precis.

A Marketer's guide to consent in 2024

Privacy, first-party data and what you need to do to be ready

Important:

Please note that the following is only our best interpretation of general EU privacy laws as well as recent case law developments, but that it in no way constitutes any legal advice. We recommend you consult your legal counsel on this to ensure your data collection and processing practices are up to date and in compliance with applicable laws and regulations.

1. Introduction

Welcome to the new age of consent

Traditional consent banners are not enough to support digital marketing activities in 2024.

With the demise of third-party cookies - which is prompting platforms to use email addresses as identifiers - and Google's new consent requirements for advertisers, we are forced to reassess how we approach consent strategies.

But fear not, we've done the research for you and created this guide to help you move forward.

We'll explore the strategic aspects and some of the legal considerations to be had when collecting and activating data for digital marketing amid technology and platform changes, this will focus specifically on what changes you need to make to collect consent for first-party user data.

Our goal? To equip you with the information you need to outline your own consent strategy that meets the opportunities and requirements of the current digital marketing ecosystem.

The time for privacy maturity

Privacy maturity involves, first and foremost, having a consent flow that empowers users with control and transparency over their data-sharing choices. But also, a compliant data strategy that allows advertisers to activate the data they need when they need it.

The sunset of third-party cookies and increased fragmentation have led to digital marketing platforms demanding more data from advertisers. First-party data is becoming the new normal, but we need to adapt our privacy strategy to meet this new status quo. We need to remember that no data foundation is sustainable in the long term if it does not include consent.

A new approach

Our research led us to two alternative methods that allow the collection of consent for activation of first-party data for digital marketing and analytics purposes:

- One is collecting consent through a detailed and comprehensive consent banner.
- The second approach is through a granular set of checkboxes in the data collection point.

Both are presented to help explore possible processes for data collection and activation, considering some of the EU/EEA's data protection requirements, but might apply in different ways to each advertisers.

We are taking into account the current state of play of digital marketing and the technical limitations posed by the tools we have at hand to build this solution. As a result, this guide aims to:

- ✓ Help you create a consent foundation to meet your advanced data strategy needs
- ✓ Help you communicate clearly with users on what data you are collecting and for what.
- ✓ Help you to activate first-party data and observed data through Google platforms

What do I need to do?

Pick one or more scenarios that describes your situation

JUST GETTING STARTED	You have no consent solution in place	**Chapters: All** If you are operating in most European markets, a consent solution is a basic requirement. This guide will help you design a solution that matches your needs and your data strategy.
ADVANCED SETUP	You are collecting email addresses and using them for digital marketing through audience lists or conversion actions.	**Chapters: 2 & 3** Make sure that your consent solution is comprehensive enough to collect the data you are using and that you have the correct consent mechanisms in place.
FIGURING OUT GOOGLE'S UPDATES	You are using Google platforms such as Google Ads, DV360 or Google Analytics 4	**Chapters: 5** You need to ensure that Consent Mode is in place by March 2024. Understanding Google's requirements and ensuring that your solution is compliant, will be the first required action from you.

2. Navigating data strategy today

Learn about the types of data, purposes of data collection and methods of data integration.

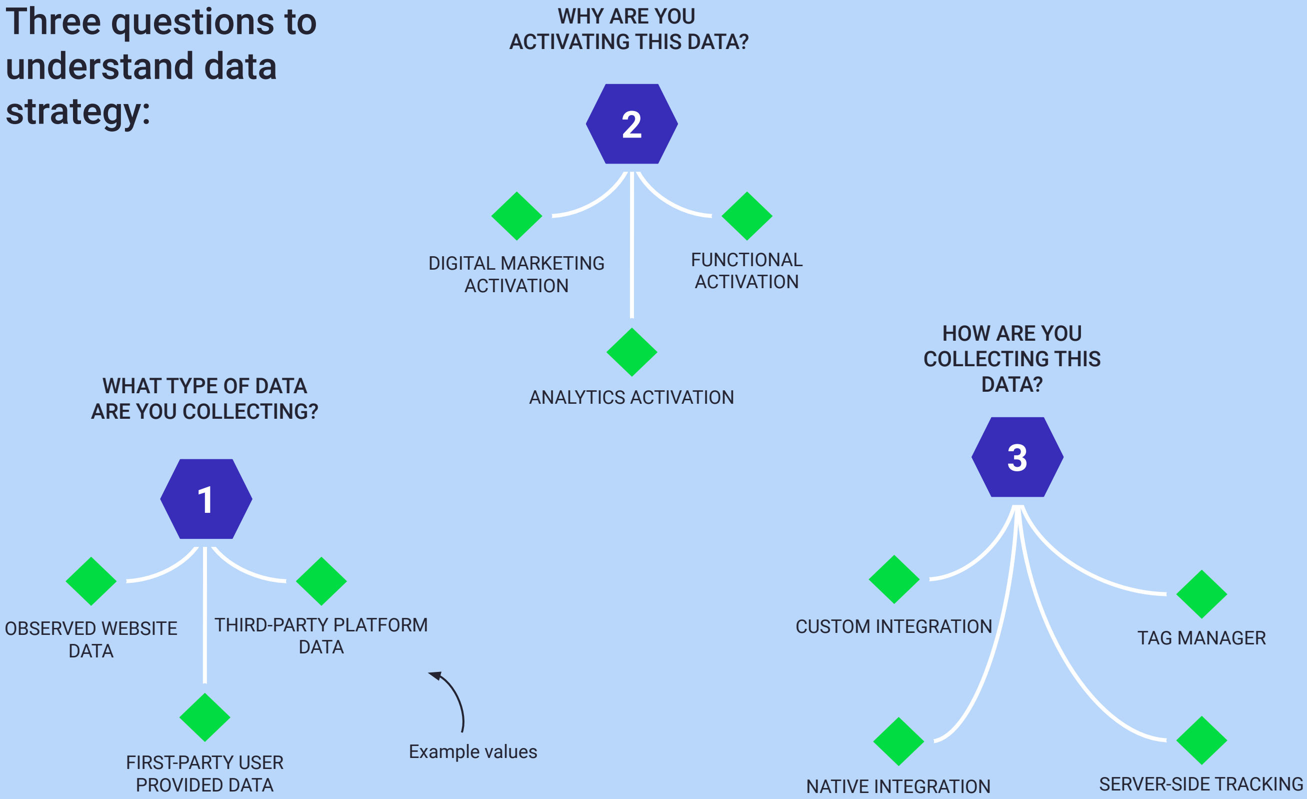
Privacy as data strategy

In this chapter, we will discuss the elements that should be considered as part of your data strategy to allow you to make agile decisions when it comes to your data collection and activation.

