone that wants to play in Europe and with European data should respect the GDPR."

That means businesses everywhere are left with a choice.

What EU privacy rulings mean for business

For any business that depends on user data to fuel their decision making—in other words, most businesses today—the news from Europe has the potential for lasting effects. Even those that want to know something as simple as how many visitors come to their site or what pages are the most popular are affected. "This is an issue that touches all aspects of the economy, all aspects of social life," Gabriela Zanfir-Fortuna, Vice President of Global Privacy at the nonprofit think tank Future of Privacy Forum, told Wired in January.

How you respond, though, is up to you. You might continue using Google Analytics, knowing it's illegal—and hoping that Google will one day become compliant (though Google has shown no signs of movement on that so far). You could hope another version of Privacy Shield will be put into place—one that's strong enough to stand up to EU regulations this time. Or you can find another digital analytics solution that gives you the functionality you need while complying with European law.

Your answer will depend on your level of risk tolerance, Guérif says. "My recommendation and the expert recommendation is to evaluate your risk, and if you're convinced by what CNIL and other data agencies are saying, then evaluate alternatives and find ways to reduce the risk."

But evaluating your risk means understanding the possible impacts of noncompliance—which comes with the possibility of hefty fines and more. It could even mean losing access to the audience data you've already collected unlawfully.

This guide is for those still assessing their risk and looking to understand the consequences of noncompliance, as well as those considering alternative solutions to help minimize both. It examines what to consider if you're putting together a privacy-first digital analytics strategy, what to look for in a solution that prioritizes compliance, and how to migrate your data safely if you do decide to make the jump.

But let's look deeper at the privacy laws you should be considering first.

Understanding EU data privacy laws

The recent rulings show us that Europe's data privacy laws have the power to affect the way you use data. More stringent than US data privacy laws, they regulate how you collect, distribute, and store personal data from European users—whether you're based in Europe or not. So if you're employing a digital analytics tool, or plan to, it pays to understand them.

Two separate privacy policies affect data practices in Europe. Let's look at each in turn.

GDPR

The General Data Protection Regulation (GDPR) is part of the European Union's privacy law, and covers, among others, the transfer of personal data outside of the EU and the European Economic Area (EEA). That means data can't be exported to countries that don't have an "adequate level of protection"—in other words, the same level of data privacy legislation as the EU.

Put into effect in May 2018, it requires that businesses be transparent in their use of personal data, notifying users and customers on the data they collect, getting a proper legal basis to process this data, and letting them know if data has been breached. GDPR defines personal data as:

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Based on this definition, major data protection authorities therefore consider analytics, audience data as personal data and has to be treated as such. That means: transparency for the users about what is done with its data, right to object to the processing, or obligation to protect this data in a proper way, with potential measures as pseudonimization and anonymization.

ePrivacy

This is still yet a European directive that deals with eletronic communications and, among others, the use of so called trackers: cookie ID, mobile ID, pixels, fingerprint, etc.

According to ePrivacy, you cannot read or write information on an end user's terminal, in other terms track a visitor/user, unless you either receive prior and proper consent or have a specific exemption.

The European Commission's proposed a latest ePrivacy regulation draft that should update the ePrivacy directive, to get a fully harmonized view of data tracking, and confidentiality in electronic communications across Europe.

Far-reaching effects

GDPR and ePrivacy may be European legislation, but—as we've already seen—that doesn't mean they only affect businesses in the EU. The Internet, after all, is border-free. "When GDPR came into force, one of the immediate results was an increase in the number of US websites denying or restricting access to EU visitors," Timo Rein, co-founder and former CEO of CRM provider Pipedrive, told Forbes soon after GDPR was brought into effect. "[T]his approach isn't sustainable."

Today, then, basically any business with a website is affected by GDPR and ePrivacy—even if they only access the most basic of audience data.

The risk of noncompliance

Using data in a way that breaches ePrivacy or GDPR can have serious consequences. If you're found noncompliant, you risk a warning, significant fines of up to EUR 20 million or 4% of your worldwide turnover, and/or a temporary or permanent ban on processing personal data. You can also be forced to delete all of the data you've already collected unlawfully.

If those aren't risks you're willing to take, creating a thought-out data strategy and finding a digital analytics provider that understands GDPR and ePrivacy—with the expertise on hand to stay on top of legislative requirements—is critical.

Creating a strategy around data privacy

Most businesses today understand the importance of digital analytics. By analyzing user behavior, you can make better business choices based on your audience needs and create better user experiences. To accomplish that, you require quality data. But if you also want to dodge future landmines, maintain user trust, and continue successfully navigating the regulatory landscape, you need a long-term strategy around data privacy—whatever that might look like.

"As a business, discuss with your data protection and legal teams, and all the teams in your company that deal with data," Guérif suggests. "Don't just make a quick decision that you will pay for potentially six months or 12 months down the line. Privacy is a risk approach—you should balance the risk of getting fined, of losing data, or of not being able to use your data."

Choosing to prioritize compliance in the long run, though, means knowing what to look for as you search for a digital analytics solution to help.

