usercentrics

Apps: the Wild West of data privacy?

GDPR noncompliance on apps in the EU

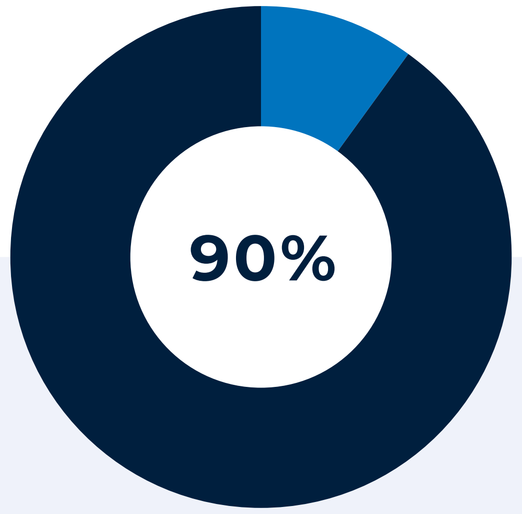
A special report by Usercentrics

Table of contents

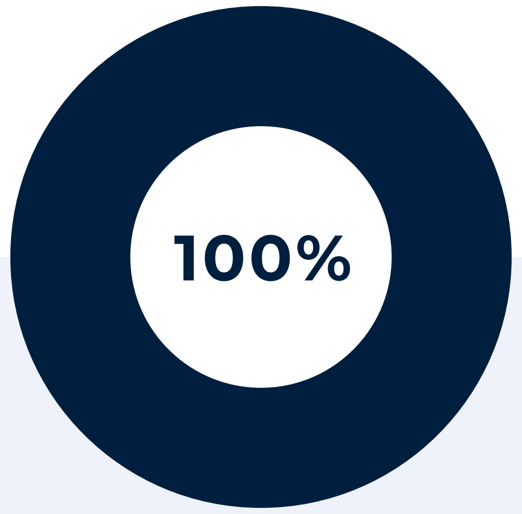
usercentrics

Key insights

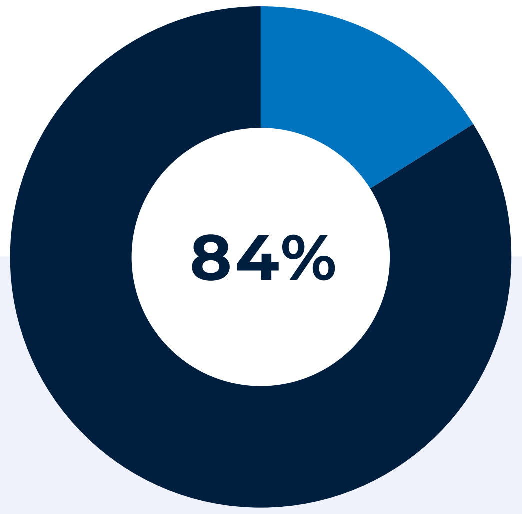
Our special report shows pervasive noncompliance across the apps market in the EU. Users are being tracked and their personal data shared with third parties without their consent – a clear breach of the core provision of the General Data Protection Regulation (GDPR) and ePrivacy Directive.



90% of the 250 apps analyzed by Usercentrics fail to achieve GDPR compliance by tracking users without their consent.



100% noncompliance was found in the category of Gambling apps, the highest level of all categories analyzed.



84% noncompliance was found in the category of Food apps, the lowest level of all categories analyzed.

Most common trackers embedded in apps can process personal data, such as IP addresses, online identifiers and users' location data.

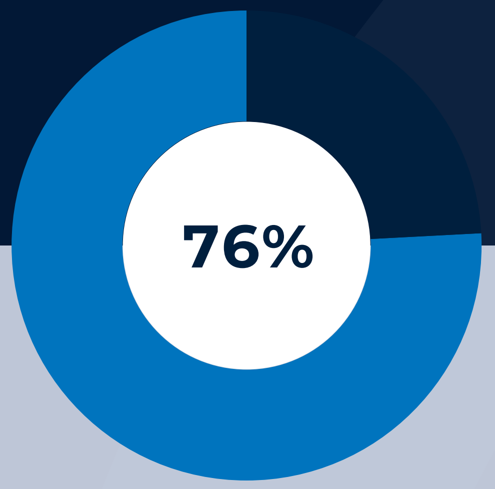
The research was conducted by Usercentrics using Apptopia, a leading app intelligence provider. 250 apps were analyzed in October 2022. See more in Appendix.

Where is the app market today?

