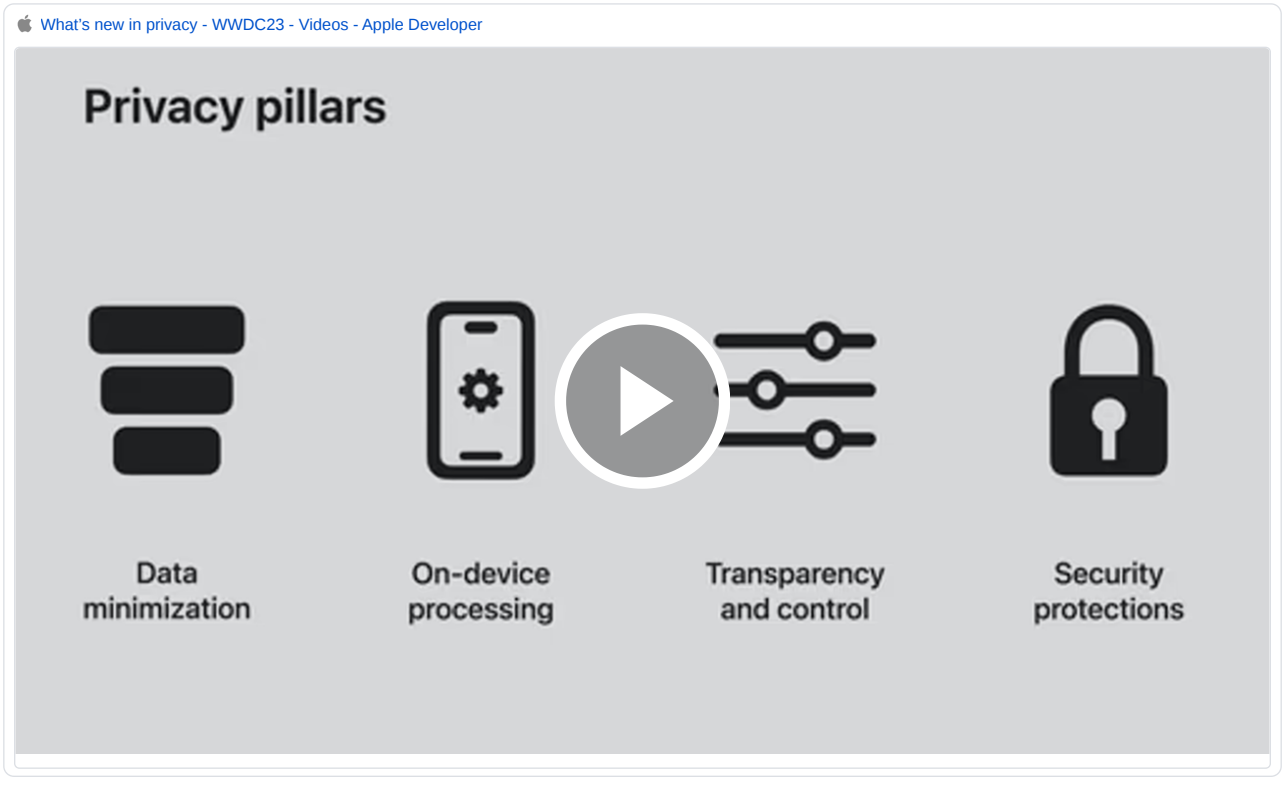
Apple Privacy Manifest in Kantar SDKs

Status	RELEASED
Version	1.0
Date	2024-01-30

Introduction

In light of the recent privacy updates announced at WWDC 2023, it is crucial for us to examine how these changes will affect the Kantar Tagging SDK. Apple's ongoing commitment to privacy, as emphasized in their latest conference, introduces several new features and updates that directly impact data collection and user privacy. This document aims to provide a concise overview of these updates and their implications for the Kantar Tagging SDK, ensuring our technology aligns with Apple's enhanced privacy standards while continuing to deliver valuable insights.

