

Netcomm Cookie Handbook: a resilient market towards a new balance



Introduction

- 1.1. General context and background information:
Phasing-out third-party cookies
- 1.2. Cookies: their features and functioning



The economic, social and regulatory framework of reference

- 2.1. The growth of the digital economy, the development of the market and the key role played by personal data
- 2.2. The regulatory framework of reference



2023: How to manage the transition period

- 3.1. Preserve
- 3.2. Inform
- 3.3. Secure



Case histories: Companies' direct experience

- 4.1. Cookieless: the way to a shared solution on privacy – by Webranking
- 4.2. Study: Pierre et Vacances. The Omnichannel handling of users' personal data – by DIDOMI



Conclusions What's next?

Preface

Digital advertising is going through a moment of deep change linked to the new Cookieless scenario. As a representative of digital commerce, and in order to support the market during this delicate phase of transition, Netcomm has sponsored the ***“Netcomm Cookie Handbook: a resilient market towards a new balance”*** to help companies understand the change that is occurring and guide them through the range of possible solutions that the market will, in time, make available.

Considering the subject's current relevance and ongoing development, this handbook is being prepared in digital format. This will allow it to be periodically revised to highlight any regulatory changes and new market developments, thus always keeping it up to date.

This handbook has a dedicated section on the regulatory framework and a practical section, developed with the help of industry member companies that have kindly shared their knowledge, skills and experience with us. All companies are welcome to contribute to this project's development by sharing thoughts and solutions to take on this important transition together.

Introduction



1.1. General context and background information: Phasing-out third-party cookies



Digital marketing is one of the most flourishing and dynamic sectors of the digital economy. Over the past years the sector has seen a radical transformation of its business models as a result of a series of factors that have enabled this very change, among which: the proliferation of smartphones, social networks and the Internet of Things, Cloud services and, of course, Artificial Intelligence. All this has been taking place in an ever-increasingly complex, interconnected and physically integrated digital environment.

Google's announcement that it will phase-out third-party cookies on Chrome starting from 2023 marks a significant change for the digital marketing sector and follows a number of other similar initiatives available on the market and adopted by other browsers too. One need only think, for example, of Apple's Safari or Mozilla's Firefox, whose default settings impede third-party cookies.

The changes we are witnessing are a clear sign of the ever-increasing general attention paid to issues of personal data protection and security.

Every innovation provides for new opportunities if an awareness of the underlying processes is acquired, together with an understanding of the reasons, and that the developments made possible by the very same technological innovation are seized.

1.2. Cookies: their features and functioning

Cookies, also known as “web markers” or “persistent identifiers”, are small blocks of text that a website transmits to a user’s terminal – tablet, smartphone, intelligent device (Internet of Things) – during its use, when browsing the web. These cookies allow data, preferences and customised settings to be saved and this information is then stored on the device and recalled at every subsequent access to enable the website to “recognise” the user and adapt to his/her requirements and/or preferences. More specifically, cookies make it possible to: *i)* facilitate the authentication process (login) to a website (“authentication cookies”); *ii)* save internet browsing data (such as language, duration of browsing session, preferences, user configurations, etc.); *iii)* save content data, such as data relating to e-commerce baskets or carts; *iv)* track browsing activity (including cross-site and cross-point) for statistical, communication and profiling purposes, such as, for example, to customise e-mail marketing offers (so-called “*behavioural advertising*”); *v)* to create “Buyer Persona” profiles for online advertising campaigns.

Different types of cookies exist.

Firstly, cookies may be classified according to their function, thereby distinguishing technical cookies from profiling ones.

Technical cookies enable websites to function properly and are used to improve user browsing experience by recalling saved information (such as language settings). This goal is also ensured by “analytics” cookies, which collect information in an aggregate fashion for statistical and analytical purposes to improve a website’s user-experience. These cookies are therefore helpful for a website owner in order to define the website’s functioning parameters and improve the website.

In addition, there are non-technical ones; in this category falls “profiling” cookies which aimed to target users for commercial purposes by tracking their internet browsing experience across websites and touch points. Non-technical cookies identify and save device IPs, record the browsing map within a website, cross-site connections and behaviour following the receipt of newsletters, and save consumer choices, habits, etc.

Linking all this information on preferences and behaviour is extremely valuable to companies; as mentioned earlier, it enables them to know their users, classify them, build their “Buyer Persona” profiles and offer targeted advertising, discounts and promotions that are in line with their preferences. However, these activities can affect people’s privacy.

Therefore, in terms of end-purpose, whereas technical cookies support user browsing experience and allow website owners to improve website performance, profiling cookies help website owners improve their relationship with visitors (by offering advertising that is in line with user preferences, attracting their interest and therefore their loyalty) and are useful to visitors in order to receive information that is aligned with their interests.



