# MARKETING DATA LITERACY

## A ROADMAP OF PERSONAL DATA IN THE DIGITAL ECOSYSTEM

March 2025

## Foreword: The Journey of Personal Data in the Digital Ecosystem

In the digital world, every online action leaves traces. To provide insight into these data ecosystems and how personal data is processed by different 'players', we follow a day in the life of Peter.

Peter, like many of us, starts his morning with a quick glance at his phone. As he visits his favorite sports site and browses social media, he leaves behind – often without realizing it – a trail of data that organizations use to provide him with a tailored digital experience.

### From First-Party to Third-Party Data: A Look Behind the Scenes

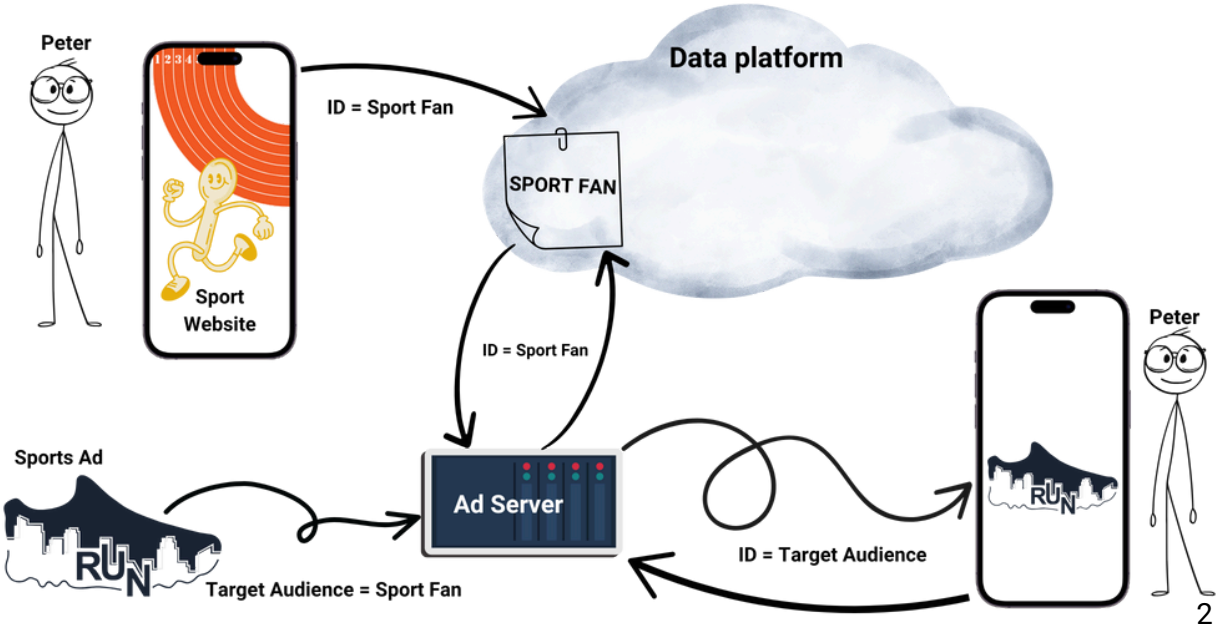
At its first stop, the news site collects first-party data, such as Peter's interests and preferences, which it uses to personalize his experience. At the same time, however, third-party data is also collected by partners and advertising companies, who further analyze his activity and combine it with other information to build a profile that extends beyond the news site itself. This data creates a broader understanding of Peter's interests, leading to ads that are sometimes surprisingly accurate.

### Consent and Tracking in a Data-Driven Ecosystem

As Peter continues browsing, a consent pop-up appears—the familiar question of whether he accepts cookies. Often without much thought, he clicks "Accept," making his data available for a variety of purposes, from personalized ads to in-depth analytics that further shape his digital experience. What he may not fully realize is that by doing this, he is making his data available to a network of parties who will continue to track his online behavior.

