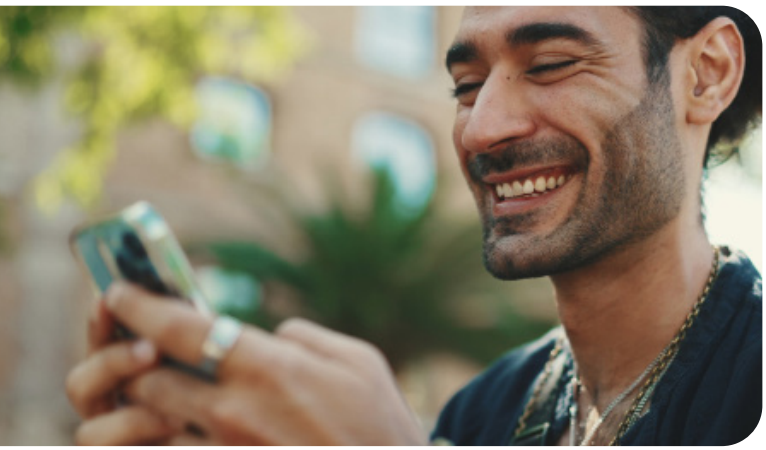
syrenis

GUIDE



Managing Consent and Privacy in the Age of AI

syrenis.com

Introduction

If privacy professionals are all boarding a single train, it's the train of Artificial Intelligence (AI). It is a bullet train, with regulatory guidance, new laws, and cutting-edge technologies changing the landscape at breakneck speed.

It is essential that privacy pros have an interest without these dedicated, thoughtful, and eager-to-learn individuals, AI initiatives could easily either spiral into an unethical and non-compliant gray area, or spiral down into such a restricted set of applications that the true power of AI would, regretfully, be lost.

On the other hand, a thoughtful approach to privacy in AI can both unlock the benefits of AI and protect individuals from privacy pitfalls.

As organizations seek new ways to utilize AI, privacy teams must be prepared to face the challenges head on without becoming the blocker to innovation.

The 3 Considerations of AI and Privacy

AI's growing influence on data management and privacy concerns is rooted in three main people-focused factors: Training, decision-making, and management.

First, AI is, at the most basic level, a set of tools designed to effectively sort through large amounts of complex data. AI also has the potential to be trained or train itself using large pools of data. When they include personal information, those large data sets bring on privacy questions of a scale and complexity not previously contemplated.

Second, AI starts us down the road of using technology to sift through large amounts of complex and non-standard data to come to complex conclusions — conclusions — a task that previously only humans could effectively do. This means we have to set our standards and guardrails on what types of important decisions about people, or important decisions that impact people, we are comfortable allowing a machine to make.

Finally, third and perhaps ironically, AI can be a resource to data managers and privacy practitioners as they do their own privacy and data protection jobs. The next generation of privacy enabling tools often employ AI to make privacy tasks that are increasingly complex — third-party risk assessments, data inventories, individual rights management, etc. – more effective, efficient, and adaptable.

If data complexity/volume, important people-impacting decisions, and sound privacy management are three top AI privacy concerns, one of the most important tools in the privacy arsenal to help guide AI initiatives around all three of these people-centric challenges is effective consent management.