Another difference concerns the subjective aspect of cookies, distinguishing first-party cookies (or so-called *publisher site ones*) from third-party cookies (different web server ones). In the first case, the text file is created by the web server, it is readable only within its domain, and allows the browsing experience to be customised through user recognition thanks to stored data. In the second case, third-party cookies are created by the web server of a third-party website, which is different from the transmitting website (visited by the user), where the code is readable also outside the domain, across a number of potentially unlimited websites, enabling cross-site tracking.

This feature has turned third-party cookies into the central tool for commercial user tracking and the creation of targeted advertising campaigns that are ever-increasingly in line with user preferences.

Concluding, if, on the one hand, cookies are a valuable tool for companies to develop behavioural advertising based on effectiveness and better conversion rates, on the other hand, their widespread use by websites (e-commerce sites, social media sites, etc.) has increased the attention paid to user privacy risks by users, lawmakers and supervising authorities. This is especially true for profiling cookies that have commercial purposes. Indeed, profiling cookies are viewed as being more disruptive to the personal sphere of users, especially when they are used for systems such as Marketing Automation.

The economic, social and regulatory framework of reference



2.1. The growth of the digital economy, the development of the market and the key role played by personal data



The development and growth of the Internet and of new technologies, especially Artificial Intelligence solutions, have, over the years, contributed to the widespread and increasing use of digital services in everyday life and to changes in user online behaviour. From e-commerce to home banking services, and from public administration services to social networks, the users' relational model has changed radically over a very short number of years.

Today's Information society is therefore characterised by the "technology and data" binomial, where the key role played by data – the true and proper engine of the digital economy – catalyses attention, putting issues of personal data protection at the centre of the political, social and regulatory debate.

Technological development, hyper-connections and increasing computing power generate a significant and potentially infinite volume of information (Big Data) which makes it possible to collect detailed indicators on individual people to create ever-increasingly accurate digital profiles. However, in certain conditions, such individual profiles may affect the rights and freedoms of individuals and their ability to make truly independent consumer decisions.

If, on the one hand, these aspects represent potentially extraordinary opportunities for businesses, on the other hand they raise questions about their possible implications and effects on the personal lives of people, thereby attracting (as we have already mentioned) the interest of law enforcing Authorities as well as greater user sensitivity.

Indeed, over the past years, we have been witnessing a continuous and increasing push towards a delicate point of balance between technological and industrial development to secure economic growth and prosperity on the one hand and respect of the fundamental rights and freedoms of individuals on the other.

These general conditions hold true for cookies too. Indeed, over time, cookies and other tracking tools have played an increasingly central role in business thanks to their ability of acquiring user information needed for profiling and clustering. This has raised questions on the role and importance of cookies and on the will that they be governed in an increasingly detailed fashion in order to meet the escalating requirements of user personal data protection.

2.2. The regulatory framework

Cookies fall within the scope of electronic communications, governed by European Parliament and Council Directive 2002/58/EC dated 12 July 2002, known as ePrivacy Directive, subsequently changed by Directive 2009/136/EC dated 25 November 2009.

Generally speaking, the directive provides that the website's administrator must disclose how the company handles and protect users' information. Companies should provide information how the website will collect and maintain users' personal data. Furthermore, it is required users' prior consent before any installation on their devices (by an explicit action).

Since the directive does not specifically define how this information should be released, the member states established their procedure applicable to manage it. Hence, each country has adopted different regulations and standards.

The European Legislator has launched an update of the regulatory framework to effectively fit the challenges new Internet and the IoT technologies adoption created.

The new ePrivacy Regulation will replace the existing directive and introduce significant changes in strategic sectors of the overall digital economy, from online advertising to direct marketing and the IoT. This will have a notable impact on all businesses in the digital communications field, including social network companies, web companies, telecommunication companies and providers, software developers and suppliers, etc.

In Italy, the directive was transposed by means of article 122 of Legislative Decree 196/2003 (Privacy Code)¹ which requires that in case of technical cookies, the data controller disclose information only without asking for the data subject' consent, considering the technical nature of the cookie).

Conversely, if non-technical cookies are used, and especially if profiling ones are used, the data controller must provide suitable information on the purpose and use of the data and has to obtain the user's prior consent to the cookies' installation (we shall soon return to the practical application of these rules).

Italian regulations are integrated alongside with the Italian Data Protection Authority, whose rulings have clarified the scope of application and made it possible to address existing interpretative doubts and shortfalls, especially in terms of requirements concerning information disclosure, and users' consent acquisition.

