GDPR Compliance for US Companies: What You Need to Know

By Craig Besnoy

Craig Besnoy is a Partner at Dunlap Bennett & Ludwig, where he advises on cybersecurity, data privacy, and regulatory compliance with a core focus on mergers, acquisitions, and strategic transactions involving data-driven and highly regulated businesses. He works extensively with healthcare organizations, financial services firms, technology companies, and investors on cybersecurity risk management, HIPAA compliance, incident response, and third-party risk oversight.

Craig has more than a decade of experience advising on complex transactions and compliance matters in which data security and privacy risk are material considerations, including acquisitions, restructurings, and growth-stage investments. His experience includes helping physician-owned practices achieve HIPAA compliance and training physicians and staff on privacy and security best practices as part of pre-acquisition readiness efforts. He is admitted to practice in New York and is recognized for translating evolving cybersecurity and privacy regulations into operationally practical and legally defensible frameworks.

DUNLAP BENNETT & LUDWIG

Every US company collecting customer data now faces a clear choice: treat privacy as a core part of its business operations or risk regulatory action and customer distrust. Privacy compliance for US companies begins with understanding state laws, such as California's CCPA/CPRA, which affect a far greater number of businesses than most realize. It also extends to international requirements, including the EU's General Data Protection Regulation (GDPR), when you have actual operations abroad.

The reality is straightforward. If you conduct business in California, process data from Colorado, Virginia, Connecticut, or any of the growing list of states with comprehensive privacy laws, you're already subject to detailed privacy regulations. These aren't theoretical concerns—state attorneys general are actively investigating and settling cases against companies that ignore consumer privacy rights.

Additionally, every US company with subsidiaries, offices, or assets in the European Union is subject to the full force of GDPR enforcement. For these businesses, privacy and data governance are not merely good practice—they are regulatory obligations with real, legally enforceable risks. If a US parent or its EU affiliate collects, stores, or processes personal data of EU residents, non-compliance opens the door to direct fines, enforcement orders, and potential disruption of business operations across European markets. Recent GDPR enforcement actions have overwhelmingly targeted multinational US brands with established EU subsidiaries or assets—because regulators can compel compliance and payment. If your company has staff, facilities, data centers, or a legal presence anywhere in the EU, GDPR is no longer theoretical; it is a day-to-day compliance imperative that impacts every customer touchpoint and enterprise system.

Why this matters goes beyond avoiding enforcement. Customers judge companies by how they handle personal information. Over the past decade, clear privacy notices, quick responses to data requests, and strong security have become baseline expectations. Companies that build privacy into operations tend to move faster on product development because they know what data they need, why they need it, and how long they can keep it. Less guesswork. Fewer surprises.

A quick, true-to-life scene helps. A mid-sized SaaS firm in Texas opens a free trial to the EU and adds a German language page with euro pricing. Marketing tags track behavior to score leads. A month later a request lands in the inbox. Please delete all my data. The team scrambles. The better scene is different. A clear intake path. A verified identity check. A one-month clock that is met with room to spare. That second scene is what this guide builds.

GDPR Scope: Who's Actually Covered and What's Your Real Exposure?

GDPR applies when you're either (1) offering goods or services **to** data subjects in the EU/EEA or UK, or (2) monitoring behavior **in** those regions. Note that UK GDPR is separate post-Brexit but follows similar rules. Location of your business doesn't matter—it's about targeting EU/EEA/UK markets or tracking people while they're in those jurisdictions.

Understanding Your Business Exposure

Most US companies we work with don't know their actual GDPR exposure until they conduct a structured assessment. The key factors that determine your risk profile include:

EU customer volume and data flows: How many EU/EEA/UK data subjects are in your systems? Are you processing hundreds or hundreds of thousands of records?

Data sensitivity and categories: Are you handling basic contact information or special-category data (health, biometric, financial)?

Vendor and third-party contracts: Which of your service providers access or process EU/EEA/UK personal data? Do your contracts create additional compliance obligations?

