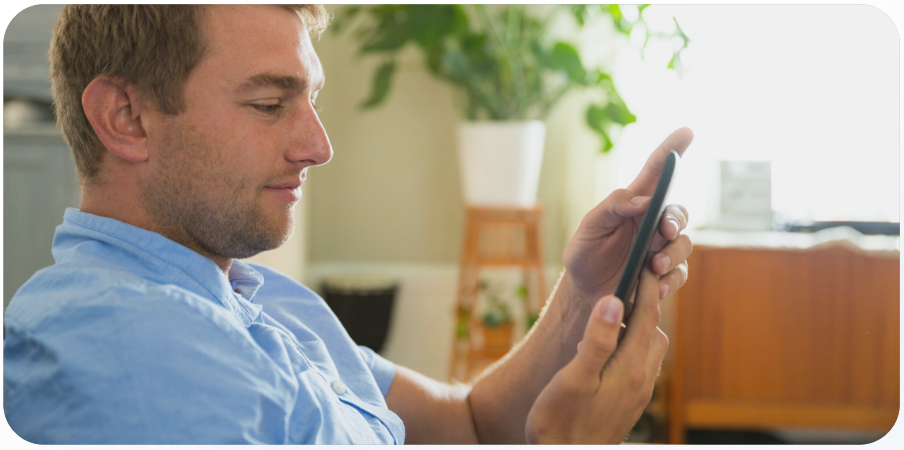
syrenis

GUIDE



Privacy 2.0:
Innovate or Stagnate

syrenis.com

Introduction

Privacy 2.0 represents the fundamental shift that's happening within the field, where we're moving away from traditional, box-ticking compliance methods and towards a future where privacy is seen as a gateway to unlocking data insights and driving business growth.

Why Now?

We've all seen the world dramatically expand when it comes to connection and technology. The last few generations have witnessed the evolution of the internet first-hand, and we're now moving at a pace never seen before.

From smart devices that predict your next move to AI assistants that manage daily tasks in the blink of an eye, technology is becoming an integral part of our lives.

This rapid advancement is not just about convenience; it's about transforming the way we interact with the world and each other.

Long gone are the days when sharing your data meant simply filling out a paper form with your name and address.

Today, every click, swipe, and interaction online contributes to a vast digital footprint, revealing insights about our preferences, behaviors, and even our future actions.

Every brand you interact with is looking for ways to streamline the experience – get things to you faster, recommend the right product, provide the best possible service. At the heart of every experience is data: an understanding of who you are as an individual, what you like and dislike, where you're located, the list is endless.

Whilst it might seem like global privacy regulation is driving this shift towards prioritizing privacy, it's playing catch up. Legislation can take years (if not decades) to come into effect and have an impact. These laws are being made to address what has essentially been a decade of unrestricted data access.

The limitations on data use are now forcing organizations to re-think how they collect data, what they do with it, and how they protect it.

Fundamentally, two things are true:

- People want control of their own data.
- Brands need data to build meaningful experiences.

For these things to work in harmony, both consumers and brands are waking up to the fact that privacy is paramount.

Businesses are coming to the realization that privacy must be leveraged as a priority. Privacy teams need to be supported and invested in, both through technology and resourcing. Moving from a traditional cost center to a business enabler, supporting their organization in expansion.

What Are The Emerging Trends and Challenges of Privacy 2.0?

- AI
- Proliferation of data & technology
- Proving value
- Moving beyond compliance

Part 1: The Thing We Can't Ignore (AI)

Artificial Intelligence (AI) is at the forefront of pretty much every department, strategy, and organization.

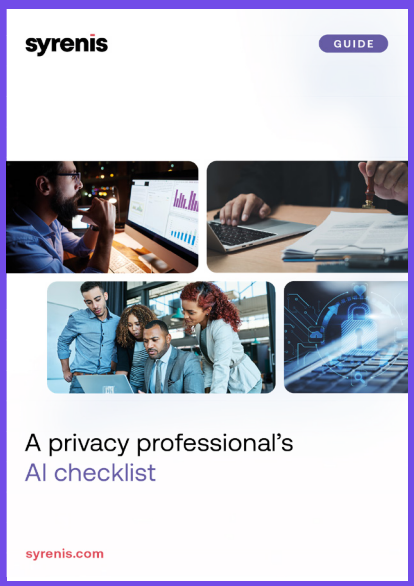
It brings both obvious challenges and potential opportunities. AI systems can process vast amounts of data to provide personalized experiences, but they also raise significant privacy concerns. The key challenge is ensuring that AI respects user privacy while delivering value.