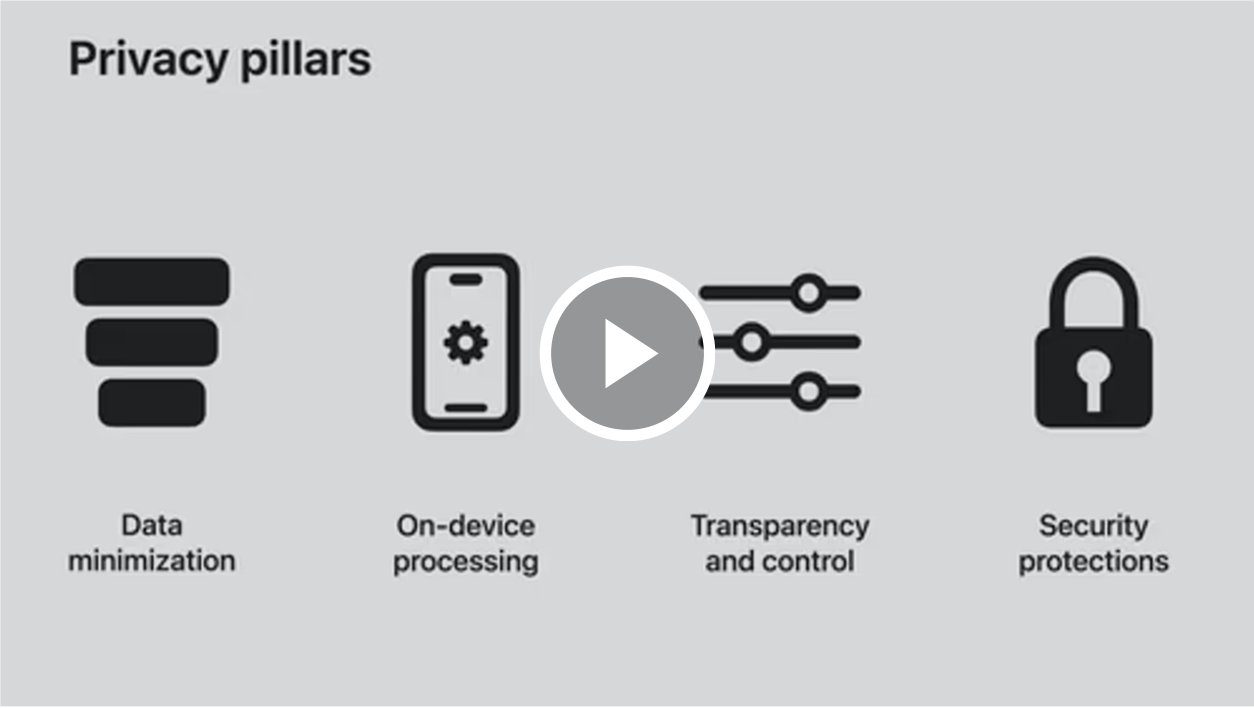


Purpose of this document

This document is designed to offer all relevant information about our SDKs that are applicable to the Apple Privacy Manifest. It defines the Privacy Manifest, details the specific information extracted by the SDK, and clarifies the purpose for which this data is gathered.

Privacy Manifest

Get started with privacy manifests - WWDC23 - Videos - Apple Developer



From spring 2024, Apple will require a privacy manifesto for every app that is to be published in the App Store. Many of these apps naturally also use external SDKs. This naturally includes our SDKs, which are used by broadcasters to measure their content.

In this chapter, we will first describe what information is collected by our SDKs, how it is to be utilised and how our privacy manifest must be specified at the end.

Data collected via the SDKs

We offer two types of SDKs. The Tagging SDK and the Streaming SDKs.
The Tagging SDK is mainly used to measure the usage of an app. This includes start, foreground, background and close events. It also offers the possibility of collecting information about displayed content or other information of interest to the app provider.

However, we mainly have the Streaming SDK in the markets. This is about measuring streamed content. This can be live streams or VOD content.

At the end of the day, we want to provide our customers with information about the use of their content. This includes information such as

- Impressions / Viewtime
- Playtime
- Streaming Views
- Stream/channel information
- Device information (device type, os, os version)
- Geo location at country level
- Screen/video resolution
- Browser Language
- Clients

In order for us to provide this information to our customers, we need to collect information from the device or app. We are very careful to be data sparing and only use as much information as is absolutely necessary. The following table shows what these are:

Information	Transmitted Data	Purpose
IDFV	`idfv=md5(identifierForVendor).substring(0, 16)` **Example:** • abd8b32cc0987e3f	We need an identifier so that we are able to get an idea of the number of users, sessions or apps in order to bundle individual activities within an app. We do not track people or devices in the SDK context! The identifiers we use are more or less unique per installed app that uses our SDK, i.e. these identifiers do not allow cross-device or cross-application tracking in the SDK context.
Kantar Id	The Kantar Id is a random UUID that we generate once in the SDK and save in the app space. `kid=md5(kantarid).substring(0, 16)`	
Cookie	We use the HTTP protocol to transport the data from the SDK to our measurement system. Our measurement system also tries to save a cookie via this protocol.	
IP	At our HTTP message endpoint, we receive the public IP address of the device via the	We use the truncated IP address to determine the geo-location at the country

