onetrust

Navigating the EU AI Act

E-BOOK | APRIL 2024

Table of Contents

DISCLAIMER:

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.

A horizontal approach: Standing apart on the global stage

In crafting its approach to artificial intelligence (AI) legislation, the European Union (EU) has opted for a horizontal legislative framework. The EU's AI legal framework embraces an industry-agnostic perspective and is meticulously designed with nearly a hundred articles.

Here, we'll look to provide a window into the EU AI Act. This piece of legislation is not just the first of its kind—but also a benchmark for global AI regulation, developed to help create a precedent in the rapidly evolving AI landscape.

Guarding values, fueling innovation

The EU AI Act is carefully balanced. It's not just about throwing a safety net around society, economy, fundamental rights, and the bedrock values of Europe that might be at risk due to AI systems; it's also a nod to the power and potential of AI innovation, with built-in safeguards designed to promote and protect inventive AI strides.

Crafting the EU AI Act has been anything but a walk in the park, with the definition of AI being one of the contentious corners. Since its inception proposal in April 2021, the Act has been a living document, seeing numerous iterations, each amendment reflecting the fluid discourse around AI technology and its implications for society.

At the trilogue meeting in December 2023, France, Germany, and Italy raised concerns about the limitations placed on powerful AI models, and wanted to take a lighter regulatory regime for models like OpenAI's GPT-4 .

After ongoing discussion, the compromise reached by the EU commission was to take a tiered approach, with horizontal transparency rules for all models and additional obligations for compelling models with systemic risk.

Where the Act stands now

On February 2, 2024, the Committee of Permanent Representatives voted to endorse the political agreement reached in December of 2023. On March 13, Parliament voted to endorse the Act, with 523 votes in favor, 46 against, and 49 abstentions.

The AI Act will enter into force 20 days after its publication in the EU's Office Journal. The provisions on prohibited systems will apply after 6 months, and obligations for providers of general-purpose AI will apply after 12 months. Most other requirements will apply after two years.

High risk systems that are intended to be used as a safety component of a product or are covered by other laws in the EU have 36 months to comply with the EU AI Act.

AI: Breaking down the concept

Originally, the Act defined machine learning, the basis of AI systems, as "including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning." The text includes an updated definition, which defines AI systems as "machine-based systems designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

The complexity of AI systems is a sliding scale, with more intricate systems requiring substantial computing power and input data. The output from these systems can be simple or mightily complex, varying with the sophistication of the AI in play.

A horizontal approach: Standing apart on the global stage

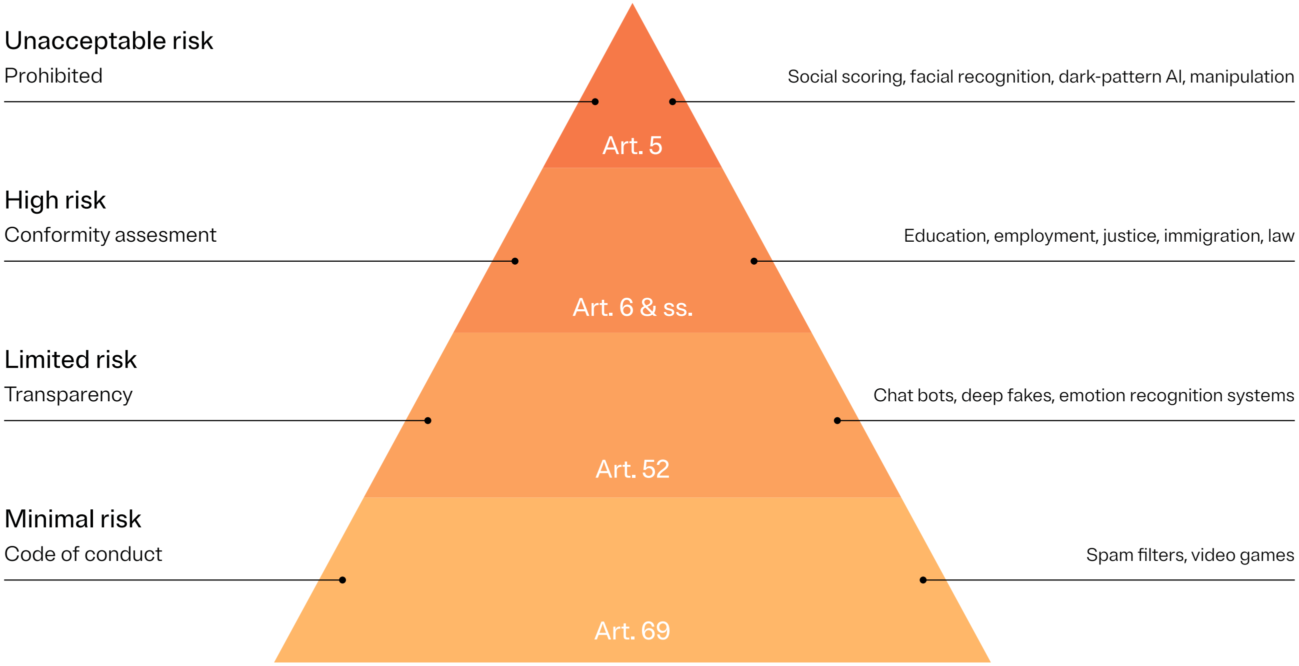
This broad definition covers a range of technologies, from your everyday chatbots to highly sophisticated generative AI models. But it's important to note that not every AI system falling under the Act's broad definition will be regulated. The Act plays it smart with a risk-based approach, bringing under its regulatory umbrella only those systems associated with specific risk levels.

