UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

VERIPATH, INC., a Delaware Corporation, Plaintiff, v. **DIDOMI**, a foreign entity, Defendant.	Civil Action No. 1:19-cv-01702-GBD **AMENDED COMPLAINT FOR PATENT INFRINGEMENT** **DEMAND FOR JURY TRIAL**

Plaintiff VeriPath, Inc. ("Plaintiff" or "VeriPath"), by and through its undersigned counsel, hereby submits this Amended Complaint for patent infringement against Defendant Didomi ("Defendant" or "Didomi"), and alleges as follows:

NATURE OF ACTION

1. This is an action arising under the patent laws of the United States, 35 U.S.C. §§ 1 and 271, *et seq*., for Defendant's infringement of Plaintiff's U.S. Patent No. 10,075,451 ("the '451 Patent"). A true and correct copy of the '451 Patent is attached hereto as Exhibit 1.

THE PARTIES

2. Plaintiff VeriPath is a corporation organized under the laws of Delaware and registered to do business in the state of New York, with its principal place of business at 665 S. Bayview Ave, Freeport, NY, 11520. Plaintiff is a patent-protected data privacy and compliance manager and data incentivization platform.

3. Upon information and belief, Defendant Didomi is a société par actions simplifiées (simplified stock company) organized under the laws of France.