	TCP/IP protocol. On receipt, the IP address is truncated before it is forwarded to the next measurement components. • 95.91.217.76 (receive) • 95.91.217.0 (processed)	level, and we hash it together with the user agent to create a signature that serves as a fallback in case we don't have an HTTP cookie or local storage cookie. This truncated IP is not stored in our raw data table, from which all other data processing jobs originate. For Geo-Resolution we're using DB-IP
User Agent	The user agent is also stored in our raw data and is supplied via a header field via the HTTP protocol.	We use the user agent to determine information about the device being used. Primarily, this includes the operating system, OS version, browser, browser version, and device type. Additionally, it is possible that we also read such information directly from the device. For this purpose, we are currently using our own technology, but in the near future, we will be using DeviceAtlas for this.
Payload	JSON-like structured HTTP Get Request	The payload has a JSON-like structure containing all variables automatically determined by the SDK. Additionally, an app provider can send further information to our measurement system, alongside the predefined variables that we require for measurement.

Privacy Manifest File

This chapter describes the entries in the Apple Privacy Manifest.

`<key>NSPrivacyTracking</key>` `<false/>`	User Privacy and Data Use describes the conditions for configuring this value. Based on these conditions, the SDK does not perform user tracking. The last chapter describes in detail the information that is automatically collected by the SDK.

`<key>NSPrivacyTrackingDomains</key>`
`<array>`
`  <string>.2cnt.net</string>`
`  <string>.tns-cs.net</string>`
`</array>`
	These domains are used by the SDK to collect the app's usage data.

`<key>NSPrivacyCollectedDataType</key>`
`<string>NSPrivacyCollectedDataTypeCoarseLocation`
`</string>`
`<key>NSPrivacyCollectedDataTypeLinked</key>`
`<false/>`
`<key>NSPrivacyCollectedDataTypeTracking</key>`
`<false/>`
`<key>NSPrivacyCollectedDataTypePurposes</key>`
	This value presumably refers to the reading of location information that can be read out via an API.
	The SDK does **NOT** use these APIs.
	We only use truncated IP addresses for location determination in order to assign a user to a specific country.
	See last chapter.

`<array>`
`<string>NSPrivacyCollectedDataTypePurposeAnalytics`
`</string>`
`</array>`	

`<key>NSPrivacyCollectedDataType</key>`
`<string>NSPrivacyCollectedDataTypeDeviceID`
`</string>`
`<key>NSPrivacyCollectedDataTypeLinked</key>`
`<false/>`
`<key>NSPrivacyCollectedDataTypeTracking</key>`
`<false/>`
`<key>NSPrivacyCollectedDataTypePurposes</key>`
`<array>`
`<string>NSPrivacyCollectedDataTypePurposeAnalytics`
`</string>`
`</array>`
	We use a cookie, the Kantar Id and the IDFV. Except for the cookie, these identifiers are hashed and shortened before being sent - see last chapter.

`<key>NSPrivacyCollectedDataType</key>`
`<string>NSPrivacyCollectedDataTypeProductInteraction`
`</string>`
`<key>NSPrivacyCollectedDataTypeLinked</key>`
`<false/>`
`<key>NSPrivacyCollectedDataTypeTracking</key>`
`<false/>`
`<key>NSPrivacyCollectedDataTypePurposes</key>`
`<array>`
`<string>NSPrivacyCollectedDataTypePurposeAnalytics`
`</string>`
`</array>`
	The app is primarily used to collect information about app usage (e.g. started, background, foreground). Furthermore, which content is consumed by the user. This includes primary videos, live streams and other content.

`<key>NSPrivacyCollectedDataType</key>`
`<string>NSPrivacyCollectedDataTypeOtherUsageData`
`</string>`
`<key>NSPrivacyCollectedDataTypeLinked</key>`
`<false/>`
`<key>NSPrivacyCollectedDataTypeTracking</key>`
`<false/>`
`<key>NSPrivacyCollectedDataTypePurposes</key>`
`<array>`
`<string>NSPrivacyCollectedDataTypePurposeAnalytics`
`</string>`
`</array>`
	We automatically use the shortened IP and the user agent.
	We receive information about the content viewed via the payload - e.g. in the case of a video: a content id, stream length, stream positions, the time on the device or other information that describes the video content.

`<key>NSPrivacyAccessedAPIType</key>`
`<string>NSPrivacyAccessedAPICategoryUserDefaults`
`</string>`
`<key>NSPrivacyAccessedAPITypeReasons</key>`
`<array>`
`<string>CA92.1</string>`
`</array>`
	Is used to save the cookie and our own Kantar Id.

File	Modified
PrivacyInfo.xcprivacy Apple Privacy Manifest	Jan 30, 2024 by Moczek, Tomasz (KM)

Privacy Report

Here you can see an example Privacy Report based on the Privacy Manifest.