AI regulation: Calibrated to risk

Here's where it gets interesting. The EU AI Act has different baskets for AI systems. Some are seen as posing an unacceptable risk to European values, leading to their prohibition. High-risk systems, while not banned, have to dance to a tighter regulatory tune. It's vital to remember that these risk categories aren't static; the Act is still in a draft stage, and as more changes come, these risk categories will likely be fine-tuned as well.

EU AI Act risk levels

The EU AI Act defines multiple levels of permissible risk: high risk, limited risk, and minimal risk.



Unacceptable risk
Prohibited
Social scoring, facial recognition, dark-pattern AI, manipulation
Art. 5

High risk
Conformity assesment
Education, employment, justice, immigration, law
Art. 6 & ss.

Limited risk
Transparency
Chat bots, deep fakes, emotion recognition systems
Art. 52

Minimal risk
Code of conduct
Spam filters, video games
Art. 69

These are the levels of "permissible risk" that are allowed by organizations, however, "unacceptable risk" is a risk level which is not allowed by organizations at which point companies need to change their models accordingly.

Unacceptable Risk — Social scoring systems, real-time remote biometric verification

High Risk — Credit scoring systems, automated insurance claims

For processes that fall into this bucket, companies need to conduct a conformity assessment and

A horizontal approach: Standing apart on the global stage

register it with an EU database before the model is available to the public.

Apart from this, these high-risk processes require detailed logs and human oversight as well.

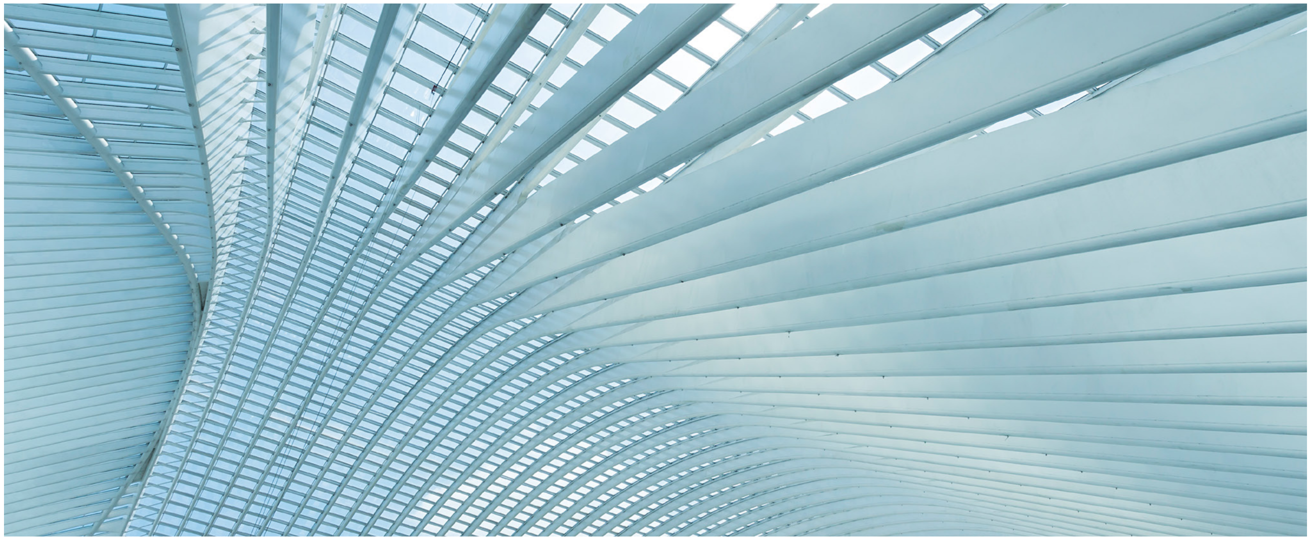
Limited Risk — Chat bots, personalization

