vinciworks

What to expect from AI & GDPR in 2025

What to expect from AI & GDPR in 2025

Not surprisingly, the intersection of the General Data Protection Regulation (GDPR) and artificial intelligence (AI) is going to be a key focus for compliance in 2025. As AI gets increasingly sophisticated - leaving massive amounts of data in its wake - it is also becoming embedded in nearly everything we do (we see you ChatGPT), putting regulators under increasing pressure to control this technology while keeping pace with its advances.

AI's growing reliance on personal data is raising concerns about transparency, consent and the potential for bias in automated decisions. This is the year companies are going to have to navigate the challenge of ensuring their AI systems and their data comply with GDPR's data protection requirements, data protection laws around the world, including the UK, and the EU's AI Act. There is even **talk of potential updates** to the GDPR to address these new challenges. It's clear that 2025 is the year in which data privacy meets innovation.

The question is who will win?

Get ready.
A new UK data bill is coming

Reforming data laws has been bandied about in the UK government for a while now. After the Data Protection and Digital Information Bill (DPDI Bill) didn't make it through Parliament before the last election, the King's Speech made it clear that the new Labour government would propose a new Digital Information and Smart Data Bill (the DISDB), to resurrect some of the features of the bill that didn't pass.

As promised, a new bill was introduced although it was renamed (again). This time it's called the Data (Use and Access) Bill, and it is anticipated that this one will go through the legislative process fairly smoothly this coming year, although some provisions might be up for grabs - such as those around the opening up of health data.

UK businesses are already managing GDPR's regulations from the EU, but this new bill could mean that they will have to think even more about how they handle data in 2025.

The bill is adding some new rules on who can access what data and how. Companies will have to think more about how they'll manage data permissions and customer requests for data sharing. This might be the year your business invests in automated systems so customers can more securely share their data with approved third parties.

Perhaps the biggest impact is that the ICO will have more power to oversee compliance. Keep an eye out for new guidance from them and get ready for more audits and a closer eye on data practices.

All this means you'll want to closely monitor the Data Bill's progress, especially the timeline for implementation. And think carefully about your e-marketing. You might be facing higher fines if you don't comply with what's coming down the line.

The EU's AI Act - Businesses need to think now about how to manage AI

The EU's Artificial Intelligence (AI) Act officially came into force this past August and compliance for prohibited practices should be in effect by this coming February. While most provisions of the regulation will apply as of next August, 2026, this coming year is the one in which the Act will be what companies doing business in the EU and using AI will need to consider, most especially if they're developing or deploying high-stakes AI systems.

The Act classifies AI by risk levels, from minimal to limited to high with a final category termed "unacceptable." Companies dealing with high-risk AI - such as healthcare, employment, law enforcement - will need to deal with stricter requirements. What do they need to start thinking about? Implementing more transparency, conducting regular audits and examining their AI use so that end-users have more insight and control.

Thanks to the AI Act, companies using AI will start thinking more about data governance, transparency and user consent. Companies will need to start figuring out how to document their AI processes, track the data that feeds into the AI models and make sure it's unbiased and safe to use.

Depending upon your business, this could mean investing in systems that monitor your AI tools. And remember, staying on top of these changes not only helps with compliance but can also build trust with customers who increasingly want transparent AI solutions.

Perhaps most compellingly for businesses creating or deploying AI within the EU, there could be some hefty fines at some point if you don't comply. So, if your company isn't already set up with clear AI policies, this is the year to make it happen.

Is 2025 the year everything changes in US data privacy laws?

Without federal legislation on data privacy, US state laws continue to go their own way with an ever-growing patchwork of requirements. Currently 20 states have data privacy laws and 2025 promises to get even more complicated with data privacy laws for eight more states coming online. Navigating this evolving landscape of state privacy laws is not simple but for most companies doing business within the US, it's critical. Non-compliance could lead to fines and legal issues, not to mention loss of consumer trust.

But is 2025 also the year that all changes? There was talk about passing the American Privacy Rights Act of 2024 (APRA), federal regulation that was introduced to standardise the various state laws and provide businesses with a clearer roadmap for compliance. This could be a game-changer for data privacy in the US, if it passes. But that's a big if, as its hearing was scuttled at the last minute in June and a new government likely has a packed agenda that might not give privacy legislation a front row seat.