Firstly, [Provision no. 229 dated 8 May 2014 "Identification of simplified disclosure processes and the acquisition of Cookie use consent"](#), provided significant indications on information disclosure. The provision established that the information must be issued in two levels: a simplified and immediately visible one (using banners, for example) and a more in-depth one, easily reachable via hyperlinks. The data protection Authority subsequently introduced additional provisions through its [FAQ of 3 December 2014 on "Information disclosure and Cookie use consent"](#), clarifying form of 6 May 2015 ["Cookies and Privacy: on the side of users"](#), and, lastly, recent Guidelines on cookies and other tracking tools of 10 June 2021.

The regulatory framework must also consider Regulation EU/679/2016 (*General Data Protection Regulation*). This regulation addresses the challenges created by technological development and globalization that have exponentially increased data collection, sharing and dissemination on a global scale. This requires to regulate the phenomena through a regulatory framework more in line with the new emerging requirements.

The Regulation addresses Cookies in recital 30², when it mentions identifiers and other online identity tools. Pursuant to the GDPR, Cookies are "pseudonymous data"³ e.g., personal data for which identifying elements are replaced by other information that can potentially allow the person to be identified. For Cookies, therefore, the Code enables (univocal) identification of the device used to browse the web and, therefore, potentially, the identification of the person using the device – which is why it is relevant in terms of profiling.

The relation between the two disciplines, the Regulation and the ePrivacy directive, is governed by the "genus-to-species" principle. The Regulation provides a general framework on the protection of a person's private sphere, including user devices used to browse the web (e.g., tablets or smartphones).

1 – Legislative Decree 196/2003, <<1. Storage and archiving of information in the terminal device of a contracting party or user, or access to previously stored information, is only permitted if said contracting party or user has given his/her consent after having been informed by simplified procedure. This does not prohibit any technical storage or access to previously stored information if the unique purpose of this information is to transmit a communication over an electronic communication network, or when strictly necessary by the service provider to provide a service that has been explicitly requested by the contracting party. For determining the simplified procedures mentioned in the first clause, the Data Protection Authority ("Garante") shall consider any proposals submitted by the most representative national consumer associations and associations of the economic sectors involved. This shall also be done to make sure that the methods which are used ensure contracting parties' and users' actual awareness. 2. For the purpose of expressing the consent of paragraph 1, specific user-friendly computer programme or device configurations can be used. 2-bis. Except for that provided for in paragraph 1, the use of an electronic communication network to access information stored on a contracting party's or user's terminal device to store information or monitor the user's activity is prohibited. >>

2. Reg. 679/2016, Recital 30 << Natural persons may be associated with online identifiers provided by their devices, applications, tools, and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, particularly when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them>>

3. Reg. 679/2016, Recital 26 << The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. (..)>>.

The Cookie Law, which is the Special Law, integrates and clarifies the general norms of the Regulation specifically in terms of information obtained and recorded on the device during interpersonal communications in accordance with article 95 of the Regulation. Therefore, if there is any conflict between the two norms, the Special Law prevails over the general one (of the Regulation).

This means that when website data controllers decide to use identifiers, they are required to respect the Cookie Law (and, where necessary, have an obligation to acquire prior consent). When the data controllers aim to process the information through analyses and profiling they have to respect GDPR rules as such activities fall within the scope of the Regulation.

Specifically, if a data controller uses non-technical cookies (or other tracking tools) he has to provide the user with all the information needed inform him about the data processing, including the purpose of the processing and the type of identifiers used. In accordance with Article 4.11, Article 7 and Recital 32 of Regulation 679/2016⁴, the data controller also needs to collect the data subject's **prior consent before the cookies' are installed on the user's terminal device**. Such consent needs to be **"free, specific, informed and unambiguous"** and **revocable** at any time.

The prevalence of the Special Law (Cookie Law) over the Regulation also means that – except for those cases provided for by the law itself – the only suitable legal basis that legitimises the installation of cookies on a user's terminal device is the user's consent (data subject). Therefore, the Legitimate Interest pursued by the controller (or by a third party) (Article 6.1, letter f of the Regulation) invoked by many operators should not be considered suitable for the purpose of data processing validity.⁵

Collecting and handling of consents calls for considerable attention if, for example, a data controller aims to use Marketing Automation systems. In such a case, data controllers have to set up their marketing campaigns properly to make sure that users/data subjects are given all necessary information in a proper and timely way.