Knowing the hidden costs of free

Despite the important role digital analytics plays, many businesses still prioritize cost savings over functionality when choosing a solution. But there are hidden costs to free tools that we're seeing play out in Europe right now. Costs that can impact user privacy.

To understand those costs, let's break down the two types of free digital analytics solutions available today.

Open Source and On-Premise
Open source, on-premise digital analytics solutions are the less common of the free alternatives. And for good reason—they don't offer the same complex user data modern businesses search for. But more than that, they make you responsible for your own security and privacy updates.

That means it's your job to keep up with GDPR and ePrivacy, as well as any changes in the data privacy landscape—and your job to update your usage if you want to comply. If you don't have the resources or know-how to keep up, you risk noncompliance.

Paying the price with data
The more common free solutions, of course, are those like Google Analytics. They offer more advanced audience data, but that comes with a caveat. "The problem when it's free is that you are the product—you, as in the user," Guérif says.

The customer data you collect is the price of entry and may be used in ways outside of your control, for user profiling and digital advertising—all without user consent. It can also be difficult for end users to opt out of data tracking and take control over how their data is utilized. What's more, providers of free solutions don't often have dedicated resources and support available to ensure you're aligned with regulatory requirements like those outlined in GDPR and ePrivacy.

"It's normal for smaller solutions or free solutions to not have experts available to talk to, to help you configure your solution in a compliant way," Guérif says. "You're more or less alone with your free tool."

Finding a privacy-first analytics solution

If free isn't your first priority, though, you can seek out a tool that has all of the functionality and data types you require. And you can choose to put data privacy at the top of your list.

When searching for a privacy-first digital analytics solution, start by considering the following

How "personal data" is defined

Remember how GDPR defines "personal data"? If you want a solution that will remain compliant, you need a provider that employs the same definition—including cookie/mobile IDs and IP addresses as personal data, for example. If the tool doesn't designate personal data in the same way, it risks becoming noncompliant.

How data is used and stored

The rulings happening across Europe have revolved largely around where data is stored and how it's being used. To adhere to GDPR, then, the private data of European users must stay in Europe or countries with the same level of data protection. Also important to look for: whether audience, navigation, and behavior data is pseudonymized, and/or anonymized, and encrypted.

Consent exemption

ePrivacy consent exemption is recognized by data protection agencies such as the CNIL. It allows a website or mobile application publisher to bypass the need to obtain prior consent from a consumer before depositing trackers (cookies/mobile ID). Consent exemption is only granted to solutions that maintain a high standard of privacy compliance and meet several conditions, including

- General compliance with the GDPR
- Collection of data that's only strictly necessary for the provision of the service requested by the user
- A purpose limited to the strict measurement of the audience

As well as ensuring stricter privacy, consent exemption can also be a sign of better quality data. A solution that meets ePrivacy exemption policies can collect 100% of audience data, as opposed to those that don't, which will only be able to access approximately 50% of the same data.

In-house expertise

GDPR and ePrivacy legislations are nuanced and the way we use data is ever-changing, meaning there's always the possibility that new precedence will be set or that widely used tools like Privacy Shield (or whatever replaces it) will no longer be considered legal. That's why a privacy-first solution needs to have GDPR and ePrivacy experts on their team, and experience guiding companies through their data privacy needs. Look for customer support as well as data and legal expertise to ensure your provider can keep up with new data privacy legislation and help you stay up to date.

Putting data privacy first

Prioritizing privacy over cost savings means you'll be confident that your provider remains on top of regulatory changes, and that you won't find yourself caught in the middle of decisions like those happening across Europe in 2022.

But moving to any new solution means migrating your data—a step that can make that data vulnerable if you don't take the right approach. So how do you do that safely while respecting your customers' privacy needs?

Migrating to a new digital analytics solution

Once you've made the decision to migrate to a new digital analytics solution, what comes next? What does it really take to implement a new solution within your organization? Implementing a new tool quickly without compromising your users' data means following a proven process.

These four steps can help

1. Data Modeling, Tagging, and Documentation

With your identified business needs in mind—as well as the reporting, site structure, data pipeline, and events taxonomy you already have in place—figure out the data model that will best serve your organization. A flexible model will allow you to make the necessary adjustments as your needs and requirements evolve over time. Involving both technical experts and business users in your analytics conversation will also help you get a holistic view of what you're looking for and how analytics and insights are used across your entire organization.

Based on the data model you decide on, create a tagging plan to identify all of the elements you need to achieve your metrics. And to get up and running quickly, consider an incremental tagging plan. Standard events like page views and clicks can be implemented in a few hours and start feeding reports, while more detailed tagging can be added along the way as your analysis needs become more sophisticated. Analytics should never be a "set it and forget it" process anyway, so this approach will allow you to unlock immediate value, then continue to build on your foundation over time.

When you have your data model and tagging in place, be sure your documentation includes business-user friendly descriptions of each metric, explaining what information a specific piece of data carries.