Revenue exposure: What percentage of your revenue comes from EU/EEA/UK markets, either directly or through vendors who serve those markets?

Physical and digital footprint: Do you have EU subsidiaries, offices, employees, payment processors, or hosting infrastructure in covered regions?

These exposure factors aren't just theoretical considerations—they directly impact both your enforcement risk and your compliance strategy.

The Enforcement Reality: What Can Regulators Actually Do to US Companies?

For companies with no EU presence, EU regulators face significant practical limitations. The European Commission and national Data Protection Authorities cannot directly enforce judgments or collect fines from purely US-based companies without physical assets, subsidiaries, or operations in the EU. Without an EU establishment, enforcement largely depends on voluntary compliance, the risk of reputational damage, or commercial consequences, such as the blocking of services within the EU.

However, companies with EU subsidiaries, offices, bank accounts, or other tangible assets face direct enforcement exposure. Regulators can—and do—compel compliance, levy fines, and issue binding orders against these entities. Recent high-profile GDPR cases have overwhelmingly targeted US companies with established EU footprints precisely because enforcement is both feasible and effective.

For companies without an EU presence, EU regulators typically require the appointment of an EU-based representative to act as a liaison for GDPR compliance and enforcement. But even with a representative, actual enforcement mechanisms remain limited without assets in the jurisdiction.

Privacy Impact Assessment: The Tool That Quantifies Your Exposure

This is where a **Privacy Impact Assessment (PIA)** becomes invaluable. A PIA is a structured, documented process that:

1	2
Quantifies your actual GDPR exposure by mapping data flows, customer volumes, vendor relationships, and business operations	**Identifies specific compliance gaps between your current practices and GDPR requirements**
3	**4**
Provides defensible documentation of your risk analysis and compliance decisions	**Guides strategic decisions about whether to pursue full compliance, partial compliance, or documented non-compliance based on evidence**

Critically, a PIA creates defensible evidence even if your company concludes that GDPR does not apply or that enforcement risk is minimal. If you later receive an enforcement inquiry, regulatory complaint, or customer challenge, the PIA demonstrates that you conducted a good-faith analysis and made informed business decisions—not that you simply ignored the issue.

For companies uncertain about their GDPR obligations, a PIA offers clarity. For companies that know they're covered but need to prioritize resources, a PIA identifies the highest-impact compliance steps. For companies concluding they have minimal exposure, a PIA documents that judgment in a way that protects the business if circumstances change.

The Reality Check: It's Probably Too Late to Avoid GDPR

Here's the straight answer: if you're collecting any data from people who might be in the EU/EEA or UK—through your website, mobile app, or marketing campaigns—you're likely already subject to GDPR (and UK GDPR separately). The law doesn't care where your business is incorporated or where your servers live. It cares about whose data you're processing and where they are when you process it.

The triggers are broader than most US business owners realize:

- Website traffic from EU/EEA/UK countries (even if you didn't target them)
- Email marketing to prospects with EU/EEA/UK addresses
- Mobile apps downloaded by people traveling in Europe or the UK
- Cloud storage or analytics that process EU/EEA/UK user data
- Employee data, if you have any staff working in covered regions

Most US companies we work with qualify on multiple grounds. The question isn't whether GDPR applies—it's how to comply without breaking your budget or derailing your product roadmap

What You're Looking At: Cost and Timeline Reality

Budget 6-12 months and **$50,000-$200,000 to get genuinely compliant**, not just paperwork compliant. These are planning ranges—actual costs depend on industry, system complexity, whether you handle special-category data, and B2C scale.

But here's the key insight for budget-conscious executives: you don't need to commit to a full compliance program on day one.

