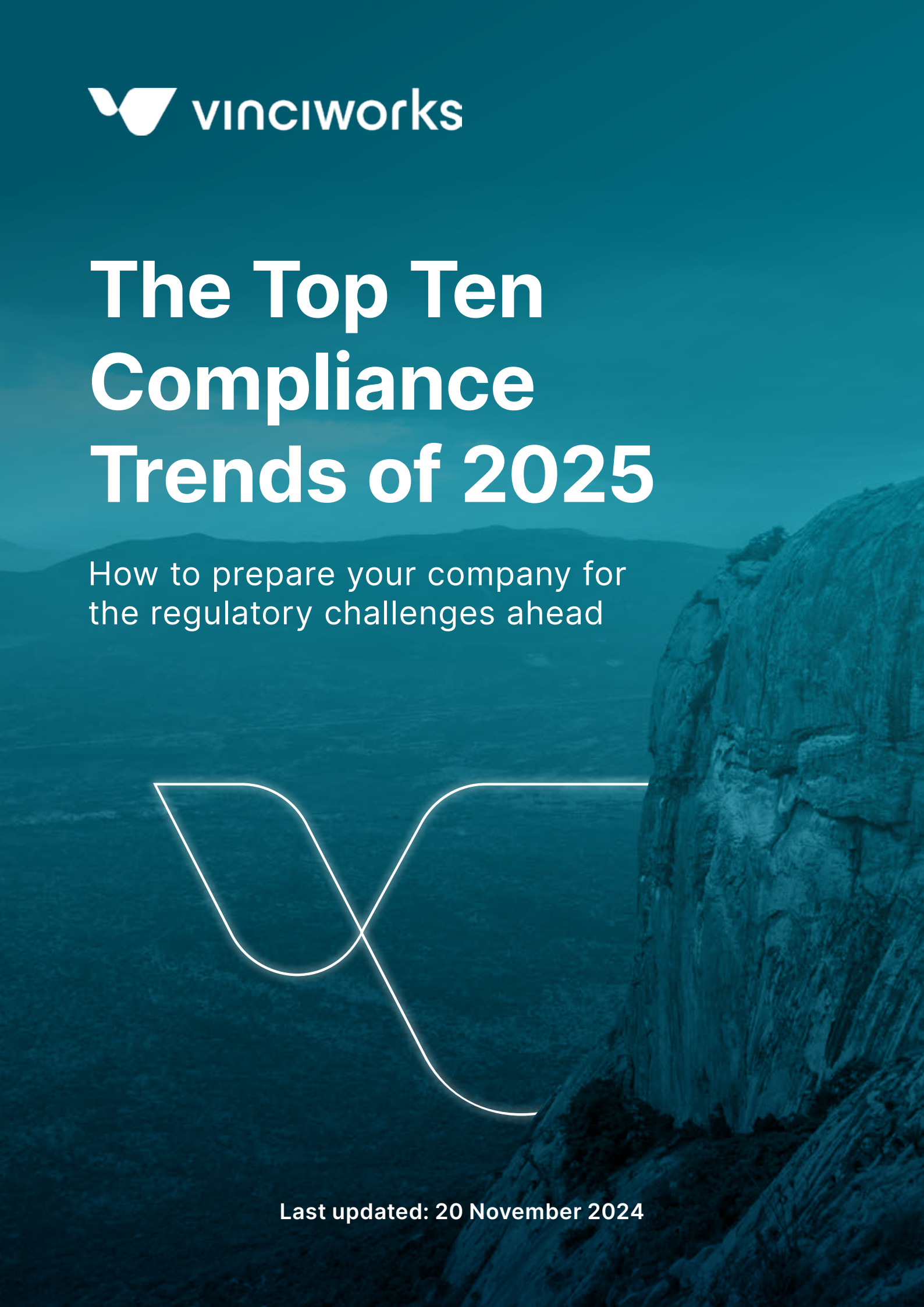
vinciworks

# The Top Ten Compliance Trends of 2025

How to prepare your company for the regulatory challenges ahead



Last updated: 20 November 2024

# The Top Ten

## Compliance Trends of 2025

**How to prepare your company for the regulatory challenges ahead**

2025 will bring significant compliance challenges for businesses across the world. The inauguration of the second Trump administration will bring immediate shifts in policy around sanctions. Companies must stay vigilant, especially regarding sanctions on countries like Russia and Iran, as violations could lead to hefty fines.