Section 1: The Need for Robust Consent Management in AI

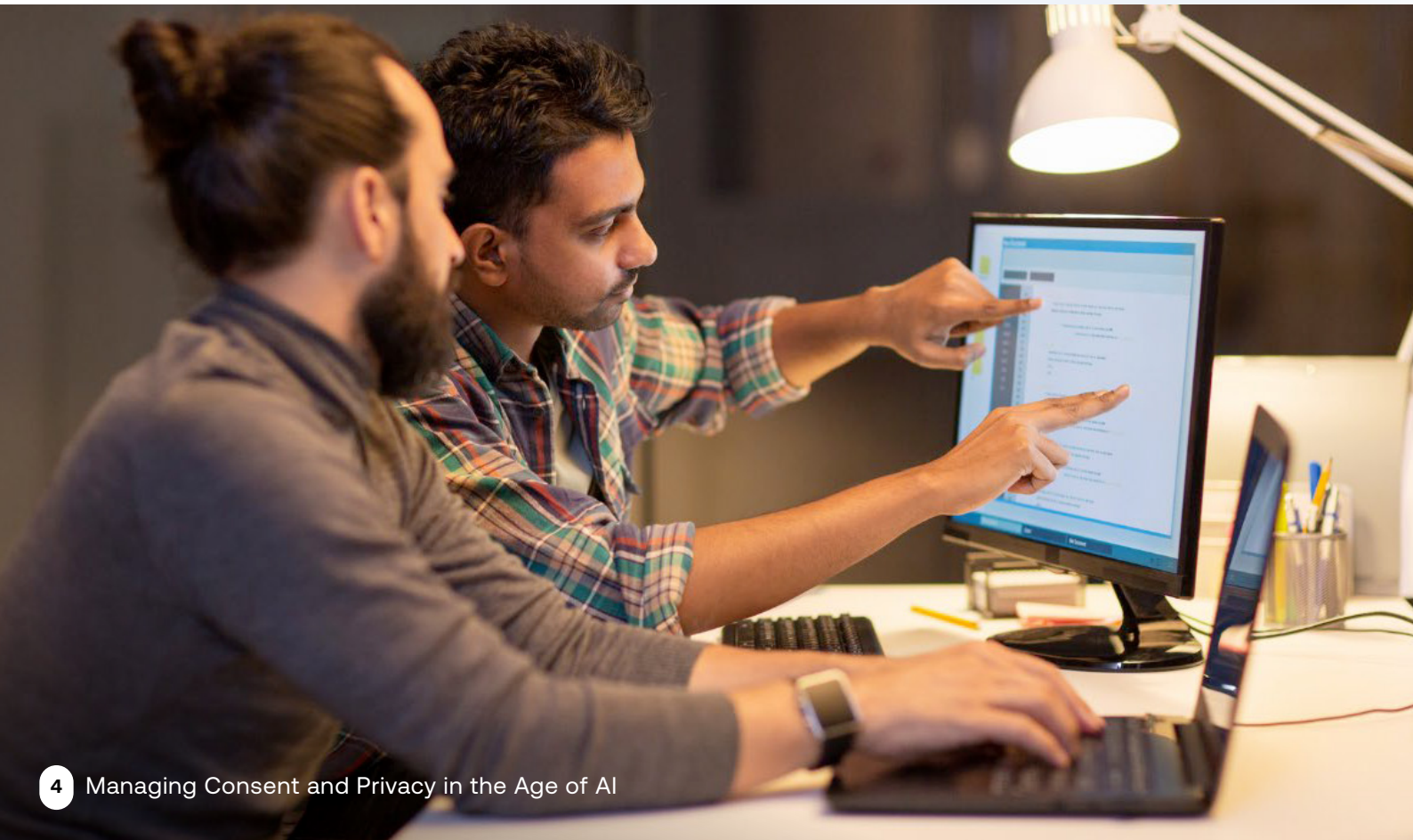
In order to understand the critical role that consent management plays in AI, it is important to understand how AI uses data.

As the United Kingdom's Information Commissioner's Office (ICO) describes, AI may use personal data both in its development and training stage, and during deployment. The data sets and purposes for developing and training an AI tool can be very different from the data sets on which that same AI tool is run, and for what purposes.

For that reason, also as the ICO suggests, consent for AI development/training may be different from consent to use data during AI deployment, which assumes a granular, robust approach to consent management.

In other words, an organization that wishes to train and/or deploy AI tools on personal data must consider separately whether it has the rights to use the data for those two, distinct purposes – and the simple, outdated "do not contact" flag in a marketing database will not provide the right level of granularity for either purpose.

The complexity of consent management related to AI goes beyond the issues of incredibly large scale of databases and development versus deployment permissions. There are some other unique challenges that AI poses to consent.



The Challenges of AI and Consent

Transparency

- Most companies control a set of legacy data for which they have disclosed a discrete set of uses when they collected the data. Most of those same companies did not contemplate using data to train AI models or deploying AI on data sets to make complex decisions, much less disclose those purposes when collecting the data. This leaves many organizations in a bind with legacy data, asking themselves the question of whether previous disclosures were enough.

- It is not uncommon for AI training and deployment efforts to use publicly available data, including data collected from social media. Most online companies post a privacy notice, but those notices are intended to be a description of that company's data handling practices. Surely a company cannot be expected to describe how other organizations might use public data in its notice and there is no way for those other organizations that might use public data to train or deploy an AI tool to reach all relevant data subjects to provide notice so transparency is challenging if not impossible.