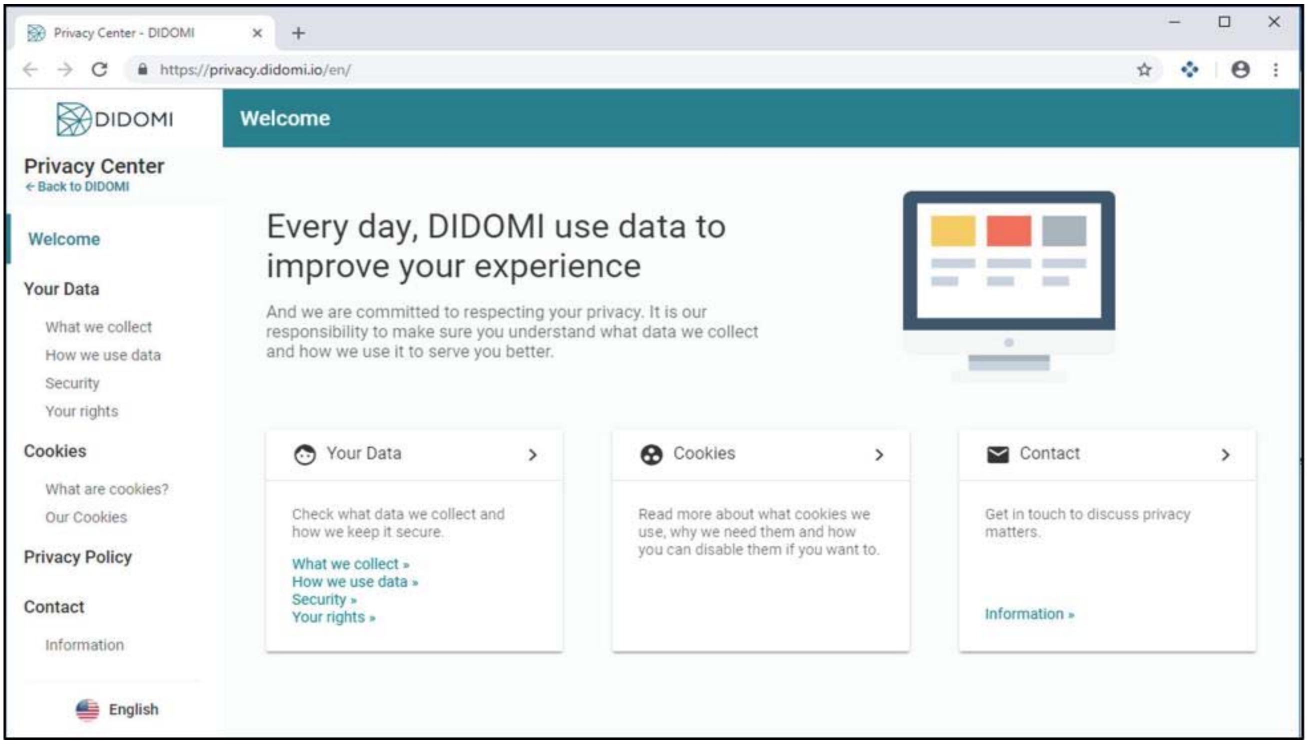
JURISDICTION AND VENUE

4. This action arises under the patent laws of the United States, including 35 U.S.C. § 271 *et seq*. Accordingly, this Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. On information and belief, Defendant transacts business in the State of New York by demonstrating, using, and selling its products. These claims arise from Defendant's demonstration, use, and sales its privacy products, including its Consent Management Platform, Compliance Console, and Privacy Center products (collectively "Privacy Products") in the State of New York and throughout the United States, as explained below.

6. Defendant conducts business in the United States. *See* Ex. 2 (https://www.datanyze.com/market-share/consent-management/United+States/didomi-market-share (last accessed June 3, 2019)). On information and belief, Defendant maintains a main office in New York, New York, where it develops, uses, sells, offers for sale, and maintains its Privacy Products. *See id*. On information and belief, Defendant's Co-Founder and Chief Technology Officer, Jawad Stouli, resides in the New York City area, and is resident in Defendant's New York City office, where he has responsibilities concerning the development and maintenance of Defendant's Privacy Products. *See* Ex. 3 (Jawad Stouli's LinkedIn Profile).

7. Defendant's website is in English and displays the United States flag. *See* Ex. 4 (https://privacy.didomi.io/en/ (last accessed June 3, 2019)).



Every day, DIDOMI use data to improve your experience

And we are committed to respecting your privacy. It is our responsibility to make sure you understand what data we collect and how we use it to serve you better.

Your Data

Check what data we collect and how we keep it secure.

What we collect »
How we use data »
Security »
Your rights »

Cookies

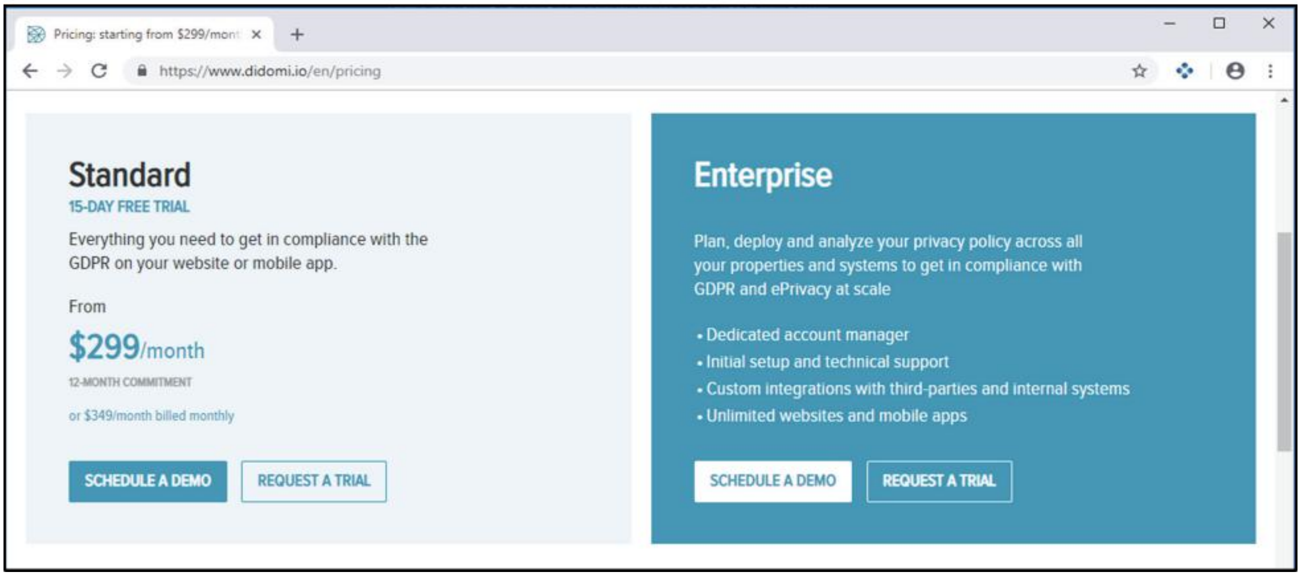
Read more about what cookies we use, why we need them and how you can disable them if you want to.