It's no surprise that privacy teams have been handed the governance of AI to their growing list of accountabilities. The skillsets align – to understand, assess, monitor and navigate.

When everyone's knocking on your door requesting to implement new AI tools, how do privacy professionals say yes without also opening the door to risk?

Obvious challenges

- **Data Security:** Ensuring that AI systems do not expose sensitive data.
- **Bias and Fairness:** Preventing AI from making biased decisions based on incomplete or skewed data.
- **Transparency:** Making AI decision-making processes understandable to users.



A privacy professional's AI checklist

To help an organization make privacy-sensitive and future-proofed AI decisions use our AI top 10 checklist to support:

- **Identifying data goals, strategy, and tactics**
- **Determine legal basis**
- **Solve transborder data flow concerns**
- **Consider data sets.**

DOWNLOAD NOW

Potential Opportunities

- **Enhanced Personalization:** Using AI to provide more tailored experiences without compromising privacy.
- **Improved Data Management:** Leveraging AI to better manage and protect user data.
- **Proactive Privacy Measures:** Implementing AI-driven solutions to identify and mitigate privacy risks before they become issues.

Part 2: Future Proof Tech

How do privacy teams adapt to a constantly changing world where technology is always moving the goal posts?

Privacy teams must be agile and forward-thinking to thrive in this dynamic environment. Here are three solutions to not only survive but thrive:

1. **Continuous Learning and Adaptation**: Privacy teams should stay updated with the latest technological advancements and privacy regulations. Regular training and development programs can help teams stay ahead of the curve.
2. **Investing in advanced Privacy Technologies:** Implementing cutting-edge privacy technologies such as di erential privacy, encryption, and anonymization can help protect user data while enabling its use for business insights.
3. **Collaborative Approach:** Privacy teams should work closely with other departments, such as IT, legal, and marketing, to ensure a holistic approach to privacy that aligns with the organization's goals.

The Risks of Legacy Tools

Legacy technology is a well-known threat to operational enterprises. Sometimes, a platform is so deeply embedded into other systems that it's almost impossible to unplug, even if it's actually useless. Outdated legacy systems and technologies can actively cause problems and hold companies back from better processes and innovations. Consent Management Platforms (CMPs) are no different.

While still a fairly new industry, there have been rapid advancements in technology and capabilities. It might seem impossible to move away from some systems due to the nature of the data they hold, but migrating platforms can be easier than you might think, with data secured and stored so that you don't lose anything vital.

5 of the biggest problems you might not realize are having a negative impact on your business:

1. **Built to Meet GDPR but Not Future Proof:** Many CMPs were developed specifically to address GDPR requirements. While this was a significant step forward, these platforms often struggle to keep up with new and emerging legislation as well as technology and innovation like AI. Brands want to do more with the data they collect while remaining respecful to user privacy and staying on the right side of the law. A CMP shouldn't hold you back from enhancing experiences and improving conversion through understanding your users' preferences.

2. **Incomplete, Slow, or Static Data Transfers:** Older consent tools often offer slow processing times and static cookie scans, leading to inconsistencies. For accurate compliance, consent data needs to be distributed across downstream systems in near real-time. Faster, accurate data transfer across your tech stack allows for more efficient operations and improved ROI. Gaps or inaccuracies in consent data can also make it difficult to process data subject requests, adding waste to an already expensive and often manual process.

3. **Limited Coverage:** Many older CMPs were designed with a narrow focus, often limited to specific regions or types of data. This limited coverage can be problematic for organizations operating in multiple jurisdictions or handling diverse data sets. Without comprehensive coverage, managing consent across all operations can lead to inconsistencies and potential compliance issues. A 'copy-paste' approach to consent management won't work anymore, especially with new legislations coming into enforcement worldwide.

