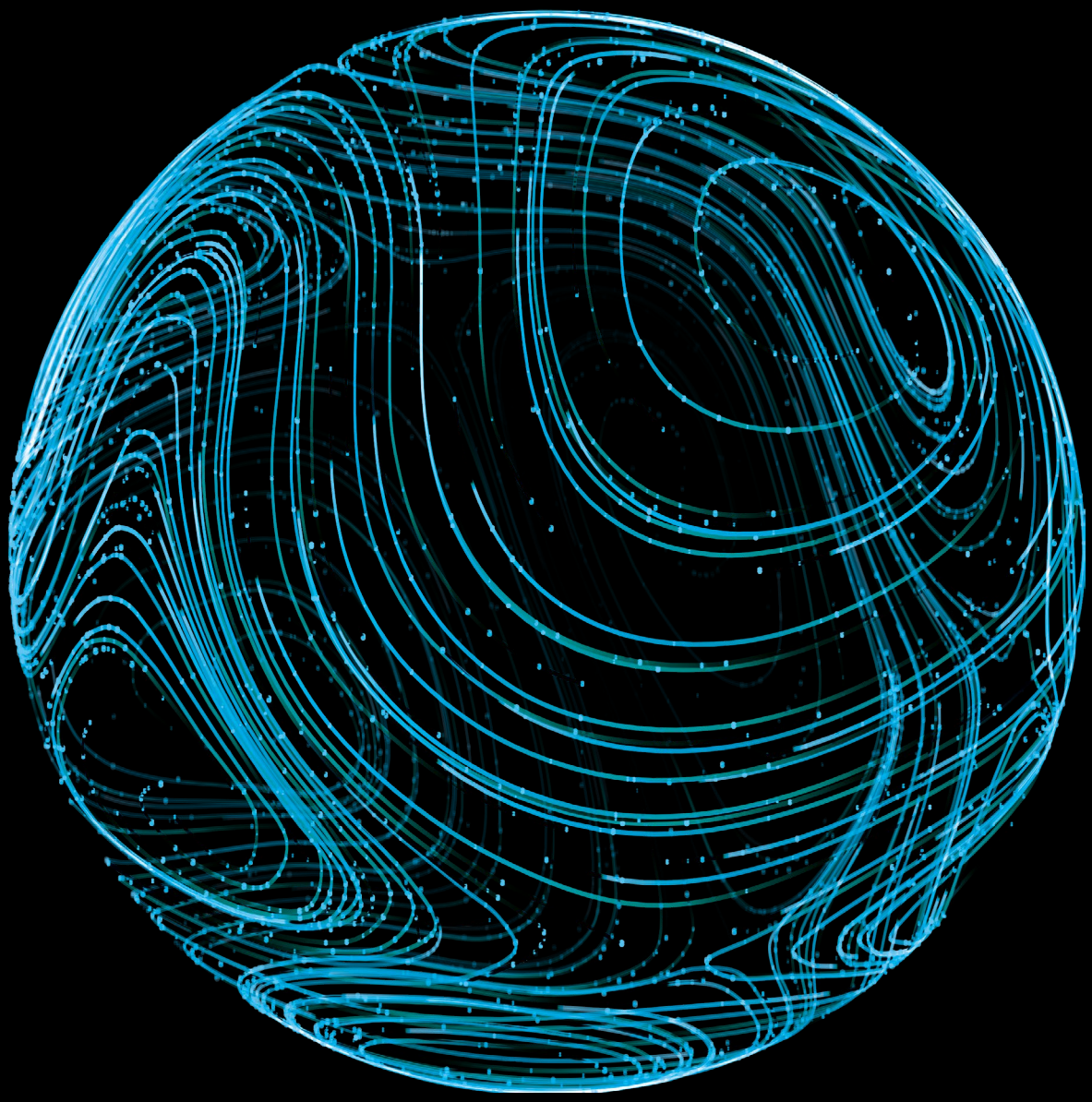
Deloitte.



# Digital Marketing in a privacy-aware world

## How to address privacy challenges

MAKING AN IMPACT THAT MATTERS since 1845

# Disclaimer

This paper is based on the current legal status quo (November 2020) and subject to change in case of developments in the relevant legal environment.

The aim of the paper is to offer a framework and an approach on how to consider privacy in digital marketing use cases. The application for advertisers' own purposes is subject to their own responsibility. The whitepaper is not intended as a substitute for thorough evaluation and approval of individual use cases by Data Protection Officers and legal departments.

The paper includes non-binding, non-exhaustive general information and does not constitute legal advice.

This whitepaper is not a consulting service for Google. Advertisers are free to use or not use Google products. Other ad tech companies may provide products which can realize comparable use cases. Statements regarding functional, technical and legal aspects represent Deloitte's point of view.

# Introduction

Today advertisers face significant and rapidly evolving changes in their market environment. Advertisers need to address new customer needs and expectations while at the same time aligning the digital touchpoints according to new privacy regulations and technical developments.

User expectations are rising as the public demands more transparency, choice and control over how personal online data is used. At the same time, users' trust in digital marketing players is declining. Users have been used to a free and open web but are increasingly concerned by the way digital marketers and publishers have come to treat personal data. Users are often unsure of how their data is being used, and hence have become more prone to deploy ad blockers, browse in the private mode or avoid publishers whose data practices are unclear.

Moreover, industry-wide changes and privacy regulations are altering the way data-driven marketing will be conducted in the near future. There are two main factors shaping this change. The first is privacy regulations (e.g. GDPR from 2018 or the upcoming e-Privacy regulation), which beside many other aspects involve managing consent and applying limitations to user-level analysis. The second is privacy-enhancing browser updates, such as limitations on third- and sometimes even first-party cookies in response to increasing consumer awareness.

Successfully navigating this changing environment is vital for advertisers of any size given the severe consequences that privacy breaches can have. These range from reputational damage to very substantial GDPR fines (up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher). Moreover, merely being compliant with the new regulations will not be enough for advertisers. Rather, the industry needs to solve this new privacy challenge for the long term. Failing this, advertisers will run the risk of losing their competitive edge and will face increasing difficulty meeting ROI targets. Hence, advertisers need to implement what might be termed "smart privacy" to make digital marketing future-proof.

This whitepaper aims to make advertisers aware of the different challenges inherent in implementing the most common use cases in digital marketing. It is based on the structured approach of the Deloitte Privacy Consideration Framework, which is introduced in more detail in chapter IV. To reduce complexity the publisher's side is not considered ("advertiser's side only").

As each digital marketing use case requires specific privacy considerations, the framework will be applied to five selected scenarios typical of digital marketing activities in Retargeting, Ad Measurement and Web Analytics. The specifications of the use cases will be described in section III. In this document, the use cases are defined based on the usage of Google solutions. However, the complexity of data protection challenges arises not only when using Google products, but also when integrating similar online tracking tools that process data in a comparable manner and to a comparable extent.

In the main part, the framework will examine the major privacy consideration topics for each use case: Use Case Modelling, Permission, Data Subject Rights Management, Risk Management and Use Case Documentation & Monitoring. Additionally, learnings and insights will be pointed out after each consideration step of the framework. We hope this will help you in the conversation with your legal department and data privacy officer (DPO) and steer the required technical and organizational changes.

After reading this whitepaper, you should be able to answer the following questions:

- Which data flows need to be considered given common digital marketing use cases (including but not limited to: Retargeting; Offline-to-Online Measurement and Web Analytics)?
- What aspects need to be considered when conducting a legal evaluation of digital marketing use case?
- How can digital marketing be conducted in a reliable and future-proof manner?

# Description of Online Marketing Use Cases

The following online marketing use cases are described based on Google solutions (as example). The only intention in the choice of Google is to reduce the complexity by limiting the number of potential technology solutions to be examined.

### Retargeting (UC1)

Advertisers use retargeting to focus on users that have previously been on the website or have interacted with specific content on this website. This re-engagement is supported by tailored ads when these users browse other websites (e.g. through Google Ads).

Exemplary impact for Retargeting with Google Remarketing:

- Increase campaign ROI by 20 percent with Google Remarketing (see example: Netshoes[1])
- Improve cost-revenue-ratio by using dynamic Google Remarketing (see example: Karstadt[2])

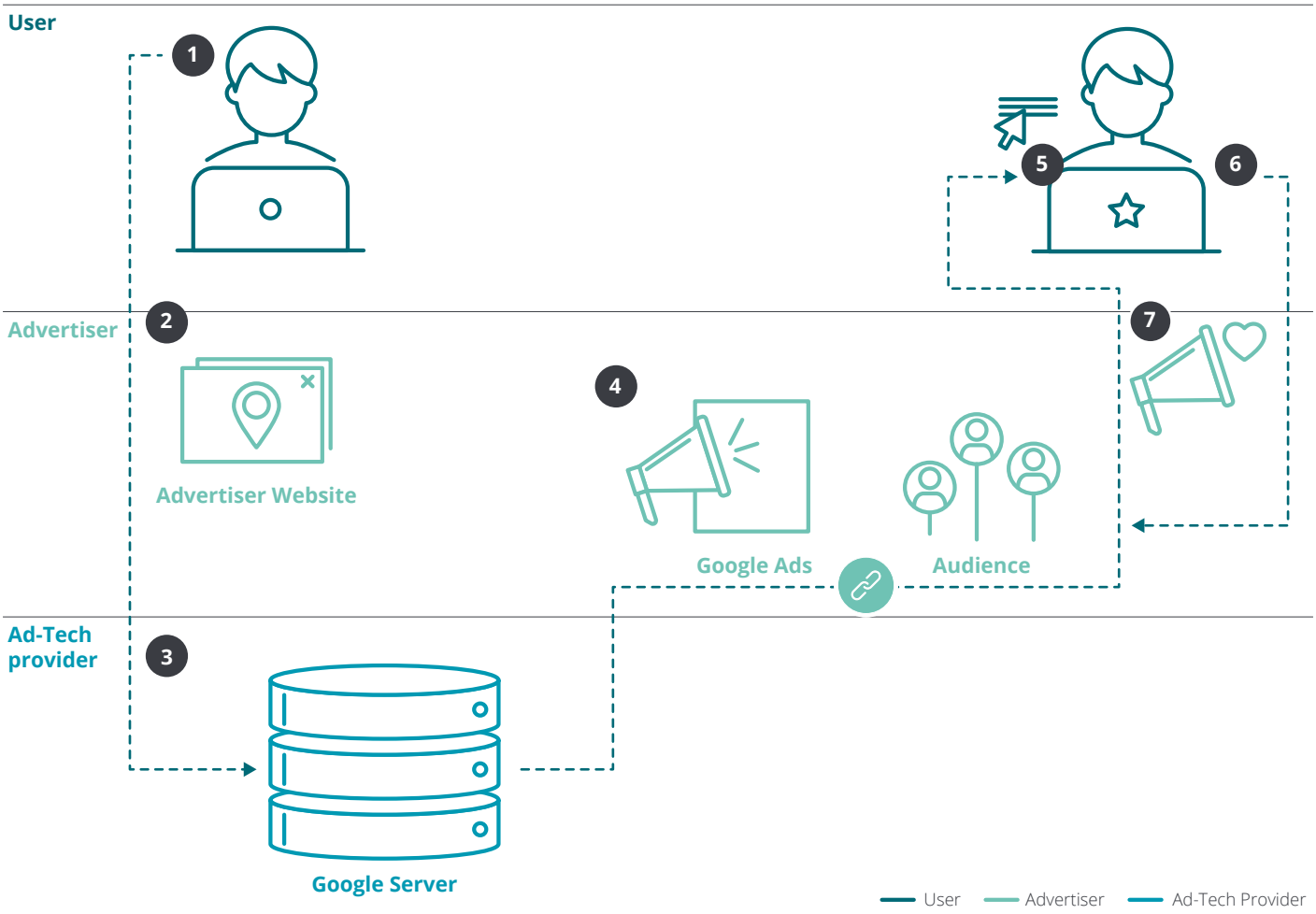
### Steps to Fig. 1

1. User accesses an advertiser's website
2. Google sets Google Ads Remarketing cookies in user's device (browser cache) containing a tracking ID
3. User's interactions* on the website are linked to the tracking ID and saved on Google server
4. Google Ads imports users meeting predefined targeting criteria into corresponding audience lists
5. User accesses Google or Google publisher network** websites
6. Google Ads recognizes the user through cookies in user's device (browser) and identifies related audience list
7. User is shown personalized ads from advertiser (e.g. latest product visited on website)