Contact

Get in touch to discuss privacy matters.

Information »

8. Defendant offers its products for sale in the United States, in U.S. Dollars, on its English-language webpage, where users can schedule a demo or request a trial of the Privacy Products. *See* Exs. 5 (https://www.didomi.io/en/pricing (last accessed June 6, 2019)) & 6 (https://www.didomi.io/en/ (last accessed June 6, 2019)).


Pricing: starting from $299/mont
https://www.didomi.io/en/pricing

Standard

15-DAY FREE TRIAL

Everything you need to get in compliance with the GDPR on your website or mobile app.

From

$299/month

12-MONTH COMMITMENT

or $349/month billed monthly

SCHEDULE A DEMO
REQUEST A TRIAL

Enterprise

Plan, deploy and analyze your privacy policy across all your properties and systems to get in compliance with GDPR and ePrivacy at scale

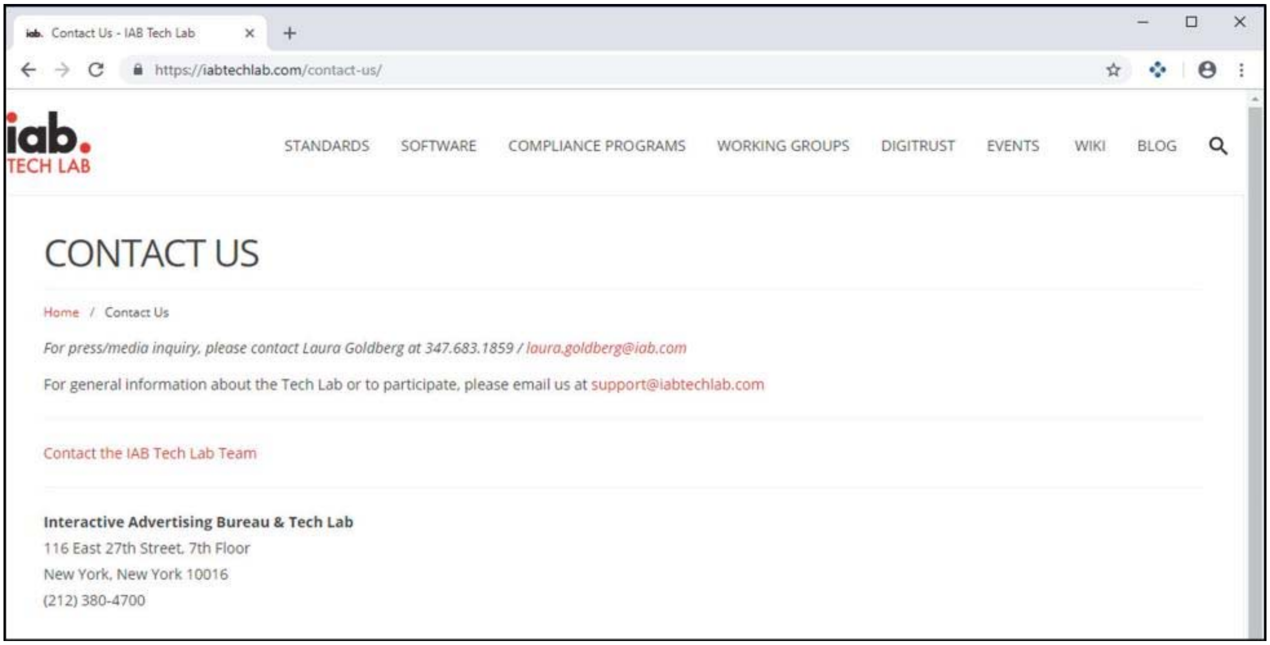
- Dedicated account manager
- Initial setup and technical support
- Custom integrations with third-parties and internal systems
- Unlimited websites and mobile apps

9. On information and belief, Defendant's website (https://www.didomi.io) is hosted on a server located in the United States.