Indeed, through cookies, Marketing Automation systems are able to identify users and



4 - In relation to consent: Article 4 -Definitions- par.11 «consent of the data subject»: any free, specific, informed and unambiguous expression of consent by the data subject, through which such party manifests its assent, by means of an unambiguous statement or positive action, that its personal data be subject to processing >>; in Article 7 and Whereas 32: "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information company services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."

monitoring their behaviour even before they have expressed their consent by visiting the website (this happens, for example, when the IP of the browsing device is saved). The data controller is therefore able to intercept the behaviour of users from when the users / data subjects receive the newsletter and to understand their reaction and browsing actions before they land on the website and give (or don't give) their consent. Thus, It is clear how important it is that users be informed of the activities that the data controller intends to carry out with their data (the purposes) and the consequences of their consent.

The main concerns lie in these two aspects: methods of communicating information and consent. many website have used invasive cookie policy that are limiting navigation (e.i. interfaces that completely block access to website content thereby acting more as obstacles than as sources of information (so called "cookie walls"). Such elements interfere with the browsing experience and prompt users to accept – thereby expressing their consent – merely as an instinctive reaction to overcome content barriers, without them having any real awareness of the consequences of their action. Clearly, such a "take it or leave it" mechanism defies the very principles described above.

The European Data Protection Board (EDPB) published [*Guidelines 05/2020*](#) on consent under Regulation 2016/679⁶ providing additional clarifications on the matter at a European level. In general terms, among the different aspects addressed, the Guidelines underline that banners or other restrictive and/or blocking solutions (such as cookie walls) should be prohibited unless, notwithstanding the use of such systems, the data processing controller allows access to website content without installing cookies – something that needs verifying on a case-by-case basis. Moreover, the Guidelines explain that swiping or scrolling through a webpage cannot be considered suitable mechanisms to indicate a user's acknowledged to the installation of cookies and actual understanding of the consequences deriving from cookie tracking.

On 9th July, 2021, the Italian DPA published the aforementioned new "*Guidelines on Cookies and other tracking tools*"⁷ which comes at the end of a consultation launched in December 2020 and six months of analysis.

Through these new guidelines the Authority aligned its previous provisions on the topic with those of the European Data Protection Board (Guidelines 5/2020 on Consent), highlighting a number of key aspects for the proper use of identifiers.

The Italian DPA confirms the prohibition of "cookie walls" as set forth above. As for consent acquisition through swiping and scrolling, the Authority underlined how merely "scrolling down" cannot be deemed appropriate consent (and therefore consent to the installation of cookies); for this to be valid, such an action must necessarily occur within a complex process, structured by design and default, capable of demonstrating the valid expression of the user's choice.

The Italian Data Protection Authority established the need to acquire the data subject's prior consent if online tracking activity is carried out with cookies and other tracking tools (in accordance with article 122 Privacy Code and Articles 4.11 and 7 of the Regulation).

5 - Compare with the *Cookie Guidelines and other tracking tools* dated 10 June 2021.

6 - *Guidelines 05/2020*, adopted on 4 May 2020, updating the previous indications set by WP29 adopted on 10 April 2018, which were in turn updated by the European Data Protection Board (hereinafter EDPB) on 25 May 2018

The Authority points out the need to ensure the user's right to revoke consent (Article 7.3) and the obligation to provide data subjects with required information (in accordance with articles 12, 13 and 14 of the Regulation), disclosing the use and type of cookies, as well as any other tracking tools, and distinguishing between technical, analytics and profiling tools. This information may be provided in short form, at a first level, and in a more in-depth form, at a second level, also through different channels and processes, to be in line with technological changes, different solutions, and available instruments. Moreover, data subjects are to be given the possibility of expressing their consent (or refusal) to the installation of cookies by means of a single action or granular selection of preferences.

Further, regarding consent, it must be pointed out that a data processing controller who uses identifiers for non-technical reasons must be able to demonstrate that prior and informed data subject consent has been obtained (free, unambiguous and informed). Unless there are changes in a user's access conditions to the website (e.g. after user's deletion of cookies) consent shall not have to be sought from the user every single time the website is accessed.

Finally, as highlighted by the Data Protection Authority in Guidelines 2021, one of the most important requirements is the general principle of Privacy by design and privacy by default (article 25 of the Regulation) be applied. This principle requires that, during the "processes" design, the Data Controller assess predefined default settings aimed at safeguarding data protection and data collection activity that is compliant with the rules. These principles must necessarily apply to Cookies as well.

In summary, given the existing regulatory framework set forth above, the **website administrator must always disclose information on the type of cookies installed**, on the end-purpose of such different cookie (technical, analytics, etc.); **if non-technical cookies are installed, data controller must acquire the data subject's prior specific consent** in compliance with the aforementioned requirements, namely: *i)* provided freely, *ii)* after having received information on the use to be made of the data collected, *iii)* these information must be provided specifically for each different purpose, and therefore for each different Cookie type installed, *iv)* provided unambiguously, which is to say by means of a positive voluntary and conscious action (and not, for example, through one requiring mere scrolling). The website administrator needs to be able to demonstrate the acquisition of the consent at all times, and data subjects must have the possibility to revoke their consent at all times.

