SCALED ACCESS

WHITEPAPER

Why Consent Management is a Priority During Your Application Build

Intro

Managing user consent is out in the open. There's no hiding from it.

Although previously considered a box-ticking exercise, GDPR and a growing distrust of data handling has jolted consent management to the foreground, making it a priority during the development and build of your applications.

What Exactly is Consent & GDPR

Consent isn't a new concept.

In its simplest form, it's when one person agrees to another's proposal. Wherever it's found, there are usually significant legal implications tied to it. Especially in areas such as social science research and medicine.

However, it also plays a big role in how organizations manage their customers' personal data.

With regards to service providers and applications, consent is a form of authorization: a person gives a provider permission to access and use their personal data for a certain purpose, "I grant access and use of this part of my data but only under certain conditions."

"Consent is a form of authorization: a person gives a provider permission to access and use their personal data for a certain purpose."

In general, users come across consent when agreeing to a service provider's terms of service because the terms tend to include a section regarding consent over how the provider will use the user's personal data.

The General Data Protection Regulations (GDPR) is an EU framework of law that obliges organizations to implement mechanisms that protect users' data and the choices they make about it.

However, on a deeper level, GDPR surpasses a simple set of laws. It empowers people to take control over how their personal data is shared online, which has largely gone unchecked for decades.

Why is Consent Management So Important

Ultimately, it's all about trust.

People provide so much personal data to organizations and rely on them to protect it. When a person gives consent to a service provider, they enter a legally binding contract that states exactly how their data can be used. They must trust that their personal data will only be accessed and used as agreed.

If the service provider allows the data to be accessed and used under conditions not stipulated to the consent the user gave, trust between the person and organization is broken and can result in significant litigation issues.

Therefore, organizations need consent management to keep them trustworthy. Consent management ensures organizations obtain consent before using personal data, and that the consent choices of the users are stored as proof.

"People provide so much personal data to organizations and rely on them to protect it."

This is where GDPR comes in.

The introduction of GDPR is an opportunity for organizations to regain customer trust by giving them real control over their personal data. Organizations shouldn't see GDPR as a burden, rather a way to strengthen their relationship with the end-users.

Organizations that go beyond the letter of the law, really giving control to their users over their personal data, will have a much stronger, long-lasting relationship with their customers than competitors.

Despite these opportunities, a report released by Eurobarometer[1] (commissioned by the European Commission) on the anniversary of GDPR's implementation in May 2019, found that although consumers may be more privacy-aware, they still don't feel in control of their personal data. The report states only 14% of respondents felt they

[1] https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222

had total control over their data and worryingly, 62% of respondents felt they had partial or no control over the information.

Another report by the UK's Information Commissioner's Office (ICO)[2] in July 2019 found similar results. It noted that one of the biggest changes since 2018 is how people would feel if their information was shared with third parties without their permission. They reported that people are significantly more likely to have negative feelings towards the organization in question.

This report suggests organizations that don't effectively protect their customers' data and consent choices are seriously risking their relationship with them.

So, while both these two reports found that the implementation of GDPR has ensured that organizations have taken concrete actions to protect users' data, and in many cases given them some form of control, there's still a significant way to go before users are in total control over how their data is used.

"Organizations that don't effectively protect their customers' data and consent choices are seriously risking their relationship with them."

Why Consent Management Must Be A Priority During Your Application Build

Organizations can't afford to delay implementing mechanisms to protect their customer's personal data due to the real risks involved with not having proper protection in place.

The scandal that engulfed Cambridge Analytica in 2018 highlights how companies can access and use people's data to influence their decision making when there aren't protective mechanisms in place.

Cambridge Analytica is reported to have influenced elections - like the USA election of 2016 - by acquiring the personal data from Facebook of over 10,000,000 users

[2] https://ico.org.uk/media/about-the-ico/documents/2615515/ico-trust-and-confidence-report-20190626.pdf

without their consent. They then targeted them with highly personalised advertising to influence the vote[3].

Stories like the Cambridge Analytica scandal have proven that managing consent can't be an afterthought during an application build. It must be a priority from its inception.

Until GDPR arrived, organizations dealt with consent management by adding a clickable box to ask for consent. Users clicked the box to accept the service providers' T&Cs.

What happened with it after? That didn't concern organizations.

There was no way for people to withdraw consent, ask for their data to be deleted nor obtain proof about their consent choices. This form of consent management was easy to implement and easy to build. However, it's no longer sufficient in the age of GDPR.

Now that regulations are in place and users are more sensitive to how their data is used, organizations must implement more robust consent management to their applications. Not only do they need to offer easy-to-understand information to users, based on how they plan on using their data, they also need to provide mechanisms that let users control how their data is used.

It's essential organizations not only try to be compliant with the law, but also strive to empower their customers to manage their personal data and consent on a granular level. Consent management needs to move the priority list when building applications.

What Does Solid Consent Management Look Like

In order to give users control over their personal data and ensure access is always subject to consent, organizations need to implement a dynamic form of consent management enabling consent to have a lifecycle.

Organizations need to change their mindset so that when a user gives consent it's just a single event in time – it's a decision the user took at that moment that allowed

---

[3] https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

their data to be accessed and used under specific conditions. Just because a user gave consent once, it doesn't mean they won't change their mind later on.

Organizations must store users' consent choices as a chain of events so they can check if the user continues to give their consent. And, every time an organization wants to access a user's personal data they need to check the users' most recent consent decision.

> **"Organizations need to change their mindset so that when a user gives consent it's just a single event in time. It doesn't mean they won't change their mind later on."**

Furthermore, organizations should provide mechanisms that enable users to control their personal data. They should provide capabilities that let users give, deny and withdraw consent; request their data be permanently deleted; and obtain receipts about their consents as proof.

In regards to organizations that operate across different countries, local laws must be considered - there are stronger privacy laws in Germany compared to Spain, for example. This means that if a user agrees to the terms of service and has given consent in Spain, and then tries to access the same service in Germany, they need to once again agree to the terms of service and give consent. The organization cannot rely on the consent given in Spain.

And, in cases where confidential data is being shared, such as health records or financial information, organizations should add consent as a condition in their access policy. Here the consent management system must feed information into the policy engine so that the access and use of confidential data is always subject to consent. This is an extremely important functional requirement, which needs to be considered during any application build that handles confidential data.

Conclusion

In summary, due to regulations and consumer awareness, organizations need to move consent management towards the top of their priority list. They need to implement a dynamic form of consent management. And, in cases where confidential data is being shared, consent needs to be included as a condition in the access policy.

Access management tools help organizations with this by offering consent management features that manage users' consent choices and their enforcement.

Next-generation access platforms ensure that no consent = no access to personal data. They can also insert consent as a condition in the access policy and take authorization decisions to personal and confidential in real-time.

And, when users request to delete, these tools can push that request to any back-end system that stores their personal data. They can also let users obtain consent receipts so they have proof about their consent choices. Finally, access management tools can ensure that only users that have agreed to the latest terms of service can access the service.

"Next-generation access platforms ensure that no consent = no access to personal data."