Diversity, Equity, and Inclusion (DEI) programs will come under increased scrutiny, particularly as opposition to DEI from politicians and the press around the world will take their lead from what's coming out of Washington, D.C. Companies will need to demonstrate the impact of their DEI initiatives, especially in sectors relying on government contracts, while also adhering to evolving global regulations.

In cybersecurity, businesses must adapt to AI-driven threats and invest in AI-based threat detection and employee training to defend against advanced cyberattacks. This includes ensuring cloud systems comply with tighter security regulations.

Geopolitical risks, particularly in the Middle East, will raise concerns around terrorist financing, requiring enhanced due diligence and transaction screening for all companies connected with global trade.

The EU's AI Act continues to affect compliance, and will require businesses using AI in high-risk sectors to implement transparency and audit measures. Similarly, California's AI legislation will enforce stricter rules on AI-driven misinformation and deepfakes, requiring audits and updated privacy policies.

Organisations should also start thinking about how to retain talent through tackling under addressed issues like menopause and neurodiversity in the workplace by offering flexible policies to retain talent and improve productivity. Meanwhile regulators are moving towards a proactive stance, focusing on real-time monitoring, predictive analytics, and stronger accountability in compliance standards. Overall, 2025 is going to be a year of significant change in the compliance world.

# Compliance will get more complicated across the world under the second Trump administration

1

The inauguration of a conservative administration under President Trump will significantly reshape the regulatory environment for companies, particularly in areas of compliance and corporate culture. As was evident during his previous tenure, President Trump's approach to governance often favours deregulation and reduced governmental oversight, alongside sometimes erratic behaviour which could prompt changes in how businesses handle a range of compliance issues. One of the most notable shifts will be in the area of international sanctions compliance.

Under the previous administration, sanctions against countries like Russia and Iran were key aspects of US foreign policy. However, the incoming Trump administration is expected to take a more unpredictable stance on these matters. While Trump's administration could relax some of the more stringent sanctions imposed on Russia, companies will need to stay alert to any sudden shifts, particularly when it comes to navigating the grey areas of dealing with businesses or entities tied to sanctioned nations. On the flip side, Iran sanctions could be vastly increase, shifting dynamics of geopolitics could mean that businesses will need to recalibrate their compliance strategies to adapt to a potentially more fragmented sanctions regime. This will require enhanced diligence from legal and compliance teams, as any inadvertent violations of sanctions regulations can result in heavy fines or damage to a company's reputation.

The potential for a trade war with Europe could also see companies caught in the middle of rising tariffs and quick-changing priorities which leave compliance teams in a spin. Navigating compliance in a shifting regulatory environment under the Trump administration will demand a delicate balance between political realities, legal obligations, and maintaining a positive corporate culture. Companies will need to remain agile, adapting to changing laws and regulations while upholding their values and commitments. As the political landscape evolves, it is essential for businesses to stay proactive, ensuring that their policies reflect both legal requirements and ethical standards in a way that resonates with employees, clients, and stakeholders alike.

# In the face of political headwinds, DEI needs to justify its impact

2

DEI programmes not just in the US but around the world will face increased scrutiny under a Trump administration. The new government's anti-DEI rhetoric and efforts to reduce federal funding for diversity initiatives will likely have an impact around the world, as anti-DEI politicians and press take their lead from the mood in Washington, D.C. Businesses should prepare to better justify the value and effectiveness of these programs, especially in sectors dependent on government contracts or federal funding. DEI practitioners may be challenged to demonstrate measurable impact and return on investment (ROI) for their initiatives, particularly in light of the political climate that views DEI programs as potentially divisive or unnecessary.

In parallel, businesses must be prepared for the possibility of new legislative restrictions that limit the scope of DEI efforts. This could include curbs on training programs focused on racial sensitivity, gender identity, or unconscious bias, especially in the context of pushback. For companies already deeply embedded in DEI work, it will be crucial to maintain transparent reporting and regularly assess the impact of their diversity programs, both to ensure legal compliance and to demonstrate the ongoing benefits of fostering an inclusive workplace. Furthermore, the global nature of many businesses will require them to stay aligned with the evolving DEI policies of other countries, including the UK, where the new Labour government has committed to expanding the Equality Act. This will likely mean UK companies will be expected to invest more in their DEI initiatives. Nevertheless, UK companies also risk their initiatives being scrutinised by politicians and the press, some of whom have taken on the 'anti-DEI' approach championed by conservative voices on both sides of the Atlantic.

# Cybersecurity compliance gets increasingly complicated

3

In 2025, companies are going to have to get proactive about their cybersecurity as cyber threats become more sophisticated. But that's where things might get complicated.

