GDPR:
An Evolution, Not a Revolution

Disclaimer
This article does not constitute legal advice, nor is this information intended to create or rise to the level of an attorney-client relationship. You should seek professional legal advice where appropriate.

Introduction

The European GDPR (General Data Privacy Regulation) replaces the existing 1995 Data Protection Directive, harmonizing the various data privacy laws that exist across all 28 EU member states.

Since our founding in Europe in 2005, Criteo has had a strong record of ensuring our technology has high levels of data privacy and security while helping our clients meet shopper expectations with advertising that is personalized and relevant. As a global company with major offices in multiple EU countries, working with thousands of advertising clients and publisher partners whose customers and users are based within the European Union, we are accustomed to dealing with country-level requirements across the world.

It is Criteo's view that consistency and certainty around privacy and data protection is a win-win for businesses and the consumers they serve. It is for this reason that Criteo is committed to GDPR compliance and why we are working with clients and partners who are subject to the new regulations, offering them support and sharing best practices for them to best manage the transition. Criteo is ready to tackle the GDPR challenge and expects limited impact of the new regulation, if any, on our clients' and partners' ability to work with Criteo.

Overall this regulatory update is an evolution that aligns data protection policies across the EU member states while providing consistent application and enforcement by local Data Protection Authorities (DPAs) in each EU member state. The objectives of the GDPR are clear:

- Modernize the legal system to protect personal data in an era of globalization and technological innovation.
- Strengthen individual rights while reducing administrative burdens to ensure a free flow of personal data within the EU.
- Bring clarity and coherence to personal data protection rules and ensure consistent application and effective implementation across the EU.

criteo

What is personal data as defined by the GDPR?

GDPR protects the privacy of EU citizens and applies to all companies collecting or processing personal data on individuals in the European Union, even if that company is not established in the European Union. A significant confirmation for the digital marketing industry is that the GDPR applies to any information concerning an identified or identifiable natural person, and this includes online identifiers such as Cookie IDs and Mobile Advertising IDs. These online identifiers are now explicitly mentioned in the definition of personal data, which confirms the broad interpretation of personal data already applied under EU laws.

It is important to note that these online identifiers were already considered personal data by many European DPAs. This is not a new requirement for Criteo as we only collect non-sensitive personal data in the form of cookies. Therefore, we are very familiar with those distinctions, and we have well-established methods for compliance while delivering performance to our clients.

There are common questions that businesses ask about when it comes to data management. Firstly, what is “Personal Data” as covered by the GDPR? Personal data is anything that contains:

- *Directly identifying information* such as a person’s name, phone number, etc.
- *Pseudonymous data or non-directly identifying information*, which does not allow the direct identification of users but allows the singling out of individual behaviors (for instance to serve the right ad to the right user at the right moment).

The GDPR establishes a clear distinction between directly identifying information and pseudonymous data. It encourages the use of pseudonymous information and expressly provides that “the application of pseudonymization to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations”[1].

The data that Criteo collects and processes for its clients and partners does not qualify as sensitive data as defined by the GDPR. How is “sensitive data” defined? It is any data that reveals:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health or a natural person’s sex life and/or sexual orientation

[1] *General Data Protection Regulation – Whereas (28)*

Criteo collects and processes for its clients and partners pseudonymous online identifiers linked to browsing events. When working with Criteo, our clients and partners only need access to pseudonymous data that does not allow the direct identification of users. This pseudonymous data includes:

- Cookie IDs
- Hashed email addresses
- Mobile Advertising IDs
- Any other technical identifiers that allow Criteo to single out individual behavior without directly identifying the individuals

What is the difference between unambiguous and explicit consent?

GDPR also establishes a clear distinction between valid unambiguous consent and explicit consent of the individual. While both forms of consent require a positive act on the part of the individual, explicit consent implies a strict interpretation of what constitutes this positive action from the user (e.g. checking a box, clicking on an "I accept" button). This applies solely to sensitive personal data such as race, religion, sexual orientation, political affiliation, and health status. Importantly, online identifiers alone (e.g. cookies) are categorized as non-sensitive personal data, therefore an explicit opt-in consent is not required.

