Usercentrics response to the new German consent management regulatory ordinance

Published by: *Eike Paulat, Director Product and Theodora Zamanakou, Senior Legal Counsel*

Munich, February 7, 2025 - As the leading European CMP provider, we strongly believe in the importance of privacy and data protection. Every European citizen has the fundamental right to control their personal data. At Usercentrics, we are committed to supporting an online experience that empowers individuals while fostering trust and transparency.

In September 2024, the German legislature released an ordinance for Consent Management Services to address the challenges posed by the frequency of displays of consent banners and pop-ups.

Enabling user consent choice via banners is critical for enabling and maintaining compliance with the GDPR and ePrivacy Directive. However, the lack of centralized consent management and signaling has made it necessary for so many sites to display banners. This requires users to have to make frequent and repeated consent choices, leading to widespread user frustration, inattention, and suboptimal browsing experience.

We welcome the German legislators' efforts to streamline user interactions with consent tools. Addressing user fatigue is a critical step toward better online user experience. However, this initiative by German legislators also presents challenges that must be carefully navigated.

Current approaches and concerns

We appreciate the initiative of German legislators to introduce more standardized consent signaling from users. However, we also have significant concerns, especially when looking into the still nebulous requirements for these services and the different approaches a consent management service could take.

Reliance on user identifiers

One principle of privacy-first design is minimizing reliance on shared user identifiers across services. Current solutions often depend on networks requiring user logins, where consent preferences are tied to a user ID. Consent preferences under the connected user ID are then shared with partners within these networks, and consent decisions rely on the shared user ID.

From our perspective, this does not solve the core goal of our privacy regulations. Consent preferences should be owned by the user and should be provided and maintained as close to the user as possible. Today, this is mainly solved by giving consent for each website separately via a banner display in a consent management platform (CMP). Consent information provided is saved client-side in the user's browser.

USERCENTRICS

Benefits of user-centric consent tools and signaling

We advocate for new solutions that store consent preferences close to the user, such as directly in the browser or through user-managed plugins. From there consent decisions can be directly signaled to website providers' CMP setup via agreed-upon standards. These methods align with privacy-first principles and offer greater autonomy to users while enabling transparency and regulatory compliance.

Instead of users seeing a banner or pop-up with every new website and having to make and save consent preferences again and again, saved client-side consent preferences can be signaled to any website. This negates the need for a "flood" of consent banner displays and relieves fatigue. Users will also need to be able to update their consent preferences locally over time as easily as they set them up initially.

Challenges for compliance and user experience

The current ordinance introduces confusion about how Consent Management Services should function in practice. The approach suggests that individuals could make general decisions through third-party tools, which would then transfer consent preferences to each website's CMP.

However, this raises significant concerns about compliance with privacy and data protection laws like the GDPR and ePrivacy Directive when processing personal data.

With the current lack of clear guidelines for how Consent Management Services will work, it's questionable whether the GDPR and ePrivacy requirement of "prior informed consent" will be met.

Issues with generalized prior consent for users

When individuals make a general consent decision before visiting a website, they may not have access to sufficient information about the specific data processing activities of each site. This generalized consent information would then apply on every site for every purpose and every controller, hence the concern about consent being adequately informed. It also risks making the user experience for using websites worse, rather than better.

Users not understanding a controller's specific data processing activities can also create a privacy compliance gap for the controller, as they are responsible for ensuring that users are adequately informed.

Issues with generalized prior consent for controllers

The GDPR requires data controllers to document and be able to provide proof of informed consent from users. If consent is provided through a third-party tool rather than directly on their platform, controllers may have difficulty accessing this information, in addition to experiencing a lack of control over its security and accuracy, leading to legal and financial risks.

Issues with reliance on third-party tools to achieve ordinance goals

Solutions that rely on third-party tools to store consent decisions for every website may conflict with the ordinance's intent. If users must still interact with CMPs during their initial visit to a website in order to record their consent preferences, banner displays and interactions will not be reduced.

Such solutions may only prevent subsequent displays of consent banners, a practice already common under current standards. Many CMPs already enable websites to respect users' consent preferences for extended periods, even if consent is denied.

Opportunities to evolve solutions, compliance, and user experience

The ordinance recognizes the need to reduce the overwhelming number of consent prompts that users encounter daily via banner or pop-up displays. The GDPR also requires that users must be able to exercise choice freely, including revoking consent as easily as it was given. User-friendliness is therefore also an important consideration for CMPs and for other Consent Management Services.

Today, comprehensive CMPs play a pivotal role in achieving this balance by providing solutions that enable privacy compliance, transparency, and ease of use. In addition to such CMPs, Consent Management Services could ease users' consent-related decision fatigue while supporting websites with all required mechanisms to enable and respect user choice.

Complex and evolving ecosystem requirements

The consent ecosystem is inherently complex — across Europe and around the world — involving diverse legal frameworks and, increasingly, policy requirements from large tech platforms. To meet these requirements advanced systems must:

- Clearly guide users through data processing information, user rights, and consent decisions with user-friendly interactions to build trust
- Equip website providers with tools to securely collect, document, manage, and signal granular consents
- Enable ongoing compliance with legal requirements for explicit, informed, and granular consent

Today, website providers mainly solve these challenges by implementing a CMP that enables a high standard of privacy compliance and is acknowledged as a suitable solution by market drivers like the IAB or Google's certified CMP Partner program.

Although key market drivers like the IAB have a standardized framework that mainly focuses on publishers, the overall ecosystem is still missing a robust and scalable standard that solves for transparent data exchanges based on the consent requirements stated above.

Usercentrics recommendations

It is essential to strengthen user-centric solutions to address these challenges in a way that is privacy-compliant and embraces privacy by design. Regulators, website operators, and consent management vendors should prioritize tools that enable users to manage their consent preferences directly within their devices or browsers. Open standards for consent signaling can further enhance user autonomy and transparency, creating an enhanced, user-friendly, and trustworthy environment.

Engaging key stakeholders is another critical step. CMP providers, publishers, browser developers, and regulators must collaborate to shape a unified framework. Especially as data privacy regulation becomes increasingly common globally, complexity is likely to increase for businesses, vendors, and users. Public consultations can serve as a valuable platform for addressing concerns and aligning on practical solutions that work for all parties involved.

Lastly, providing detailed guidelines is imperative, along with clear timelines for review and updates. The German legislature should clarify the technical and legal requirements for Consent Management Services to ensure consistency, practicality, and scalability. This particularly needs to include proper guidance on how these services should be integrated with existing consent management implementations on websites.

Clear guidance will help data controllers navigate the ever-evolving complexities of compliance without introducing unnecessary burdens or risks.

Press contact: *Hannah Sinz, Sr. PR Manager, pr@usercentrics.com*

About Usercentrics

Usercentrics is a global market leader in solutions for data privacy and Privacy-Led Marketing. We believe in creating a healthy balance among data-driven business and Privacy-Led Marketing to unlock sustainable growth for every size of enterprise. Usercentrics Cookiebot CMP is our plug-and-play SaaS, our App CMP handles user consent on mobile apps, and Usercentrics Web CMP serves companies with enterprise-grade custom requirements for unifying consent and data from capture to processing. Helping clients like Daimler Truck AG, ING, and Konica Minolta achieve privacy compliance, Usercentrics is active in 195 countries on more than 2.3 million websites and apps, with 5,400+ resellers, and handles more than 7 billion daily user consents.