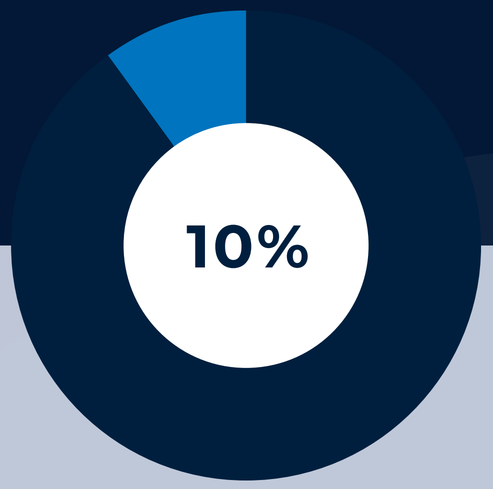
In the four years since the EU's landmark General Data Protection Regulation (GDPR) took effect, the apps market in the EU remains the Wild West of noncompliance. Most people think of "cookie banners on websites" when they hear "GDPR", but the same rules for obtaining end-user consent also apply to apps.

In October 2022, Usercentrics conducted research into the EU apps market. **We found that 90% of the apps we analyzed fail to comply with the GDPR and the ePrivacy Directive because they track personal data from users without their consent.**

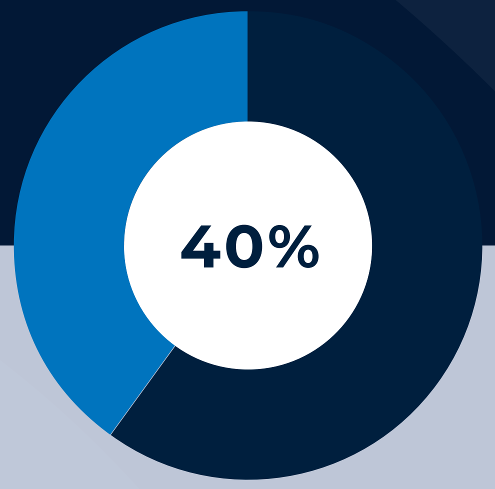
Recent studies paint a similar picture of the apps market today:



A recent study by Appvisory found that **76% of one million apps failed to comply** with the GDPR's requirements to obtain user consent before tracking personal data.



A recent Oxford study found that only **10% of two million apps were GDPR-compliant.** The same study also found that, on average, apps transfer personal data to ten third-party companies.



A recent study by Deloitte and Google found that **40% of 4,150 users reported deleting an app due to data privacy concerns** within a year of the study, highlighting the real consequences for app publishers if they don't respect consent and compliance.

In short, **the apps market in the EU is failing compliance on a major scale, risking both fines and loss of user trust.**

Where will the app market be tomorrow?

It's clear by now that consent and compliance have moved beyond simply being a legal requirement.

A recent study by Ipsos and Google of 20,000 EU consumers shows the **clear benefits of putting the user in control through consent and providing them with a "privacy-first" experience.**

Notably:

- Providing a positive privacy experience can increase the share of brand preference by 43%.
- The negative impact of providing a poor privacy experience is almost as severe as that of a data breach.
- Monetary incentives for sharing data (e.g. offering discounts for opt-ins) may not always have a positive effect and can reduce the level of trust.
- When people trust a brand, they are twice as willing to share their personal data.
- Increasing consumers' feelings of control is the single most impactful way to earn their trust and boost brand preference.

The stark contrast between the undeniable market benefit of being privacy compliant versus the reality of the high level of noncompliance found in our research shows that **the EU apps market is still in a limbo.**

GDPR enforcement is ramping up and more and more websites are transitioning to a more sustainable and user-centric approach to growth and revenue by including end-user consent at the core of their operations.

Mobile applications also have to follow the GDPR and the ePrivacy Directive requirements by asking their users for consent before allowing third-party tracking technologies to collect their data.

But respecting user consent won't harm apps' business, as publishers might think. On the contrary, it will **most likely become a great benefit for the app,** as more and more current studies show.

Consent choice will not only build the foundation of a more trustful digital exchange, but could ultimately be the key to protect app monetization opportunities and bring higher revenue.

It's a win-win situation benefitting both the user and the app publisher.

usercentrics

What can mobile app companies do now?

Getting consent from end-users in compliance with the EU's GDPR and the ePrivacy Directive should be a **major priority** for app companies in order to avoid legal fines, loss of valuable consumer trust and brand reputation.