The legislation is also complicated by the fact that states like California, which have strong privacy laws in place, want to keep their standards, while others argue that a single federal law would make things simpler across the board. APRA tries to manage this by allowing some state laws to stay in effect, but it's proving to be a tricky balance. Add to that the fact that the tech industry isn't thrilled about some of APRA's more rigorous rules, like data minimization and biometric data protections, which could be costly to implement and the concern over some of the enforcement provisions, especially the right for individuals to sue companies. All this means APRA is stuck.

What everyone does agree on is that companies doing business in the US in 2025 will face increased regulation and more enforcement when it comes to managing their data. States are increasingly recognizing opt-out mechanisms, requiring specific contract provisions with third-party vendors and creating requirements around user data disclosures. For now, businesses will need to ensure their privacy policies and consent mechanisms are not only robust but also flexible enough to adapt to each state's unique mandates.

US agencies like the Federal Trade Commission (FTC) and the Securities and Exchange Commission (SEC) will likely continue to target companies that fail to adequately protect consumer data, particularly in healthcare and AI applications. Keep an eye on these enforcement actions, as they often set precedents. Same goes for class-action lawsuits around online tracking and "session replay" software which we could see more of in 2025. Businesses should review their data tracking and consumer consent practices to ensure full compliance with state-specific requirements, especially where customer interactions are involved.

Love your cool, new technologies? Be prepared to love the regulations too this year

2025 is the year that the UK and the EU will focus on trying to get a handle on emerging technologies especially in data privacy, cybersecurity and ethical tech use. Companies with products that use any of these devices (that's a lot of you) need to get ready. The EU's Digital Operational Resilience Act (DORA) comes into force as of January and it targets financial institutions and critical sectors to strengthen their cybersecurity frameworks. The Cyber Resilience Act entered into force in the second half of 2024 and is just gathering steam with products needing to be compliant in the EU by 2027. It mandates high security standards for everything from operating systems, firewalls and routers to software embedded within other devices - remember the Internet of Things (IoT)? - that are sold or available in the EU.

In the UK, the Online Safety Act is coming online now, with companies required to manage risks associated with harmful online content. This is especially urgent for social media platforms that will need to enforce strict age checks and make sure to protect young users from harmful material.

Companies using generative AI (and who isn't?) need to be aware that both the UK and EU are pushing for more AI transparency, ethical usage and risk management. There's the EU's AI Act, which is starting to come into force and will categorise AI systems by risk level and impose stricter obligations on high-risk systems, promoting safer and more ethical AI practices across Europe. The UK for now is releasing guidance and encouraging companies to adopt ethical practices voluntarily. But it is anticipated that the UK is gearing up for some kind of AI regulation. There have been moves towards a more regulatory framework as the technology advances and public discussions on ethical AI use grow.

Companies need to make sure to stay aware so they can develop compliance strategies that incorporate these technologies in a responsible, ethical and legal way.

GDPR without borders

As businesses continue to expand internationally, they must contend with an increasingly complex web of data protection laws, with more countries adopting GDPR-like standards. Brazil and China are two countries that have implemented rigorous frameworks similar to the EU's, imposing strict requirements on data handling and cross-border transfers, that have both seen recent updates. In August 2024, Brazil's Data Protection Authority (ANPD) introduced Resolution 19/2024, which establishes Standard Contractual Clauses (SCCs) for international data transfers under the LGPD. Brazilian companies now have until August 2025 to replace existing transfer contracts with these new SCCs. Meanwhile, China's personal data landscape relies on multiple laws, including the Personal Information Protection Law (PIPL), Cybersecurity Law (CSL), and Data Security Law (DSL), all of which enforce strong data protection and cross-border transfer measures. Recent changes to China's data protection laws reflect a desire to strike a balance between data security and facilitating smoother cross-border business operations.

In July 2023, the Brazilian Data Protection Authority (ANPD) issued its first fine for data protection violation, against Telekall, a small telemarketing company, for violating data subjects' rights. In addition, the ruling noted that the company failed to appoint a data protection officer, did not provide an adequate legal basis for processing personal data, and did not cooperate during investigations. This decision highlights the fact that no company is too small to be targeted for failing to comply, and serves as a reminder to all businesses to stay on the line with data protection compliance.

For businesses working internationally, these regulations mean that compliance with only one standard, such as GDPR, is no longer sufficient. Global organisations must adapt their data protection practices to meet varied legal standards across regions, taking local laws into account to avoid penalties and ensure secure data handling. As more countries move toward GDPR-inspired regulations, multinational companies must adopt flexible, cross-border compliance frameworks to meet these diverse requirements.