2. Implementation

One of the most critical components of your implementation will be connecting your previous resources—metrics, taxonomies, etc.—to your new system. This will help create a seamless transition for your end users by providing them with the same level of understanding of your new system that they had of your legacy system. To achieve that, keep a few things in mind:

- Choosing a Tag Management System (TMS) that's integrated with your analytics tool will allow you to leverage your existing data layer wherever possible, easing the transition. Without a TMS, you'll likely need additional support from technical teams, which could slow down your process.
- Switching every tool at once can create confusion among teams and impact the continuity of your reporting. If you're already using business intelligence tools, choosing an analytics solution that's integrated with those platforms will make your life easier. These integrations will help you get up and running more quickly by feeding data from the new system into existing reports, dashboards, and visualizations that serve the needs of your teams.
- Regardless of the BI tools you use, also consider any reporting that's native to your previous analytics tool and needs to be replaced. Choosing a new tool with strong out-of-the-box reporting and data visualization capabilities will allow you to get up and running immediately, without spending precious time building and customizing new interfaces.

If your new analytics provider has onboarding or implementation consultants, these resources will also be invaluable to you at this stage in ensuring your implementation remains regulatory compliant.

3. Quality assurance and auditing

You want to follow implementation with a series of checks to ensure tags are implemented correctly and data appears within the platform as expected. Consider this a safety valve that will ensure your data isn't leaking.

Most implementation projects will include a period of overlap, where you have access to analytics on both your legacy and new solution. Use that stage to test what should be identical datasets against each other in each solution, to understand how they compare and whether your delivery is correctly in place, and to identify any issues you need to address.

Depending on the systems you're switching between, you may have expected discrepancies between your datasets, but your new provider should be able to help you predict what that might look like.

4. Training and onboarding

With everyone from web analysts and product managers, to marketing teams, sales reps, and company managers utilizing your digital analytics tool, training is an integral step. Everyone using the platform should understand how it works and have access to the metrics they need to make decisions.

This is where your documentation comes in as well. If you can embed your definitions in a centrally managed data model, it will help your team understand what they're looking at, in a language that makes sense to them.

Building analytics into your day to day

Once it's up and running, digital analytics can become a daily activity as you develop the specific reports, dashboards, and visualizations that will serve the needs of your business users. Your analytics provider—as well as any outside experts or consultants you employ—should be able to help you stay up to date with new developments and opportunities, to ensure you continue to get the most out of your data while also staying in line with regulatory needs.

How Piano Analytics can help

Piano Analytics (formerly AT Internet's Analytics Suite Delta) is a digital analytics solution that offers functionality across a range of use cases, with a unified data model that supports real-time queries and 1,400 event parameters. And at Piano, the privacy and security of user data is one of our highest priorities, with measures in place that ensure user data remains private and that data privacy laws are maintained at all times.

Strict Compliance with GDPR and ePrivacy

Piano Analytics complies with the legal requirements set forth by the GDPR and ePrivacy. We use a US-IaaS/Cloud provider that follows the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE), and that is approved by the CNIL and the European Data Protection Board.

Strong Policies on Data Usage

We only collect data strictly necessary for the provision of the service defined by our customers and expressly requested by the end-user. The purpose is limited to the strict measurement of your audience and data is always 100% owned by our customers.

Consent Exemption

Piano Analytics has a consent exemption that is officially recognized by the CNIL allowing a publisher of a website, a mobile application, or any connected platform to not expressly obtain prior consent from the end-user/ consumer before using a tracker (depositing cookie/mobile iD, etc.).

In-House Data Expertise

Piano has a long history of helping businesses navigate and adhere to evolving data privacy regulations. We are experts in GDPR and ePrivacy and have extensive experience guiding companies through privacy regulations worldwide. Our team of consultants and privacy experts accompany clients throughout the process of implementing the ePrivacy consent exemption and putting their data into action.

Conflict-Free Data

We never use, sell, or transfer data, or engage in any activity that would otherwise breach GDPR or local regulations. The standard and unique purpose of our solution is to collect, process, and store pseudonymized audience, navigation, and behavior data on behalf of our customers. We also have additional technical measures in place like anonymization or encryption.

Trusted Across Europe

Piano is certified as an approved European data provider by audience measurement, data, and research agencies across the continent, including the Alliance pour les chiffres de la presse et des médias (ACPM) and Médiamétrie in France, the UK's Audit Bureau of Circulation (ABC), and Stichting KijkOnderzoek (SKO) in the Netherlands.

Putting Privacy First

With Piano Analytics, you get the benefit of an advanced analytics platform that allows you to share high-quality data across teams, easily query large volumes of data, and customize your measurement strategy to meet your business needs. All with the peace of mind that comes with a privacy-first digital analytics solution.

Data is integral to modern business, and your digital analytics strategy is critical to meeting your audience needs. But the current data privacy landscape is more difficult to navigate than ever before—and the digital analytics tool you choose to use can make the difference between compliance and noncompliance with regulations like the GDPR and ePrivacy.

The question is: How much risk are you willing to take on? And are you willing to face the high consequences of noncompliance?

By choosing a digital analytics solution that puts privacy first, and migrating your data safely, you can continue to make audience data a part of your daily decision-making process—all while mitigating your risk and remaining compliant with ever-evolving data privacy laws.

And with our proven expertise, Piano Analytics can help you achieve that.