* User's interaction with content and features on the website, e.g. click, navigation, transaction

** Google Publisher Network is a collection of websites that can be used by publishers to show ads.

**Fig. 1 – Visualization (Google solution example)**




Source: Illustration created by Deloitte - Illustration does not include totality of data flows or data storage

### Conversion Import (UC2)

It is extremely relevant for advertisers to understand whether digital marketing efforts have an impact on offline sales as well. This is why marketers look at what is known as an ad's conversion import. This is a metric gauging the potential for importing offline conversions into the corresponding ad distribution system (e.g. Google Ads) to match for example ad clicks that resulted in a conversion. These insights can help an advertiser optimize media buying decisions.

Examples of impact for Conversion Import with Google Ads:

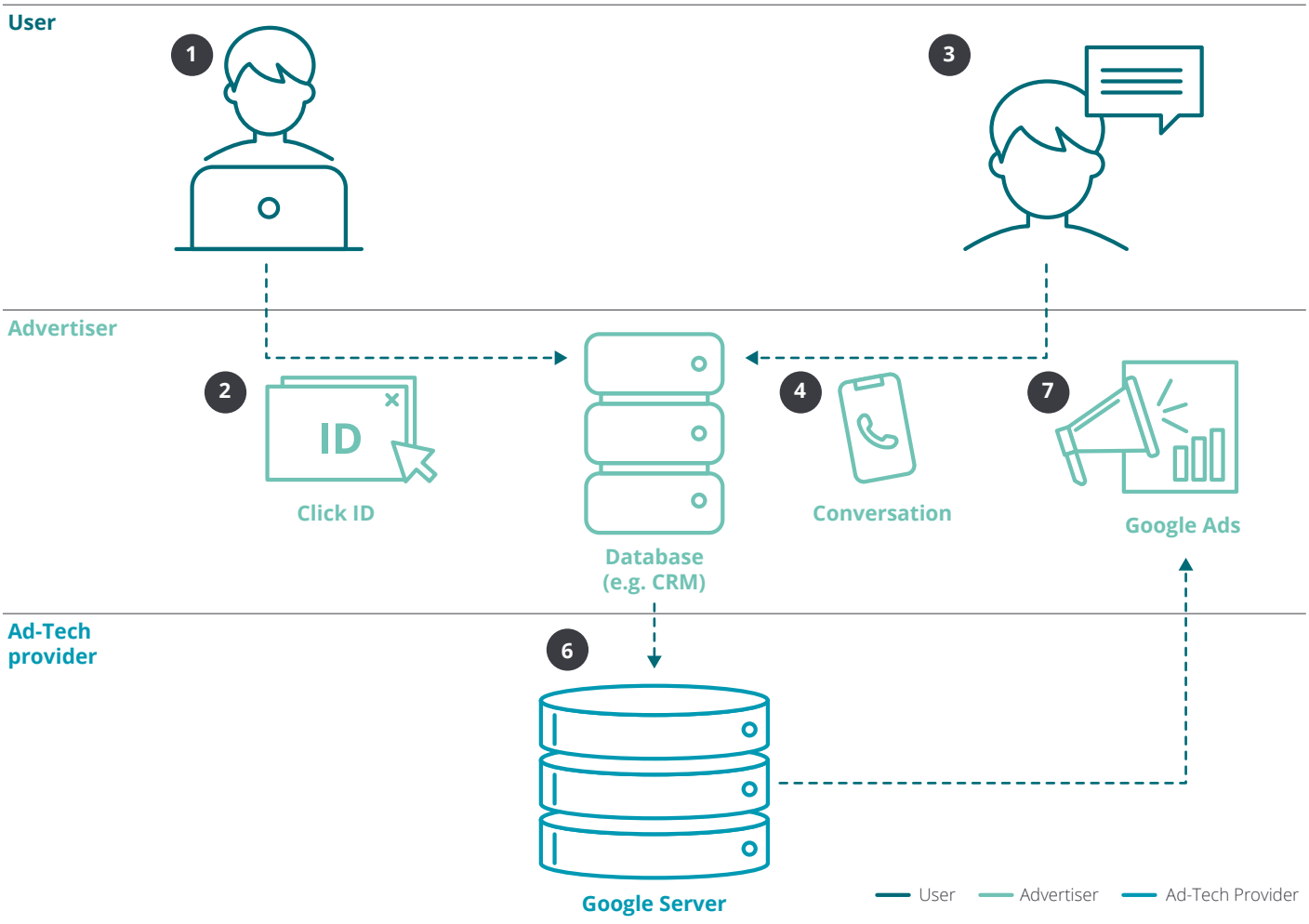
- Increase number of leads by 27 percent by importing call conversions with 69 percent lower CPA (see example: Verti[3])
- Increase campaign-generated revenue by 81 percent by activating own conversion data (see example: Flaconi[4])

### Steps to Fig. 2

1. User accesses advertiser's website through Google Ad
2. Advertiser detects user-specific click ID in user's device (browser cache) and stores it
3. Customer places an order via phone (exemplary, conversion* specified by the advertiser)
4. Conversion data is captured through call tracking and stored on advertiser's database
5. Conversion data is merged with the click ID in the advertiser's data base
6. Advertiser sends merged data to Google server
7. Advertiser can perform analyses on the attributed conversion data in order to measure ad impact

* Conversion depends on advertiser's offering and marketing goals e.g. registered lead or store visit.

**Fig. 2 – Visualization (Google solution example)**




Source: Illustration created by Deloitte - Illustration does not include all data flows and does not claim completeness with regards to data flows or data storage.

### Web Analytics pure (UC3)

An advertiser can make use of an analytics solution to gain insights about the engagement of consumers with their own website. The web analytics solution (e.g. Google Analytics ) will collect data through the user's device and provide the processed data to an interface for the advertiser to perform analysis on. The advertiser can then derive insights to improve user experience and ultimately sales as well
Note: All Google Analytics use cases are equally valid for Google Analytics 360. If the descriptions here only refer to Google Analytics, this is merely for the sake of simplicity.

Exemplary impact for Web Analytics pure with Google Analytics:

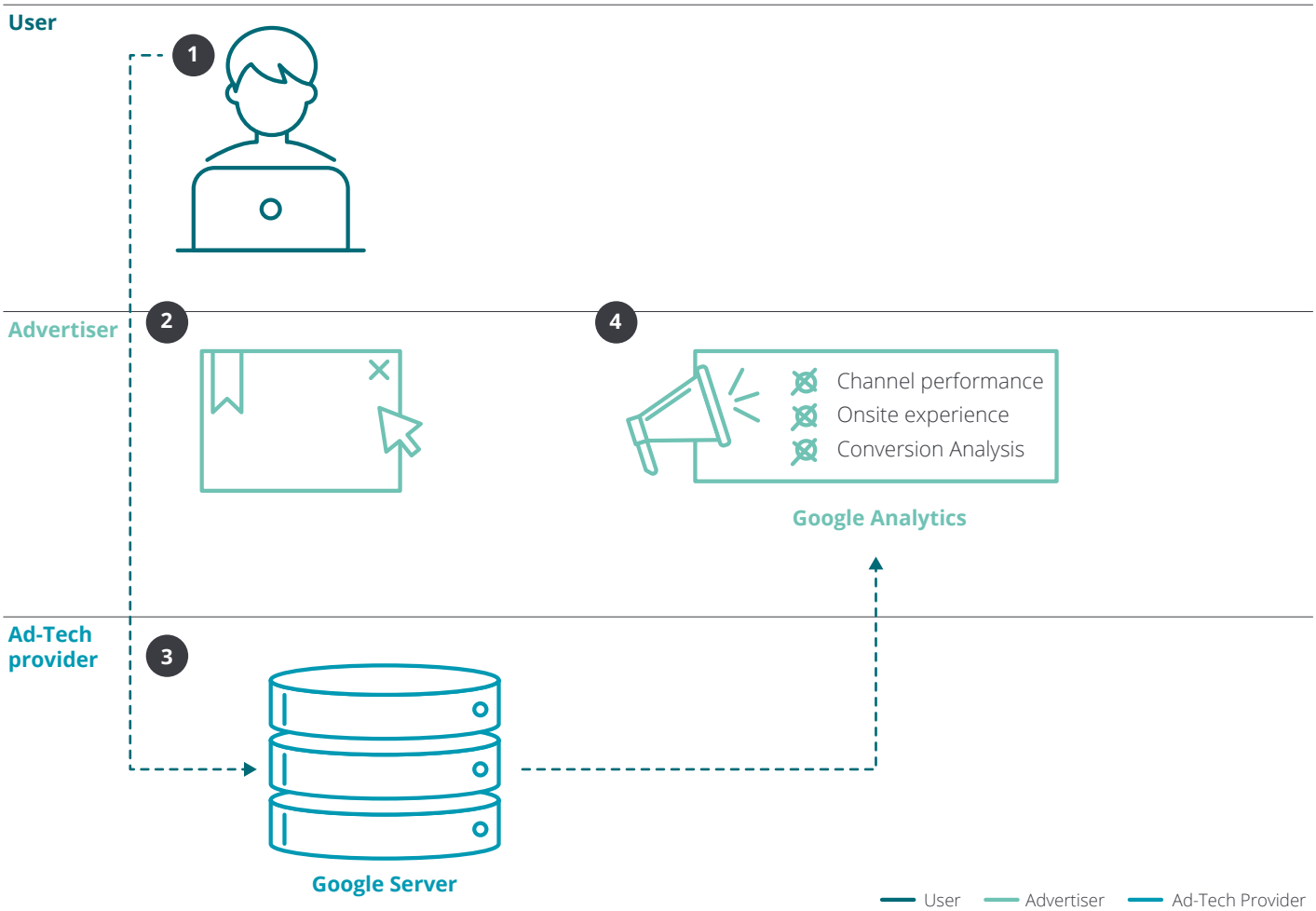
- Understand user behavior, increase user engagement and conversion rates (see example: Wyndham Vacation Rentals[5])
- Understand if users are finding what they are looking for (see example: Cancer.org[6])
- Understand user shopping behavior (see example: Mumzworld[7])

**Steps to Fig. 3**

**1.** User accesses advertiser's website
**2.** Advertiser sets Google Analytics cookie in user's device containing a tracking ID (the client ID) for the measurement of user's onsite behavior. GA cookie is classified as 1st party cookie.
**3.** User's interactions* on the website are linked to the client ID and saved on Google server**
**4.** Advertiser can perform analyses on the gathered behavioral data with advanced reportings offered in their Google Analytics account

* User's interaction with content and features on the website, e.g. click, navigation, transaction
** Google Analytics is a data processor under GDPR because it collects and processes data on behalf of its clients, pursuant to their instructions. Google customers are data controllers who retain full rights over the collection, access, retention, and deletion of their data at any time.