- Also, many of the more modern privacy laws require clear, granular explanations of data collection, uses, and sharing. As the CNIL says in its AI guidance, "an artificial intelligence (AI) system based on the use of personal data must always be developed, trained, and deployed with a clearly defined purpose (objective). This objective must be determined, in other words established in advance at the design stage of the project." However, general purpose AI tools may be trained and deployed for a variety of purposes not contemplated at the original time of data collection, so it can be difficult if not impossible to create a purpose definition to express in a privacy notice with the required level of detail.

Informed Consent

- Closely tied with transparency is the principle of consent, and many jurisdictions require specific, explicit, separate opt-in consent in order to rely on consent for legal basis or when dealing with sensitive personal data. Few large data sets, especially public data sets, have obtained a valid opt-in consent specifically for AI model training and/or deployment. Moreover, as noted above, AI was not a "thing" at the time organizations collected their legacy data, so it would have been impossible for those organizations to obtain valid opt-in consent for a practice it could not have anticipated, much less described.

- Also as noted above, the specific purpose of a general AI tool may not be apparent at the time of development, so an organization may find it challenging to obtain a valid opt-in consent for its model training.

- Similar to the transparency challenge expressed above, even if they could reach data subjects to ask for consent, organizations face a challenging task of obtaining explicit, specific consent for general purpose AI tool development, training, and deployment – since they may not have yet contemplated specific purposes.

- If opt-in is required, most jurisdictions also require the ability to subsequently opt-out. Even if opt-in consent is not required, many AI purposes relate to secondary business purposes, so opt-out consent may still be required. In addition to the previously noted problems of reaching relevant data subjects to allow for an opt-out, AI brings with it the question of to what extent should data subjects be allowed to opt-out. If an individual opts-out, does that withdrawal apply only to future AI uses, or must the organization somehow withdraw the impact of that data subject's personal data from the training model or the analytics? Is that even possible?

AI Legislation as It Stands

Regulations and regulator guidance impacting AI are popping up everywhere. Some data protection authorities remind us that existing, general purpose privacy regulations cover AI just as they cover other data handling practices. For example, the UK's ICO and France's CNIL data protection authorities have issued practical guidance in applying their relevant data protection laws to AI.

Other jurisdictions have passed or are considering legislation to address privacy and AI. In the US, about a third of states have passed some sort of AI law. The EU has its new AI Act, and other countries, states, and provinces have followed. Moreover, regulators are enforcing laws applied to AI activities.

With such a flurry of interest and activities, risks associated with poorly managed privacy have only increased in the world of AI.

Since transparency and consent are such key components to both requirements related to AI and enforcement actions, it is fair to say that risks of inadequate consent management, including inadequate notice, include legal risks (fines, sanctions, legal disputes), ethical risks (trust erosion, reputational decline), and operational risks (data integrity issues, bias, and poor business decisions based on wrong information).

(Correct at the time of writing – August 2024)

Section 2: Building a Scalable Consent Management Platform

Given the central nature of strong consent management when implementing responsible, compliant AI, a scalable consent and preference management platform (CPM) can ease a company's transition into this new technology.

If your organization is considering licensing or building one, here are some key features and technology requirements of an effective consent management platform to consider.

Key features of a Consent Management Platform

1 **Centralized Consent Management and Recordkeeping**

- Platforms that provide a single source of truth for consents and preferences will help alleviate uncertainty in application across large technology stacks.
- As both AI and general-purpose privacy laws require demonstrable compliance – the ability to prove compliance – accurate and detailed record keeping can reduce risk with regulators as well as reduce uncertainty in sometimes complicated circumstances.

2 **Dynamic and Granular Consent Options**

- A primary benefit of managing consents through a consent management platform is having real-time visibility into consent and preference interactions.
- Allowing data subjects to give consents real-time, in context, and with granularity can help increase positive response rates and provide a more positive experience.

3 **Easy-to-use Interfaces for Data Subjects to Manage Their Consent**

- Data subjects who clearly understand options and can express preferences through an attractive and logical interface may suffer less from mental burden overload, trust the experience, and be more likely to tolerate the granularity of consents needed for effective AI.

4 **Integration With AI Systems to Ensure Compliance in Real-time**

- AI systems often sift through large volumes of data, some of which may be personal data that requires consent. Easy integration between a consent management platform and AI systems can make the difference between a smoothly running AI project and many, complicated manual human interventions.