What does this mean and how does it apply to your business? The GDPR provides six legal bases for data collection and data processing in Europe. So, if you're collecting personal data of any kind, there must be a legal basis for it. The six legal bases are:

- The vital interest of the individual
- The public interest
- Contractual necessity
- Compliance with legal obligations
- Valid unambiguous consent of the individual
- Legitimate interest of the data controller

It is important to note that all of these six legal bases carry the same legal value, which means that they are self-sufficient and exclusive from one another. For businesses in the marketing or digital marketing industry, or those who collect data for the purposes of marketing, the two legal bases that could be applicable are: 1) valid unambiguous consent of the individual, and 2) legitimate interest of the data controller.

Our view at Criteo is that valid unambiguous consent is the most applicable basis for our clients and partners who collect personal data, including online identifiers.

Collecting consent for cookie retargeting has been the rule in Europe since 2009, and with the adoption of the ePrivacy Directive (a.k.a., the cookie directive). Criteo's clients and publisher partners who do not process sensitive data, but rather work with data related to web browsing, shopping intent and shopping history linked to pseudonymous technical identifiers are already used to complying with such requirements.

We anticipate that the rules on valid unambiguous consent will be an evolution of the already very protective laws that exist in Europe. The CNIL (French Data Protection Authority, and supervisory authority of Criteo) provides the same recommendations for collecting users' consent[2] and recommends several easy-to-use technical solutions for website administrators to leverage.

The conditions required by the GDPR for a valid unambiguous consent are very similar if not identical to the conditions already detailed by the Working Party of the Article 29 in a past opinion[3]:

> ***Specific information:*** *"To be valid, consent must be specific and based on appropriate information provided to the individual. In other words, blanket consent without specifying the exact purpose of the data processing is not acceptable."*
>
> ***Timing:*** *"As a general rule, consent has to be given before the data processing starts."*
>
> ***Active choice****: "Consent must be unambiguous. Therefore, the procedure to seek and give consent must leave no doubt as to the data subject's intention. There are in principle no limits to the form consent can take. However, for consent to be valid it should be an active indication of the user's wishes. The minimum expression of an indication could be any kind of signal, sufficiently clear to be capable of indicating a data subject's wishes, and to be understandable by the data controller."*
>
> ***Freely given****: "Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent."*

How does the "legitimate interest of the data controller" apply?

For the interest to be legitimate, the purpose of the data processing needs to be reasonably expected by users. The processing of personal data for direct marketing purposes may be regarded as and carried out as a legitimate interest. However, this legitimate interest cannot override the fundamental privacy rights of users, and appropriate security measures must be implemented to mitigate potential risks to users' privacy.

---

[2] *CNIL: "Cookies how to make my website compliant"* *https://www.cnil.fr/fr/cookies-comment-mettre-mon-site-web-en-conformite*
[3] *Working Party of the Article 29 – 2013 Guidance on obtaining consent for cookies:* *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf*

The basic standards that must be met before attempting to claim a legitimate interest are:

- An explanation of what data is being collected, the specific purpose for which such data is collected, as well as how that affects a browser's online experience. For example:

  "Our [website/app] uses cookies/advertising IDs for the purpose of advertising. This enables us to show our advertisements to visitors who are interested in our products on partner websites and apps. Re-targeting technologies use your cookies or advertising IDs and display advertisements based on your past browsing behavior. To read more and/or oppose to their services, please refer to their privacy policy listed below." [Add link to your partner's privacy policy. e.g. Criteo's privacy policy is at: http://www.criteo.com/privacy/]

- A way for users to control their experience, including an opt-out choice, that is easy to use and access, with language that explains how that will affect a browser's ad experience.
- Easy access to a privacy policy, as well as information on any industry privacy standards or commitments your business has adopted. For example: Criteo is a member of the Network Advertising Initiative.