**Fig. 3 – Visualization (Google solution example)**




Source: Illustration created by Deloitte - Illustration does not include all data flows and does not claim completeness with regards to data flows or data storage

### Web Analytics & Ad Measurement (UC4)

Advertisers can make use of an analytics solution to gain insights about the engagement of consumers with their website. The web analytics solution (e.g. Google Analytics) collects data through the user's device and provides the processed data in an interface for advertisers to perform analysis. Advertisers can thereby link valuable onsite activities like a purchase conversion to their marketing activities. This allows the optimization of ads and targeting against the actual onsite behavior of similar prospects.

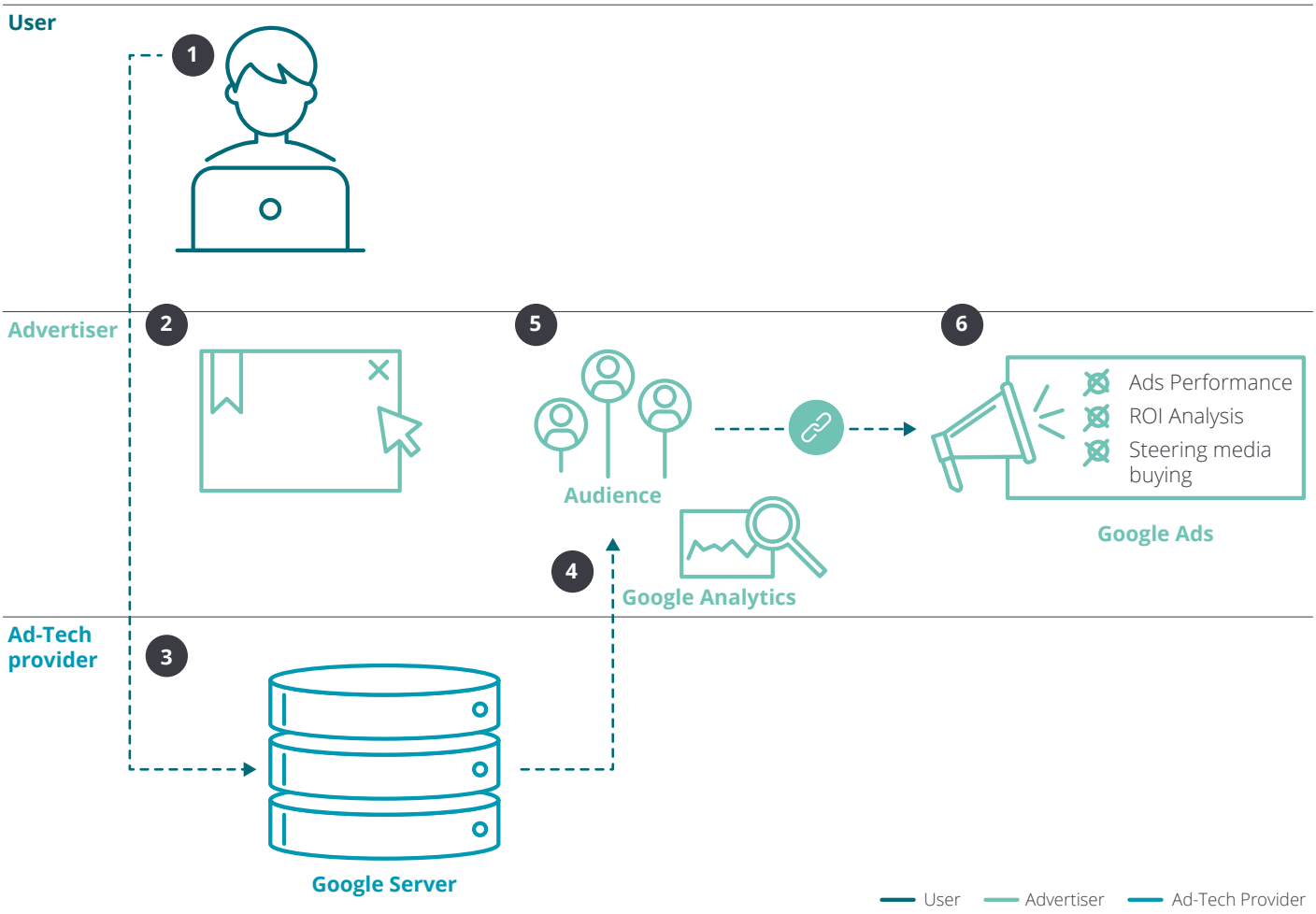
Exemplary impact for Web Analytics & Ad Measurement with the Google Marketing Platform:

- Understand user acquisition channels, increase conversion rate by 28% (see example: Matalan[8])
- Increase return on ad spend by 30% (see example: Panasonic[9])

**Steps to Fig. 4**

1. The user accesses the website of advertiser
2. The advertiser sets Google Analytics cookie in user's device containing a tracking ID (the client ID) for the measurement of user's onsite behavior. GA cookie is classified as 1st party cookie.
3. Interactions* of the user on the website are linked to the client ID and saved on Google server
4. The advertiser can perform analyses on the gathered behavioral data with advanced reportings offered in their Google Analytics account
5. Advertiser imports Analytics goals and reports into Google Ads
6. Advertiser can measure the success of ads considering valuable user activities on the website

**Fig. 4 – Visualization (Google solution example)**




Source: Illustration created by Deloitte - Illustration does not include all data flows and does not claim completeness with regards to data flows or data storage

### Web Analytics & Retargeting (UC5))

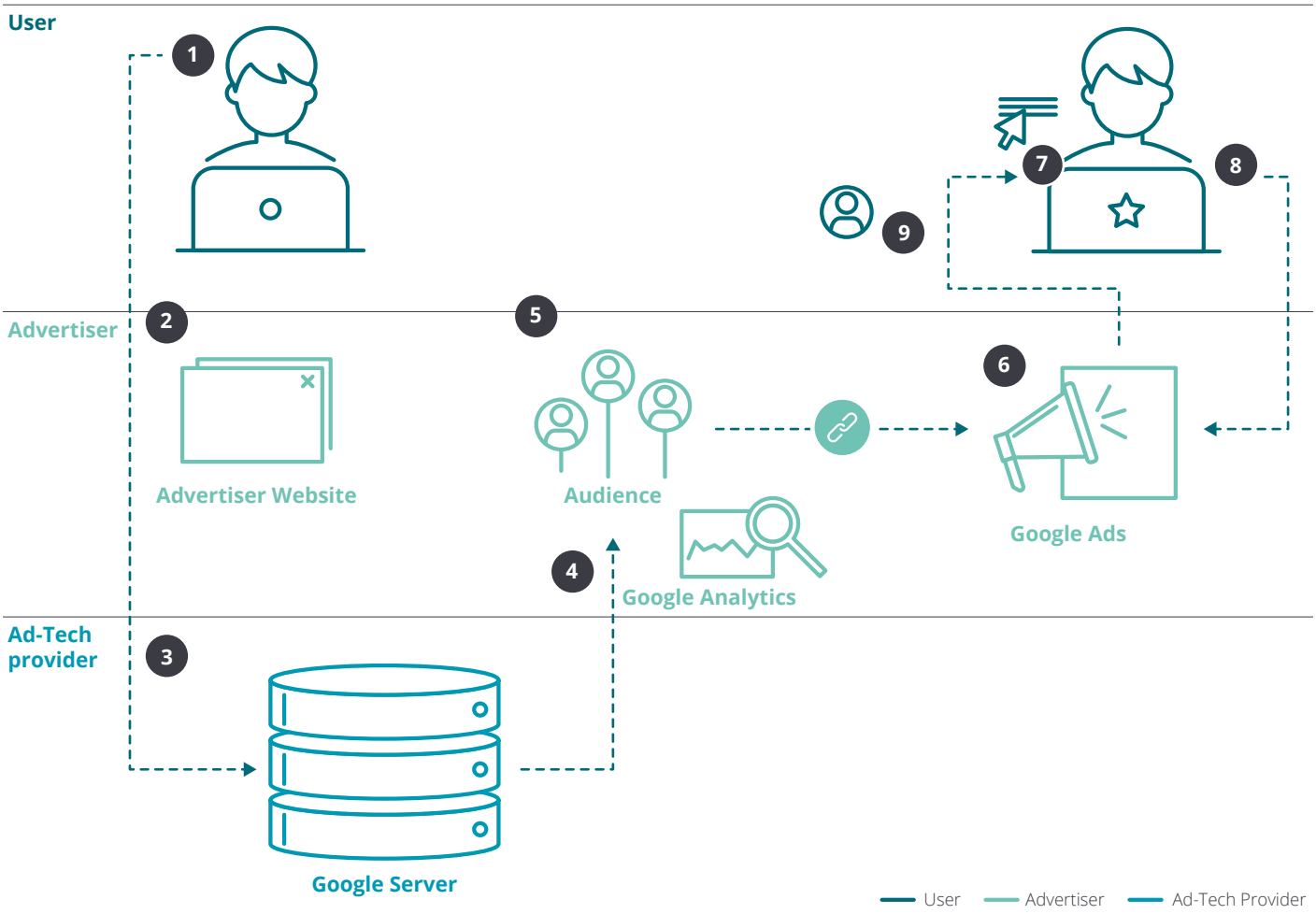
Advertisers can define retargeting audiences in their analytics solution and share them with their ad distribution solution for advanced online targeting. These retargeting lists are created based on users' onsite behavior, which allows advertisers to strategically position relevant ads to the user in relation to the user's interests or phase in the conversion funnel.
Exemplary impact for Web Analytics & Retargeting with Google Analytics and Google Remarketing:

- Re-engage with your most valued users, realizing a 300 percent higher click-through rate (see example: Panasonic[10])
- Increase revenue with Google Remarketing campaigns (see example: Mumzworld[11])
- Create granular audience segments with 69 percent higher post-click sales and 87 percent lower CPA (see example: BT[12])

### Steps to Fig. 5

1. The user accesses the website of advertiser
2. The advertiser sets Google Analytics cookie in user's device containing a tracking ID (the client ID) for the measurement of user's onsite behavior. GA cookie is classified as 1st party cookie
3. Interactions* of the user on the website are linked to the client ID and saved on Google server
4. The advertiser can perform analyses on the gathered behavioral data with advanced reportings offered in their Google Analytics account
5. Advertiser defines remarketing audiences based on Google Analytics measurement values (e.g. products added to basket without purchase)
6. Predefined audiences are pushed to Google Ads through the product linking with Google Analytics
7. The user accesses websites of Google or Google publisher network**
8. Google Ads recognizes the user through cookies in user's device (browser) and identifies related audience list
9. The user is being shown personalized ads from advertiser (e.g. latest product visited on website)

**Fig. 5 – Visualization (Google solution example)**

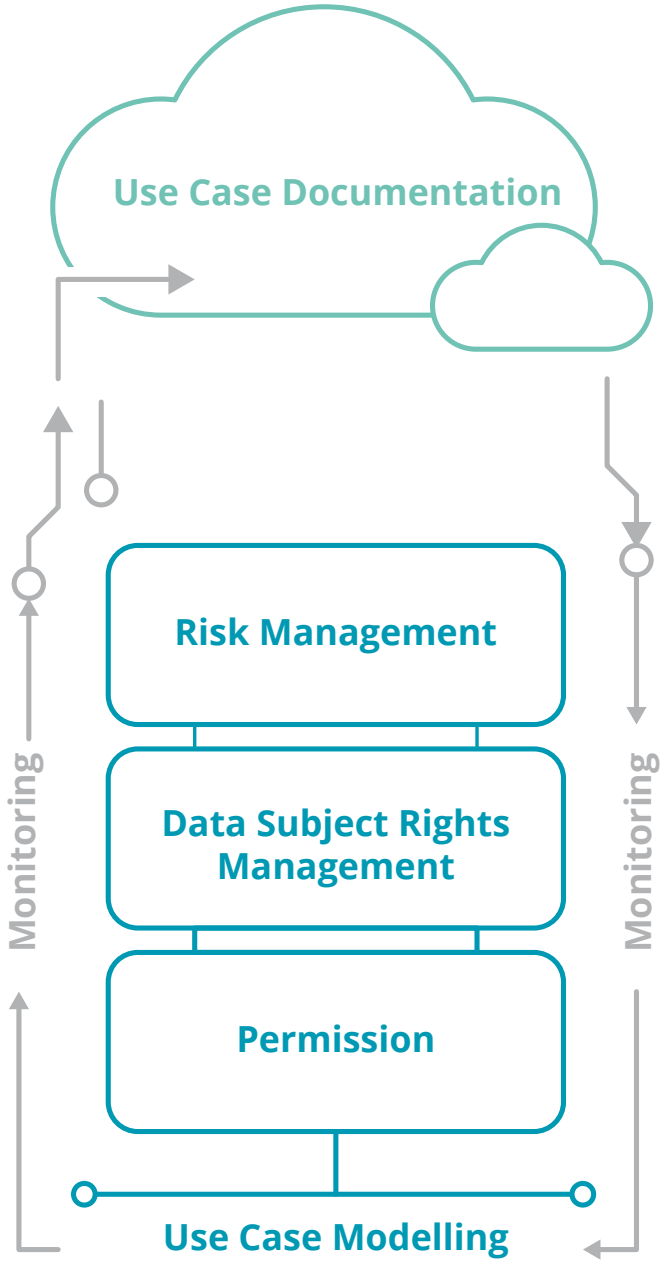



Source: Illustration created by Deloitte - Illustration does not include all data flows and does not claim completeness with regard to data flows or data storage

# Introduction to the Privacy Consideration Framework

The Deloitte Privacy Consideration Framework is intended as guidance for the implementation of privacy related requirements whenever advertisers plan to conduct online marketing. The framework consists of 5 main components which guide advertisers in ensuring use-case related privacy compliance. However, the correct implementation of these requirements will always be the responsibility of the advertisers. The framework's components are the following:

**Fig. 6 – Components of the Privacy Consideration Framework**

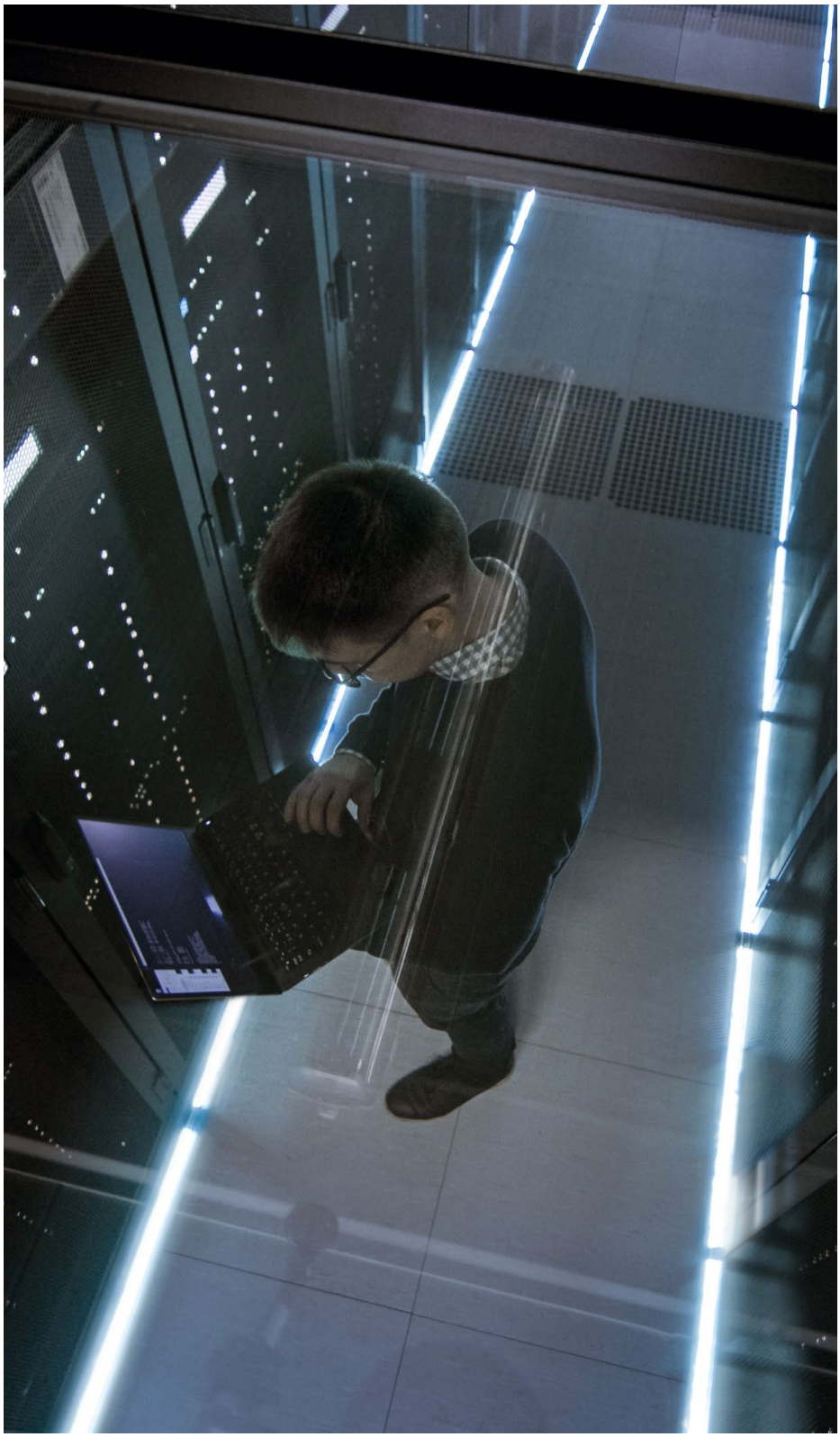


# Use Case Evaluation Insights

The following describes the components of the Privacy Consideration Framework and the activities to be performed within these components. Besides a brief description of these activities, the following sections include general considerations and recommendations for the respective activities and important insights from the application of the Privacy Consideration Framework to the selected use cases.

# Use Case Modelling

Use Case Modelling involves capturing the individual functional requirements of the use case. These requirements determine the relevant data protection provisions and their respective implementation.



## Goals & Purposes

**What to do?**

- Advertiser defines objectives to be achieved by the use case
- The processing activities are assigned to specified, explicit and legitimate purposes

### What are typical purposes for the use of online tracking solutions?

- Analytics: Improvement of interface design and product placement
- IT security: Protection against fraud, abuse, security risks and technical issues
- Advertising success measurement: Optimization of budget allocation for online marketing
- Advertising: Effective use of advertising spaces (e.g. AI-bidding), audience management and personalized retargeting

### Insights from use case evaluations

**All use cases: Purposes affect the choice of user data categories to be processed**

- The purposes of the processing activities defined by the advertiser strongly affect the choice of user data categories to be processed
  **Example:** Reach measurement of a website with a web analytics tool, e.g. Google Analytics, could be fulfilled by counting the number of visitors without tracking their exact surfing behavior

**All use cases: Purposes affect the choice and the configuration of the online tracking solution**

- The purposes also affect the choice and the configuration of the specific online tracking solution
  **Example:** If only web analytics is required, a basic version of a web analytics tool, e.g. Google Analytics, might be enough

**All use cases: Thorough analysis of purposes helps with transparency towards the users**

- If the advertiser thoroughly works through all purposes of the use case, a clearer and more transparent description of the use case can be communicated towards the user (i.e., in the consent declaration and privacy notice)

### Processing Activities & Online Tracking Solutions

**What to do?**

- Advertiser drafts the use case including the best suited online tracking solution, databases as well as systems and identifies all data flows (e.g. as data flow diagram)
- Advertiser identifies each single processing step within the data lifecycle from collection to deletion

### What are typical data processing activities in online marketing?

- Collection, storage and analysis of behavioral patterns linked to tracking identifiers
- Transmission of data sets to other databases and other organizations
- Usage of data for the targeted placement of advertising campaigns
- Erasure, anonymization and aggregation of data

**What is fingerprinting and what distinguishes it from cookies as tracking mechanisms?**

- Fingerprinting is "the capability of a site to identify or re-identify a visiting user, user agent or device via configuration settings or other observable characteristics"[13]
- Unlike with cookies, users cannot disable or clear their fingerprint in the browser settings, and therefore have no control over how their information is collected
- Fingerprinting is therefore not incorporated in any of Google's online tracking solutions

### Insights from use case evaluations

**All use cases: Efficient and compliant implementation requires cross-functional effort**

- Marketing, IT, data privacy and legal need to join forces
- No function can do it alone, thus skills from all are needed

**All use cases: Use case designs are a matter of advertiser's choice**

- Similar use cases can be very different depending on the respective configurations
  **Example:** Google Analytics' Data Sharing function provides advertisers with the option to share user data with Google. This enables Google to pursue its own purposes, such as developing and improving the products and services it offers[14]
- Similar use cases can also vary due customer-defined scope
  **Example:** Inclusion of additional user data categories from onsite databases, implementation of additional online tracking solutions from different ad tech providers or integration of additional databases
- Different configurations and additions can respectively result in different evaluations and increase the privacy requirements
  **Example:** For example, Google Analytics Data Sharing involves more extensive data processing activities, which might result in a higher risk for the website users. Another implication of the data sharing option is that the advertiser would have to agree to the Google Measurement Controller-to-controller terms in addition to the Processor terms.[15] If the advertiser does not activate the data sharing option, only the Processor terms may apply for the use of Google Analytics pure. However, conclusion of the correct data protection contracts for the different Google Analytics modes is crucial and demands thorough evaluation (for more see section "Partner Selection & Contract Conclusion").