California cracks down on AI

California is at the forefront of AI regulation in the U.S., with new laws set to reshape how businesses use artificial intelligence by 2025. The state already had the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), from 2018 and 2020, which required businesses to disclose the logic behind automatic decisions and allow consumers to opt out of AI-driven profiling. In September 2024, CA Governor Newsom signed 17 new bills covering the deployment and regulation of GenAI technology, the most comprehensive legislative package in the US on this emerging industry, cracking down on deepfakes, requiring AI watermarking, protecting children and workers, and combatting AI-generated misinformation.

Though coming out of California, the bills will have global effects, as most of the world's largest AI companies are based in the Golden State and nearly all that aren't will still do business there. In 2025, organisations will need to ensure that AI systems are designed to comply with the new comprehensive legislation. Additionally, organisations may face increased scrutiny if they cannot demonstrate compliance.

Statistics underscore the growing concern: According to a recent report from customer experience specialist CX Network, two in five (43%) of CX professionals are concerned about ethical AI use. In addition, a YouGov survey found that 55% of respondents say they don't trust AI much (23%) or at all (32%) to make unbiased decisions. Even more (62%) don't trust it to make ethical decisions, and 45% don't trust it to provide accurate information. By 2025, businesses that fail to comply with these evolving regulations may face steep penalties—up to $7,500 per violation. To avoid fines and reputational damage, businesses should conduct AI audits, update privacy policies, and implement robust data governance frameworks well in advance.

Mind your own data: GDPR continues to evolve

The past two years have seen GDPR enforcement and fines ramping up: In 2023, approximately €2.1 billion in fines were imposed in the EU due to violations of GDPR. Also in that year, an average of €4.4 million was incurred per violation, up from around €500,000 in 2019. The growing regulatory scrutiny around AI and data privacy set critical precedents that businesses must understand as they approach compliance in 2025.

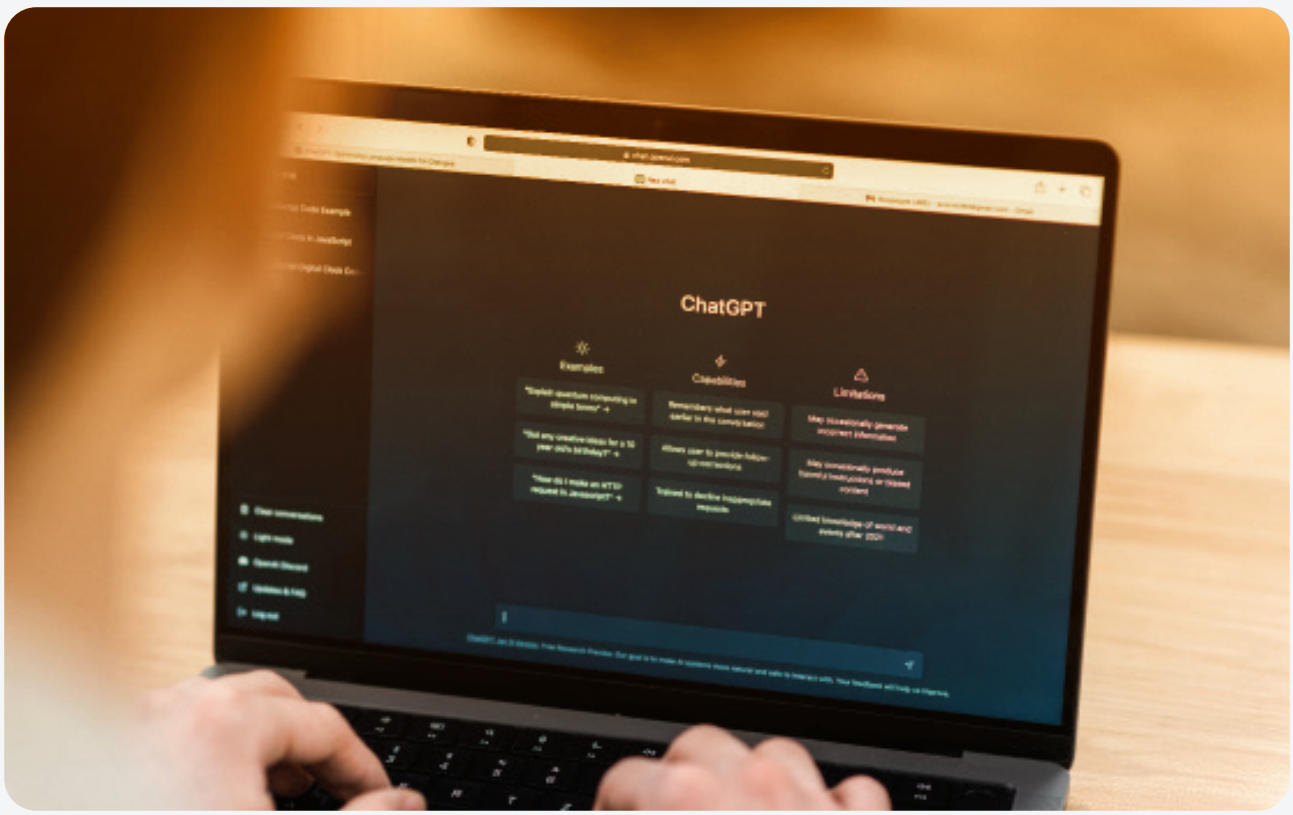
Recent blockbuster fines have targeted almost every app on your phone: Facebook, Instagram, TikTok, Whatsapp, and X/Twitter have been fined over €2.9bn for GDPR violations. One notable smaller recent fine involved Klarna, a digital payments provider, which was fined 650,000 euros after a routine audit revealed that their privacy notices were insufficiently detailed. Although there was no breach or complaint, the Swedish data protection authority found that Klarna had failed to clearly explain how they were storing personal data, emphasising the importance of transparency and accuracy in privacy policies. Although this fine was relatively small, it sends a strong message about the importance of proactive and diligent compliance, even in the absence of data breaches or formal complaints.