We will go through a three-step process: Types of data, purposes of data collection and methods of data integration. By the end of this, you should have a clearer understanding of the state of play of data collection for digital marketing purposes.

Following these steps is the first step in reaching compliance, they will give you the clarity you need to define your consent needs.

Three questions to understand data strategy:



WHAT TYPE OF DATA ARE YOU COLLECTING?

1

OBSERVED WEBSITE DATA

THIRD-PARTY PLATFORM DATA

FIRST-PARTY USER PROVIDED DATA

Example values

WHY ARE YOU ACTIVATING THIS DATA?

2

DIGITAL MARKETING ACTIVATION

FUNCTIONAL ACTIVATION

ANALYTICS ACTIVATION

HOW ARE YOU COLLECTING THIS DATA?

3

CUSTOM INTEGRATION

TAG MANAGER

NATIVE INTEGRATION

SERVER-SIDE TRACKING

Mapping the types of data

There are many types of data involved in a digital marketing setup. In this guide we will take a look at the three main types of data that can be integrated into marketing platforms for data activation: observed website data, user-provided first-party data and third-party platform data.

These definitions are an important starting point because consent needs to be specific to the data that you are collecting and users need to be sufficiently informed.

01

Observed website data

Some signals that we classify as observed data are well-known to most advertisers, such as website purchases, pageviews, product views, form submission events. These events normally happen online and can easily be collected through tag management systems. They often come attached with observed user signals such as IP addresses or pseudonymous identifiers like client IDs.

Other observed signals are considered to be more advanced, such as those that often happen offline like user interactions with sales representatives, account cancellations or a lead qualification. In most cases, tracking events that happen offline will require an integration and these events will also have to be paired with an observed pseudonymous identifier such as a Client ID so that the integration works well.

02

User-provided signals (first-party user data)

User-provided signals are those that are inputted by users and often stored on CRM platforms or ecommerce platforms. An example of first-party user data that can often be shared with digital marketing platforms are hashed email addresses or telephone numbers. In the case of B2B advertisers, another example would be company size, sector or name. These are signals that can be collected through simple online forms or through offline sales systems. They can be integrated with digital marketing platforms directly through tag management systems when they are collected online or through CRM integrations. More recently, a number of platforms have launched functionalities that collect user-volunteered data automatically, which is also something that needs to be taken into account.

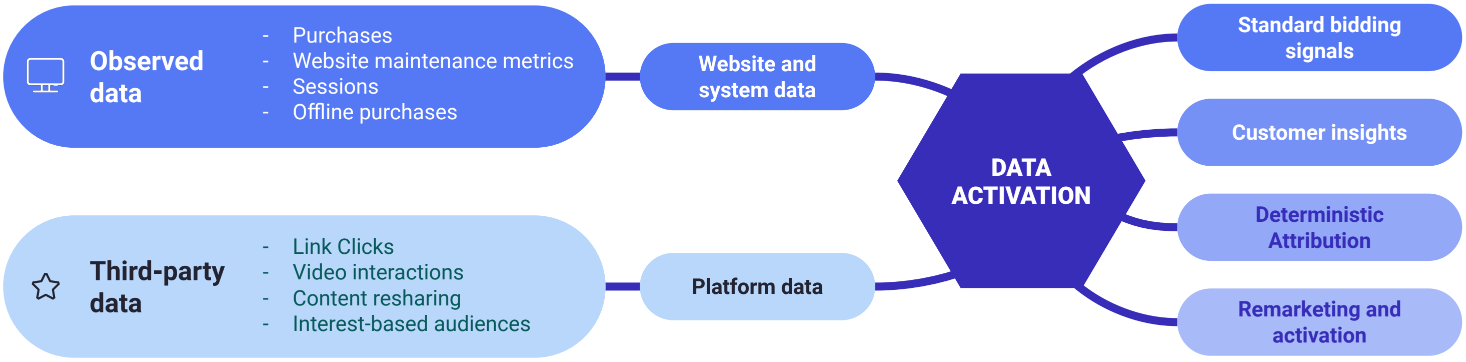
03

Platform data

Platform data makes up the last pillar of the data foundation for digital marketing. When we refer to platforms in this context, we are including ad serving platforms, search engines and social media. Each one of these are collecting their own data, which is controlled by their own agreement with end users.

From 2019 to 2024

Digital marketing data in 2019



Observed data
- Purchases
- Website maintenance metrics
- Sessions
- Offline purchases

Third-party data
- Link Clicks
- Video interactions
- Content resharing
- Interest-based audiences