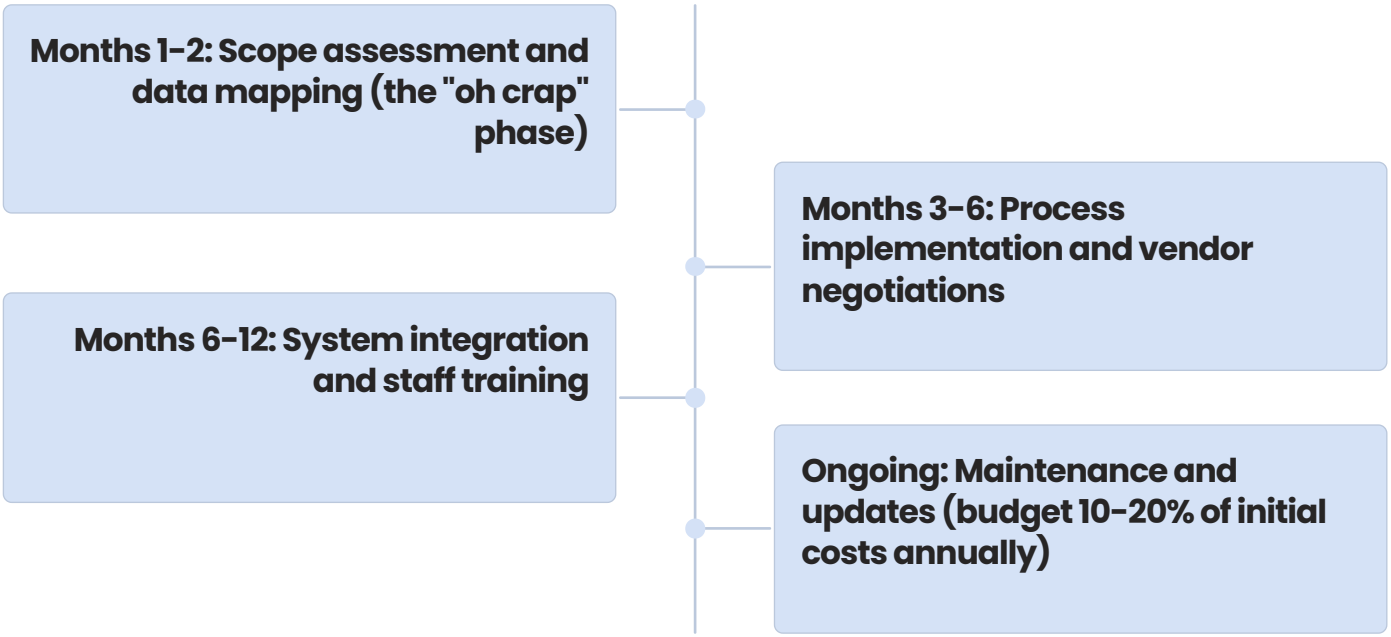
A Privacy Impact Assessment costs $15,000-$75,000 depending on company size, data complexity, and vendor ecosystem—far less than full compliance implementation. For many companies, a PIA is the smartest first step because it:

- **Clarifies whether full compliance is actually necessary** based on your specific business exposure
- **Identifies the highest-priority gaps** so you can focus limited resources on what matters most
- **Provides a roadmap** for phased implementation rather than an all-at-once commitment
- **Creates documentation** that protects your business even if you decide not to pursue full compliance

This creates a **low-barrier entry point** that gives leadership the information they need to make strategic decisions about privacy investment. You're not committing $200K blind—you're investing $15K-$75K to understand exactly what you're facing and what your options are.

We've seen startups handle basic compliance for under $25,000 by making smart technology choices early. We've also watched mid-size companies spend $300,000+ fixing problems they created by ignoring GDPR for too long.

The pattern we see most often:



DPA case backlogs for privacy enforcement haven't improved since COVID either. Cases are taking 18-24 months to resolve, which means uncertainty drags on longer than anyone wants.