The users are informed by means of a banner (first "level" information) of suitable size for the device used and the banner must not prevent access to the website's content. Banner shall have a command (marked, for example, with an X) that enables it to be closed without giving generalized consent to cookies and other profiling tools, maintaining the default settings. The banner needs to have a hyperlink to more in-depth information on the data processing, including the type of cookies, their end-purpose, the consequences of consent, the duration of data storage periods and, above all, the possibility for the user to refuse consent for each type of cookie.

Box summarising current regulations

Valid acquisition of consent:

- First level information (banner or other tool that informs the user about the use of cookies and of their purpose, with a hyperlink to more in-depth information).
- More in-depth second level information (describes type, duration and purpose in greater detail).
- Possibility of expressing consent to the installation of cookies in a granular form for each purpose.
- Active action by user: consent is validly acquired if it arises from an active action of approval or refusal by the user to the installation of cookies for each cookie purpose.
- Consent is not validly obtained when it is a result of mere scrolling, continued swiping or browsing, confirming pre-flagged boxes.
- Consent is not validly obtained when it is a result of mere scrolling, continued swiping or browsing, confirming pre-flagged boxes (except for specific cases set out in the Guidelines)
- Possibility of closing the information banner (by using, for example, a command marked with an "X") and default access to the website's content (without, therefore, the installation of non-technical cookies). The user must retain the right to refuse the installation of profiling cookies without surrendering the right to browse the website.

The website owner must be able to demonstrate valid acquisition of consent by storing system logs. Such logs need to be stored for a period set by the website owner according to the principle of accountability. This principle needs to take into account the owner's needs as well as the rights of the users. These rules apply to all devices (smartphones, tablets, etc.) that enable the installation of identifiers, and does not therefore apply to cookies alone.

2023: How to manage the transition period

3.1. General context and background information: Phasing-out third-party cookies – by Google



Based on what has been set forth above, the overall picture is somewhat complex.

On the one hand we have an increasing sensitivity towards issues of personal data protection and, more generally, compliance with regulations, whilst on the other hand we have third-party cookies, one of the most important and strategic resources in online advertising, which will soon be phased-out. This leaves us with having to manage a treasure trove of information and to find new solutions to two conflicting needs: protection of the user-data party and growth of commercial activity.

**What activities and actions could companies pursue to
manage this transition phase?**

How to manage the transition

What:

This section highlights the market implications and impacts of privacy related changes and the consequent actions required to manage this change.

Introduction

“The growth of online businesses has come with an increased demand for privacy from users. Searches for ‘online privacy’ have grown by more than 50% year over year when comparing April until June 2020 to the same time last year. The number of people online increases and protection of their privacy is critical. Brands that are able to win people’s trust will be able to grow”.

Matt Brittin, Google

[READ THE ARTICLE HERE AND DOWNLOAD THE MARKETER AND PUBLISHER PLAYBOOK](#)

Google recommends this framework to manage the transition:

Preserve



Use existing measurement to satisfy the privacy expectations of people and lawmakers.

Inform



Close gaps in observable data by using additional signals that allow for a comprehensive modelling.

Secure



Invest in technology for privacy protection.

Resources:

[B2B BEST PRACTICES HERE](#)

Preserve

What:

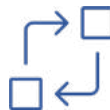
Management of the current infrastructure based on cookies: in the short-term the market will still depend on third-party cookies, therefore it is necessary to pay a high level of attention to compliance. This is particularly true now, following the regulatory changes introduced by personal data protection Authorities.

1. Maximization of 1st party data and durable tagging

[Read article](#)



Build direct relationships



Offer value in exchange for data



Boost advertising performance

1st party data Transparency

[Read article](#)

Unblock 1st party data potential

[Read article](#)

Seek BCG 1st party data

[Read article](#)

[Read article](#)

2. Use of 3rd party Cookies in line with the existing regulation

Inform

What:

Data will become increasingly less observable. We will therefore need to close data gaps through modelling, for which we will need additional signals.

1. Measure conversions in a way that respects user consent


[Read article](#)
[Read article](#)

2. Google Consent Mode

“Without cookies, advertisers experience a gap in their measurement and lose visibility into user paths on their site. They are no longer able to directly tie users’ ad interactions to conversions, whether the users are repeat visitors or whether those users have arrived from paid or organic traffic sources. To help close this gap, we’re introducing conversion modelling through Consent Mode. This will help marketers preserve online measurement capabilities, using a privacy-first approach.”