For limited risk processes, companies need to ensure that they're being completely transparent with their customers about what AI is being used for and the data involved.

Minimal Risk — For any processes that companies use that fall into the "minimal risk" bucket, the draft EU AI Act encourages providers to have a code of conduct in place that ensures AI is being used ethically.

Conformity assessments

Of these risk levels, high-risk systems will pose the highest compliance burden on organizations, as they'll have to continue to meet obligations for conformity assessments. Conformity assessments (CA) require companies to ensure that their "high-risk" systems meet the following:



- The quality of data sets used to train, validate and test the AI systems; the data sets must be "relevant, representative, free of errors and complete"
- Detailed technical documentation
- Record-keeping in the form of automatic recording of events
- Transparency and the provision of information to users
- Human oversight

This assessment is mandatory before a high-risk AI system is made available or used in the EU market. It ensures that AI systems comply with EU standards, particularly if there are significant modifications or changes in intended use. The main responsible party for CA is the "provider"—the entity putting the system on the market. However, under certain circumstances, the responsibility can shift to the manufacturer, distributor, or importer, especially when they modify the system or its purpose.

A horizontal approach: Standing apart on the global stage

Who performs a CA?

The CA can be done internally or by an external “notified body.” Internal CAs are common as providers are expected to have the necessary expertise. Notified bodies come into play particularly when an AI system is used for sensitive applications like real-time biometric identification and does not adhere to pre-defined standards.

During an internal CA, the provider checks compliance with quality management standards, assesses technical documentation, and ensures the AI system’s design and monitoring are consistent with requirements. Success results in an EU declaration of conformity and a CE marking, signaling compliance, which must be kept for ten years and provided to national authorities if requested.

For third-party CAs, notified bodies review the system and its documentation. If compliant, they issue a certificate; otherwise, they require the provider to take corrective action.

How often should you perform a CA?

Conformity assessment isn’t a one-off process; providers must continually monitor their AI systems post-market to ensure they remain compliant with the evolving draft EU AI Act. In cases where a notified body is involved, they will conduct regular audits to verify adherence to the quality management system. Robustness, accuracy and cybersecurity

Engaging all players in the AI game

The EU AI Act is not just handing out responsibilities to AI providers; it’s casting its net wider to include various actors in the AI lifecycle, from users to deployers. And its reach is not just limited to the EU; it has global ambitions, affecting entities even outside the EU, thus having implications that are worldwide.

Fines: A significant deterrent

With the EU Parliament’s recent adjustments to the EU AI Act, the fines for non-compliance have seen a hike, now standing at a maximum of 35 million euros or up to 7% of global turnover. For context, these fines are 50% greater than that of the GDPR, which has maximum fines of $20M or 4% of global turnover, underlining the EU’s commitment to ensuring strict adherence to the EU AI Act.

Charting the course towards regulated AI

The EU AI Act is a bold statement by the EU, meticulously balancing the act of fostering AI innovation while ensuring that the core values and rights of society are not compromised. With the Act inching closer to its final stages of approval, it’s crucial for everyone in the AI space to keep an eye on its development.