**UC2 Conversion Import: No cookie involved**

- Conversion measurement does not need to involve cookies

### Partner Selection & Contract Conclusion

**What to do?**

- Advertiser selects ad tech providers that offer the best fitting solutions for their individual use case
- Advertiser concludes data protection contracts with ad tech providers
- In case the advertiser transfers user data into a country that is not a member of the EU or the European Economic Area (e.g. because the ad tech provider processes data in the USA), the data transfer must either be covered by an adequacy decision, appropriate safeguards (such as use of the Commission's Standard Contractual Clauses) or binding corporate rules

### Advertisers need to identify parties involved in the processing activities:

- The GDPR defines three types of roles in this regard: controllers, joint-controllers and processors
- An advertiser must conclude data protection contracts with each of its providers
- These serve to address GDPR requirements for processing user data on both sides

Many service providers already offer pre-formulated data protection contracts (i.e. Google[16]). However, these sample contracts should be carefully reviewed in consultation with the legal department.

### Insights from use case evaluations

**UC1 Retargeting, UC2 Conversion Import, UC4 Web Analytics & Ad Measurement, UC5 Web Analytics & Retargeting: Two independently acting controllers when using Google Ads products**

- Google offers Controller-to-Controller terms for the use of Google Ads products
- Under these terms, both the advertiser and Google constitute independently acting controllers for use cases that incorporate Google Ads products; However, this should be examined carefully
- Following these terms, each party takes full accountability for those data processing activities each party performs for their own purposes and, thus, is responsible for the implementation of compliance

**UC3 Web Analytics pure: Google as processor and advertiser as controller when using Google Analytics (pure)**

- Google offers Processor terms for the use of Google Analytics
- Under these terms, the advertiser will be considered the controller while Google will act as processor for the provision of Google Analytics; however, this should be evaluated carefully as the opinions of the supervisory authorities may conflict[17]
- A processor contract assigns full accountability for privacy compliance to the advertiser performing data processing activities for their own purposes by using Google Analytics
- As an exception to the above-said, Google, under the Google Measurement Controller-to-Controller terms Google will be considered an independently acting controller for the processing activities that Google performs with the data Google obtains through the activation of Google Analytics Data Sharing; however, the Processor terms, under which Google acts as a processor, will continue to apply to the provision of Google Analytics for the purpose of performance management

### Data Categories

**What to do?**

- Advertiser identifies all categories of users' personal data collected and processed by online tracking solutions
- Where the advertiser wishes to match the online data with further personal data (e.g. user's email address), they make sure that the additional data is actually necessary for the defined purposes of the use case

### What are the typical data categories of user data in online marketing?

- Online identifiers, such as the IP address, an individual cookie identifier or a URL and user-specific identifier
- Surfing behavior linked to an ID such as keywords searched, videos viewed, interaction with content, browsing and clicking patterns, URLs visited, products viewed or purchased, persons contacted (e.g. through content sharing)
- Geo-location
- Device and browser data

Ad tech providers collect and process different types of data. Google's approach in the company's help center is described as an example.[18]

**Important considerations**

- Most of the online user data collected will be considered personal data under the GDPR and some of it may qualify as pseudonymous data
- Personal data is any information related to an identified or identifiable person
- Unique online identifiers are used to connect information with an individual, allowing advertisers and ad tech providers to easily address this individual along their online journey
- Hence, the GDPR and related data protection laws will apply to online marketing use cases

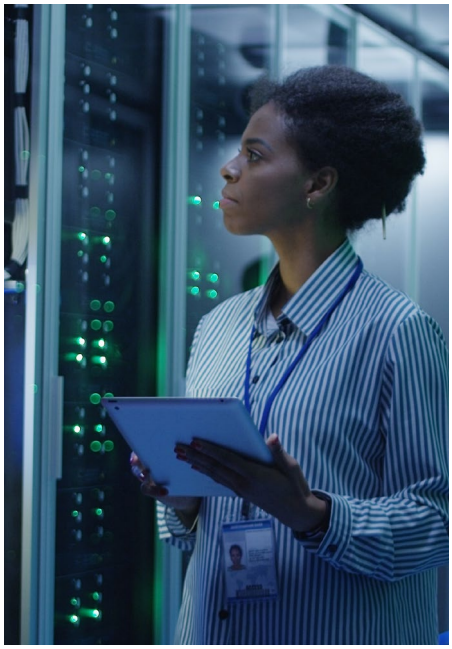
### Insights from use case evaluations

**All use cases: Some use cases use less data than others**

- Depending on the use case, different amounts of data will be collected, stored and processed further
  **Example:** While Ads Conversion Import by default will use only the smallest amount of data possible (only click ID and customer defined conversion data), Google Remarketing requires at least the IP address, browser and device data, tracking IDs and user's onsite activities

**All use cases: Customers can choose to expand the processed amount of data**

- Advertisers can select the granularity of collected onsite activities or conversions
  **Example:** Conversions could be defined as purchases vs. products put into a shopping basket
- Advertisers can opt to include other additional data not collected by the solution (e.g. CRM data)
- These decisions have implications on the amount and sensitivity of the user data processed and on the overall impact of the use case on the users' rights and freedom



### Storage Duration

**What to do?**

- Advertiser chooses an appropriate retention period from the options provided within the online tracking solution
- Advertiser defines storage periods for the processed user data stored on their on-premise database/s

### How to fulfill the requirement of deleting data in online marketing?

It is recommended to

- thoroughly assess when the purposes are fulfilled and which legal retention requirements might affect the data storage period
- keep track of data distribution across involved parties and databases in order to guarantee that all data is deleted once the purpose is fulfilled
- work with parties involved to find practical solutions

### Insights from use case evaluations

**All use cases: If the advertiser is the controller for processing data for their own purposes, they will also be responsible for determining the appropriate storage periods**

- Advertiser needs to define use-case specific and purpose-related storage periods
  **Example:** Data collected through Google Analytics and stored in on-premise databases might be used by different departments with different function- and purpose-specific periods, such as extended periods for the storage of security logs

**UC3 Web Analytics pure: Advertiser can choose from options provided by Google**

- Google allows advertisers to choose from several options for the deletion of data in Google Analytics[19]
- Advertisers will be responsible for choosing appropriate purpose-related storage periods for data stored in Google Analytics

**UC1 Retargeting, UC2 Conversion Import, UC4 Web Analytics & Ads Measurement, UC5 Web Analytics & Retargeting: Actual data deletion in the Google Ads tools is triggered either through non-optional deletion procedures set by default or through the user's actions**

- Non-optional deletion procedures[20]:
  - After 9 months: Google anonymizes the user's IP address in logs by removing a part of the address
  - After 18 months: Google anonymizes log data by removing the cookie or advertising ID information in both logs and ad server databases
- User's actions[21]:
  - Beyond the above, signed-in Google users can delete past searches, browsing history and similar activity from their My Activity accounts; when these events are deleted, they are no longer linked to that user's signed-in ads profile
  - Users also have the option to delete cookies
- Unlike Google Analytics, Google Ads will not allow an advertiser to influence deletion of user data processed in Google Ads products; the advertiser can only control the duration of their usage (i.e., life span of audience lists), which can range from 1 to 540 days resp. 18 months (sometimes at least 30 days)[22]

# Permission

Having legal permission is the mandatory prerequisite for putting your use case into practice.

However, finding the appropriate and justified legal basis can be demanding and a complex procedure. Especially the decision between informed consent and legitimate interest and the subsequent balancing of interests requires a great deal of supporting arguments, legal knowledge and sensitive consideration of the individual case. This is a sensitive point and one that operating departments should not act on lightly, especially not without consulting the legal department or the data privacy office beforehand.

## Legal Basis

**What to do?**

Advertiser selects a legal basis for each data processing activity

### Choosing an appropriate legal basis is not only compulsory but also essentially determines the possibilities of data processing

- It is legally required that each data processing activity and, consequently, also the whole use case be built on an appropriate legal basis
- The chosen legal basis might influence or even restrict the extent of the data processing
  **Examples:**
  - Informed consent: Advertiser can define and transparently communicate the extent of data processing activities in the declaration of consent
  - Legitimate interests: Extent of the data processing activities depends on balance of interests and largely on what the user expects

### Which legal bases are best suited for online marketing?

- **GDPR legal bases:**
  - The user voluntarily gives their informed consent to the data processing activities
  - The advertiser or another party has overriding legitimate interests to process the data; the advertiser must conduct and document a thorough balancing of the conflicting interests of the users and the advertiser
- **Important provisions of the E-Privacy Directive ("Cookie Directive"[23]) and national transpositions:**
  - The "Planet 49" judgement of the European Court of Justice[24] made it clear that the use of cookies and comparable online tracking technologies requires obtaining the user's permission unless these technologies are strictly necessary in order to provide the website explicitly requested by the website user
  - The court came to its decision by applying provisions of the EU E-Privacy-Directive as well as the GDPR definition for consent
  - Important: In the context of online marketing and the use of cookies and comparable technologies, overriding legitimate interests (GDPR legal basis) will only constitute a valid legal basis, if the data processing activities are strictly necessary to provide the website explicitly requested by the website user
  - However, each EU country has incorporated the E-Privacy Directive into respective national law, which the advertisers from these countries need to apply as relevant law for their use cases
  - Advertisers should therefore make themselves aware of their own national E-Privacy law

### What are the implications for the technological configuration of the tracking mechanisms to be used?

- If the advertiser needs to obtain a user's informed consent for the processing activities, the tracking mechanisms may not be triggered until the user declares their informed consent
- If the advertiser is not required to obtain a user's informed consent, the tracking mechanisms may be activated as soon as the user enters the website (unless the user has objected beforehand)