Henrique De Freitas, Google

[READ THE ARTICLE HERE](#)

Consent mode
(details)

[HERE](#)

Guide to implementati for
Developers

[HERE](#)

How Google uses
Consent Mode data

[HERE](#)

Secure

What:

The aim of Privacy Sandbox is to create web technologies that protect the online privacy of people and give both companies and developers the tools needed to build thriving digital businesses and keep the web open and accessible to all.

Privacy Sandbox

"Since 2019, we've been working on a collaborative open-source effort — the Privacy Sandbox — to develop a set of new privacy-preserving technologies that make third-party cookies obsolete and enable publishers to keep growing their businesses and keep the web sustainable, with universal access to content. It's a polarity to balance, but one we think is critical to keep the web open, accessible and thriving for everyone".

Marshall Vale, Google

[READ THE ARTICLE HERE AND HERE](#)

[Read article](#)

Everything you need to know about the Privacy Sandbox

[HERE](#)

Case histories: Companies' direct experience

4



As we have seen, third-party cookies are not the only resource available on the market to carry out successful advertising campaigns. Companies are developing new solutions to meet conflicting needs.

Let's look at a few practical examples.



4.1. Cookieless: the path towards a shared solution on privacy – by Webranking

Nereo Sciutto, CEO and Co-founder of Webranking



The scenario we are moving in

The big digital players are the ones who have shaped the way the world works – and consequently have shaped the way in which the large market that we live in works. They are the players to whom we owe the birth and structure of this environment to, and, consequently, the rules of the game we must all follow: from the people who use the technology in their daily lives to the companies that exploit it to distribute, promote and sell their products or services.

It is precisely because of their enormous importance that big digital players are often called upon to take some form of social responsibility for the world they work in and, in so doing, set the rules of the game for all their service users. It is for this reason that, rather than having public regulators impose rules of conduct, **the big players (some more than others) have preferred to propose forms of market self-regulation**. The power that comes from the sheer volume of service users that these big internet players enjoy means that changes do not only have repercussions for their own users, but on other operators as well.

This is precisely the case with Google's decision to stop using third-party cookies on its Chrome browser. But just as Google made this move – following the direction it has taken with other initiatives – Apple has done exactly the same with its Safari browser.

When?

Through the main associations and bodies that represent the industry, Google has always proposed that the sector make use of this moment to find new shared solutions for privacy protection and, at the same time, continue to exploit the Internet as a communication channel. For this reason, in addition to communicating its future phasing-out of third-party cookies, Google proposed several market solutions to be discussed and improved. Google's proposal was to switch after market consent was obtained.

The birth of new privacy-safe alternatives for investors was a pre-requisite for innovation.

It appears clear – at the time of writing – that the negotiating table, which has expanded to now include organizations such as W3C, public regulators and antitrust bodies, has led to a significant slowdown in discussions, prompting Google to postpone its project to the end of 2023.

This must not lead us to believe that the matter lies so far in the future that there is no need to deal with it now. There are two reasons for this: firstly, other players are moving in the same direction and may affect the market without either notice or seeking broad consent. Secondly, many of the activities that companies need to implement in preparation for this “new world” are slow-moving ones, requiring a certain period of time for change-over and adaptation. So better start now.

A safety car

The most important point to note is that the entire market, across all industry sectors, will face a sort of reset or restart – just like when a safety car is deployed on a racetrack, having the effect of bunching all competitors together for a new start.

The rules will change for everyone and no part of the market will have a competitive advantage over another. The change is in some ways universal. If we look at it in this way, it is clear that **rather than being a threat, as so many envisaged to be at first, it can actually be a great opportunity.**

How to prepare as advertising investors?

There is only one key to success: we need to think about how to do more with less.

With less external data and with less information collected by others. The key **is to cherish our clients’ or prospects’ information as the most precious thing we have to improve our ability to reach out to them and reduce the costs of doing so.**

All the solutions that the market is looking at and proposing are going in this direction. Third parties existed because they were useful to first parties; and the latter are the investors. So called first-party data, the data we possess or can collect, will become the new currency of business. And we need to find it (potentially even from within our own organisations, hidden in other functions), validate it and organise it so that it can be used and then monetised. This data will also need to be protected just like any other asset on our balance sheet. This is because the players with lots of data, and that are able to use it, will be the players who will restart faster once the safety car leaves the track.