Website and system data

Platform data

DATA ACTIVATION

Standard bidding signals

Customer insights

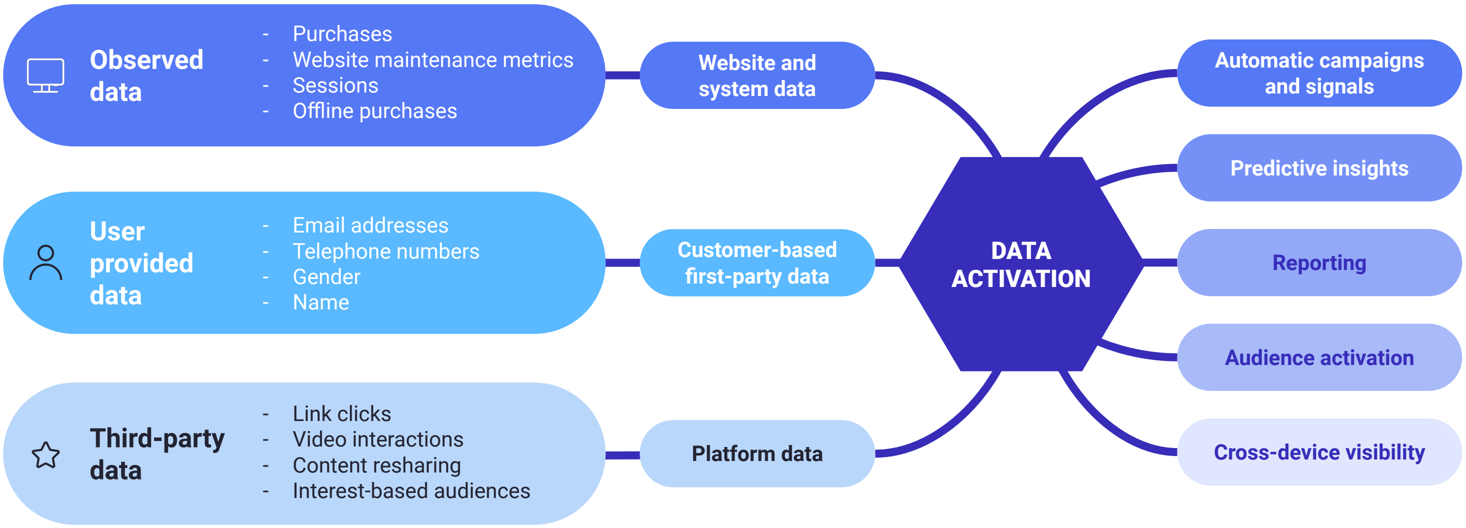
Deterministic Attribution

Remarketing and activation

What changed

- Digital is more fragmented
- More competitive market
- Regulations are getting stricter
- Tech is more advanced
- More data of worse quality

Digital Marketing data in 2024



Observed data
- Purchases
- Website maintenance metrics
- Sessions
- Offline purchases

User provided data
- Email addresses
- Telephone numbers
- Gender
- Name

Third-party data
- Link clicks
- Video interactions
- Content resharing
- Interest-based audiences

Website and system data

Customer-based first-party data

Platform data

DATA ACTIVATION

Automatic campaigns and signals

Predictive insights

Reporting

Audience activation

Cross-device visibility

The purposes of activation

We have arrived at the purpose of activation which, in this context, is not the top-level strategic value of activation, but the answer to the question: Why would you like to activate this data?

Documenting data activation use cases will require a governance effort, but this will be a valuable resource in the future as it will maximise opportunities, streamline strategic actions and minimise compliance risks.

At this point, we land on a common question about first-party data activation: can a company use the consent flow for newsletter signup as a valid consent mechanism to activate first-party data for digital marketing purposes? And the answer is that under our interpretation, newsletter and direct email activation falls under a different processing activity – Direct Marketing – which requires specific consent.

If we are taking the digital marketing use cases specifically, we think that these are two useful initial categories to work with:

Analytics activation

When we refer to data being used for analytics purposes, we are implying that even when this data is collected on individual levels, it will be aggregated and used to improve reporting only. A tool that activates CRM data for reporting purposes only is enhanced conversions.

Marketing activation

When we refer to data being used for marketing activation, we are thinking of data that can be activated on an individual level. For example, if you share an email with Facebook for custom audiences, you can add that specific email - or group of emails - to an audience and target them specifically.

Regardless of whether it is observed data, or first-party user data, analytics activations are one-way avenues: Even when they are employing user identifiers, these cannot be activated on an individual level, because they are designed to support reporting only. The exception to this rule might be website personalisation and testing. Volunteered data collected for analytics or reporting purposes is often deleted right after utilisation.

Data used for marketing and optimisation can often be activated on an individual level for a set period of time. This includes delivering personalised advertising and adding users to lookalike audiences. The key to how long data is available for activation depends on how long cookies remain in the browser or the data retention periods set on each platform.

What if a tool doesn’t fit a single specific category?

There are many cases such as this one and at times it is not easy to distinguish.

Take Google Analytics. One might be able to export audiences from Google Analytics straight into marketing platforms. It is possible, however, to disable advertising features for opted out users, so the solution is straightforward.

A tool such as enhanced conversions is less easy to analyse. The grey-lines between analytics and marketing are blurred, so we prefer to categorise it as a marketing tool which is a more overarching category.

Integrating data and breaking silos

There are many methods for data integration that will vary from advertiser to advertiser and from the types of data that are being handled. Their common denominator is that integrations will use events or user identifiers to merge datasets together and produce a seamless picture.

When it comes to performance marketing endpoints, there are four notable means of data integration:

Out of the box plugins:

A common method of integration is through out-of-the-box plugins or tags that fetch data as it is submitted. This method is very common today and often available through Google Tag Manager. It doesn't afford much flexibility or personalisation.

Native connections:

Another method of integration uses native connections that are already inbuilt on both sides, an example of that is SalesForce's native connector to Google Ads.

Custom CRM integrations:

You can also build a custom integration to connect the data on your CRM system with digital marketing platforms through common identifiers. Data can also be joined through a data warehouse like Big Query and then distributed back to Google Analytics.

Server-side tagging:

Finally, server-side tag management systems that are able to distribute data from an advertiser's servers' straight to digital marketing platforms can be used.

Consent and methods of data integration

Once you define the purpose of your data activation and the method you can use to integrate your system, you will be able to map out what the consent requirements are for that particular activation and integration and what technical requirements you need to meet in order to safely integrate your data.

What comes first? Purpose or method?

Always put purpose before method in your prioritisation. You need to start thinking about why you need to activate data and what value you get out of it before planning your integration.This is also a legal requirement, as companies shouldn't collect data that serves no purpose in its strategy, which needs to be mapped in your privacy policy.

3. A consent solution for 2024

Unsure of how to strike the balance between getting the most out of your data while also protecting users' privacy? Look no further; this chapter has you covered.

Consent in a nutshell

We hope to equip advertisers to make the decisions that will allow them to use their data to its maximum possible extent while also protecting users and granting them the control and data ownership they are accountable for. Having said that, decisions must always be made on a case-by-case basis depending on the specific circumstances at hand.

Traditionally, advertisers have relied on consent banners to collect website data such as purchases or sessions (observed website data), but with emails (first-party user data) becoming more commonly used by platforms, there is a need for a new standard of consent.

Collecting first-party user data and processing it for purposes such as analytics or marketing, will require a valid legal basis. The advertiser must determine what this legal basis is and fulfil all applicable GDPR requirements (including but not limited to information provided to data subjects).

Certain user-provided first-party data can be hashed or pseudonymised, but it may still constitute personal data under applicable regulations (e.g. the GDPR) because it can be used to identify users individually.

Our recommendation is that the legal basis for collection and activation of both first-party and website data should be consent, and that valid consent for each purpose should be collected from users before data is processed and shared with platforms.