### Insights from use case evaluations

**UC1 Retargeting, UC5 Web Analytics & Retargeting: Google demands for the advertiser to obtain the user's consent**

- If the advertiser incorporates Google's Remarketing services or cookies where local law requires a consent, Google expects the advertiser to obtain the user's consent for the use of Google services (see EU user consent policy for more information[25])

**UC2 Conversion Import, UC3 Web Analytics pure, UC4 Web Analytics & Ad Measurement: The option to use a legal basis other than the informed consent is possible in limited individual cases**

- The main source of requirements for the lawful use of cookies and comparable technologies besides the GDPR is the EU E-Privacy Directive
- Unless the use of cookies and the like is strictly necessary for providing the requested functions of a website, advertisers should obtain the user's informed consent in order to be compliant with EU law
- The advertiser is responsible for determining whether using the ad tech provider's solutions on their website is strictly necessary for the website to function
  **Example:** Advertisers could argue that the implementation of a web analytics service on their website is strictly necessary from a security point of view: A Web Analytics system could be the first and fastest indicator on a website to detect signs of a hacker attack
- For UC2 and UC4, a case-by-case, diligent examination is required. In the vast majority of cases, an informed consent requirement will be the solution of choice; As the law stands, invoking a different legal basis (e.g. legitimate interests) will carry high risks
- If the informed consent is obtained in keeping with the GDPR provisions, it can indeed constitute a sound legal basis

**UC2 Conversion Import, UC3 Web Analytics pure, UC4 Web Analytics & Ad Measurement: If the tracking mechanisms are strictly necessary in order to provide the requested service as stipulated by the E-Privacy Directive, these mechanisms can be used without a consent by invoking the GDPR's "legitimate interest" provision. Additionally, no other national provisions may be applicable. If both conditions are met, the legal basis "legitimate interest" may be applicable. The following indicators[26] can be used when weighing up conflicting interests on the part of the advertiser and their users:**

- Users' reasonable expectations regarding the overall extent of the processing activities when a user visits the advertiser's website
  - Informed consent may be required if this extent exceeds users' expectations
  - Legitimate interest may constitute a sufficient legal basis if the extent is within users' expectations
  - Example: Do users expect third parties will use their data for different purposes of their own when users enter and use the advertiser's website?
- Involved parties obtaining and processing the data
  - Informed consent may be required if the advertiser involves many internal or external stakeholders (e.g. another marketing partner)
  - Legitimate interest may constitute a sufficient legal basis if the advertiser involves fewer internal or external stakeholders
- Merger of user data sets with Google's online identifier

  - Informed consent may be required if a merger of data sets will allow an advertiser to gain a deeper understanding of their users and how or why they use the advertiser's website
    **Example:** Identifier is matched with customer account information
  - Legitimate interest may constitute a sufficient legal basis if data sets are not matched with the identifier
    **Example:** If earlier purchases by the same user are matched with recent purchases rather than being considered and evaluated separately, this could lead to a completely new interpretation regarding the user's interests and personality. A merger of different purchases may even result in the creation of sensitive information about the user.

- Granularity of data will determine the value of information about a user's behavior or interests
  - Informed consent may be required if online user events are defined at a more granular level
  - Legitimate interest may constitute a sufficient legal basis if online user events are defined at a less granular level
    **Example:** Conversions could be defined as purchases, or products being placed into an online shopping basket or other events that might be relevant for the advertiser because they allow a deeper understanding of the user's needs. Contrary to this, conversions could also be defined as simple purchases leading to a less deep understanding of the user's needs. Another example would be a web analytics cookie recording the exact keyboard, mouse and swipe movements vs. simply counting the visits of the website.

- Number of users subjected to processing data and extent of data processing
  - Informed consent may be required if an advertiser collects and processes data from a significant number of users and/or stores the data for a long period of time
  - Legitimate interest may constitute a sufficient legal basis if the advertiser collects and processes data from a small number of users and/or stores the data for a short period of time
    **Example:** An advertiser regularly extracts data from a web analytics tool to accumulate the customer's email address with the web analytics data or conversion data on the on-premise database, which leads to building a long-term profile of a known customer.

- Length of observation
  - Informed consent may be required if the same user can be tracked for a long time (e.g. because of long cookie lifespan)
  - Legitimate interest may constitute a sufficient legal basis if the same user can only be tracked for a short time (e.g. because of short cookie lifespan)

- Common industry standards
  - Informed consent may be required if data processing activities are not considered common industry standards
  - Legitimate interest may constitute a sufficient legal basis if data processing activities are considered common industry standards

- Unconditional possibilities to opt out of data processing activities
  - Informed consent may be required if the advertiser cannot provide unconditional means of opting out
  - Legitimate interest may constitute a sufficient legal basis if the advertiser can provide unconditional means of opting out

- Use case combining different use cases of which at least one requires an informed consent
  - Informed consent may be required (for UC3 Web Analytics pure, UC4 Web Analytics & Ad Measurement only) if Web Analytics pure or/and Conversion Import require an informed consent
  - Legitimate interest may constitute a sufficient legal basis (for UC3 Web Analytics pure, UC4 Web Analytics & Ad Measurement only) if Web Analytics pure and Conversion Import do not require an informed consent

## Consent Banner

**What to do?**

If applicable: Advertiser can obtain an informed, voluntary and unambiguously given consent from the user

### What are GDPR requirements concerning the consent declaration?[27]

**Freely given**

- No cookie wall obliging the user to declare their consent, unless the consent is necessary for the performance of a contract or the provision of a service
- Option for the user not to agree to the data processing (e.g. "I do not agree" button)
- Integrated option to consent to data processing activities at a granular level

**Specific & informed**

- Declaration should include necessary information expressing the extent of the data processing activities (e.g. purposes, parties included, tracking mechanisms involved, etc.)
- In case of advertiser using multiple information layers, data subject should still be to understand the extent of the data processing and what the consent is asked for
- Further information should be made available within the privacy notice

**Clear indication**

- Option for the user to express their clearly given consent to the data processing (e.g. no preset slide controls or pre-ticked checkboxes)

**Proof of given consent**

- Advertiser must be able to demonstrate that a user has given their consent (e.g. by keeping records of given consents)

**Access to notices**

- The privacy notice and legal notice should be no more than "one click away"

**Withdrawal**

- Provision of an easy possibility to withdraw the consent at any time (e.g. possibility to move the slide controls into the other direction or to un-tick the checkbox)

### Insights from use case evaluations

**All use cases: Consent banner positioning and design should be discussed cross-functionally**

- Relevant functions (marketing, IT, data privacy office and legal) should discuss the adequate placement of the consent banner on the website so as to guarantee legal compliance, enhance the website traffic and the user acceptance rate
- A/B testing should be considered to evaluate the number of users consented to a data processing activity depending on the cookie banner interface design (e.g. color, font etc.), placement (e.g. overlay) and content

**All use cases: The law does not provide conclusive guidance concerning the content and interface design of a consent banner**

- Since the law does not give conclusive specifics concerning the implementation of a consent banner, Google offers a checklist on the implementation of consent mechanisms to navigate the uncertainty (for more see EU user consent policy for more information[28]); However, the checklist should be evaluated carefully
- While the law does not give any specifics, trends begin to emerge, companies copy off of each other, consent management platforms set standards and, probably most importantly, official bodies form the EU or member states give advice on how to put the legal requirements into practice (for some examples see sources in footnote 16)
- Main trend is differentiating between the purposes
  **Example:** Differentiation between necessary for the proper functionality of the website or used for special functionalities, a better website performance and advertising

# Data Subject Rights Management

Being able to transparently communicate to your website users what happens to their data and to fully perform on their requests is not only obligatory but also builds trust.

## Transparent Notices

**What to do?**

Advertiser updates the privacy notice on their website accordingly to the data processing activities within the use case

### What does an ideal privacy notice look like?

- Clear and plain language
- User-friendly (e.g. skipping marks, symbols and a separate cookie notice)
- Describing all relevant facts pursuant to GDPR (if applicable: comprehensive description of the legitimate interests of the controller or another party)

### Insights from use case evaluations

**All use cases: The advertiser as a controller is responsible for keeping a website's privacy notice up to date**

- The advertiser must inform the website users about the data processing activities performed on the website
- This includes the data processing activities involved in the use of the online tracking solution: It is vital to provide sufficient information on the online tracking solution
- It is recommended to integrate a link to the ad tech provider's privacy notice as this will enable the user to read more details on the products and related processing of user data
  **Example:** Google's Privacy Policy[29] should be appropriately referenced

## Data Subject Enquiries

**What to do?**

Advertiser establishes effective processes in order to fulfill data subject rights adequately

### How can advertisers appropriately respond to data subject enquiries?

- Companies usually have internal processes in place for responding to data subject enquiries (e.g. provide an input channel for external requests or set up a workflow for the internal processing of requests)
- These processes should also be used for enquiries coming from users that are subject to online tracking solutions implemented by the advertiser
- Ad tech providers for their part should provide technological means for the advertiser to fulfil the enquiries, so that the advertiser can easily extract relevant data sets from the solution and perform the necessary action on them (e.g. deletion of data sets)
- If these conditions are met, fulfilment of data subject rights should not be an issue

### What are generally occurring problems in online marketing with regard to data subject rights and how can you address them?

- Using online tracking solutions and identifiers may constitute an infringement of these rights
  **Example:** Users send requests for data subject rights by e-mail or through a provided online form
- An emerging challenge in this regard is how advertisers can link the request to the corresponding ID and user data
- It is recommended to find practical solutions in cooperation with ad tech providers
- A practical solution might be a function offered by the ad tech provider that enables users to change and delete data on their own
- Advertisers should also consider not to process additional user data and link it to online identifiers if this is just for the sake of data subject rights fulfilment

### Insights from use case evaluations

**All use cases: Google offers several solutions for users and advertisers to modify user data according to users' requests:**

- My Account[30]
- My Activity[31]
- Non-account holders form[32]
- User Explorer[33]
- Auto-delete controls[34]

**All use cases: The advertiser is an independently acting controller and is thus responsible for introducing effective processes for the fulfilment of data subject rights**

- The advertiser has to introduce effective processes for the fulfilment of data subject rights

# Risk Management

In risk management, the data protection risks for users arising from the use case need to be thoroughly examined and comprehensively documented. On this basis, both preventive as well as reactive technical and organizational measures can then be designed and implemented.