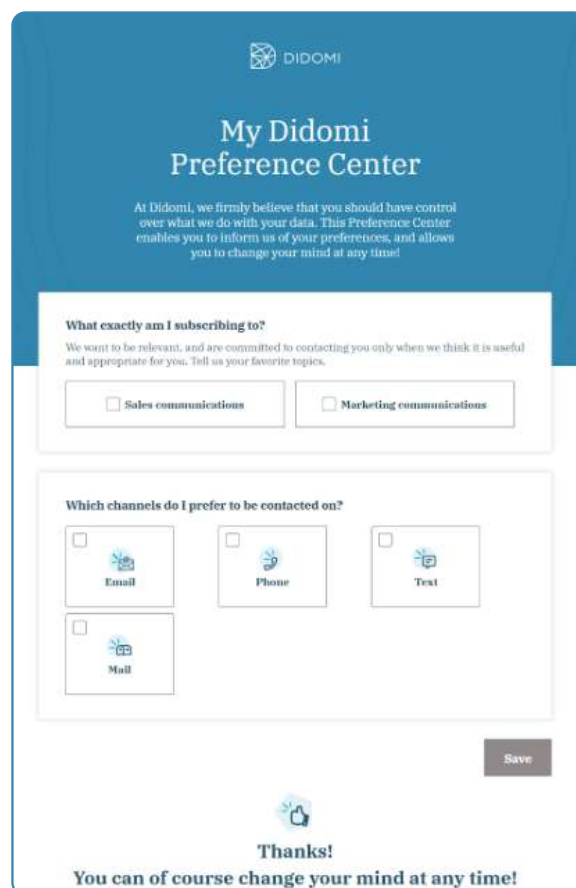
My conclusion

My wish is that this initiative of Google, and the initiatives of the others that will inevitably follow, may lead to a better balance for people and for those investors who are seeking their attention. For this new balance to be reached I can only **hope that shared solutions among operators will be developed, leading to the birth of a new toolbox for agencies and investors. A toolbox that is clear, shared and capable of addressing the demand for greater privacy whilst at the same time retaining effectiveness for those that invest in digital channels.** Or – as I find myself saying more and more often – in “digitally reached” channels, which are already more numerous than you might think.

4.2. Case Study: Study: Pierre et Vacances. The Omnichannel handling of users' personal data – by Didomi

The Preference Center (PC) is a space dedicated to handling users' personal data based on their brand communication preferences.

It centralizes first-party data that might be disorganised and stored across many different company systems.



The screenshot shows the 'My Didomi Preference Center' interface. At the top, the Didomi logo is displayed. Below it, the title 'My Didomi Preference Center' is centered. A paragraph explains that users have control over their data and can change their preferences at any time. The main section is titled 'What exactly am I subscribing to?' and includes a subtext: 'We want to be relevant, and are committed to contacting you only when we think it is useful and appropriate for you. Tell us your favorite topics.' There are two checkboxes: 'Sales communications' and 'Marketing communications'. Below this, another section titled 'Which channels do I prefer to be contacted on?' shows four options: 'Email', 'Phone', 'Text', and 'Mail', each with a checkbox and an icon. A 'Save' button is located at the bottom right of the form. At the very bottom, there is a thumbs-up icon, the word 'Thanks!', and the text 'You can of course change your mind at any time!'.

[LEARN MORE](#)

1 Background information

The PVCP Group needed a **standard solution** to make the clients of its different brands aware of its **other brand offers**, in order to lead to increased revenues at contained costs.

2 Integrated products



Consent Management Platform (CMP)



Preference Center

3 Advantages of the Didomi solution

- **Secure users' trust** through transparency
- **Leave control** in the hands of users and consumers.
- **Facilitate** multi-brand subscriptions (newsletters, SMS, email...)
- **Improve the quality** dei 1st party data nel CRM
- Allow users to **keep their consents updated and with preferences** in 5 different languages across 7 EU countries.

“

We saw 3 advantages through Preference Center integration:
Our customer center can always be up-to-date on the CRM thanks to delegated consent, our clients can actively choose the channels and brands they wish to interact with, and our team has seen an increase in marketing revenue thanks to customer loyalty work

”

Salomon Bentolila . Directeur Clients & Données . Pierre & Vacances Center Parcs Group