By the time Peter finishes his morning, he – like many others – has unknowingly participated in a complex data ecosystem. His activities are stored, analyzed, and used to both personalize his experience and generate valuable insights for businesses.

In the following chapters of this whitepaper, we will explore in detail the different stages that personal data like Peter's goes through and the role of the players within this ecosystem.



# INDEX

# PETERS COLLECTED AND MANAGED DATA FROM AN ADVERTISER PERSPECTIVE

Every interaction Peter has with a site or ad provides valuable information, which is carefully captured in a complex ecosystem. This system is designed to refine marketing efforts, personalize content, and optimize the conversion path . Peter's data is collected in various ways and through various techniques.

For example, when Peter clicks on an ad or browses products, the advertiser captures **first-party data** such as click behavior, session duration, and product interests. This data forms the basis for real-time personalization, dynamically adapting content and offers to Peter's interests. In addition to first-party data, **third-party data** is also collected, from external sources such as data exchanges, DSPs , and social media APIs . This third-party data adds cross-platform insights that provide a broader profile of Peter's interests, allowing advertisers to approach him in an even more relevant way.

### Technical Analysis: Data Types

To collect and use data effectively, advertisers must distinguish between different data types, each with their own sources, usage rights and applications:

**1. First-party data**

- **Definition:** Data collected directly by the advertiser, for example through Peters interactions on their own website or app.
- **Examples:** Click behavior, purchase history, and completed forms such as emails.
- **Advantages:** High relevance and accuracy, because the data comes directly from the user. Also easy to manage within privacy rules, because the data is in-house.
- **Challenges:** It often requires technology investment (such as CRM systems) to collect and manage this data, and its reach is limited to existing customers.

**2. Second-party data**

- **Definition:** First-party data from a partner organization, shared on the basis of a direct collaboration.
- **Examples:** Data shared between a retailer and a brand.
- **Pros:** Reliable and high quality, as it comes from a trusted source with a similar target audience.
- **Challenges:** Depends on partnerships, which requires legal agreements and technical integrations. Also, privacy of shared data must be carefully handled.

**3. Third-party data**

- **Definition:** Data collected by a third party with no direct relationship with the user.
- **Examples:** Demographic data purchased through data brokers, or audience segments from advertising networks.
- **Benefits:** Large scale and helps reach new audiences.
- **Challenges:** Increased privacy concerns and reduced accuracy due to distance from the source, and regulatory restrictions such as GDPR.

## Data Collection Tools: Cookies and Tags

Data is collected using two main techniques: cookies and tags . A simple analogy will help you understand the difference between cookies and tags. Imagine Peter is on a pub crawl:

At the first pub he gets a stamp on his wrist (cookie) that records his visit. When he orders drinks, he receives a receipt (tag) with details of his order. At each pub he visits he gets a new receipt, but the stamp remains the same and identifies him when he returns to previous pubs. This allows the pubs to recognize him, and the bouncer can see from the receipts that Peter is a frequent customer, which gives him extra benefits.

### Summary:

- A **cookie** (stamp) remembers who Peter is and when he has been before.
- A **tag** (voucher) records details about his actions during his visit.

### A more technical description of both techniques:

- **Tags are pieces of:** Track user behavior and interactions, such as with Google Analytics.
  - **Conversion tags:** Measure the effectiveness of ads by tracking conversions.
  - **Remarketing tags:** Target users with ads after they visit a site, such as with the Facebook Pixel.
  - **Tag Management Systems (TMS):** Tools like Google Tag Manager help manage and implement tags without directly modifying the website code.

- **Cookies** are small text files placed on Peter's device by the website to store information about his session and preferences.
  - **Different types of cookies:**
    - **Functional and performance cookies:** These remember sessions and preferences to improve the user experience.
    - **Advertising and tracking cookies:** Contain first-party and third-party cookies that are necessary for personalization and targeting.
    - **Security cookies:** Strengthen security, such as 'HTTP- only ' cookies.
    - **Historical cookies:** Such as Flash cookies and zombie cookies, which are becoming less common.
  - **Most used cookies:**
    - **First-party cookies:** Set by the website itself to manage user preferences and sessions.
    - **Third-party cookies:** Set by third parties to track user behaviour across multiple sites and build a profile.