Based on the technical requirements and our understanding of how data is collected and processed by digital marketing platforms, we developed two alternatives for advertisers who want to collect consent for first-party data:

1. Collect consent for first-party data using your typical consent banner, but updating the copy to encompass a comprehensive communication of how data is collected and processed for each type of data.
2. For a more cautious and advanced approach, use granular consent checkboxes at the point of data collection.

The evolution of the traditional consent banner

Traditional consent banners

Normally comprehensive enough for collection of cookie-based website data. Often focusing on cookie usage and not on data collection, which means that it might not be specific enough for first-party data collection.

Comprehensive consent

Adapted to the collection and activation of first-party data for digital marketing purposes. It shares the same consent mechanisms as the traditional banner, but improves communication, shifting it away from communicating cookies to a more specific approach mentioning first-party data as well as observed website data.

Consent checkboxes

For an advanced approach, additional consent checkboxes might serve as a mechanism for privacy mature advertisers. This approach might demand development time and resources.

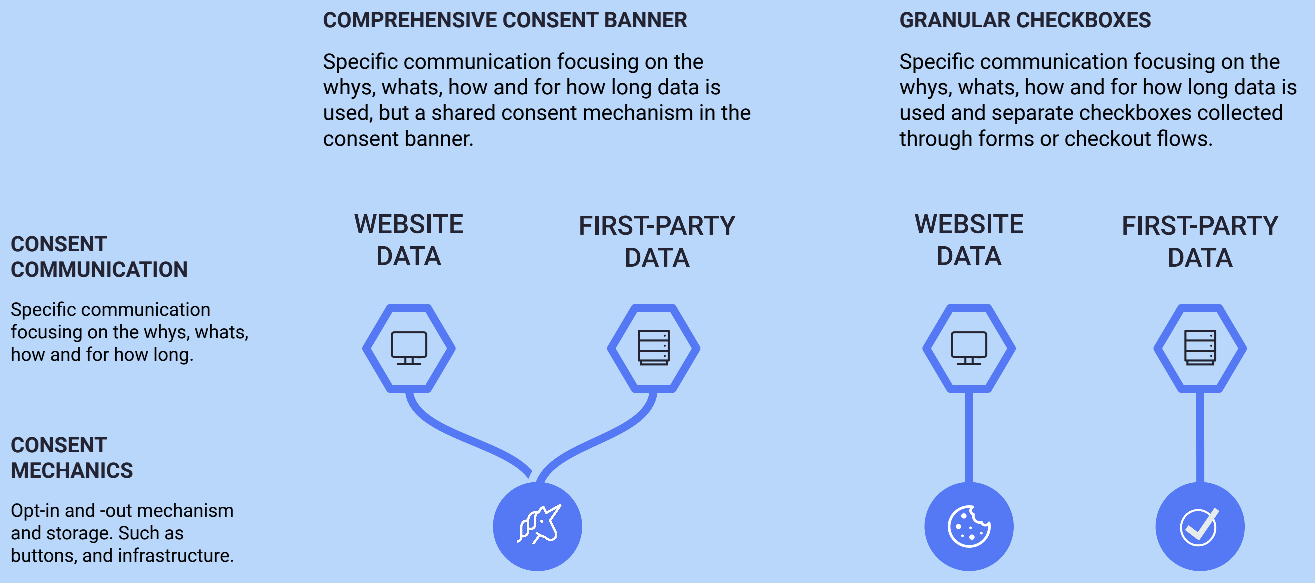
What makes a good consent flow?

Our assessment is that advertisers might be able to rely on consent banners and policies when collecting and distributing first-party user data, however, in most cases, the banner will need to be adapted because common out-of-the-box solutions do not cover the basic requirements for first-party activation.

Consent under the GDPR needs to be freely given, specific, informed and unambiguous to be considered valid. Consent will only be valid for the granular processing activities covered by that banner, which in the case of traditionally worded cookie consent banners, is generally collection of data through cookies and activation of that data for set purposes. Most standard consent banners do not cover the collection and activation of e-mail addresses or other user-provided signals specifically, focusing only on cookies or observed website signals.

Our solution is that a comprehensive consent banner that addresses communication needs for both observed and user-provided first-party data can serve as the same consent mechanism to obtain consent, but advertisers might also choose an advanced route.

It is important to note that most advertisers today use Consent Management Platforms to manage their consent solution so any solution needs to be compatible with what is provided by these platforms. In our perspective, the ideal consent flow is, above all, achievable and manageable. A solution that is too complex will not meet its purposes. With that in mind, we came up with technically sane solutions that we think will meet current requirements:



COMPREHENSIVE CONSENT BANNER

Specific communication focusing on the whys, whats, how and for how long data is used, but a shared consent mechanism in the consent banner.

GRANULAR CHECKBOXES

Specific communication focusing on the whys, whats, how and for how long data is used and separate checkboxes collected through forms or checkout flows.

CONSENT COMMUNICATION

Specific communication focusing on the whys, whats, how and for how long.

CONSENT MECHANICS

Opt-in and -out mechanism and storage. Such as buttons, and infrastructure.

Consent checklist

We prepared a checklist elements we recommend you look into when it comes to evaluating your consent solution. Remember that under our model, first-party data and observed website data will share the same mechanism, but have their own communication requirements.

Consent communication

Observed website data

- Information about **why** the advertiser is using website and navigation data present on the banner and policy
- Information about **what** website data is being collected present on the banner and policy
- Information about **who** website data is shared with present on the banner and policy
- Information about **how** users can change their minds and opt out of sharing their website behaviour present on the consent policy and banner
- Information about **how long** website data is attached to cookies on the users' browsers present on policy

First-party user data

- Information about **why** the advertiser is using first-party data present on the banner and policy
- Information about **what** first-party data being collected and activated present on the banner and policy.
- Information about **who** first-party data is shared with
- Information about **how** users can change their minds and opt out of sharing their first-party data
- Information about **how long** first-party data is attached kept by partners (data retention).

Consent Mechanics

First-party user data and observed website data

- Solution allows users to opt in to tracking of website data and of sharing their first-party data with advertising platforms
- Solution allows users to change their mind and own their decision
- Solution allows users to access the information they need to understand what is happening with their data

Granular consent checkboxes

Consent communication and mechanics

- Information about first-party data being collected and activated present on the form being used for collection
- Information about why the advertiser is using first-party data present on the form being used for collection
- Allows users to opt out of sharing their first-party data for digital marketing purposes
- Allows users to access the information they need to understand what is happening with their first-party data

KEY:	Traditional consent solution	Comprehensive consent solution	Shared consent mechanism	Granular consent checkboxes
	✓	✓	✓	✓

Do we need an advanced approach to consent?