10. On information and belief, Defendant's employees, customers, purchasers, users, developers, and/or partners use the Privacy Products in the United States.

11. For example, Defendant identifies IAPP (International Association of Privacy Professionals), based out of New Hampshire, as one of its clients. *See* Ex. 7 (https://iapp.org/about/ (last accessed June 3, 2019)). Upon information and belief, IAPP uses Defendant's Privacy Products.

12. Defendant is a member of multiple IAB Tech Lab working groups, which are based out of New York City. *See* Exs. 8 (mobile group - https://iabtechlab.com/working-groups/the-gdpr-mobile-technical-sub-group/ (last accessed June 3, 2019)), 9 (blockchain group - https://iabtechlab.com/working-groups/blockchain-working-group/ (last accessed June 3, 2019)), & 10 (IAB Tech Lab location in New York City - https://iabtechlab.com/contact-us/ (last accessed June 3, 2019)).



CONTACT US

Home / Contact Us

For press/media inquiry, please contact Laura Goldberg at 347.683.1859 / laura.goldberg@iab.com

For general information about the Tech Lab or to participate, please email us at support@iabtechlab.com

Contact the IAB Tech Lab Team

Interactive Advertising Bureau & Tech Lab
116 East 27th Street, 7th Floor
New York, New York 10016
(212) 380-4700

13. Upon information and belief, Defendant has entered into a partnership with Connecthings, Inc., which has an office in New York located at 188 Grand Street, New York, New York 10013, to promote its Privacy Products. *See* https://www.connecthings.com/contact-us/ (last accessed June 6, 2019).

14. Defendant conducts substantial business in the State of New York, including (1) on information and belief, committing at least a portion of the infringing acts alleged herein and (2) regularly transacting business, soliciting business, and deriving revenue from the sale of services, including infringing services, to entities in the state of New York which are related to the claims herein. *See* Exs. 5 & 6 (offers for sale and to schedule a demo on website, in English language). Thus, Defendant has purposefully availed itself of the benefits of the State of New York, such that the exercise of jurisdiction over Defendant would not offend traditional notions of fair play and substantial justice.

15. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 and 1400.

THE '451 PATENT

16. Plaintiff is the owner by assignment of all right, title, and interest in and to the '451 Patent, entitled "Methods and Systems for User Opt-in to Data Privacy Agreements," which was duly and legally issued on September 11, 2018 by the United States Patent and Trademark Office. The '451 Patent is valid, enforceable, and currently in full force and effect. *See* Ex. 11 (Patent Assignment).

17. The '451 Patent claims, among other things, methods for controlling access to a user's personal information in the management of the user's privacy of such personal information on computer systems by allowing the user to opt-in to data sharing arrangements as part of data privacy agreements.

18. The ’451 Patent solved and improved the technological drawbacks of the then-current data collection and privacy schemes by creating a technologically improved system and application that efficiently collects and manages user consent and data in real-time while permitting the use of enhanced functions of the website or mobile application accessed by the user based on the received consents. *See, e.g.*, Ex. 1 at 2:29-45.

Technological Problems and Drawbacks of Conventional Data Collection and Privacy Schemes

19. Online services, as well as the mobile device applications that can be used to access those services, are ubiquitous, allowing users to, among other things, socialize, bank, shop, and navigate. The convenience these services offer, including the personalized features and intuitive capabilities based on user preferences and past activities, make them nearly indispensable for many. Yet there is a tradeoff for such convenience: such services and applications must gather volumes of information about the user in order to be useful to the user. *Id.* at 1:25-33. Vast amounts of personal information may be collected as a user moves through the digital world, including purchasing (and even browsing) history on ecommerce sites, social media activities and relationships, favorite websites, dining habits, and the like. *Id.* at 1:45-50.

20. Due to the sensitivity of such information, many states and countries, including the United States, have enacted strict requirements for presenting users with a privacy policy detailing how their personal information will be used, and require users to provide their consent prior to collecting the personal information. *Id.* at 1:51-55. Because of these requirements, users are essentially presented with an ultimatum at the outset: either (a) agree that personal information may be collected and used or (b) be denied access to the website or application. *Id.* at 1:55-60.