### Are all cookies bad and will they be phased out in the future?

Cookies are often the subject of privacy discussions , particularly in the context of GDPR and other legislation. While some cookies are essential to a smooth online experience, such as first-party cookies that remember preferences and login statuses , third-party cookies have been heavily criticized for their ability to track users across multiple websites.

Third-party cookies, which are mainly used by advertising and tracking services, are often seen as invasive, because they create a detailed profile of user activities. For this reason, browsers such as Safari and Firefox block these cookies by default. Google Chrome has indicated that it will not abolish third-party cookies after all.

While third-party cookies may be disappearing, this does not mean the end of tracking. Alternative techniques such as browser fingerprinting and device tracking are gaining ground. These methods use unique characteristics of devices and browsers to track users, raising new questions about privacy.

### Is all that actually allowed?

In the next chapter we will delve deeper into the laws and regulations surrounding the collection and use of data such as Peter's. Because how far can advertisers actually go in collecting and using personal data?

# 2

# PRIVACY AND CONSENT MECHANISMS IN THE DIGITAL LANDSCAPE

While advertisers focus on collecting and exploiting data like Peter's, there are specific rights that protect Peter as a user. At the same time, companies must adhere to laws and regulations to ensure that individuals' data is managed in a secure and transparent manner. This chapter describes Peter's rights under current law and the frameworks that advertisers must adhere to.

### Peter's rights: consent and Privacy by Default

The introduction of the GDPR (General Data Protection Regulation) in 2018 has significantly strengthened the privacy rights of individuals like Peter. It gives him the following rights in relation to his data:

- **Consent:** Before personal data can be processed, explicit consent must be obtained. This means that advertisers cannot hide consent in long, complex terms and conditions. Consent must be freely given, specific and informed, and Peter can withdraw it at any time.
- **Privacy by Default:** Under the GDPR, privacy is the default setting. This means that services and products must be set up with the highest privacy protection by default, without the user having to set anything up. Data is collected in a limited way and used only for necessary purposes, and companies must ensure secure data storage.

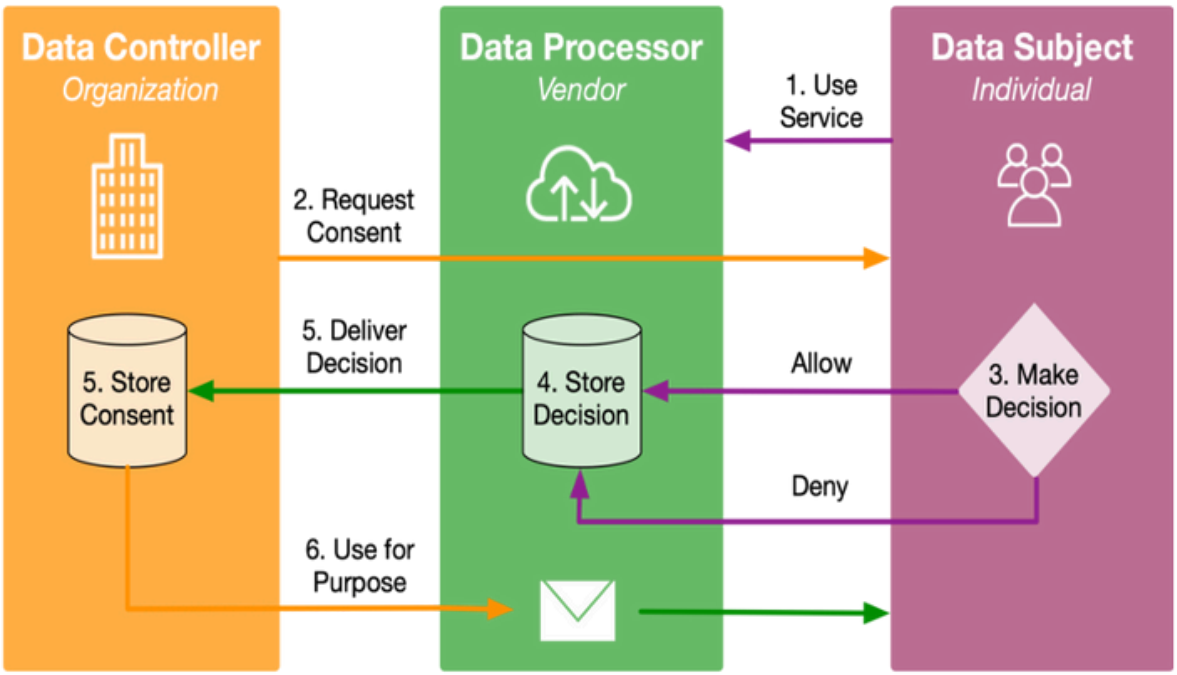
### In addition to these basic rights, Peter also has other rights, including:

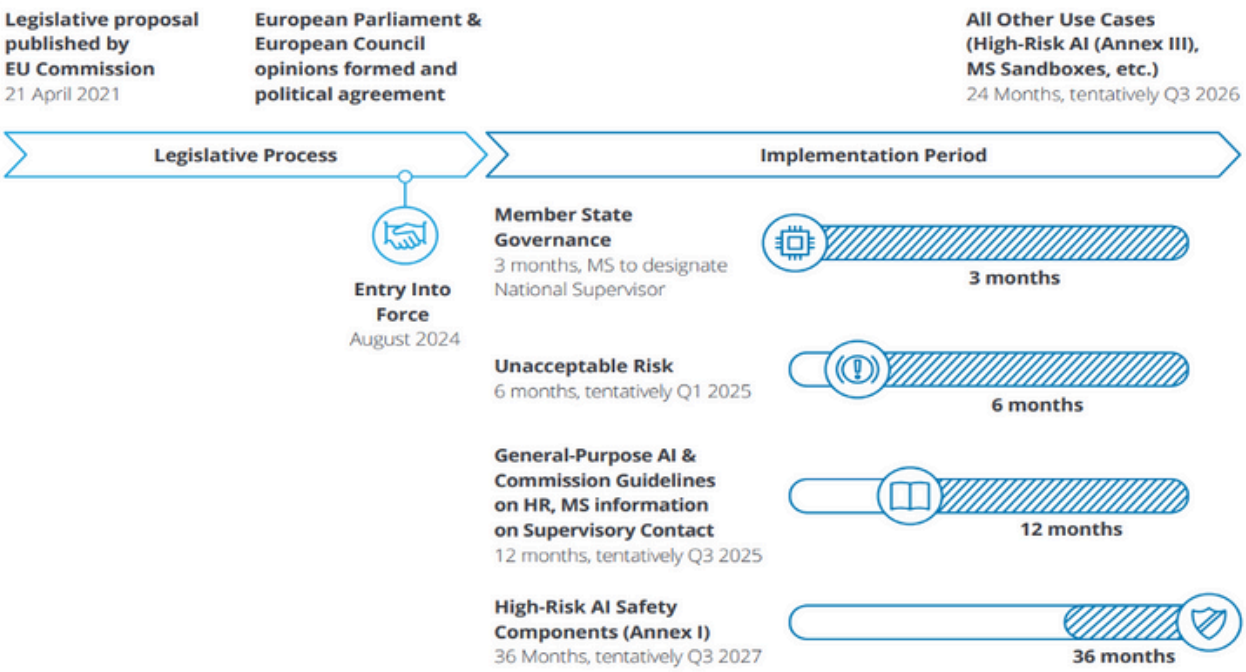
- **The right to be forgotten:** This allows Peter to request that his data be deleted.
- **The right to data portability:** This enables Peter to transfer his data to another service provider.
- **The right to access:** Peter can request which data has been collected and how it is used.