4. **Limited Configuration:** Flexibility is crucial in consent management, as different organizations have unique requirements and workflows. Unfortunately, legacy platforms often offer limited configuration options, making it challenging to adapt the system to specific needs. This lack of flexibility can result in inefficient processes and increased administrative burden, as organizations may need to rely on manual workarounds to achieve their goals.

5. **Frankenstein Solutions:** Over time, many legacy CMPs have evolved into "Frankenstein" solutions, with various modules and features bolted on to address new requirements across privacy and compliance, like data mapping or third-party risk management. This often leads to a disjointed and cumbersome system that is difficult to use and maintain. A more integrated and streamlined solution is needed to ensure e icient and effective consent management.

Bonus – the cost factor: Many businesses are lured in by low-cost contracts only to find huge price increases at contract renewal. The initial low cost may seem attractive, but the long-term financial implications can be detrimental. It's essential to carefully evaluate the total cost of ownership when selecting a CMP.

Part 3: The ROI of Privacy Programs

Moving Privacy From a Cost Center to a Business Enabler

Privacy programs should be seen as strategic assets rather than mere compliance requirements. Organizations that recognize the importance and power of privacy to move the needle are seen as innovators; seizing the opportunity to collect consented data at scale that unlocks better insights and enhanced capabilities.

The problem	The solution	The business impact
Compliance is seen as the office of 'no'	Use advanced tools that centralize data consent and preferences to demonstrate clearly permissioned data access across every touchpoint	Projects that drive business value get the green light because you've got the confidence to say yes – compliance become the enabler
High compliance costs as a result of manual processes	Implement automated privacy management tools to streamline tasks, minimize errors and make better use of time saved	Reduced operational costs, improved operational efficiency, time to focus on bigger projects that drive broader change
Lack of consumer trust because of outdated processes, lack of options, confusing policies	Build more transparent data practices and communication with privacy-first design and implementation across your processes and systems, choosing technology that can enhance privacy experiences from cookie banners through to preference portals	Increased customer loyalty and retention – consumers buy from brands they trust and this is the foundation you need to build from
Risk of data breaches and fines because of manual processes, proliferation of datacollection and lack of visibility	Proactive risk management and robust security measures through real-time consent and preference data processing – know exactly what you have consent to use, instantly	Avoidance of financial penalties and reputational damage

Part 4: Beyond Compliance

What Do We Do When Compliance Is Done? Innovate

How can brands use the data they collect to go beyond compliance to transform customer experience, increase sales, and add ancillary revenue streams?

Hyper Personalization at Scale:
With privacy at the fore of consented data, businesses can gain deep insights into customer preferences and behaviors. This allows for the creation of highly personalized experiences that resonate with individual users. Hyper-personalization comes from utilizing artificial intelligence and machine learning alongside real-time data to generate advanced insights – build experiences completely tailored to unique instances of each individual user to not only enhance customer satisfaction but also build loyalty and drive higher engagement.

Data-driven Decision Making:
With more accurate data you can make data-driven decisions, from informing where online digital spend should focus and shaping future product development to prioritizing content strategies that increase engagement. By analyzing this data, businesses can uncover valuable insights that inform strategic decisions. This can include identifying emerging market trends, optimizing product development, and improving operational e iciencies. Data-driven insights enable businesses to stay ahead of the competition and adapt quickly to changing market condition.

Predictive Analytics:
Leveraging consented data for predictive analytics allows businesses to anticipate future customer behaviors and trends. This can be particularly useful for forecasting demand, managing inventory, and planning marketing campaigns. Predictive analytics can also help in identifying potential risks and opportunities, enabling proactive measures to be taken.

Cross-promotional Networks:
Consented data can also open up opportunities for cross-promotional activities. By understanding the preferences and behaviors of their customers, businesses can identify complementary products and services that may be of interest. This can lead to strategic partnerships and collaborations that enhance the overall value proposition for customers, for example through retail media networks where you offer specific, related advertisements based on insights.

syrenis

Contact us
hello@syrenis.com

US Office
Suite 700 3379 Peachtree Road NE
Atlanta, Georgia 30326, United States
+1 844 585 6264

UK Office
V2, Sci-Tech Daresbury, Warrington,
WA4 4AB United Kingdom.
+44 (0) 20 4551 9501