Here's a checklist for making your app privacy compliant:

- ☑ **Audit the technology your mobile app is using,** i.e. identify all SDKs installed in your app(s) and document the scope of each third-party technology and what data it accesses.
- ☑ **Explain what the tracking technologies are doing and why (make it a part of your comprehensive privacy policy),** e.g. inform users about what data is collected, how and why.
- ☑ **Let users know you are applying tracking technologies** (e.g. trackers included in SDKs) via a consent banner, and remember to show the banner before any SDK starts collecting data!
- ☑ **Obtain valid user consent as per the GDPR,** i.e. consent needs to be explicit, informed, documented, granular, freely given, and easy to withdraw for the end user.
- ☑ **Enable users to access your service even if they do not consent for tracking technologies to use their data,** e.g. if a user refuses data processing, they can still use the app, but only essential tracking technologies needed for the app to function can be activated.
- ☑ **Collect and process data only after obtaining valid consent,** i.e. ensure that SDKs are not loaded until the end user has given consent.
- ☑ **Document and store consent,** e.g. in case of an audit by data protection authorities (DPAs).
- ☑ **Opting out must be at any time as easy and simple as opting in.**
- ☑ **After opt-out, ensure that no further data is collected or forwarded.**

Ensuring compliance with the EU's GDPR and ePrivacy Directive can be time-consuming and technically difficult. This is why **Consent Management Platforms (CMPs)** have quickly become one of the most popular tools to help companies get data privacy compliance right.

Today, plug-and-play SDKs enable quick integration of a CMP into apps, which makes the entire process of ensuring GDPR and ePrivacy compliance easy and automatic.

If you already have a Consent Management Platform (CMP) integrated on your app, make sure it is compliant with the GDPR requirements by following the above checklist.

One of the most valuable benefits of having a CMP on your app is the automation it brings to your compliance requirements: **it makes compliance easier** so you can focus on your core business.

By having a CMP on your app, you can reduce the legal complexity of compliance while making sure that your app is always ahead with state-of-the-art consent technology.

But most importantly, you will **build trust with your users and help make our digital ecosystems more sustainable** for everyone involved.

If you have any questions about your app privacy compliance, contact one of our experts at apps@usercentrics.com

*These statements do not constitute legal advice. If you have any legal questions, you should align with the relevant data protection authority or a lawyer. The implementation of a data protection-compliant CMP is ultimately at the discretion of the respective data protection officer or legal department.