How a Privacy Impact Assessment Guides Your GDPR Decision

A well-executed PIA helps you decide between three distinct paths:

> **1. Full GDPR Compliance Program**
>
> Right for companies with significant EU revenue, large EU customer bases, EU subsidiaries or assets, or high-sensitivity data processing. You implement comprehensive controls, processes, and documentation across all ten core GDPR requirements.
>
> **2. Targeted Partial Compliance**
>
> Right for companies with limited EU exposure or specific high-risk processing activities. You implement core protections (data subject rights, security, vendor agreements) while documenting why certain requirements don't apply to your business model.
>
> **3. Documented Non-Compliance with Defensible Evidence**
>
> Right for companies with minimal EU presence, no EU assets, and low enforcement risk. You document your risk analysis, implement basic data protection practices, and maintain evidence of your business judgment—but don't pursue full GDPR compliance.

The PIA provides the factual foundation for choosing the right path. It's not a legal opinion—it's a systematic analysis of your actual business operations, data flows, and risk exposure that enables informed decision-making.

The Ten Things That Actually Matter

Most GDPR guides give you fifty requirements. We've learned to focus clients on the ten that actually drive enforcement actions and customer complaints.

1. Figure Out If You're Actually Subject to GDPR (Spoiler: You Probably Are)

Start with traffic analysis. Pull your website and app analytics for the past year. How many sessions came from EU/EEA/UK countries? Even small percentages add up—we had a client discover they were processing 15,000 EU user sessions monthly from a website they thought was "purely domestic."

Check your marketing signals: Euro/pound pricing, European/UK shipping options, ads targeted at EU/EEA/UK cities, website translations into European languages. Any of these can establish intent to target those markets.

The monitoring test trips up more companies: if you're running behavioral ads, cross-device tracking, or location services that profile users while they're in covered regions, you're subject to GDPR regardless of targeting.

Don't forget the representatives. If you're subject to GDPR without an EU establishment, you likely need an EU representative under Article 27. Same for UK GDPR—you'll need a separate UK representative. These are frequently overlooked but often enforced requirements.

We always tell clients to document the analysis either way. If you conclude GDPR doesn't apply, keep the evidence. If it does apply, that's your starting point for everything else. **This is exactly what a Privacy Impact Assessment provides**—structured, defensible documentation of your applicability analysis.

2. Map Your Data and Create Records of Processing

This is where most of your initial budget goes, and it's the foundation everything else builds on. You can't protect data you can't find, and you can't delete data you don't know exists.

Records of Processing (ROPA) are mandatory under Article 30 for most organizations that aren't micro-enterprises. This isn't optional documentation—it's the backbone for audits and fulfilling data subject requests.

We typically see three categories of data that companies miss:

01

Log files that store IP addresses, device IDs, and session data

02

Third-party integrations that copy data behind the scenes

03

Employee systems that process EU/EEA/UK staff or customer data

3. Pick Legal Bases That Actually Make Sense

GDPR provides six legal bases for processing personal data. The right choice depends on what you're doing:

Product functionality → Contract performance or legitimate interests

Analytics and behavioral ads → Often consent (especially for ads) or legitimate interests with a documented assessment and opt-out

Security and fraud prevention → Legitimate interests

HR data → Legal obligation or contract performance

Marketing to new prospects → Usually consent

Consent isn't always riskiest, but it comes with strict requirements: you have to get it before processing starts, prove it was freely given, and honor withdrawal instantly. For non-essential cookies and advertising, consent is often required under the ePrivacy rules, which are layered on top of the GDPR.

When relying on legitimate interests, run a documented balancing test that weighs your business needs against people's reasonable expectations. Keep this assessment with your records.

4. Build a Data Subject Rights Process That Actually Works

EU/EEA/UK residents can request access, deletion, portability, and corrections of their data. They can also object to processing or ask you to restrict it. You have **one month** to respond to most requests, with a possible **two-month extension** for complex requests (but you must notify them of the extension within the first month).

The verification process trips up a lot of companies. You need to confirm identity without collecting more personal data than necessary. We've seen companies create new privacy problems by demanding passport copies to verify deletion requests.