Technological Requirements

1 **Scalability: Handling Large Volumes of Data and Multiple Data Points**

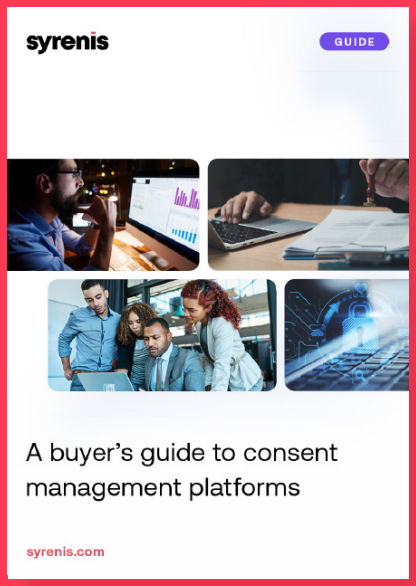
- The very nature of AI often requires large amounts of data and multiple data points. Implementing a consent management platform that can handle consents and preferences relating to large amounts of complex data can be essential for effective AI implementation.

2 **Interoperability: Integrating With Various AI and Data Management Systems**

- Even if an organization only uses one AI tool currently, future needs may require the organization to branch out to other, more advanced tools. A consent management platform that operates smoothly with a variety of systems, including multiple AI systems, can help future-proof consent management.

3 **Security: Ensuring Data Protection and Privacy by Design**

- Strong security features and practices are “table-stakes” for a preference management platform. A consent management platform provider can and should be able to answer questions easily and clearly about encryption, security frameworks, and certifications, and security protocols (including related to integrations).
- Privacy protections, including access controls and features that allow for privacy by default, will also be important factors to consider when selecting a tool.



A buyer’s guide to consent management platforms

DOWNLOAD NOW

Section 3: Operationalizing Consent Management in AI Projects

Selecting a consent management platform is only half the battle. Successful implementation is critical to success. The following are a few key steps to successfully implementing a consent management system.

Assess Current Consent Management Practices and Gaps:
A clear understanding of current consent management practices, plus any current or expected future gaps, will help ensure that the new consent management platform reflects best practices and enables ongoing compliance. Remember to consider consent model(s) (opt-in, opt-out, hybrid), differences in jurisdictions, emerging privacy law requirements (especially around AI, sensitive data, and automated decision-making), and the right granularity of consent.

Define Requirements Based on Regulatory and Operational Needs:
Consider how the organization uses personal data today and, to the extent possible, how the organization will want to use personal data tomorrow. Carefully review regulatory guidelines about AI and other emerging practices of interest to predict trends for future regulations.

Choose and Customize a Consent Management Platform:
Select the consent management platform that meets requirements and satisfies softer wishes, like customer support – but then take the time to implement in a way that addresses specific needs in a customized way. It is far easier to customize options during initial implementation than later down the road. You also want a platform that can scale with you as you collect more data, and ideally one that can adapt to new technology, like AI, as it continues to evolve.

Train Staff and Ensure Ongoing Compliance:
There is always a learning curve for employees using any new technology, and a consent management platform is no exception to this rule. Supporting staff adequately through training, support calls, spot checks, and documentation can help alleviate the fear, uncertainty, and doubt that decreases user acceptance and successful longer-term implementation. Instituting reasonable controls and regular reporting can help make sure that any small problems that crop up are identified and handled early.

Final Thoughts

It is useful to note that privacy professionals though sometimes lost in the technology shuffle during selection and implementation of a new consent management platform – have a critical role in the process.

Not only do the privacy pros know the must-haves and nice-to-haves of consent management, but they are also most often the people who lead consent management in the organization. In other words, they will have to live with the resulting system and so have the most stake. Moreover, the privacy office typically stays abreast of not only trends in the external regulatory world related to privacy, but also feels the impact of trends in data subject questions, requests, and concerns.

The privacy office is often an effective intermediary among the different groups involved in consent management platform selection and implementation. The privacy office can interpret for IT, IS, Legal, Compliance, Marketing, and other teams, helping them all work together towards the common goal of effective, efficient, compliant, and consumer- and business-friendly consent management.

An organization that is considering AI as a business advantage will find it useful to consider whether its current consent management tactics can keep up with that advanced technology. If not, a robust consent management platform may be in order. Investing sooner, rather than later, in strong and granular consent management can help an organization prepare for the data uses of tomorrow's technology needs by collecting data with clear consents today.

Combined with the other advantages of building customer trust, enhancing compliance, and building flexibility for data – a strong consent management investment just makes sense.

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