As previously mentioned, the recommendations in this document are based on the assumption that traditional consent banners tend to be focused exclusively on cookies and similar tracking technologies. A traditional cookie banner consent flow is therefore only appropriate for the collection of the type of data specified in such banners, which is typically observed website data. Different types of data need to be specifically mentioned and mapped out.

Provided it is clear enough and fulfils the GDPR requirements, this can be achieved by changing the communication in the current banner, but we also provide an alternative that includes a two-step approach.

The main issue our research found with the advanced approach is that it is that it would demand working closely with your Consent Management Platform to develop a tailored solution. With this in mind, we recommend creating a long term strategy with iterative steps towards a full advanced setup.

Comparison between the three possibilities

Traditional consent banners

Focus on cookies and data-types focused on cookie identifiers.

Does not specify the types of data that are encompassed within the cookie-based category.

Mentions third-party tools, which is good.

Normally considers cookie-duration instead of data retention.

Granular consent banners

Specifies the type of data that is being collected, mentioning both observed and first-party data.

Lists third-party tools that will receive users' first-party data.

Includes a more descriptive definition of how data will be retained.

Will also include an explanation of how data is kept safe.

Has specific communication for first-party data, but shares a single mechanism for observed and first-party.

Granular checkboxes

Includes a checkbox asking for consent when the data is collected.

Includes a tailored mechanism to allow users to remove consent.

Is integrated with your CRM system.

Bringing everything together

In conclusion, advertisers have two alternatives when designing a consent solution: either relying solely on their consent banner or choosing a more advanced architecture.

If advertisers decide to rely on their consent banner, they need to make sure that this refers to both observed and user-provided first-party data. Naturally, this should also meet the criteria and the GDPR requirements for consent. If the banner is specific enough, it might serve as the single mechanism to obtain consent for activation of first-party data for both digital marketing and analytics purposes.

If advertisers on the other hand would like to build a more robust and advanced architecture, they could obtain consent for first-party data collection through a separate flow that includes consent checkboxes in the forms and checkout flows that are used to gather information.

The full picture: Data types, examples and activation

DATA TYPE	Observed navigation data	User provided first-party data
EXAMPLES	*Online events such as pageviews, sessions and conversions.* *Offline events such as cancellations, offline upselling or phone calls.*	*Form data such as email address or phone number.*
ANALYTICS ACTIVATION	*Collect navigation data on your analytics platform for cross-channel attribution.*	*Employ first-party user data for advanced product analytics and predictive modelling.*
MARKETING ACTIVATION	*Collect navigation data on digital marketing platforms for campaign attribution, cookie-based audience creation and cookie-based lookalike audiences.*	*Activate user data to create durable audiences on social media platforms and onboard it to platforms for lookalike audiences.*
CONSENT MECHANISM	*Consent banner*	*Granular consent checks or granular consent banner*

Image 5: This table shows everything we've covered so far, laying out the three types of data advertisers can collect. What is therefore not mentioned here is platform data, the integration methods, purposes of activation and recommended consent mechanism.

4. Illustrated examples

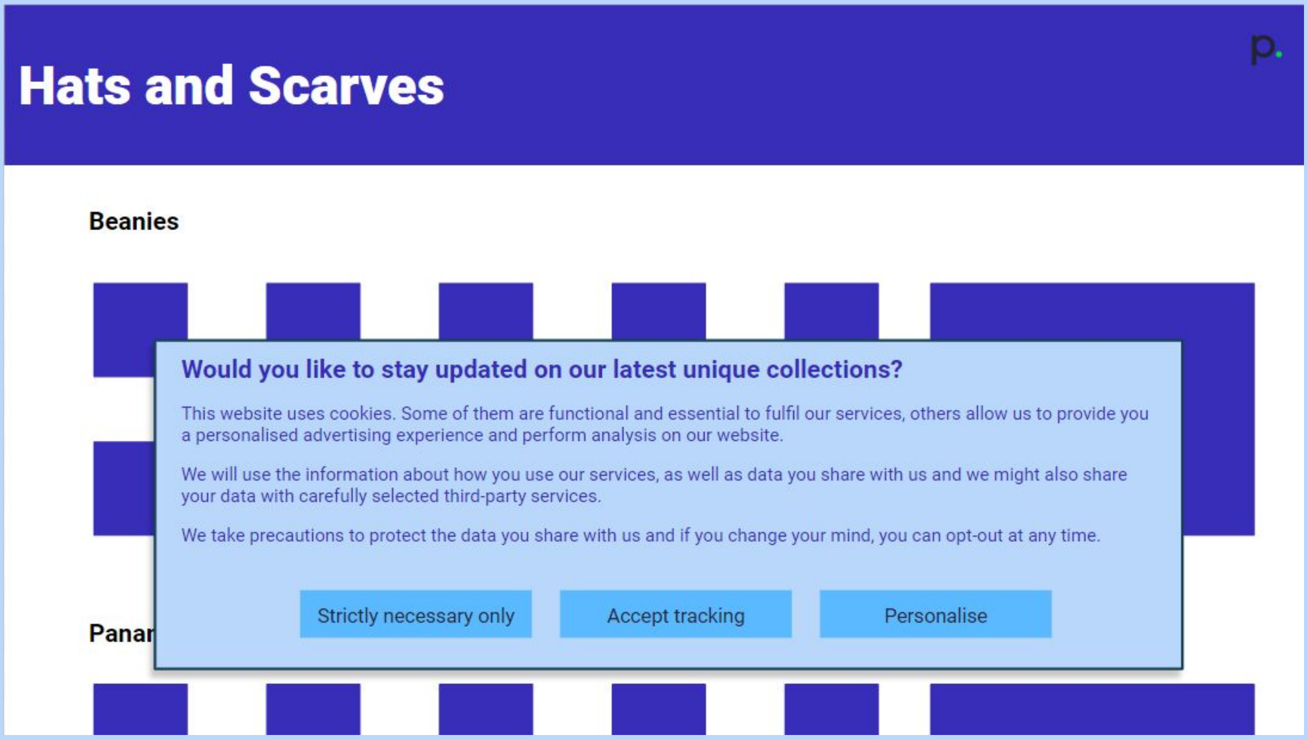
Illustrated examples for the visual learners.