Build templates for common scenarios and train those who handle the inbox. The person responding needs to understand both the technical systems and the legal requirements. Customer service reps who don't know the difference between anonymization and deletion cause expensive problems.

Track request volumes and response times. Patterns often reveal bigger issues—if you're getting lots of deletion requests from marketing subscribers, your unsubscribe process probably isn't working properly.

5. Handle Special Categories and Children's Data Carefully

Special-category data (health, biometric, religious views, etc.) and children's data require extra care. For children, the **age of digital consent varies from 13-16** across EU member states, so know your target markets.

These data types often require explicit consent, have stricter security requirements, and face higher penalties for breaches. Document your assessment of whether you process these categories and what additional protections you've implemented.

6. Assign Privacy Responsibilities (DPO vs Privacy Lead)

A **Data Protection Officer is legally required** when you conduct large-scale systematic monitoring, process special-category data on a large scale, or you're a public authority. For everyone else, appoint a named privacy lead with clear responsibilities.

Don't underestimate this role—they need to understand both technical systems and legal requirements, have authority to escalate issues, and stay current on regulatory guidance.

7. Write Privacy Notices People Can Actually Understand

Your privacy notice should explain what information you collect, why you need it, who has access to it, and how long you retain it. In plain English, not legal boilerplate.

The notice needs to match reality. We've seen enforcement cases where companies claimed they only kept data for "legitimate business purposes," but actually stored everything indefinitely because nobody had established deletion procedures.

Make the notice accessible to EU/EEA/UK visitors specifically. Geo-aware banners work better than hoping people find the link in your footer. If you're targeting specific countries, translate the key sections.

Handle cookies properly. Essential cookies (login, security, shopping cart) don't need consent. Non-essential cookies (analytics, advertising, social media) typically fall under ePrivacy rules. Make the distinction clear in your cookie banner.

8. Build Privacy by Design Into Development

Article 25 requires privacy by design and by default. Connect this to concrete development practices: data minimization (collect only what you need), purpose limitation (use data only for stated purposes), and retention by design (automatic deletion when purposes expire).

This is where the "ship faster" benefit becomes real. When privacy requirements are baked into your software development lifecycle, you avoid the scramble of retrofitting compliance later.

9. Security Controls That Match Your Risk Profile

GDPR requires "appropriate technical and organizational measures" but doesn't specify exactly what that means. The answer depends on the type of data you process and its sensitivity.

Start with the basics: encryption at rest and in transit, multi-factor authentication for administrative access, access controls based on business need, and audit logging for systems that store personal data.

Document your risk assessment and control selection. When regulators investigate security incidents, they want to see evidence that you made thoughtful choices based on actual risk, not just implemented random security measures.

Test your controls regularly and fix findings promptly. The best documented security program won't help if you ignore vulnerability scans or patch management.

10. Get Your Vendors Under Control

Most US companies rely on cloud providers, marketing platforms, analytics services, and other vendors that process EU/EEA/UK data on their behalf. Each one needs a data processing agreement that includes specific instructions, security requirements, and breach notification procedures.

Don't just sign vendor templates. Make sure the terms actually cover your use case and data flows. We've seen companies discover their CRM vendor didn't support data deletion requests, or their email platform was storing data in countries not covered by transfer agreements.

For international transfers: Standard Contractual Clauses require **Transfer Impact Assessments** to evaluate government access risks. The EU-US Data Privacy Framework offers another path for certified importers. For UK transfers, use the **International Data Transfer Addendum** or UK-specific agreements.

Plan for vendor changes. Services get acquired, data locations shift, and security practices evolve. Review key vendor relationships annually and when services change significantly.

Conduct Impact Assessments for High-Risk Processing

Data Protection Impact Assessments (DPIAs) are required for processing that poses high risk to individual rights. That includes large-scale profiling, sensitive data processing, location tracking, and automated decision-making with legal effects.

The assessment should describe the processing in business terms, identify specific risks to people, and document concrete mitigations. Generic risk registers don't satisfy the requirement.