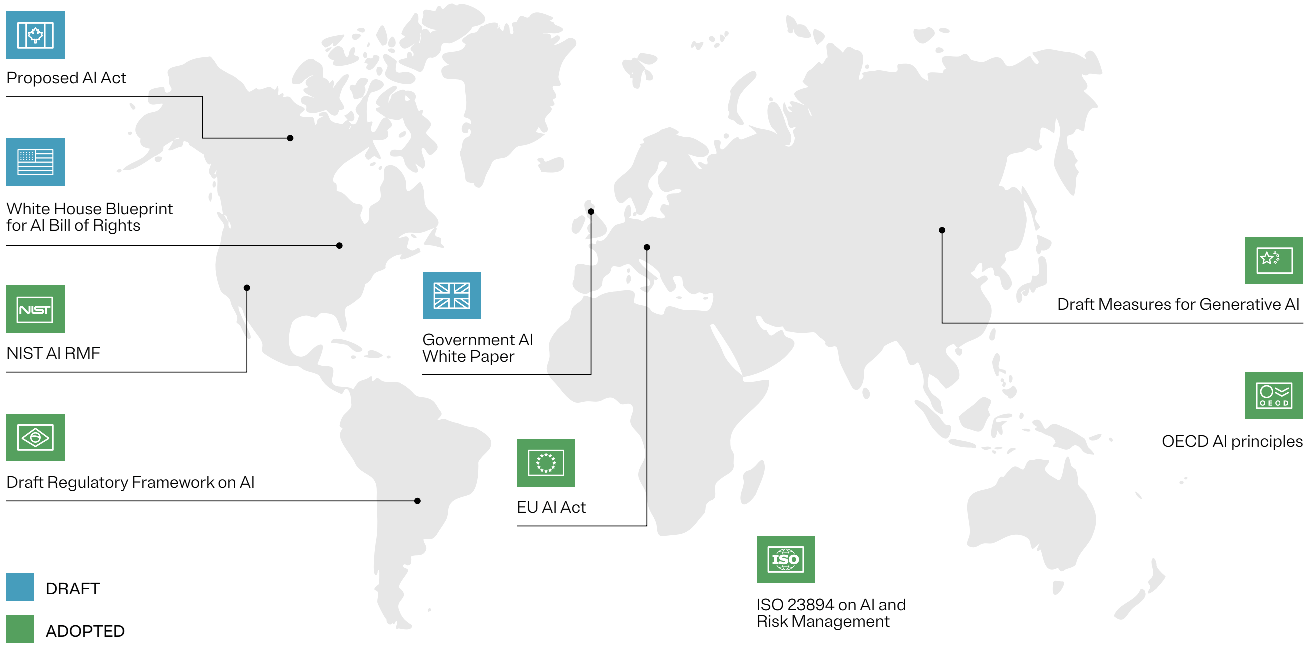
Whether you’re a provider, user, or someone involved in the deployment of AI, preparing for a future where AI is not just a technological marvel but also a subject of defined legal boundaries and responsibilities is imperative. This introduction offers a glimpse into the EU AI Act’s journey and potential impact, setting the stage for the deeper analysis that unfolds in the subsequent sections. So, buckle up and let’s dive deeper into understanding the nuances and implications of the EU AI Act together.

AI frameworks: A global perspective

A landscape in flux: The global heat map of AI frameworks

The global AI framework landscape underscores the imperative need for more cohesive international rules and standards pertaining to AI. The proliferation of AI frameworks is undeniable, calling for enhanced international collaboration to at least align on crucial aspects, such as arriving at a universally accepted definition of AI.

Within the tapestry of the European Union's legal framework, the EU AI Act is a significant thread, weaving its way towards completion. Concurrently, there's a mosaic of initiatives at the member-state level, with authoritative bodies across various nations rolling out non-binding guidelines, toolkits, and resources aimed at providing direction for the effective use and deployment of AI.


Proposed AI Act
White House Blueprint for AI Bill of Rights
NIST AI RMF
Draft Regulatory Framework on AI
Government AI White Paper
EU AI Act
ISO 23894 on AI and Risk Management
Draft Measures for Generative AI
OECD AI principles
DRAFT
ADOPTED

Efficient future processes through AI

AI promises quicker, more efficient, and accurate processes in various sectors. For example, in insurance, AI has streamlined the assessment process for car accidents, optimizing a process that was once manual and lengthy. This example serves as a testament to AI's potential to significantly improve various aspects of business and everyday life.