### Legislation and regulations for companies

Advertisers and other companies that work with data must comply with multiple regulations to ensure that the rights of users like Peter are respected. The most important legal frameworks are:

- **GDPR (2018):** This European regulation sets strict requirements for the collection, storage and processing of personal data. Companies operating within the EU or processing data of EU citizens must adhere to principles such as lawfulness, fairness, transparency and data minimization. GDPR forces companies to be transparent about their data practices, gives users control over their own data and sets high fines for infringements.
- **Digital Services Act (DSA, 2022):** The DSA focuses on regulating online platforms and aims to create a safe and transparent digital landscape. Among other things, it regulates the responsibility of platforms to tackle illegal content and harmful practices, which further supports the privacy and security of users.
- **Digital Markets Act (DMA):** The DMA specifically targets large online platforms (the "gatekeepers") to promote fair competition and prevent abuse of market power.
- **Artificial Intelligence Act (AI Act):** Although this law focuses on AI systems, it is relevant to companies that use AI for data collection and analysis. The AI Act requires organizations to handle AI ethically and limits the use of AI that poses a high risk to user privacy.




## What happens once Peter gives permission?

When Peter gives consent via a Consent Management Platform (CMP) on a website or app, such as by clicking “I agree,” he initiates a series of data processing activities. While this may seem like a simple action, Peter is actually giving permission for the website or service to collect specific information about him. Depending on the platform, this information can range from his IP address and location to his browsing behavior and personal preferences.

Websites often use tracking technologies such as cookies and tags to monitor Peter's activity across websites and app sessions. With his consent, this data can be collected and used for a variety of purposes, such as improving the user experience or showing targeted advertising. In some cases, Peter's data is even shared with third parties, such as advertising networks (e.g. Meta, Spotify, Google) or analytics providers (e.g. Google, Adobe, Comscore).

### Corporate Responsibility

Once consent is granted, the responsibility lies with the organization to manage Peter's data responsibly. Under the GDPR, companies must:

- **clear and legitimate grounds** for the dataprocessing and inform users of the specific purposes of data collection;
- **transparency** to maintain user trust by clearly communicating what data is collected and why;
- **protective measures,** such as encryption and anonymisation , to secure personal data and minimise the risk of breaches.

It is important to note that consent is not a blank approval. Peter retains the right to withdraw his consent at any time. Once he does so, the organisation is obligated to stop processing his data and delete it, if requested. Furthermore, GDPR states that companies may not reduce the quality of their service to users who refuse consent, giving Peter more control over his privacy.

### Privacy and Compliance - Transparency and Consent

The GDPR and other regulations emphasize the importance of transparency and compliance for advertisers and platforms. To stay in line with this legislation, advertisers must:

- **Provide transparency:** users must always be clearly and comprehensibly informed about what data is collected, for what purpose and how long it is stored;
- **Obtain consent:** the use of data, especially through cookies and tracking methods, requires explicit consent from the user, which must be able to be modified or withdrawn at any time;
- **Ensuring data quality and security:** Using high- quality first-party data is typically the most privacy-friendly option, but companies must ensure that all collected data is stored securely and used only for the specified purposes.

# EVERYONE'S ROLE IN THE FUTURE

The information we've covered so far illustrates the importance of Peter and other users maintaining control over their data, and the responsibilities companies have to ensure privacy. At its core, this comes down to a "data trade-off": the implicit or explicit agreement between users and service providers, where users share their personal information in exchange for access to services, features, or content.

This data trade-off is the foundation of the modern internet economy. Access to many of the free services we use every day — social media, search engines, news sites — is often funded by targeted advertising that relies on collecting user data. The question remains, however, whether users like Peter are fully aware of the data they are giving up, and whether the value they get in return is commensurate with the price they pay in terms of privacy.