There are some key questions every business must be able to answer in order establish whether there is a legitimate interest:

- What is the purpose of the operation?
- Is it necessary to meet one or more specific organizational objectives?
- Does the GDPR or other legislation specifically identify the processing activity as being a legitimate activity, subject to the completion of a balancing test and positive outcome?
- Is there another way of achieving the objective?
- Would the individual expect the processing activity to take place?
- What is the nature of the data to be processed? Does data of this nature have any special protections under GDPR?
- Would the processing limit or undermine the rights of individuals?
- Is a fair processing notice provided to the individual? If so, how? Are they sufficiently clear and up front regarding the purposes of the processing?

What is Criteo's approach to data privacy?

At Criteo privacy is our guiding principle. We go to great lengths to protect and process data in compliance with applicable Privacy and Data Protection Laws. This includes the GDPR.

Our product teams develop every feature with privacy in mind; it's the cornerstone of Privacy by Design, a sophisticated approach that ensures an industry-leading level of safety for marketers and consumers alike.

Privacy by Design is Criteo's long-standing practice and commitment to ensuring industry-leading privacy, security and safety for consumers and marketers. Key elements include:

- As required by the GDPR, we have had a designated Data Privacy Officer since 2013 along with a team of privacy experts.
- These experts are part of the Product and R&D organization. They perform ongoing Privacy Impact Assessments to monitor potential risks during the product lifecycle and proactively mitigate those risks.
- The Data Privacy team delivers company-wide privacy training, enforces codes of conduct, and is integral to ensuring that we build best-in-class products and services.
- We regularly review and document our internal policies, amend existing privacy policies as necessary, and enforce these policies with our partners and vendors.

Strict Security Measures

As required by GDPR, Criteo already maintains strict security measures when collecting consumer data from our clients. We utilize modern pseudonymous methods, including MD5 and SHA-256 double-hashing processes, that can be considered best practices under the GDPR, and never willingly store any directly identifying personal information about individual consumers. For compliance and optimal performance, we store EU consumer data within the European data center that is physically closest to them.

Ad Choices: A Focus on Consumer Rights and Control

Criteo has long recognized the need to balance relevant advertising experiences with privacy expectations while empowering consumers to control their experiences. Consumers understand this trade off. This is why Criteo committed to the Ad Choices program as early as from 2008 to allow consumers, with a single click, to see exactly where Criteo is using data, and how we protect their privacy. When a consumer chooses to opt-out, we immediately stop tracking and retargeting. We then remove all identifiers from their browsers, making it impossible to target them in the future. Per EU data protection regulations, collected consumer-level data is only kept for 13 months.

Industry Leadership: Investing in Standards and Certifications

Criteo has an extensive number of certifications already in place that are reviewed annually by governing and standards bodies, including:

- Network Advertising Initiative Standards
- IAB Europe

- Digital Advertising Alliance Self-Regulatory Principles for Online Behavioral Advertising
- European Digital Advertising Alliance's Self-Regulatory Principles
- Digital Advertising Alliance of Canada's Self-Regulatory Principles
- TrustArc Trusted Data Collection Certification

What are your responsibilities?

GDPR requires companies that retrieve data from within EU countries to comply with the new regulations involving data protection and data security. This also applies to global enterprises based outside the EU if they target an EU audience. GDPR can benefit your business by consolidating the various data privacy laws that exist across all 28 EU member states. To that end, Criteo is helping our clients and partners make sure they know what steps to take to become GDPR compliant themselves.
Here are a few best practices to consider in your compliance journey:

Designate a Data Protection Officer (DPO)

GDPR requires the designation of a Data Protection Officer (DPO) in any case where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of sensitive data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health conditions or sexual orientation, etc.) or personal data relating to criminal convictions and offences.

This role would monitor and manage both the data and operations necessary by the regulations. Additionally, the DPO would have to prove they have no conflicts of interest in terms of data protection for your organization.