Traditional consent

Typical cookie consent banners are not enough to ensure that advertisers are able to activate first-party data in digital marketing platforms to the best of their ability. With that in mind, we put together three examples to illustrate the suggestions we presented.

The first example is a typical consent banner that refers only to cookie usage and alludes briefly to observed user data. This is a banner we would not consider sufficient for first-party activation but might be enough for activation of observed website data.

Demo consent flow: A banner for collection of observed website data



Would you like to stay updated on our latest unique collections?

This website uses cookies. Some of them are functional and essential to fulfil our services, others allow us to provide you a personalised advertising experience and perform analysis on our website.

We will use the information about how you use our services, as well as data you share with us and we might also share your data with carefully selected third-party services.

We take precautions to protect the data you share with us and if you change your mind, you can opt-out at any time.

This solution is grounded on a simple consent banner for observed website data only.

Why we like this solution

Good consent UX and clear consent USP that ties into the specific product.

With this solution we could

Activate tracking of observed data for marketing and analytics purposes for users who have accepted and provided consent.

What is missing

Specific mention of what data is being collected beyond cookies.

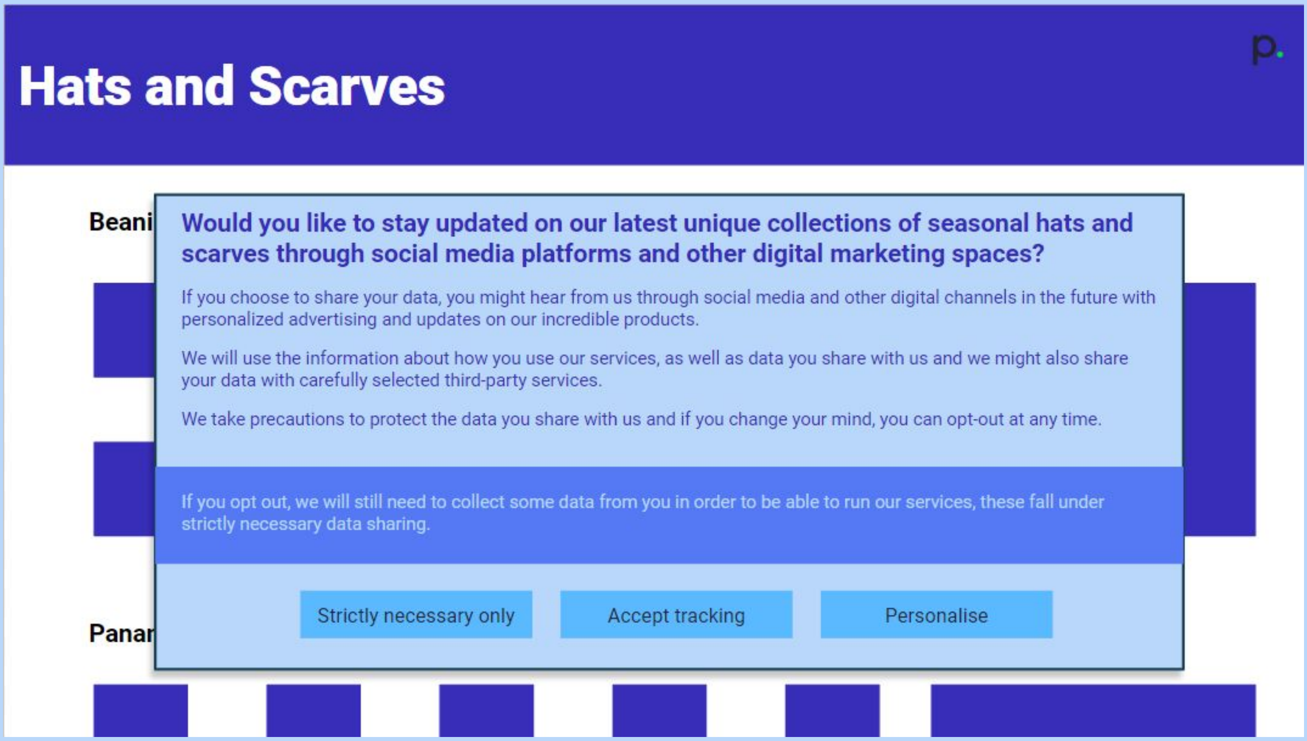
With this solution we could not

Activate first-party data for marketing or analytics purposes.

Granular consent banner

When it comes to first-party user data collection and activation, we provide two alternatives for consent collection: one uses a granular banner with advanced explanation, the other uses granular opt-in checkboxes at the point of collection. The main challenge at hand when it comes to consent for first-party data is making sure that there is clear explanation of what data is being collected, which is something that most solutions overlook.

Demo consent flow: A banner for collection of first-party user data



Hats and Scarves

Would you like to stay updated on our latest unique collections of seasonal hats and scarves through social media platforms and other digital marketing spaces?

If you choose to share your data, you might hear from us through social media and other digital channels in the future with personalized advertising and updates on our incredible products.

We will use the information about how you use our services, as well as data you share with us and we might also share your data with carefully selected third-party services.

We take precautions to protect the data you share with us and if you change your mind, you can opt-out at any time.

If you opt out, we will still need to collect some data from you in order to be able to run our services, these fall under strictly necessary data sharing.

This is a solution that is grounded on an advanced consent banner that encompasses both first-party and navigation data.

Why we like this solution

Clear explanation of what data is being collected and for what purpose.

Explicit mention of both navigation and first-party data and who it will be shared with.

Good consent UX and clear consent USP that ties into the specific product.

With this solution we could

Activate automatic tracking of user features post consent for marketing purposes.