usercentrics

External resources

Apptopia

Study by Appvisory

Study by University of Oxford

Study by Ipsos and Google

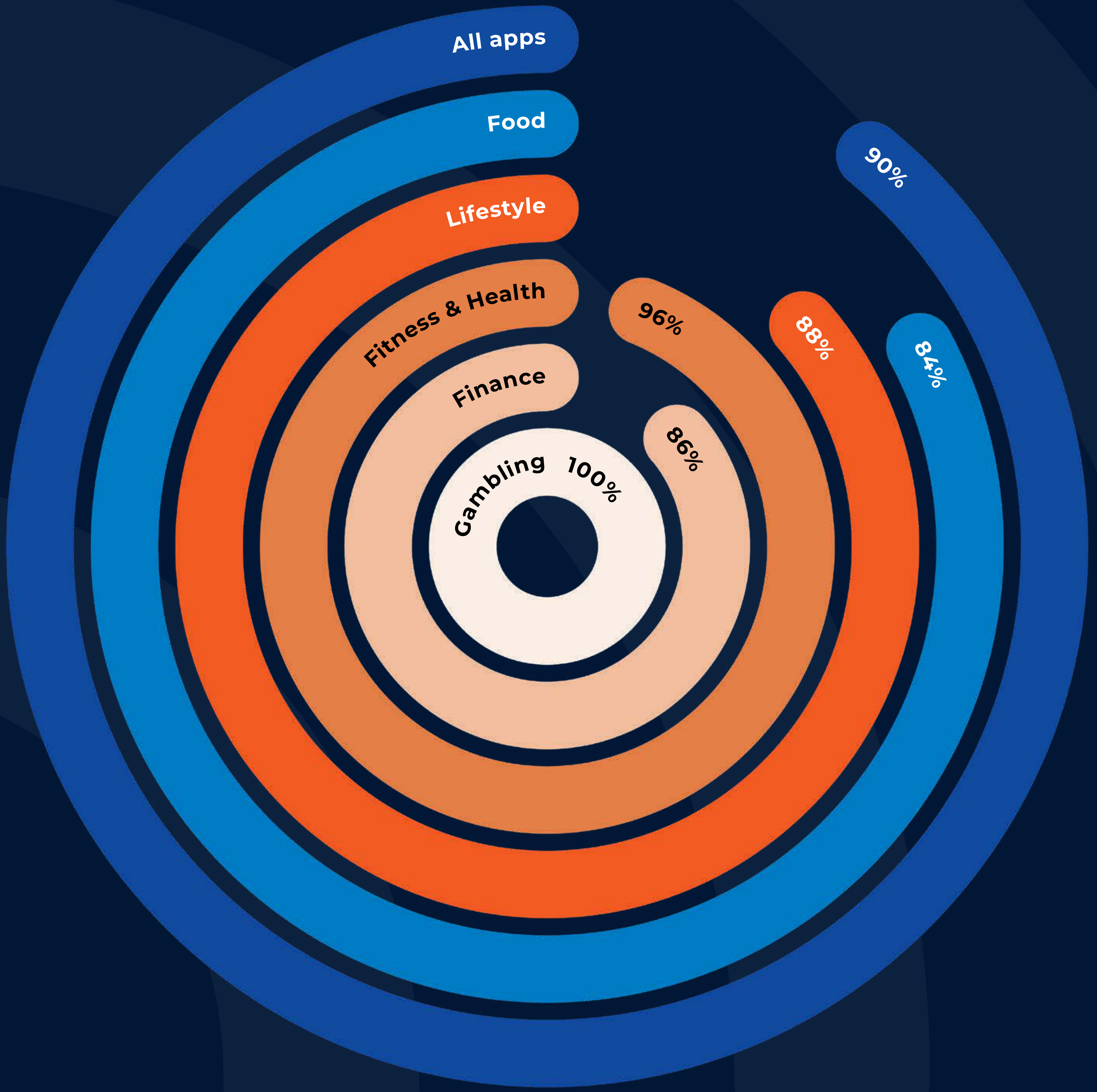
Study by Deloitte and Google

usercentrics

Appendix

Table of app noncompliance levels

Category	Average level of noncompliance for each category (%)
All apps	90
Food	84
Lifestyle	88
Fitness & Health	96
Finance	86
Gambling	100



usercentrics

Methodology

To conduct the research, Usercentrics used the “SDK intelligence insights” tool from Apptopia, a leading app competitive intelligence provider.

250 apps were selected across five popular categories (Food, Lifestyle, Fitness & Health, Finance and Gambling) that all have tracking technologies embedded, processing personal data from users via trackers contained in the SDKs.

For each category, a total of 50 apps were selected, all of which:

- have third-party trackers installed for the purpose of analytics, attribution, monetization and/or marketing
- have users in the EU
- have a minimum 50,000 daily active users

The criteria were selected following the consent requirements in the GDPR and ePrivacy Directive and the way they have been interpreted and implemented by data protection authorities across the EU.

Each app was downloaded on devices inside the EU to check if a Consent Management Platform (CMP) was installed to enable us – as users – to reject the embedded tracking technologies and keep our personal data private.

If the app had a consent banner installed, it was checked to see whether it complied with legal standards, i.e. did the consent banner offer “accept” and “decline” buttons, list all the tracking technologies in use on the app, and was the purpose of tracking described to the user.

About Usercentrics

Usercentrics is a global market leader in the field of Consent Management Platforms (CMP). We enable businesses to collect, manage and document user consents on websites and apps in order to achieve full compliance with global privacy regulations while facilitating high consent rates and building trust with their customers. Usercentrics believes in creating a healthy balance between data privacy and data-driven business, delivering solutions for every size of enterprise. Cookiebot CMP is our plug-and-play SaaS, our App CMP handles user consent on mobile apps, and Usercentrics CMP serves companies with enterprise-grade custom requirements for unifying consent and data from capture to processing. Usercentrics is active in more than 180 countries, with 2000+ resellers, and handles more than 100 million daily user consents.

Benefits of using the Usercentrics Apps CMP (SDK) on your app:

- **Ease of use** - a plug-and-play SDK that automates the legal complexities of compliance
- **High customizability** - built to fit any domain and design seamlessly to enhance customer trust for optimized opt-ins
- **State-of-the-art tech** - unrivaled technology tested and optimized robustly to ensure no negative influence on the app performance
- **A/B testing capabilities** - obtain as much trust as possible from your app users and test the message that works best with A/B testing tools
- **Analytics** - keep track of the performance of the SDK via granular analytics with full data export capabilities.

Book a meeting with us and find out how to reduce noncompliance risks such as fines, and boost consumer confidence in your app.

Visit usercentrics.com to learn more.

usercentrics