Make Sure your DPO is Ready to Collaborate

Your employees are your best bet to help you understand what your company's current data protection policies might be lacking. Make sure the DPO, legal, compliance and IT teams have a clear and comprehensive understanding of your company's data practices. They should work together to help you create a compliant process by which your organization collects data in a collaborative manner.

Provide transparency and control

The information and consent language you provide to your customers should be as clear and transparent as possible. Your website should make it explicitly clear exactly what your customers are opting in and out of, and exactly what types of data they are providing to you. This is a major factor of being compliant with GDPR.

Put data governance first

You must implement a Privacy Impact Assessment (PIA) process for all processing that might risk the rights of individuals. Additionally, your company must be able to explain how the personal data it collects are being collected, used, or even edited, and have processes in place that allow EU citizens to easily provide, review and/or reject the data. The GDPR states it's mandatory to ensure your company's data infrastructure maintains a record of processing activities and provides visibility into the compliance of your practices.

Monitor employee and contractor access to data

You must establish strict employee authorization policies that limit access to data and ensure privacy. These policies should be continuously updated to reflect your company needs and monitored for breaches, especially regarding data transfers. In Chapter V of GDPR, transfer destinations outside the EU must also meet the same protection and governance conditions as organizations within the EU.

GDPR requirements are stringent, and being wholly prepared for it will require much more than ticking boxes off a checklist with vendors you work with. But GDPR, as we see it, can only be a good thing for businesses and consumers alike as it provides consistency and certainty around privacy and data-protection.

How does GDPR affect Criteo's solutions?

At the core of our technology is the Criteo Shopper Graph which gathers the shopping behavioral data collected from across the Criteo Commerce Marketing Ecosystem and fuels our solutions for commerce marketing.

Criteo Shopper Graph is broken down into three trusted data collectives that combine three key types of data on shoppers:

- Pseudonymous technical identifiers
- Interests for the product and services of our customers
- Measurement statistics on the performance of our services

We continuously ensure that this data is limited to what is strictly necessary for our services in order to deliver relevant information to shoppers on the products they want at the right place, at the right moment and with the right messages. For example:

- Criteo uses robust data hashing algorithms to ensure that no directly identifying information of shoppers is stored on our systems.

- We never store any data for longer than strictly necessary and respect the recommendations of EU Data Protection Authorities on cookies and digital advertising.
- Provide user-friendly choice mechanisms: all Criteo products have the same easy opt-out process accessible in all our ads and privacy policy. We are also a registered member of the NAI, DAA and IAB Europe opt-out platforms that allow customer to oppose to targeted advertising.
- Consumers can easily opt-out of Criteo's service by clicking on the Ad Choices link on the ad, and learn about why they are seeing the ad. Once a user opts-out of Criteo services, all collected information will be deleted or made irretrievable, including any user data that you have on-boarded as part of a Criteo campaign.

Conclusion

As businesses in the digital marketing industry update their practices to comply with GDPR, it is important to remember that EU citizens are well aware of targeted advertising, understand the identifiers that drive it, and expect to see ads that are relevant. Criteo partnered with IPSOS[4] to field a consumer survey to understand the expectations of EU users and how they relate to targeted online advertising. We surveyed 3,000 Internet users, ranging in age from 16 to 65 in France, UK and Spain, establishing a representative demographic sample across gender, age, region, and income level.

Specifically, we found that:

- 90% of Internet users are aware of behavioral retargeting
- 68% are aware that cookies enable targeted advertising
- 75% expect to be served ads that match their interest
- 73% would rather see relevant ads than pay an additional fee to avoid seeing ads

Criteo believes protecting consumers' privacy and being clear and transparent about business practices is of primary importance to all. When customers understand exactly how their information is being used and are given control over their personal browsing data, it strengthens their trust in and loyalty to a company.

We're well-aware and prepared for the implications of the GDPR, and look forward to helping our clients and partners understand our products and services better. By working together to understand and prepare for the regulations, we can all look forward to business as usual.

[4] *Criteo-IPSOS Study, 2017*