Involve technical teams early. The lawyers can identify legal requirements, but engineers know whether proposed mitigations are actually feasible within your systems and budget.

Prepare for Data Breaches

GDPR requires notification to authorities within 72 hours of becoming aware of breaches that pose risk to individual rights. Individual notifications are required for high-risk breaches.

Develop an incident response plan that outlines clear roles, escalation procedures, evidence preservation protocols, and communication templates. Practice with tabletop exercises so the team knows what to do under pressure.

The 72-hour clock starts when you become aware of the breach, not when you complete your investigation. Initial notifications can include basic facts with more details to follow, but you can't wait until you have complete information.

Document decision-making throughout the process. Data Protection Authorities review incident response timelines and require evidence of appropriate urgency and care.

When You Need Legal Help Right Away

Some GDPR situations require immediate attention:

- **You get a formal complaint or regulatory inquiry from a DPA**
- **A major vendor changes data processing locations or practices**
- **You discover significant gaps in data deletion or security procedures**
- **You're planning European expansion or major system changes**
- **A data breach affects EU/EEA/UK personal data**

The earlier you involve experienced counsel, the more options you typically have. We've seen disputes that could have been resolved with process improvements turn into formal enforcement actions when companies waited too long to get help.

Making GDPR Manageable for Your Business

Look, GDPR compliance takes longer than you want, costs more than you budgeted, and you'll never have perfect certainty about every edge case. But it's manageable if you treat it like any other operational risk rather than a legal mystery.

The advantage of working with attorneys who understand both privacy law and business operations is that we can help you make smart tradeoffs. There's no point building gold-plated consent management if your real problem is vendor oversight. There's no benefit to perfect data mapping if you can't actually respond to deletion requests.

We focus on practical outcomes based on what we've seen in hundreds of similar cases. Can you respond to subject access requests reliably? Do you know where EU/EEA/UK data lives in your systems? Can you stop processing when someone objects? Get those fundamentals right, and you're ahead of most companies still arguing about whether they're "really" subject to GDPR.

After handling these matters for years, we've learned that realistic assessments beat wishful thinking every time. Every hour your team spends scrambling to respond to privacy complaints is an hour not spent on revenue-generating activities. Every dollar spent on emergency compliance could have gone toward business growth if you'd planned ahead.

Start with a Privacy Impact Assessment

If you're facing GDPR uncertainty, **don't start with a $200K compliance program**. Start with a Privacy Impact Assessment.

A PIA gives you:

- **Clear answers** about your actual GDPR exposure based on your specific business operations
- **Documented evidence** of your risk analysis and compliance decisions
- **A practical roadmap** showing exactly which steps matter most for your business
- **Defensible documentation** if you face regulatory inquiries or customer complaints
- **Strategic options** to pursue full compliance, targeted compliance, or documented non-compliance

For $15K-$75K depending on your company's complexity, you get clarity on a $50K-$200K decision. That's the kind of return on investment that makes sense for executives managing limited budgets and competing priorities.

We've helped dozens of US companies navigate this exact question. Some move forward with full GDPR programs. Some implement targeted controls for specific high-risk areas. Some document their minimal exposure and focus resources elsewhere. But they all make those decisions with clear evidence rather than guesswork.

Ready to understand your actual GDPR exposure? Let's start with a Privacy Impact Assessment. We'll analyze your business operations, data flows, and vendor relationships to give you clear answers and practical options—not generic compliance advice.

Dunlap Bennett & Ludwig is a veteran-owned law firm with offices across multiple states. Our privacy and business attorneys combine legal expertise with practical operational experience to help companies navigate GDPR compliance while maintaining focus on their core business objectives.

To learn more about Dunlap Bennett & Ludwig, call **888-306-4030** or email **clientservices@dbllawyers.com**.

Please note: *This article is for informational purposes only and does not constitute legal advice. The legal process is complex and highly dependent on the specific facts of your case. For guidance on your unique situation, we invite you to schedule a confidential consultation with our experienced legal team.*