Companies are going to turn to tools driven by artificial intelligence (AI) to identify vulnerabilities and suspicious behaviour in real-time. But guess who will also be wielding AI? Those cybercriminals you are trying to stay one step ahead of. Ransomware attacks, data breaches and phishing scams will evolve this year, as cyber criminals try to exploit what they can. From remote work setups to connected smart devices, everything is vulnerable.

Companies need to prepare for AI-generated malware, sophisticated deepfake scams and autonomous cloud attacks, where hackers use automation to breach networks and access sensitive data quickly. Companies will need to consider AI-based threat detection to stay a step ahead and invest in automated cloud security solutions that can counter fast-moving attacks. Emphasis will be placed on zero-trust architecture, a security model that assumes no one is safe and continuously verifies everyone.

With human error still accounting for most breaches, you will also want to prioritise employee education on cyber hygiene. Training should become more frequent and more realistic as they try to help people spot the latest scams.

Regulatory demands around cloud security are also going to get tighter. UK companies that rely on cloud services should ensure compliance by strengthening their cloud infrastructure and consider unified security platforms for easier compliance management and real-time threat monitoring.

Governments around the world are likely to try to push stricter regulations, like requiring businesses to report incidents faster and invest in better security measures. For consumers, it might mean more privacy protections. But for companies, it's a clear sign that in 2025 cybersecurity is going to be a real business priority.

# With Lebanon grey listed and possible new sanctions on Iran, doing business in the Middle East will be even trickier

4

Terrorist financing compliance will become increasingly complex for international businesses in 2025 as Lebanon was grey listed by the Financial Action Task Force (FATF). This flags Lebanon as a jurisdiction under increased scrutiny and financial institutions around the world will be looking closely at Lebanese transactions for signs of potential financial crime. With the incoming Trump administration promising new sanctions on Iran which is heavily financially tied to Lebanon via the terrorist group Hezbollah, doing business in the Middle East will become even more complex.

For Lebanon, this could mean stricter international banking relationships and increased transparency if the country wants to avoid further economic isolation. Iran's influence across the region will come under much more scrutiny if new US sanctions are implemented. Despite Turkey and the UAE being removed from the FATF grey list, these countries remain remarkably high risk for terrorist financing given their proximity and links to groups under sanction. The UAE was even kept on the EU's list of high risk jurisdictions in defiance of the FATF.

Any business with connections to the region will need to ramp up due diligence, making sure to screen all transactions and partnerships that could be flagged as risky. There will be a need for clear documentation and verification from counterparts and additional checks on clients, suppliers or financial flows that could involve Middle Eastern counterparties. Expect these transactions to take longer and compliance costs to increase.

# The EUs AI Act takes shape: Businesses need to think now about how to manage AI

5

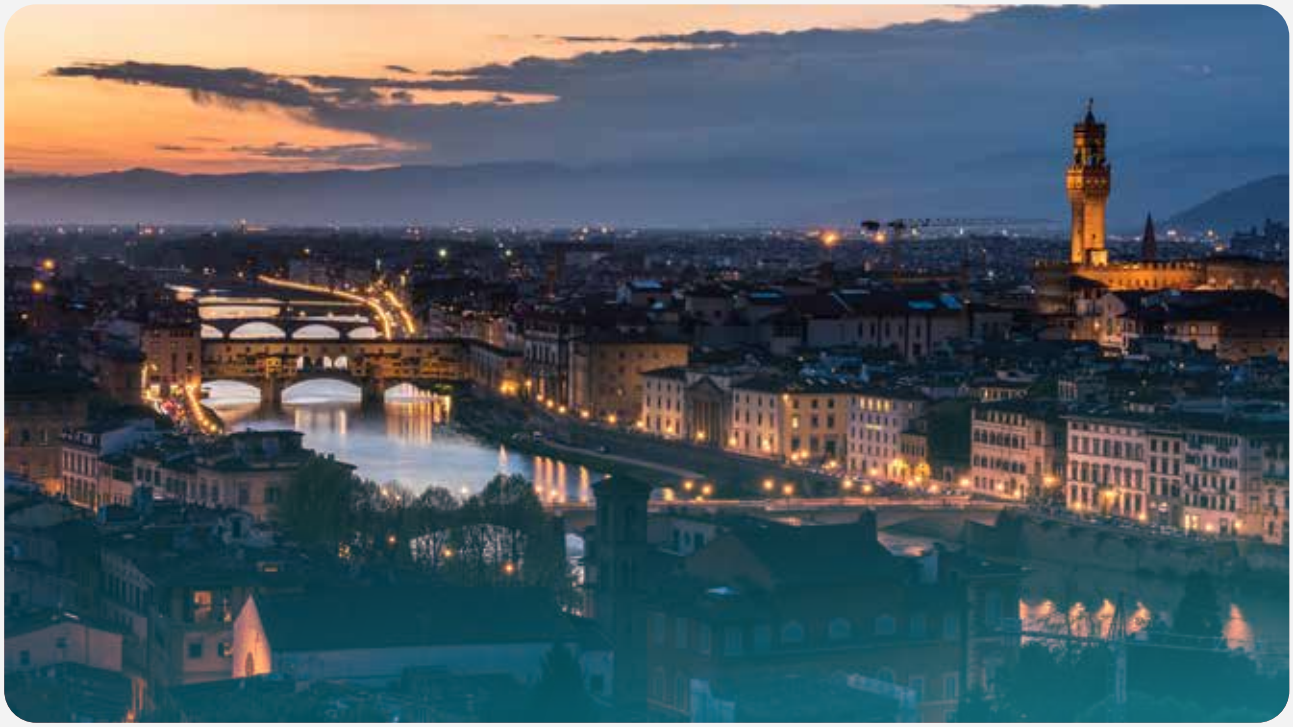
The EU's Artificial Intelligence (AI) Act officially came into force this past August and compliance for prohibited practices should be in effect by this coming February. While most provisions of the regulation will apply as of August, 2026, this coming year is the one in which the Act will be what companies 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.