### Risk Assessment & TOMs

**What to do?**

- Advertiser executes a risk assessment considering the severity and probability of negative consequences the data
- Advertiser implements technical and organizational measures (TOMs) to ensure that the use case is designed and executed in compliance with the requirements of the GDPR
- Advertiser ascertains whether a data protection impact assessment (DPIA) is necessary
- If applicable: Advertiser executes the assessment and follows further provisions with regard to the data protection impact assessment (e.g. consultation of supervisory authority)

**The GDPR requires controllers (and processors) to implement technical and organizational measures (TOMs) based on the risk level of the processing:**

- TOMs are to guarantee a comprehensive GDPR compliance - especially with regard to the security of user data
- Online tracking solutions usually come with TOMs aiming at fulfilling all GDPR requirements and especially ensuring a certain level of security
- The advertiser needs to implement additional measures concerning the data processed by the online tracking solution, which the ad tech provider cannot offer **Example:** Advertiser needs to ensure that only employees requiring access to the processed data are provided with log-in information for the online tracking solution. Also, advertiser should establish a rights- and role-based access control system

**Do online marketing use cases typically require a DPIA?**

- Online marketing use cases usually require a careful consideration whether or not a DPIA must be conducted
- This is the case if the processing qualifies as bearing a high risk for users Example of an implementation where a DPIA could be necessary: The use case involves profiling, affects many users and collects a large amount of information about the respective user
- A publication by the Article 29 Data Protection Working Party on the DPIA might help[35]

**What are possible technical and organizational measures in online marketing?**

- Collection of data categories limited by default
- Contractual obligation between the parties involved not to use the data for further purposes
- Automated pseudonymization and anonymization of online identifier
- Automated aggregation of surfing patterns
- Automated deletion of cookies and user data on a server
- Secure authentication process for the access to user data
- Protection of the hardware used to store the user data
- Appropriate access management
- Encryption mechanisms

**Insights from use case evaluations**

**All use cases: Google solutions and services come with pre-defined and pre-implemented TOMs**

- All incorporated solutions and services provide TOMs
  **Example:** Google explicitly prohibits the import of further personally identifiable data into the Google Ads Remarketing servers, for more see Google's Article on Business and Data[36]

**All use cases: The advertiser as an independently acting controller is responsible for planning and implementing further TOMs**

- The advertiser needs to plan and implement further TOMs as required by the overall level of risk of the use case
- The advertiser will also be responsible for evaluating whether a DPIA is necessary

## Privacy Incidents

**What to do?**

Advertiser establishes effective processes to manage privacy incidents adequately

### What could be typical online privacy incidents?

- Passwords accessed by non-authorized parties
- User data disclosed following cyber attacks

**How can advertisers manage privacy incidents?**

- Companies usually have existing processes for managing privacy incidents (e.g. the procedure for submitting an incident and examining whether a data breach has actually occurred, which stakeholders are involved at what point in time or who will be responsible for public announcements)
- These processes should be applied to data processing activities around online marketing
- The obligation for the processors to immediately notify the controller should be included in their data processing agreement

### Insights from use case evaluations

**UC3 Web Analytics pure: Obligations to comply with reporting requirements are stated in contract**

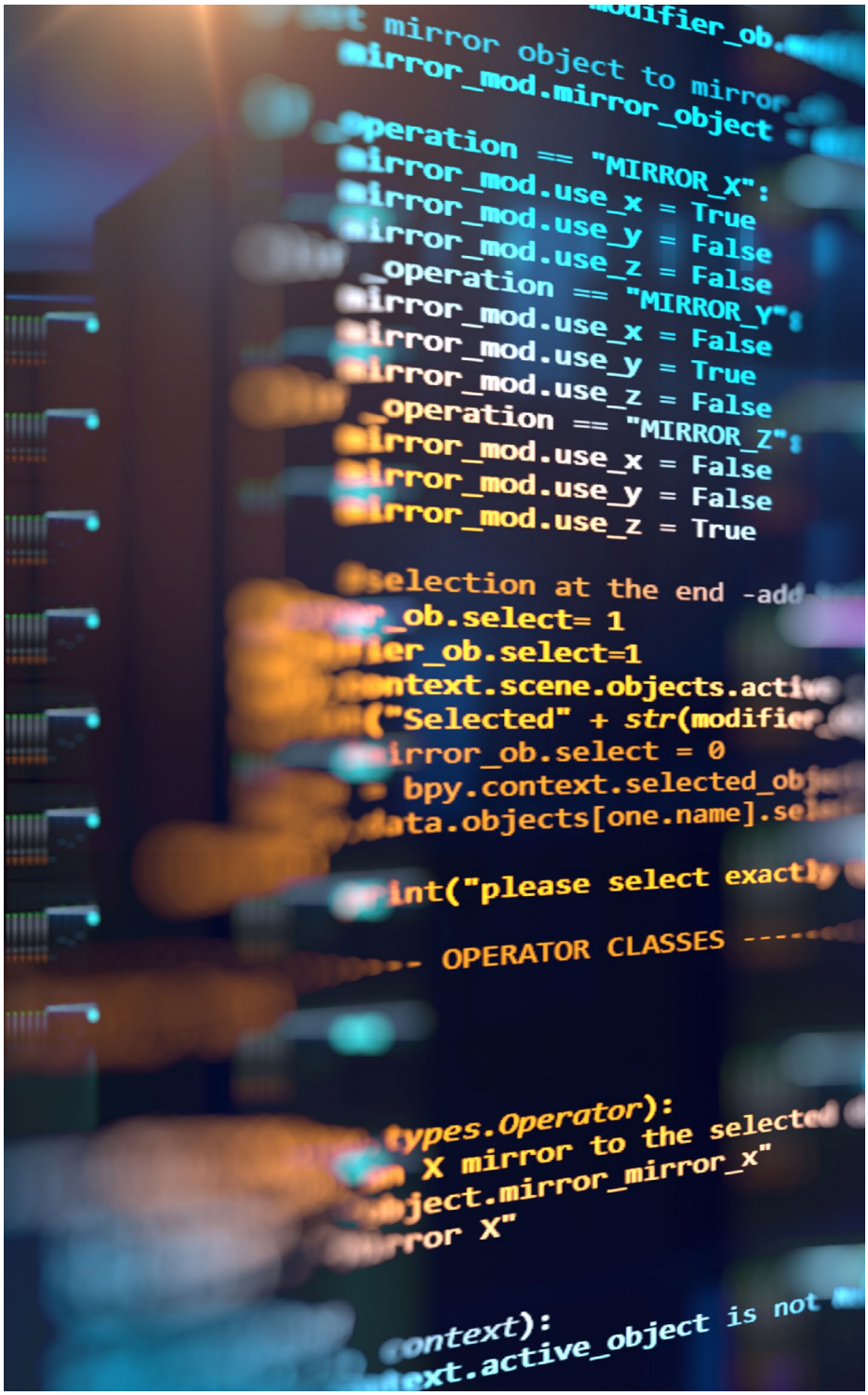
- The Processor Terms for the use of Google Analytics include provisions that oblige Google as the processor to immediately report data protection incidents to the controller (see the Processor Terms for detailed information[37])

**All use cases: The advertiser as an independently acting controller is responsible for introducing effective processes to manage privacy incidents**

- The advertiser is required to introduce effective processes for the management of privacy incidents

# Use Case Documentation & Monitoring

Use Case Documentation & Monitoring: Finally, the formal documentation must be completed in the legally required format of a Records of Processing Activities. Furthermore, it is essential to monitor changes to maintain privacy compliance.



## Records of Processing Activities

**What to do?**

Advertiser completes the documentation for the records of processing activities according to the data processing activities of the use case

### How can advertisers maintain the records?

- Companies usually have existing internal processes for the maintenance of the records of data processing activities (e.g. define how and when possible changes are monitored, who makes the change or new entry into the records and which body will issue the approval)
- These processes should be used for data processing activities in the context of online marketing
- The entry into the records is obligatory but does usually not constitute an obstacle

### Insights from use case evaluations

**All use cases: The advertiser as a controller is responsible for the correct completion and maintenance of the records**

- The advertiser is required to comprehensively and thoroughly analyze the use case in order to correctly create the entry in the records of data processing activities
- A chart gathering relevant use case information (i.e., processing activities, purposes, data categories, recipients, storage periods and technical and organizational measures) can help in creating the records

**UC3 Web Analytics pure: The advertiser has the contractual duty to provide all relevant information necessary for Google to comply with its legal obligation to maintain a record of processing activities performed on behalf of the advertiser**

- Google provides Google Analytics pure, making Google the processor of the advertiser and hence subject to the legal obligation to maintain a record of processing activities carried out by Google on behalf of the advertiser
- This includes, for instance, the name and contact details of the processor and the controller or the categories of processing
- For this reason, Google expects the advertiser to submit all relevant information required by Google to comply with its legal obligation to maintain the records[38]

## Monitoring

**What to do?**

Advertiser establishes effective processes to ensure continuous monitoring of changes of the data processing activities and changes of legal situations and to adjust the above-mentioned requirements in accordance to the changes

### How can advertisers manage monitoring?

- Companies usually have existing change processes (e.g. trigger identification, evaluation of implications, change planning, communication with and involvement of stakeholders, conduct of change)
- If these processes or their basic structures apply, they could be used to initiate and conduct a change concerning the implemented privacy requirements

### Insights from use case evaluations

**All use cases: Marketing should stay in close communication with privacy and legal department**

- The marketing business unit should notify the privacy and/or legal department of any use case changes as early as possible
- The basic use cases as specified above could lead to an increase in complexity by including more data, databases, solutions and partners
- The more complex a use case is, the longer it may take to obtain the final business approvals

**All use cases: The legal use case examinations are subject to changes in the legal landscape, jurisdictions and authorities' opinions**

- European privacy provisions are adapting to the digital progress and therefore might change from time to time
- Judgements of national courts or the EU Court of Justice can determine how to understand interpret privacy provisions correctly
- Data Protection authorities publish important content on how to exercise privacy provisions
- All these changes and opinions should be monitored and considered in the legal use case examinations

# Conclusion & Future-Proofing Tactics

In a privacy-aware world, advertisers' digital marketing efforts need to conform to changing user expectations and behaviors and comply with evolving regulatory and technological environments. We believe that the theoretical assessment of common use cases in digital marketing presented here shows that compliance with current privacy requirements is possible. However, being compliant varies very much with the specific implementation and configuration of various ad tech tools as well as established internal processes and collaboration with your agencies or tech providers.

A profound analysis of each use case will always be necessary and will always require a final evaluation by your internal data privacy officer. Our Deloitte Privacy Considerations Framework can help structure this evaluation along the following main components: use case modelling, permission, admin, data subject rights management and finally risk & monitoring. Keep in mind that our framework provides a structure and approach to guide your individual evaluation but certainly requires legal and technical expertise as well as compliance with the latest legislative and regulatory changes.

Next, we summarize the key learnings of the applied privacy consideration framework to the pre-selected use cases and conclude with an outlook on future-proof tactics for digital marketing in a privacy-aware world.