While data collection offers many benefits, such as personalized experiences and ease of use, it always comes with privacy risks. Data breaches, unauthorized data sharing, and the creation of detailed user profiles can erode user trust. Regulations like GDPR attempt to redress this balance by strengthening user rights and holding companies accountable for transparency and ethical data management.

The challenge going forward is clear: advertisers and service providers must continue to find a way to use data in an ethically responsible way, while always protecting user privacy. In this chapter, we look ahead and explore the steps companies can take to strike this balance and maintain the trust of their users.

### The Advertiser's Role

Advertisers must continue to be diligent about various technical aspects of data management. Data privacy and compliance are non-negotiable. While Peter may have quickly agreed to cookie tracking, advertisers must ensure they adhere to privacy frameworks such as GDPR and CCPA. This includes maintaining transparency around data usage and implementing mechanisms for data subject rights, such as withdrawing consent or deleting data.

Another crucial element is data integration and hygiene. Advertisers often have to deal with multiple data sources. Proper integration via CDPs (Customer Data Platforms) or DMPs (Data Management Platforms) ensures that Peter's data is stored in a unique profile, minimizing silos and maximizing the accuracy of personalization algorithms.

Finally, frequency capping and cross- channel optimization are essential to prevent ad fatigue. With advanced programmatic ad serving and tracking across channels, advertisers need to apply intelligent limits on ad exposure while ensuring Peter experiences a balanced, cohesive story. Overexposure to identical ads can lead to diminishing returns, so implementing AI-driven frequency management is key to maintaining engagement without oversaturation.

## The Role of Government

In the wake of GDPR, we've seen a wave of new regulations emerge across the globe, from California's CCPA to Brazil's LGPD, all emphasizing the need for greater transparency and control over personal data. Technological innovation, particularly in areas like artificial intelligence (AI) and machine learning, will play a significant role in shaping the future of privacy. These technologies rely heavily on data to function, raising questions about how to maintain privacy in an age of big data. Privacy-enhancing technologies (PET's), such as differential privacy and (homomorphic) encryption, will likely become more prominent as companies attempt to balance data usability with user privacy.

At the same time, we can expect a continued push for greater user sovereignty over data. Concepts such as data ownership and data portability are likely to gain traction, allowing individuals to decide how their data is used and monetized.

Governments could incentivize and subsidize schools to teach children early on the concept of digital tracking and the results of privacy-conscious behavior. Also, government monitoring and enforcement is still developing, and we have not yet seen how this will develop in the future. There is not much transparency and clarity about how governments monitor compliance with data protection laws and impose fines for violations.

## Peter's role

Finally, let's not forget that all these efforts by organizations and governments are worthless without Peter's own awareness and willingness to exercise his data privacy rights. While companies and legislators can provide the framework, the ultimate choice lies with users like Peter. By being aware of what he shares and carefully considering his options, he can actively contribute to a responsible data culture.

When it comes to using data, user responsibility also plays a role. Users like Peter need to be aware of the value of their data and the implications of sharing it. Consumers often give away information without being aware of the potential consequences. For example, Peter might decide to share his data with a weather app in exchange for free access. As long as he knows that this choice means he can be targeted again later, this is a fair trade-off. However, if Peter would rather pay for an ad-free experience, this should be accessible at a reasonable price. The tricky part here is that there is no clear standard for what a fair price is, as this depends on market, location and other factors.

## Conclusion

While the path forward is uncertain, one thing is clear: privacy and consent mechanisms will remain central to discussions about the future of the internet. Organizations that successfully strike the right balance between data-driven innovation and user privacy will be better positioned to thrive in the digital age. Governments with foresight in education, regulation, and transparency in enforcing those rules will lead the way. Ultimately, the future of data governance will require a collaborative effort, with advertisers, governments, and users working together to create a digital environment that is both valuable and respectful.