# California cracks down on AI

6

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.

# The culture wars at work - balancing gender critical and transgender views

7

One of the most high-profile and contentious issues in workplace equality today revolves around transgender rights and gender-critical beliefs. This area highlights the importance of having sound policies that balance these potentially conflicting rights under the Equality Act in the UK, and a variety of local legislation in the US and other countries.

Under many national equality laws, in particular the UK's Equality Act, **gender or sex reassignment** is protected. This means that individuals who have undergone, are undergoing, or plan to undergo sex reassignment cannot be discriminated against on that basis. At the same time, employment tribunals have also established that **gender-critical beliefs**—the view that a person cannot change their biological sex—are also protected under the Equality Act's provision for religion and belief. This means that individuals cannot face workplace discrimination for holding or expressing such beliefs.

Workplaces are thus tasked with navigating a delicate balancing act between these two protected rights. For instance, some employees holding gender-critical beliefs have successfully argued at employment tribunals that they were unfairly treated or pushed out of their roles for expressing these views, often on their personal social media outside work hours. There have been cases where gender-critical feminists faced severe backlash, including what has been described as "witch hunts," for simply articulating their protected beliefs in a personal capacity.

Conversely, transgender employees have also won tribunal cases after experiencing discrimination in the workplace. Examples include employers refusing to update IT systems with their new name, continuing to use their previous name on official records, or failing to provide inclusive policies for transgender employees. Such actions can create a hostile environment and undermine the protections guaranteed by the Equality Act.

Workplaces should prepare for strong views, and in particular how vocal activists on either side of this (or any other hot-button cultural issue) could cause a compliance issue. In a recent employment tribunal case, an employee protested the organisation's voluntary policy encouraging staff to include pronouns in email signatures by modifying his own signature to read "XYchromosomeGuy/AdultHumanMale." Despite requests from management to remove this addition, he refused, leading to his dismissal. The tribunal concluded that the termination was not a response to his beliefs but to the provocative and inappropriate way he expressed them. The employee's actions were deemed disruptive to the organisation's efforts to promote inclusivity and posed potential harm to its reputation and relationships with service users.

The answer is clear, consistent policies that uphold the rights of all employees while promoting respect and understanding between differing perspectives.

# Addressing menopause at work is becoming critical

8

Menopause in the workplace is no longer a topic companies can afford to ignore. It is a pressing issue of diversity, inclusion, and employee wellbeing—and it's costing businesses talent, productivity, and money.

The statistics are alarming: 60% of women have taken time off work due to menopause symptoms. Furthermore, 99% of women report that menopause symptoms have negatively impacted their careers.

Businesses are already aware of the high costs of staff turnover, particularly when it comes to experienced employees with invaluable institutional knowledge. The financial impact of replacing such staff is significant, far outweighing the costs of creating supportive workplace policies. Add to this the well-documented benefits of fostering diversity and inclusion, and it becomes clear: addressing menopause at work is not just the right thing to do—it's a business imperative.