## Key Insights from the Use Case Evaluation

### Existing privacy consideration framework and information in place

- A privacy consideration framework helps break down complex use cases and prepare a clear decision template for the internal data privacy office

### Efficient compliance implementations are cross-functional efforts

- Design and implementation of online marketing use case should be supported by data protection experts
- Marketing, IT, data privacy office and legal need to cooperate in this field
- No function can do it alone. Rather, skills from all will be required
- This is especially important because client-specific use cases need to be explained

**Use Case Modelling: It all depends on the specific use case**

- Different use cases or similar use cases with different individual configurations or customer-individual additions will have different legal implications; This is very important to fully understand your use case
- It is possible for advertisers to shape most online tracking solutions so that they become more privacy-friendly (e.g. choose not to activate Google Analytics data sharing)
- The purposes can affect the choice of the online tracking solution (e.g. if only web analytics is required, a basic version of a web analytics tool, e.g. Google Analytics, might be sufficient)
- Depending on the advertiser's use case, different types of data categories will be collected, processed, and stored
- Methods such as fingerprinting do not provide choice and control for users. By contrast, cookie-based methods leave the final decision to the user (e.g. user can disable cookies in browser)

**Permission: A thoughtful assessment can help tackle the main uncertainty**

- The choice of the adequate legal basis is legally necessary and essentially determines the possibilities of data processing
- Clarity of need for an informed consent varies by use case
- Even though a clear guidance is not always possible, there are several indicators for and against an informed consent which advertisers may use as navigation
- Platforms have also policies, which can be used as further guidance
- There is no conclusive legal information on how to implement a consent banner for full compliance
- However, public authorities, courts, commercial institutions and the online marketing market in general provide high-level guidance on the implementation of a consent banner and standards begin to emerge (e.g. tracking tool classification)

**Data Subject Rights Management, Risk Management, Use Case Documentation & Monitoring: Obligatory but generally not an issue**

- Requirements are legally obligatory but generally do not constitute an obstacle for the implementation of the use case
- With regards to the use cases analyzed in this paper, Google established a standardized approach for the fulfilment of some of the legal requirements, which ultimately can save the advertisers time and money (e.g. solutions for fulfilling users' enquiries)
- Advertisers can use already existing internal processes in order to execute requirements around privacy
- Advertisers should be very sensitized with regard to changing external conditions (e.g. changing or evolving law or public opinions) or internal conditions (e.g. changing in collected data sets, purposes, used online tracking solutions) in order guarantee a continuous compliance

## Future-Proofing Tactics: What advertisers should be doing to ensure a privacy-aware data driven marketing

As the digital ads ecosystem continues to evolve and technical adaptations restrict the ability to collect cookie data as we know it from the past, businesses in general and advertisers in particular will have to change how they operate and interact with their customers. While fewer data might be available, there are new advancements in technology that can overcome data strategy holes.

A fundamental shift into the predictive era based on machine learning is occurring. Adopting new technologies, having a test-and-learn mentality, and employing multiple measurement solutions are becoming the strategies that will help marketers achieve their goals.

Lastly, keep in mind that the compliance with regulatory requirements and adaptation to changing consumer expectations with regards to privacy and data handling is the core fundamental of any digital marketing effort across all industries and European markets.

# Glossary of terms

01. 1st party data: Data which a company collects directly from its audience, e.g. website usage or CRM system.
02. 3rd-party cookies: Cookies set by a third party (e.g. ad tech platform) on a publisher's website to track user and offer online advertising services.
03. Audience: A group of website users characterized by similar attributes (e.g. age range, interests) defined by the advertiser. An advertiser defines audiences to show the right ads to the right user at the right time.
04. Click ID: A digital label assigned by Google Ads to identify a specific ad and measure a user's corresponding interaction.
05. Controller: A natural or legal person who determines the purposes and the means of the data processing activities alone or jointly with others (Article 4 (7) GDPR).
06. Conversion: Completion of a defined goal by a website user e.g. purchase on a website or registration to a newsletter.
07. CRM (Customer Relationship Management): A system storing customer data to provide information about the customer lifecycle and support customer-specific relationship management.
08. Data Protection Impact Assessment (DPIA): An evaluation of the impact that high-risk data processing activities might have on the protection of personal data (Article 35 GDPR).
09. Data Subject: The identified or identifiable person whose personal data is being processed (Article 4 (1) GDPR).
10. Data Subject Rights: A variety of legally determined options for data subjects to obtain insights into and affect the processing activities performed on their data (Articles 12-22 GDPR).
11. E-Privacy Directive: European Union directive on privacy and electronic communications (Directive 2002/58/EC and Directive 2009/136/EC).
12. GDPR: European Union's General Data Protection Regulation (Regulation 2016/679/EU).
13. Google Ads: An online advertising platform allowing advertisers to display advertisements within the Google ad network to web users.
14. Joint Controllers: Two or more controllers jointly determining the purposes and the means of data processing activities (Article 26 GDPR).
15. Personal data: Any information related to an identified or identifiable natural person. Most of user data collected online is considered personal data since unique identifiers allow advertisers and ad tech providers to address specific users along their online journey. Sometimes it might even be possible to find out a user's exact name or private address.
16. Privacy incident: A breach of personal data such as a disclosure to a non-authorized party (Article 35 GDPR).
17. Processor: A natural or legal person who processes personal data on behalf of the controller (Article 4 (8) GDPR).
18. Records of Data Processing Activities: A legally compulsory internal documentation of all data processing activities performed on personal data by the controller or the processor (Article 30 GDPR).
19. Retargeting (Google Remarketing): A method in online marketing in which a user having recently visited a website can be tracked and readdressed on other websites through the use of an individual online identifier.
20. Technical and organizational measures (TOM): Measures to ensure that data processing activities are performed in accordance with the provisions of the GDPR (Articles 24, 25, 32 GDPR).
21. User consent: An action in which the user indicates (e.g. via a content banner) that they agree to a specific processing of their user data.
22. User ID: a unique identifier of one website user set by the website owner. It is used to collect information on website behavior and recognize the user, if returned to the website.

# Endnotes


01. Source: Google https://www.thinkwithgoogle.com/marketing-resources/netshoes-doubles-roi-with-remarketing/
02. Source: Google https://www.thinkwithgoogle.com/intl/de-de/insights/markteinblicke/karstadt-nayoki-dynamisches-display-remarketing/
03. Source: Google https://www.thinkwithgoogle.com/intl/de-de/insights/markteinblicke/wie-verti-uber-mobile-sem-kampagne-konversionen-und-offlinevertrieb-steigert/
04. Source: Google https://www.thinkwithgoogle.com/intl/de-de/insights/markteinblicke/google-smart-bidding-flaconi-aktiviert-eigene-conversion-daten/
05. Source: Google https://marketingplatform.google.com/about/resources/analytics-360-boosts-wyndham-website-engagement/
06. Source: Google https://marketingplatform.google.com/about/resources/american-cancer-society-donations-rise-with-analytics/
07. Source: Google https://marketingplatform.google.com/about/resources/mumzworld-reaches-return-on-ad-spend-with-analytics/
08. Source: Google https://marketingplatform.google.com/about/resources/analytics-360-helps-matalan-lift-conversion-rates/
09. Source: Google https://marketingplatform.google.com/about/resources/panasonic-improves-return-on-ad-spend-with-analytics-360/
10. Source: Google https://marketingplatform.google.com/about/resources/panasonic-improves-return-on-ad-spend-with-analytics-360/
11. Source: Google https://marketingplatform.google.com/about/resources/mumzworld-reaches-return-on-ad-spend-with-analytics/
12. Source Google https://marketingplatform.google.com/about/resources/bt-display-and-video-360-buys-informed-by-analytics-360/
13. Source: The World Wide Web Consortium (W3C) https://www.w3.org/2014/strint/papers/41.pdf
14. Source: Google https://support.google.com/analytics/answer/1011397?hl=en
15. Source: Google https://support.google.com/analytics/answer/9024351?hl=en
16. Source: Google Processor Terms: https://privacy.google.com/businesses/processorterms/, Controller-to-Controller Terms: https://privacy.google.com/businesses/controllerterms/, Measurement Controller-to-Controller Terms (https://support.google.com/analytics/answer/9012600
17. Source: German data protection authorities: DSK, Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich, May 2020 https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf
18. Source: Google https://support.google.com/google-ads/answer/6389382, https://policies.google.com/privacy?hl=en-US#infocollect
19. Source: Google https://support.google.com/analytics/answer/7667196
20. Source: Google https://privacy.google.com/businesses/retention/
21. Source: Google https://privacy.google.com/businesses/retention/
22. Source: Google https://support.google.com/google-ads/answer/7664943?hl=en
23. Directive on privacy and electronic communications (Directive 2002/58/EC and Directive 2009/136/EC)
24. Source: European Court of Justice, case C-673/17, "Planet49", October 2019 (http://curia.europa.eu/juris/celex.jsf?celex=62017CJ0673&lang1=de&type=TXT&ancre=)
25. Source: Google https://www.google.com/about/company/user-consent-policy/
26. Sources: Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, April 2014 (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf); German data protection authorities: DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, March 2019 (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf)
27. The following sources can give navigation for implementing a consent banner GDPR compliant: Article 4 (11), Article 7, Recitals 32, 42 and 43 GDPR; European Court of Justice, case C-673/17, "Planet49", October 2019 (http://curia.europa.eu/juris/celex.jsf?celex=62017CJ0673&lang1=de&type=TXT&ancre=); EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, May 2020 (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf); German data protection authorities: DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, March 2019 (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf); United Kingdom's Information Commissioner's Officer: How should we obtain, record and manage consent? (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/); France's Commission Nationale de l'informatique et des Libertés: CNIL's guidelines on cookies and tracking devices, July 2019 (https://www.cnil.fr/en/cookies-and-other-tracking-devices-cnil-publishes-new-guidelines)
28. Source: Google https://www.google.com/about/company/user-consent-policy/
29. Source: Google https://www.google.com/url?q=https://policies.google.com/technologies/partner-sites?hl%3Den&sa=D&ust=1592814086386000&usg=AFQjCNE2LlhnQzU3md04EJtyuJAcxUcCKQ
30. Source: Google https://policies.google.com/privacy?hl=en-US#infodelete
31. Source: Google https://myactivity.google.com/myactivity
32. Source: Google https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&hl=en&rd=1&pli=1
33. Source: Google https://support.google.com/analytics/answer/6339208; https://developers.google.com/analytics/devguides/config/userdeletion/v3
34. Source: Google https://www.google.com/url?q=https://www.blog.google/technology/safety-security/automatically-delete-data/&sa=D&ust=1591258572102000&usg=AFQjCNFgD63hJbKTreeFQzHCuEjmF_13LA
35. Source: European Commission https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
36. Source: Google https://privacy.google.com/businesses/
37. Source: Google https://privacy.google.com/businesses/processorterms/
38. Source: Google https://privacy.google.com/businesses/processorterms/

# Contacts

**Stefan Buchholz**
Partner
Risk Advisory | Cyber
Tel: +49 (0)221 9732 4307
stbuchholz@deloitte.de

**Dr. Lars Finger**
Partner
Consulting | Deloitte Digital
Offering Lead Marketing & Commerce
Tel: +49 (0)40 32080 4948
lfinger@deloitte.de

**Maximilian König**
Senior Manager
Consulting | Deloitte Digital
Marketing & Commerce
Tel: +49 (0)40 32080 4368
maxkoenig@deloitte.de

Deloitte.



Issue 02/2021