Regulations are expected to continue to evolve in 2025. While a major overhaul of GDPR seems unlikely, ongoing developments like the proposed Digital Markets Act, the Artificial Intelligence Act, and the proposed Cyber Resilience Act will shape the future of data privacy, moving towards compliance requirements that are more specific and less open to subjective interpretation. Additionally, the growing emphasis on ESG, driven by the Corporate Sustainability Reporting Directive, underscores the need for responsible data governance as part of broader sustainability efforts.

ChatGPT: Gamechanger or GDPR mega risk?

As AI becomes deeply embedded in workplaces, businesses must stay vigilant about compliance with GDPR and similar data privacy laws. A recent statistic showed that 68% of large UK companies use at least one AI technology, and indeed, integrating ChatGPT and similar tools into the workplace can lead to significant productivity gains. But with adoption comes heightened risk. One of the biggest challenges is the potential for data breaches if employees unintentionally share sensitive information with AI platforms like ChatGPT. Such incidents often occur during routine tasks, where employees may input private or regulated data without realising the risk.

GDPR mandates that organisations protect personal data rigorously, and the penalties for non-compliance under this and parallel regulations in other jurisdictions are substantial and always increasing: companies are finding that regulators are applying more and more aggravating factors to judgments which are increasing the fines to even higher levels. In 2024, the average total cost of a data breach reached $4.88 million, underscoring the financial impact that companies can face from even a single mishap. Additionally, ethical questions should be taken into account. Clear policies on AI usage, employee training, and regular audits will become evermore essential in 2025 to maintain compliance in this rapidly evolving area. As AI continues to advance, maintaining a proactive approach to data privacy will be essential for businesses aiming to balance innovation with legal accountability.



How VinciWorks can help

As data and AI technology continue to evolve, push boundaries and break new ground, regulation will continue to try to keep pace and balance innovation with privacy and security issues. For this year, we will see how legislation will attempt to ensure that data-driven technologies will maintain a healthy respect for individual rights. This tension will likely - and hopefully - continue to challenge and inspire us to develop digital ethics that can manage the exciting new efficiencies and creative solutions that are headed our way.

eLearning **Courses**

VinciWorks makes compliance training and eLearning that works.

Available in every language you speak. Built by us.
Ready for you.

About us

We believe compliance enables business. Compliance is an opportunity to be one step ahead, so your organisation can focus on advancing the business.

For over 20 years, VinciWorks has been at the leading edge of re-envisioning compliance tools and training. Our creative and driven team works hard everyday, challenging the traditional compliance industry to become forward-thinking, interactive and engaging. From our vast library of 800+ courses, to the award-winning Omnitrack training and compliance management software, to a curated catalogue of world class resources, VinciWorks is here to support your organisation every step of the way.

We constantly have our finger on the pulse, being the first to adapt our products to new regulations and market changes that impact our customers' businesses. Our flexible solutions ensure that every one of our products is tailored to our customers' unique business needs, placing them at the heart of everything we do.

vinciworks

www.vinciworks.com
enquiries@vinciworks.com
+44 (0) 208 815 9308