Menopausal symptoms—including fatigue, memory issues, and anxiety—can severely affect productivity. Women often feel pressured to overcompensate at work, leading to stress, burnout, and exacerbated symptoms. The workplace culture of "grinning and bearing it" perpetuates harmful stereotypes and drives talented women out of the workforce at a time when they are often at the peak of their careers.

Becoming menopause friendly does have a straightforward solution. It involves offering flexible and hybrid working arrangements to help employees manage symptoms and medical appointments without feeling penalised. This can include flexible hours, work from home option, quiet spaces, temperature control and reasonable adjustments.

Ignoring menopause doesn't just hurt employees; it hurts the business. A lack of support leads to higher turnover, increased recruitment costs, and a widening gender pay gap. Women leaving due to menopause symptoms often hold senior roles, and their departures impact representation at higher levels, perpetuating inequities.

Implementing menopause leave demonstrates a company's commitment to diversity, inclusion, and employee wellbeing. It boosts retention, enhances productivity, and positions businesses as forward-thinking and inclusive employers.

# Be prepared for regulators to take an even more proactive approach

9

Regulators are stepping up their game this year. They have been increasingly moving from a reactive - “let’s wait for the crisis to happen" - mode to a proactive - “let’s prevent the crisis from happening” - approach. But this year, this shift in mindset is going global, which means this is the year that it will land, hard.

The US DOJ launched a whistleblower pilot program this past year that incentivizes voluntary reporting of corporate misconduct by offering financial rewards, especially for significant violations. The SEC allowed the Cloopen Group to avoid penalties in its compliance failures thanks to self-reporting, collaboration and remedial actions, such as firing employees involved in fraud and improving internal controls. The European Council established the Anti-Money Laundering Authority (AMLA) to prevent money laundering and terrorism financing through enhanced supervision of high-risk entities across the EU.

And then there’s the UK’s Economic Crime and Corporate Transparency Act (ECCTA) which is coming into force this year. The Act focuses on proactive prevention rather than reactive enforcement. It also introduced the senior manager offence, a significant change in corporate criminal liability.

Prosecutors no longer have to prove that “the directing mind and will” of a company was behind wrongdoing. With ECCTA, any senior manager who has engaged in criminality around fraud, tax evasion, sanctions breaches, money laundering, false accounting and bribery can find their actions result in corporate prosecution.

And it’s not just your businesses’ operations but your supply chains too. Senior managers will need to ensure that due diligence is conducted across the supply chain on a risk-based and ongoing basis, to ensure there is no criminality in any of the goods or services purchased in the supply chain. If not, the proceeds of these goods can become criminal property, and dealing in criminal property is a money laundering offence.

This shift is driven by a combination of emerging risks and advances in technology that make early detection more feasible. Waiting for scandals to erupt is so 2024. With tools like predictive analytics and real-time monitoring, suspicious activity can be flagged and financial crimes can be prevented before they take root.

This could change how you approach compliance. You need to anticipate risks and ensure there are safeguards throughout your operations. Regulators will expect companies to know their supply chains inside out, spot red flags early and develop robust systems to manage vulnerabilities. This might create more work up front, but you are also reducing the likelihood of costly enforcement actions or reputational damage.

# A new UK Data Bill is coming

10

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.

# Get more in-depth analysis and practical advice on compliance with our live webinars

Sign up to one of VinciWorks interactive webinars and have your questions answered live by our compliance experts. First quarter 2025 webinars are ready for you to sign up. All times are midday UK time unless specified. Get in touch with us at enquiries@vinciworks.com or visit vinciworks.com/webinars to register.

| | |
|---|---|
| 9 January 2025 | The compliance agenda in 2025 - what you need to know |
| 13 January 2025 | Health and safety compliance in 2025 |
| 14 January 2025 | AI & data protection compliance in 2025 |
| 15 January 2025 | AML & financial crime compliance in 2025 |
| 16 January 2025 | AML Core Group (invite only) |
| 16 January 2025 (3pm) | Equality, diversity and inclusion compliance in 2025 |
| 22 January 2025 (3pm) | The Trump administration and compliance |
| 29 January 2025 | Making compliance software work for you |
| 12 February 2025 | Tax evasion and financial crime compliance |
| 19 February 2025 | How to manage supplier onboarding |
| 26 February 2025 | UK GDPR changes: Data (Use and Access) Bill |
| 5 March 2025 | Managing sanctions and proliferation financing risks |
| 12 March 2025 | Protected belief and the UK Equality Act |
| 19 March 2025 | Health and safety and the UK Employment Rights Bill |
| 26 March 2025 | Making your organisation's information secure and safe |
| 2 April 2025 | Managing the risks of bribery breaches |

# 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