21. However, privacy policies can be difficult to locate and impenetrable to read, often stuffed with legalese and dumped onto a website. *Id.* at 1:63-65. As a result, users rarely read the

privacy policy and often have no idea how their personal information is being used. *Id.* at 1:62-65.

22. Further compounding the problem, different jurisdictions require consent for different information and different uses of such information. *Id.* at 2:1-3. Accordingly, an identical application offered to two different users in two different locations may be required to obtain different types of consent, or risk alienating or annoying some users by applying the strictest requirements to all users. *Id.* at 2:8-13.

23. Once collected, some personal information may legally be sold to and purchased by third parties, such as marketers and researchers, who may in turn use the information for their own uses. *Id.* at 2:14-16. Purchasers of personal information must trust the assurances of the seller that the data is "clean" (*e.g.*, that the personal information was collected in accordance with the necessary consent and other requirements). *Id.* at 2:18-21. If that trust turns out to be misplaced, the purchaser may be liable as sellers often require indemnification from purchasers in the event that the personal information was illegally collected. *Id.* at 2:22-25.

The '451 Patent's Solution and Technological Improvement of Conventional Data Collection and Privacy Schemes

24. To solve and improve the technological problems of conventional data collection and privacy schemes discussed above, the '451 Patent introduced an improved system for allowing users to opt-in to data sharing arrangements as part of data privacy agreements, so that users are provided immediate and clear transparency into the data being collected and how it is being utilized. The patented system also efficiently collects and manages user opt-in consent and data in real-time.

25. The '451 Patent discloses specific steps detailing an improved method of allowing users to view and opt-in to privacy policies and data sharing agreements, which include

(1) generating and populating a disclosure matrix clearly explaining to a user in an organized and concise manner what personal information will be collected and how it will be used, (2) offering the user the option to receive additional details and explanation as to the personal information to be collected and how it will be used, (3) allowing the user to provide or withhold informed consent for such uses, and (4) allowing the user to selectively provide consent for different uses of different types of personal information. *Id.* at 2:36-45.

26. For example, the '451 Patent discloses a system for controlling access to a user's personal information by (1) obtaining personal information about a user of an application, (2) determining a required permission from the user for at least one proposed use of the personal information, (3) presenting to the user a first offer to provide access to at least one enhanced function of the application in exchange for the required permission, and (4) responsive to the user providing the required permission, providing the user with access to the at least one enhanced function of the application. *Id.* at 3:3-13. The personal information may include information such as the user's name, location, address, age, gender, household income, marital status, and transactional history. *Id.* at 3:27-31. The proposed use may include analytics, market research, market segmentation, and disclosure to third parties. *Id.* at 3:32-33. The at least one enhanced function of the application may include a reduced number of commercial advertisements presented to the user in the application. *Id.* at 3:18-20.

27. The '451 Patent discloses several improvements over conventional data collection and privacy policy systems. For example, by arranging the application component, the permission component, and the privacy display component in a distributed manner, where the application component executes on the user's device (*e.g.*, smartphone), the permission component executes on a server or other system remote from the application component, and the privacy display

component presents information (*e.g.*, as a website) on a system remote from the application component, the entity operating the application component can display privacy policy information in a standardized format that can be changed by the entity or the user. *Id.* at 11:22-41.

28. As another example of an improvement over conventional data collection and privacy policy systems, the use of a permission component remote from the application component allows for permission rules and requirements to be updated (due to changed user preferences, changes in the law, or otherwise) without requiring changes to the application component running on the user's device. *Id.* at 11:42-47. Because updates to an application typically interrupt use of the application, and require the user to agree to the updates, a user who declines to install such an update may have his/her personal information collected under an out-of-date permission scheme, thereby making the collection out of compliance. *Id.* at 11:47-52. The use of the system taught by the '451 Patent avoids such problems by allowing for updates to be made to the rules executed by the permission component without disruption to the user. *Id.* at 11:52-55.

<u>Defendant's Knowledge of the '451 Patent and Infringement</u>

29. No later than February 6, 2019, Defendant received written notice that it infringes the '451 Patent via an email from Plaintiff to Mr. Romain Gauthier. *See* Ex. 12.