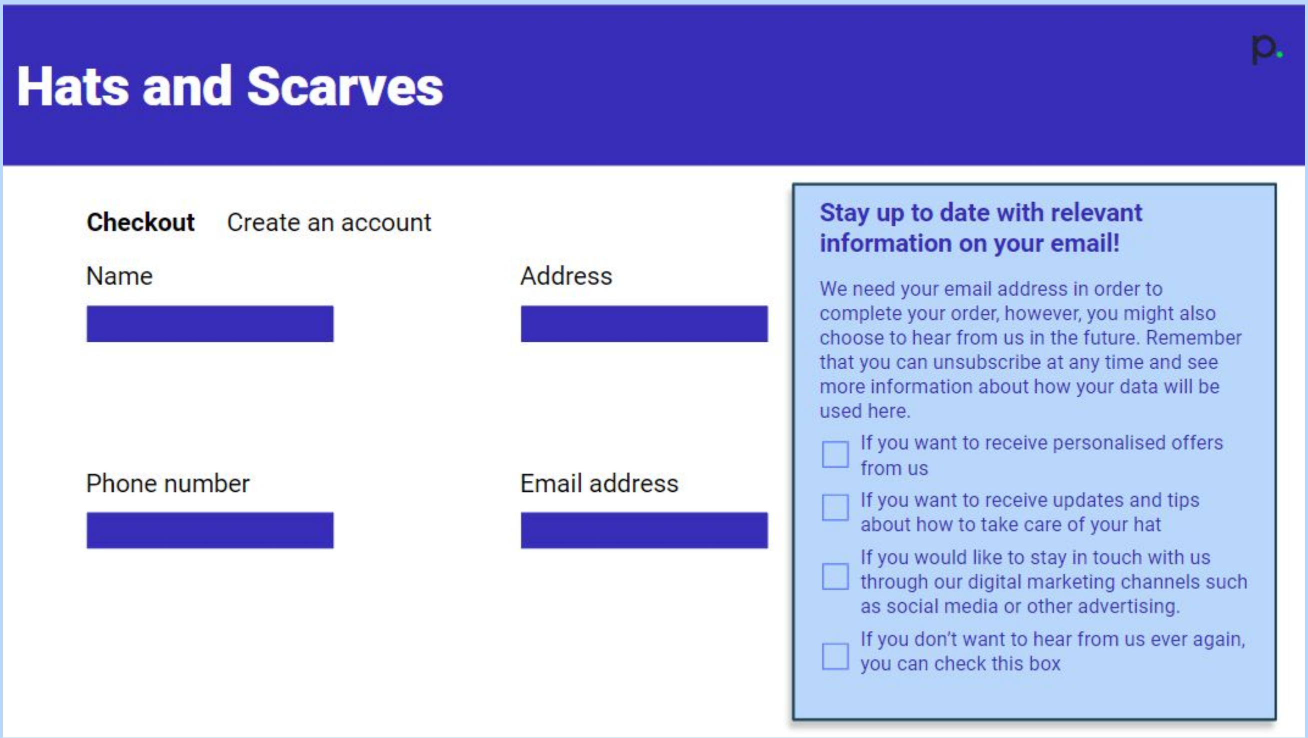
Activate Meta CAPI and send e-mail addresses for data enrichment, if consent has been provided.

Activate Google Analytics 4 tracking for marketing and analytics purposes, if consent has been provided.

Advanced checkboxes

The third example is our advanced suggestion, which uses granular consent checkboxes. A draft example of how to ask for additional consent to activate users’ data for specific purposes. In this fictional case, consent is being asked to activate email addresses for measurement purposes.

Demo consent flow: A consent flow using granular checkboxes



Hats and Scarves

Checkout Create an account

Name

Address

Phone number

Email address

Stay up to date with relevant information on your email!

We need your email address in order to complete your order, however, you might also choose to hear from us in the future. Remember that you can unsubscribe at any time and see more information about how your data will be used here.

□ If you want to receive personalised offers from us

□ If you want to receive updates and tips about how to take care of your hat

□ If you would like to stay in touch with us through our digital marketing channels such as social media or other advertising.

□ If you don’t want to hear from us ever again, you can check this box

This is an advanced flow that includes granular opt ins on the checkout flow for first-party data collection. It is a low-risk solution, but doesn’t afford automatic activation because of technical limitations.

Why we like this solution

Granular checkboxes to collect first-party data on the checkout flow are an elegant low-risk approach.

Explicit mention of first-party data collection.

Good UX and advanced first-party data strategy approach.

With this solution we could

Onboard audience lists on Social Media platform for marketing activation, if users have opted in.

Activate Meta CAPI and send e-mail addresses for data enrichment.

What is missing

Technically, this solution doesn’t allow activation of automatic user data collection such as advanced match. Advertisers should bear in mind that building the data integrations to enable a solution such as this one would demand an advanced setup.

5. Google's requirements

What you need to know.

Consent is now a requirement

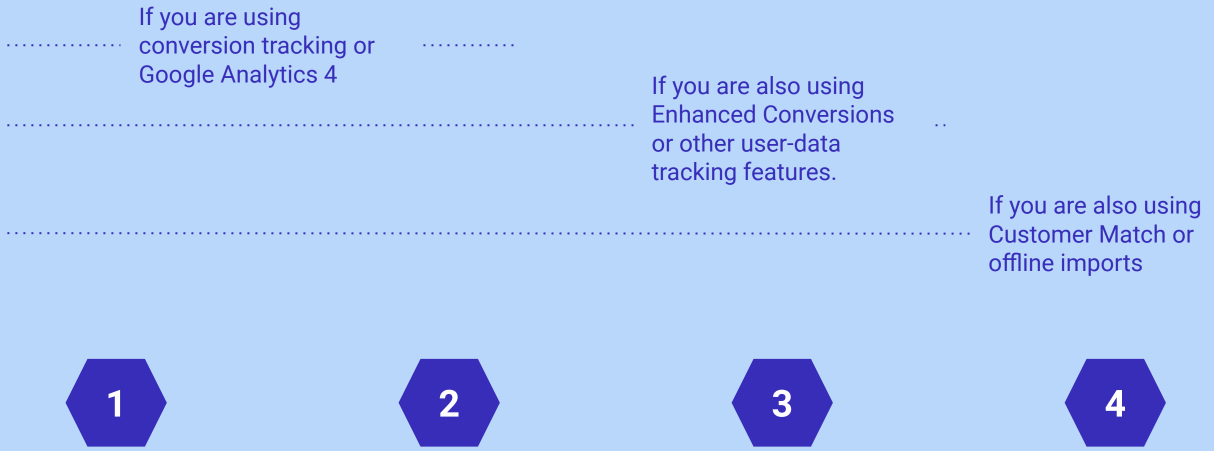
Google has announced that it will enforce new privacy requirements to all advertisers in Europe by requiring them to send consent parameters to the platforms using Consent Mode. This comes as a response to the Digital Markets Act, a competition law that poses new requirements on tech companies operating in the European market.

Advertisers that do not have Consent Mode in place will not be able to continue using many of Google's features from March 2024 and this will only become more strict throughout the year. So if you are relying on Google's tech stack, this is something that you should pay attention to. But what exactly do you need to do?