But engaging with AI is a nuanced dance, a careful balancing act between leveraging its unparalleled potential and navigating the associated risks. With its transformative and disruptive capabilities, AI invites cautious and informed engagement.

Recognizing its transformative power while preparing for the challenges it brings to the table is essential for individuals and organizations alike as they navigate the dynamic landscape of artificial intelligence in the modern age.

Weighing AI's pros and cons in business

Risks: Transparency, accuracy, and bias

Despite its myriad advantages, AI isn't without substantial challenges and risks. For starters, some AI systems, which may be perceived as "black boxes," have been the subject of intense scrutiny and debate over transparency issues. This concern is particularly salient with larger AI systems, such as extensive language models, where there's a lack of clarity on the training data employed. This raises significant copyright and privacy concerns, which need to be addressed head-on.

Furthermore, the struggle with ensuring the accuracy of AI systems persists, with several instances of erroneous AI responses and predictions documented. Notably, bias that may arise in AI systems—stemming from the prejudiced data they may be trained on—poses a risk of discrimination, requiring vigilant monitoring and rectification efforts from stakeholders involved.

AI as solution: Turning risks into opportunities

Interestingly, AI isn't just a challenge; it is also a potential solution to these conundrums. For instance, AI can be leveraged to identify and mitigate biases within datasets. Once these biases are discerned, strategic steps can be taken to rectify them, ensuring that AI can be harnessed optimally to maximize its benefits while minimizing associated risks.

Developing AI governance: The way forward

Laying the foundations for AI governance

With the dynamic and complex AI landscape unfolding rapidly, there is an urgent need for legal and privacy professionals to lay the groundwork for robust AI governance and compliance programs. A wealth of existing guidance provides a preliminary roadmap for the essential requirements of such programs, with senior management's endorsement being a pivotal first step in this endeavor.

Engaging C-suite executives and ensuring they comprehend the magnitude and intricacies of AI's influence is crucial for fostering a culture of AI responsibility throughout the organization. This initiative transcends mere compliance, extending to building trust in AI applications – a cornerstone for successful business operations.

Practical steps towards an AI governance framework

On the material front, organizations can use practical guidelines for ethical AI use. These guidelines are aligned with the AI principles from the Organization for Economic Cooperation and Development (OECD):

1. **Transparency:** Efforts should be directed towards demystifying AI applications, making their operations and decisions understandable and explainable to users and stakeholders.
2. **Privacy Adherence:** AI applications should respect and protect users' privacy, handling personal data judiciously and in compliance with relevant privacy laws and regulations.
3. **Human Control:** Especially in high-risk areas, there should be mechanisms for human oversight and control over AI applications, ensuring they align with human values and expectations.
4. **Fair Application:** Strategies for detecting and mitigating biases in AI applications should be implemented, promoting fairness and avoiding discrimination.
5. **Accountability:** There should be comprehensive documentation and recording of AI operations, allowing for scrutiny, accountability, and necessary corrections.

AI ethics policy: A critical element

The establishment of AI Ethics Policies, informed by ethical impact assessments, is essential in navigating challenges and making informed, ethical decisions regarding AI use. For example, instead of outright blocking certain AI applications, ethical impact assessments can guide organizations in implementing nuanced, responsible use policies, especially for sensitive data. Ethical considerations should inform every step of AI application, from inception and development to deployment and monitoring.

Inclusive AI governance: A size-agnostic imperative

IImportantly, AI governance is not an exclusive domain of large corporations with extensive resources. With AI use cases proliferating across various sectors, companies of all sizes will inevitably engage with AI, necessitating AI governance frameworks tailored to their specific needs and capacities.

Developing AI governance: The way forward

A few universal principles apply regardless of the company's size. First, securing executive buy-in and adopting a multidisciplinary approach is imperative for successful AI governance implementation.

Second, organizations should commence with high-level principles as a starting point, even if they are small or merely purchasing ready-made AI models. Training and upskilling employees across various functions, including procurement and technology, is also vital to understand and mitigate the risks associated with AI tools and applications.

Embedding core governance principles

Six core governance principles need to be embedded into AI governance programs:

1. Governance and Accountability: Establishing a structure for accountability, possibly through AI oversight committees or ethics review boards, is essential. Governance should be enforced throughout AI's lifecycle, from inception to operation.