30. On information and belief, subsequent to February 6, 2019, Defendant has continued to directly infringe, literally and/or under the doctrine of equivalents, one or more claims of the '451 Patent by, without authority or license from Plaintiff, making, using, selling, offering to sell, and/or importing its Privacy Products into the United States, in violation of 35 U.S.C. § 271(a). On information and belief, Defendant has continued to directly infringe one or more of the method claims of the '451 Patent by testing, repairing, and/or using its Privacy Products in the United States.

31. On information and belief, subsequent to February 6, 2019, in addition to directly infringing the ’451 Patent pursuant to 35 U.S.C. § 271(a), literally and/or under the doctrine of equivalents, Defendant has continued to indirectly infringe the ’451 Patent by instructing, directing, and/or requiring others, including its customers, purchasers, users, developers, and/or partners in the United States to perform all or some of the steps of the method claims, literally and/or under the doctrine of equivalents, of the ’451 Patent, pursuant to 35 U.S.C. § 271(b). On information and belief, Defendant has actively induced infringement by remaining willfully blind to its customers, purchasers, users, developers, and/or partners’ infringement despite believing there to be a high probability its customers, purchasers, users, developers, and/or partners infringe the ’451 Patent.

32. On information and belief, subsequent to February 6, 2019, Defendant has continued to make, use, sell, offer for sale, and/or import into the United States its Privacy Products with knowledge that the Privacy Products are a material part of inventions claimed by the ’451 Patent and are especially made or adapted for use in an infringement of the ’451 Patent. On information and belief, Defendant knows that the Privacy Products are not staple articles or commodities of commerce suitable for substantial non-infringing use. Defendant’s actions contribute to the direct infringement of the ’451 Patent by others, including its customers, purchasers, users, developers, and/or partners, in violation of 35 U.S.C. § 271(c).

COUNT I: DIRECT INFRINGEMENT OF U.S. PATENT NO. 10,075,451

33. Plaintiff hereby re-alleges and incorporates by reference the allegations set forth in the foregoing paragraphs as though fully set forth herein.

34. The ’451 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The ’451 Patent has been in full force and effect since its

issuance. Plaintiff owns by assignment all rights, title, and interest in and to the ’451 Patent, including the exclusive right to seek damages for past, current, and future infringement thereof.

35. Pursuant to 35 U.S.C. § 271(a), Defendant is liable for direct infringement, literally or under the doctrine of equivalents, of at least claim 1 of the ’451 Patent, by having made, used, offered for sale, sold, and/or imported into the United States infringing products, including at least its Privacy Products.