Luca, Marketing data manager

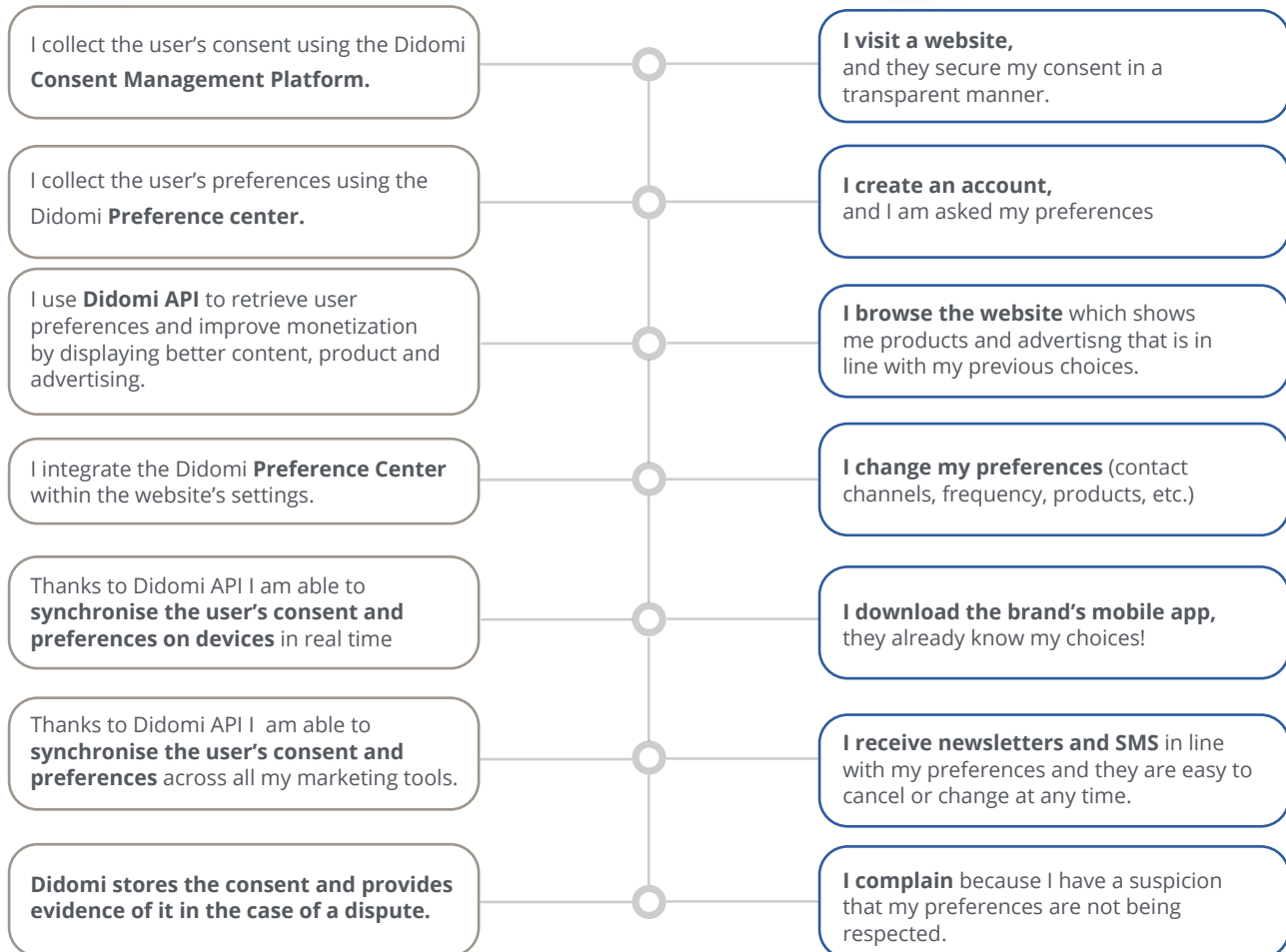


"Didomi makes data handling easier and helps me maintain compliance with regulations"

Giulia, User



"This brand respects my consents and preferences in full transparency"



Results achieved:

- Greater consumer **trust**
- Innovative and **transparent** collecting of data
- Greater number of **consents** collected
- Better **profiling** and increased revenue from email marketing.
- Authentic **omnichannel** marketing effort.

[LEARN MORE](#)

Pierre et Vacances-Center Parc has chosen to refocus on the **data** that users agree to give when they book a holiday – such as email, type of holiday, family profile – offering a tangible benefit in exchange: **it makes its clients' holiday choices easier.**

[LEARN MORE](#)

Conclusions: what's next?



Based on the information we have presented it is clear that the ongoing change process is very complex. As we have pointed out, a new awareness has arisen in relation to data processing with a need for greater process transparency – where innovation and compliance may find common ground.

The direct statements made available by companies show that it is time to shift our attention away from the “loss” of third-party cookies and towards the opportunity for innovation and corporate strategy rethinking. Strategies need to be redesigned to better meet consumer-user expectations.



We wish to thank Google, Webranking and Didomi
for their kind collaboration.

netcomm
IL COMMERCIO DIGITALE ITALIANO