2. Human Oversight: Adopting a human-centric approach, with trained human reviewers at various stages, is crucial for ethical AI application.

3. Fairness and Ethics Alignment: AI outputs should align with fairness and ethical standards, reflecting an organization's culture and values.

4. Data Management: Implementing robust data management processes, tracking modifications to datasets and mapping data sources, is key for reliable AI systems.

5. Transparency Enhancement: Ensuring that AI decision-making processes are transparent and understandable is necessary for building trust and compliance.

6. Privacy and Cybersecurity: Addressing legal data processing requirements, conducting privacy impact assessments, and mitigating AI-specific cyber risks are imperative for secure and compliant AI applications.

Given the pace at which AI is evolving and its profound implications, organizations must proactively develop and implement AI governance programs. By adopting a set of core governance principles and practices, organizations can navigate the AI landscape responsibly, ethically, and effectively. These principles, informed by ethical considerations, legal compliance, and a commitment to transparency and accountability, will guide organizations in harnessing AI's benefits while mitigating its risks, ultimately fostering trust and success in the AI-driven future.

Value-driven AI governance

As organizations delve deeper into the realm of AI, developing and implementing AI governance programs aligned with their values is paramount. These governance frameworks should not only ensure compliance with legal standards but also reflect the ethical commitments and values of the organizations.

Whether it's about making tough trade-offs between transparency and security or deciding on the ethical use of data, a values-driven approach to AI governance provides a reliable compass guiding organizations through the intricate landscape of AI applications and ethics.

Final thoughts and tips on AI governance

AI, GDPR, and data privacy

When considering the interaction between AI, the draft of the EU AI Act, and GDPR, it's crucial to acknowledge existing guidance on utilizing AI in line with GDPR. Noteworthy resources include the toolkit provided by the UK's Information Commissioner's Office (ICO) and the comprehensive guidance and self-assessment guide offered by France's CNIL. These tools offer valuable controls and checklists, assisting organizations in ensuring compliance of their AI use with GDPR requirements.

A starting point for aligning data usage within AI frameworks with GDPR principles is to conduct diligent Data Protection Impact Assessments (DPIAs) to ensure that all these processes remain compliant.

AI governance start point: Privacy professionals are well-positioned to serve as orchestrators, bringing together various functions and skillsets within organizations to address AI governance comprehensively. This collaborative approach not only ensures compliance but also functions as a business enabler, fostering a proactive and informed approach to emerging challenges and opportunities in the AI landscape.

Keep calm and AI: Embrace technological developments with a sense of calm and curiosity. Engaging with the fast-paced and continually evolving field of AI requires a willingness to learn and adapt, acknowledging that understanding and addressing the risks and potentials of AI is a journey rather than a destination.

Evolution of Professional Roles: With the continuous changes in technology and data processing, the roles of data protection officers are evolving, potentially transitioning towards "data trust officers". It's imperative for professionals in the field to be open to assuming new roles and responsibilities as the technology and regulatory landscape transforms.

To give your organization a 5-step plan to get started:

1. Engage with AI governance programs immediately; proactive engagement is crucial.
2. Secure management buy-in since AI governance requires a multi-stakeholder, enterprise-wide approach.
3. Assemble a diverse and skilled team, encompassing legal, compliance, data science, HR, information security, and external experts
4. Prioritize, set realistic and achievable goals, and consider adopting a phased approach to AI governance.
5. Stay abreast of AI developments, actively engage with industry peers, and participate in AI governance initiatives to foster a collaborative and informed community.

With the evolving landscape of AI, organizations must proactively engage with AI governance. A collaborative, multi-stakeholder approach is necessary to address the complex challenges and opportunities presented by AI.

To learn more about how AI Governance can help your organization, request a demo today.

Request demo

onetrust

REQUEST A DEMO TODAY AT ONETRUST.COM

As society redefines risk and opportunity, OneTrust empowers tomorrow's leaders to succeed through trust and impact with the Trust Intelligence Platform. The market-defining Trust Intelligence Platform from OneTrust connects privacy, GRC, ethics, and ESG teams, data, and processes, so all companies can collaborate seamlessly and put trust at the center of their operations and culture by unlocking their value and potential to thrive by doing what's good for people and the planet.