The simple answer is that you have to collect consent from users to continue using the features you have in place. If you are using Enhanced Conversions, you will have to collect consent for that. If you have offline conversion imports, you will have to collect consent for that. And you need to communicate to Google that you have done so.

What you need to implement by March 2024

Advertisers that don't have this in place will no longer be able to use conversion tracking or audiences on Google platforms from March onwards.



If you are using conversion tracking or Google Analytics 4

If you are also using Enhanced Conversions or other user-data tracking features.

If you are also using Customer Match or offline imports

1. Ensure that you have a consent flow on your website or app that will support your data collection needs.

2. Implement Consent Mode for observed website data on top of your existing consent flow.

3. Implement Consent Mode V2 for observed website data and first-party user data. Update your consent banner.

4. On top of revising your consent banner, go through your audience lists ensuring that consent is captured and transmitted to platforms with audience members following the latest consent API.

Google Consent Mode

Consent Mode is a Google feature used to transmit to Google, information about your users' consent options and minimise the impact of consent banners on advertisers' data.

When Consent Mode was launched, back in 2020, it was a tool to enable improved marketing performance. However, in 2023, Google announced that sending consent parameters to its marketing platforms using Consent Mode would become a requirement.

With the launch of Consent Mode V2, the latest update to Google's feature, advertisers are able to use it to collect consent for both observed and user-provided data. While the Consent Management Platform will still be employed to collect and store consent values, Consent Mode can help process the requests. This is a welcome feature and we recommend that advertisers using Google platforms should build their consent backend on top of this logic.

While the most common implementation of Consent Mode will happen through Google Tag Manager, you will need to have it in place when you are using plugins or native connectors as well. If you are sending data to Google Ads directly from your ecommerce platform, for example, you will need to adapt that integration.

The full picture: Data types, examples and activation

CONSENT MODE PARAMETER	Description	Data type
AD_STORAGE	*Observed website data such as pageviews or purchases tracked for advertising storage. Ad Storage works as a blocker, meaning that requests will be blocked when the parameter is denied.*	Observed website data
ANALYTICS_ STORAGE	*Observed website data such as pageviews or purchases tracked for analytics storage. Analytics Storage works as a blocker, meaning that requests will be blocked when parameter is denied.*	Observed website data
AD_ PERSONALISATION	*Additional parameter to protect hybrid data that can be used for two purposes.*	Mainly observed website data
AD_USER DATA	*Additional parameter to protect hybrid data that can be used for two purposes.*	Mainly user provided first-party data

Audiences and imports

While there has been a buzz around the new version of Consent Mode, an important change launched by Google is around the upload of audience lists and offline events, which will now require advertisers to pass consent parameters in order for them to be processed.

Our understanding is that from March 2024, audiences that do not contain consent parameters will no longer be available for optimisation and retargeting.

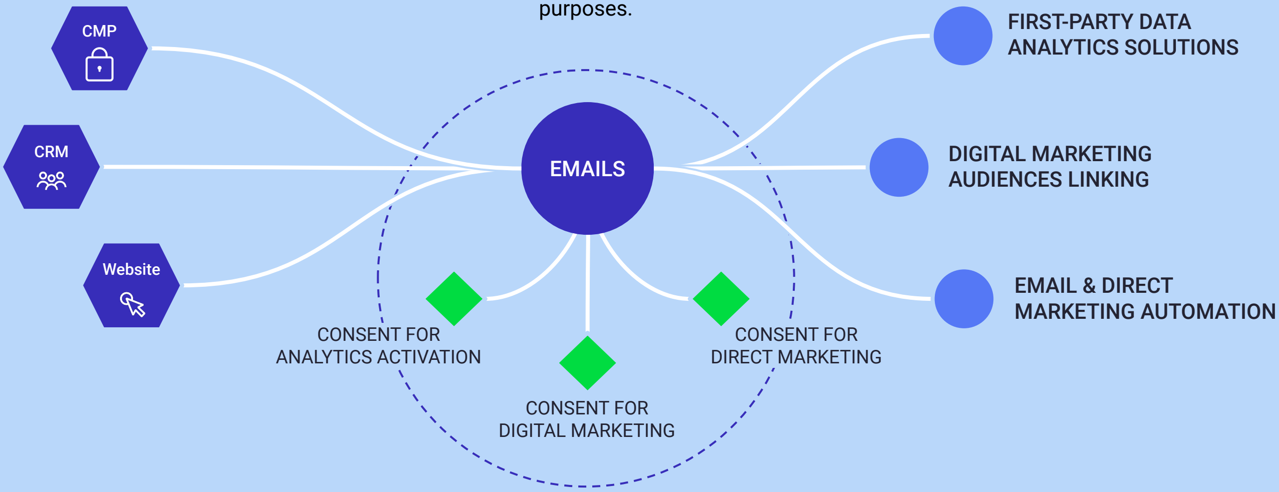
This change will add significant new governance needs for advertisers who will be forced to incorporate consent in their data architecture and ensure that there are processes in place to honour users consent. If you are using native integrations, you will need to understand how these platforms will adapt, if you have your own custom process, you will need to rethink your strategy.

Detailed guides for advertisers can be found on this link, but this is an illustration of how an integration with a CRM platform to fetch consent information would be built.

Example of integration for collection of consent

USER OBJECT

The joining of first-party data with consent parameters makes a complete user object that can be activated through different platforms and exported for audience building purposes.


CMP
CRM
Website
EMAILS
CONSENT FOR ANALYTICS ACTIVATION
CONSENT FOR DIGITAL MARKETING
CONSENT FOR DIRECT MARKETING
FIRST-PARTY DATA ANALYTICS SOLUTIONS
DIGITAL MARKETING AUDIENCES LINKING
EMAIL & DIRECT MARKETING AUTOMATION

Thank you

Author: Celina Belotti

If you are still left wondering what your next step should be, we're here to help!

Get in touch with one of our privacy experts here.

In the meantime, here are some articles you might find useful.

Building a compliant first-party data foundation

A call for advertisers to build and activate compliant first-party data foundations.

Read more here.

Future-proofing your privacy strategy

Where privacy meets digital maturity? First-party data is the key to unlocking privacy maturity.

Read more here.

What is changing?

The DMA, the DSA and what advertisers should be thinking about.

Read more here.

precis.