Usercentrics CEO Mischa Rürup talks all things privacy with Cybernews

"Companies should make it easy for users to decide on the collection and handling of their personal data"

Munich, April 7, 2022 - While governments worldwide issue legislations to regulate and protect user data, many websites find ways to obtain personal information in violation of established laws.
The pandemic has certainly pushed everyone to improve their cybersecurity posture, either by learning how to spot malicious emails or by implementing tools to protect their computers from online threats. Nevertheless, many casual Internet users don't even realize that their data is being collected and analyzed for various purposes. While that might not seem like a big deal, website visitors are often forced to jump through hoops just to refuse to supply their data. Our guest today strongly believes that it shouldn't be the case.
To talk about user consent, we sat down with Mischa Rürup, the CEO of Usercentrics. Mischa emphasizes that providing transparency and user control are the key elements to building trust for companies.

Tell us how it all began. What was the idea behind Usercentrics?
Successful marketing needs good data quality. However, the collection of such data also requires the consent of each user and should be transparent. Aware that marketing needs to rethink third-party data in favor of first-party data, I started with the idea for Usercentrics after selling my previous company intelliAd.

Can you tell us a little bit about what you do? Why is using a consent management platform important?
There is a strong shift in consumer concerns and businesses' priorities in the direction of user trust. Citizens are increasingly demanding more clarity into – and control over – how their information is being used. Privacy, technology, MarTech, and diverse frameworks can be hard to understand, and on the customer side, this could lead to quitting the relationship with a company. So if companies want users' data, they need to create trust, and trust starts with transparency, clarity, and user control over that data.
A consent management solution enables companies to collect, manage, and document user consent on digital channels such as websites or apps while maintaining high consent rates for data processing. In this way, website owners and companies give users the opportunity to object to the tracking of certain characteristics, such as location, when visiting websites and interacting with apps — in each case in accordance with the data protection regulations here.

You recently joined forces with Cookiebot CMP. What does that mean for Usercentrics?
The ambition of our newly formed joint venture with Cookiebot CMP is to become a category-defining leader for consent management solutions. With the merger, our product variety for consent solutions has become a lot wider, and we can serve customers' needs from every segment. Cookiebot CMP is our plug-and-play SaaS for smaller businesses and organizations, 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.

Have you noticed any new types of cyber threats emerge during the pandemic?
The increasing online dependency of people around the world also creates new opportunities for cybercrime. An Interpol report from 2020 shows an increase in malware and ransomware, as well as a rise in phishing scams and fraud online. Ad fraud has now become a billion-dollar business. One factor driving this development is the aggressive use of bots, which in turn are responsible for fake and low-quality traffic and lead to wasted advertising spend on the marketer's side. Together with our partner fraud0, we, therefore, help marketers optimize their ad spend using intelligent software.

In your opinion, what are threat actors usually trying to gain by taking advantage of user data?
Threat actors may have different motives, for example, political, economic, or social. Some may want to highlight human rights, show a corporation its vulnerabilities, or go after companies or branches whose ideologies they do not agree with. These could be assigned to hacktivism. Cybercriminals, though, may want to profit from stealing data in a financial way, by selling personal data on underground black markets.

Some experts believe that keeping up to date with data privacy trends and requirements could be the selling point for customers. Can you share some tips for businesses looking to make their privacy policy user-friendly?
Companies should make it easy for users to decide on the collection and handling of their personal data and create the greatest possible transparency. The shift towards user privacy, transparency, and 'consent first' will continue in 2022. Companies and website operators will not be able to aggregate data without the consent of their users. The acceptance rate is a door opener to marketing success, and the right implementation of a CMP can lead to trust and a successful customer relationship. Transparency on what is being tracked, the right wording, and design are the key drivers here.

Keeping up with privacy policy requirements can sometimes be complicated.
Which details are often overlooked by organizations?
In terms of a consent management platform, companies should avoid the following points when implementing their cookie banner:

- No reject button in the first layer
- Pre-set to opt-in sliders or boxes
- No granular selection option
- Implied consent by continued navigation
- Hidden imprint or privacy policy

An example: If a store operator keeps track of how many users they've had in a day, that's okay. But if they profile users, display other products, and adjust prices accordingly, they always need consent. And this must be given knowingly, transparently, and in a way that's informed in advance. The user needs the right of

choice and must also have equal ability to refuse. Many operators still make the mistake of not granting this right.

What data privacy issues would you like to see solved in the next few years?
We see an increased number of fines because of GDPR compliance failures. Since the GDPR took effect in May 2018, we've seen over 800 fines issued across the European Economic Area (EEA) and the UK. GDPR fines have ramped up significantly in recent months. The sum total of GDPR fines levied in Q3 2021 hit nearly €1 billion — 20 times greater than the totals for Q1 and Q2 2021 combined. These numbers underline the necessity of solutions such as Consent Management Platforms that save users' privacy by giving them back sovereignty, freedom of choice, and their right to information.

Would you like to share what the future holds for Usercentrics?
We now have more than 220 employees in 10 countries and recently added Donna Dror as our new Chief Revenue Officer. Most recently, she was responsible for Similarweb's Go-To-Market (GTM) strategy while driving growth across all customer segments and company sizes. She also had a key role in leading the company to its successful IPO in May 2021. The appointment is also intended to accelerate revenue growth in core markets. Our ambition is to define the category of consent management and to bring about standardization for consent management. It is important for Europe that strong local players help to maintain data sovereignty against other legalities in order to keep data transfers to third countries transparent or to exclude them if necessary.

Read the original interview on Cybernews here.