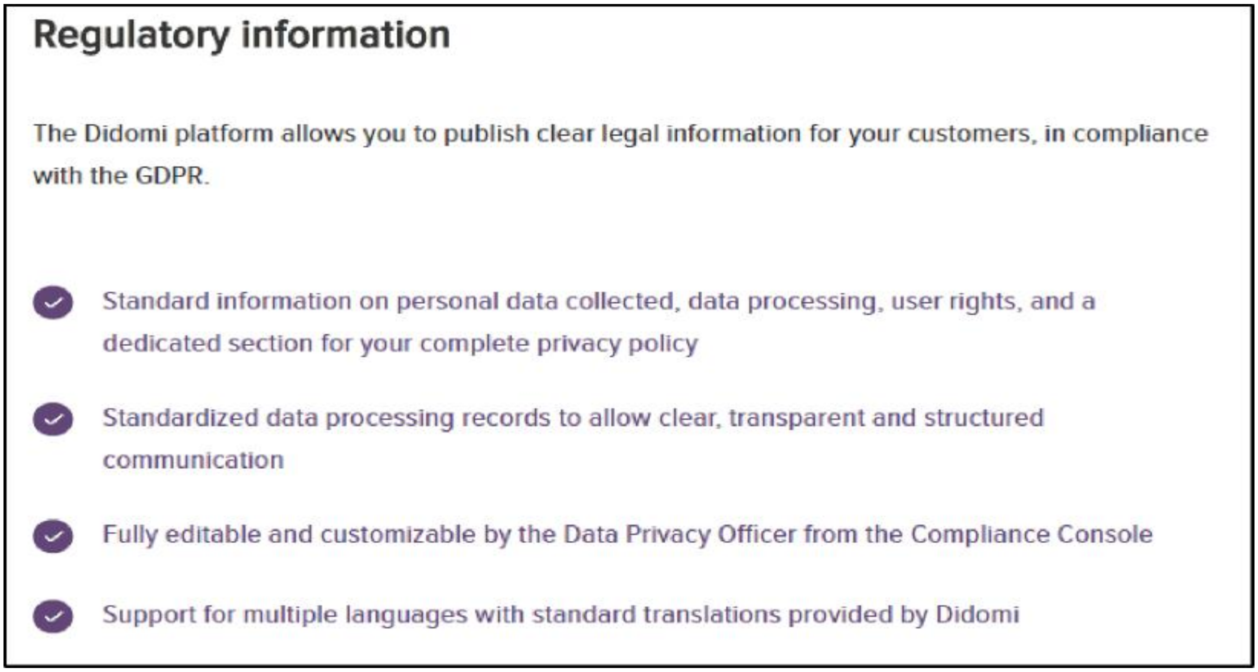
36. Attached as Exhibit 13 is an exemplary claim chart comparing claim 1 of the ’451 Patent to Defendant’s Consent Management Platform, one of its Privacy Products. Plaintiff does not intend Exhibit 13 to be comprehensive or limiting and Plaintiff expressly reserves its rights to pursue all available infringement arguments as this case progresses. Upon information and belief, other products that Defendant uses or offers for sale also infringe the ’451 Patent.

37. Claim 1 of the ’451 Patent, for example, recites:

> A method for controlling access to a user’s personal information comprising:
>
> providing a software component for inclusion in an application, the software component having an application programming interface (API);
>
> obtaining, from the application executing on a device of a user of the application, personal information about the user of the application, the personal information obtained via the API by the software component executing on the device;
>
> identifying the type of the obtained personal information;
>
> determining, based on at least the type of obtained personal information, a required permission from the user for at least one proposed use of the obtained personal information;
>
> presenting, to the user, a first offer to provide access to at least one enhanced function of the application in exchange for the required permission; and
>
> responsive to the user providing the required permission, providing the user with access to the at least one enhanced function of the application.

38. Defendant and/or its Privacy Products infringe at least claim 1 of the ’451 Patent by performing the steps of at least claim 1 of the ’451 Patent as explained below. Additionally, Defendant controls and/or directs others, including but not limited to its customers, purchasers, users, developers, and/or partners, to practice the steps of at least claim 1 of the ’451 Patent as explained below.

39. Defendant’s Privacy Products enable web sites and mobile applications to comply with GDPR and other data protection and privacy regulations.



Regulatory information

The Didomi platform allows you to publish clear legal information for your customers, in compliance with the GDPR.

✓ Standard information on personal data collected, data processing, user rights, and a dedicated section for your complete privacy policy

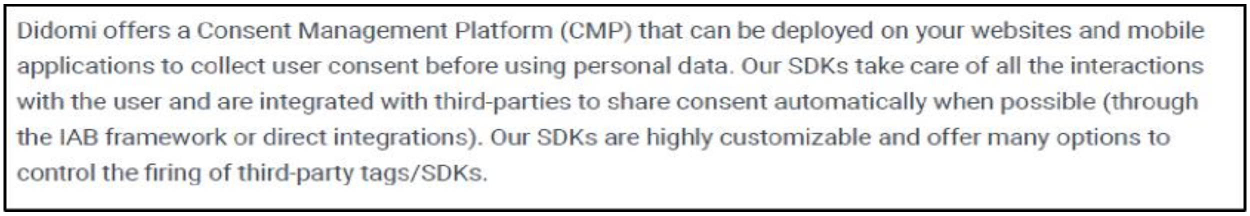
✓ Standardized data processing records to allow clear, transparent and structured communication

✓ Fully editable and customizable by the Data Privacy Officer from the Compliance Console

✓ Support for multiple languages with standard translations provided by Didomi

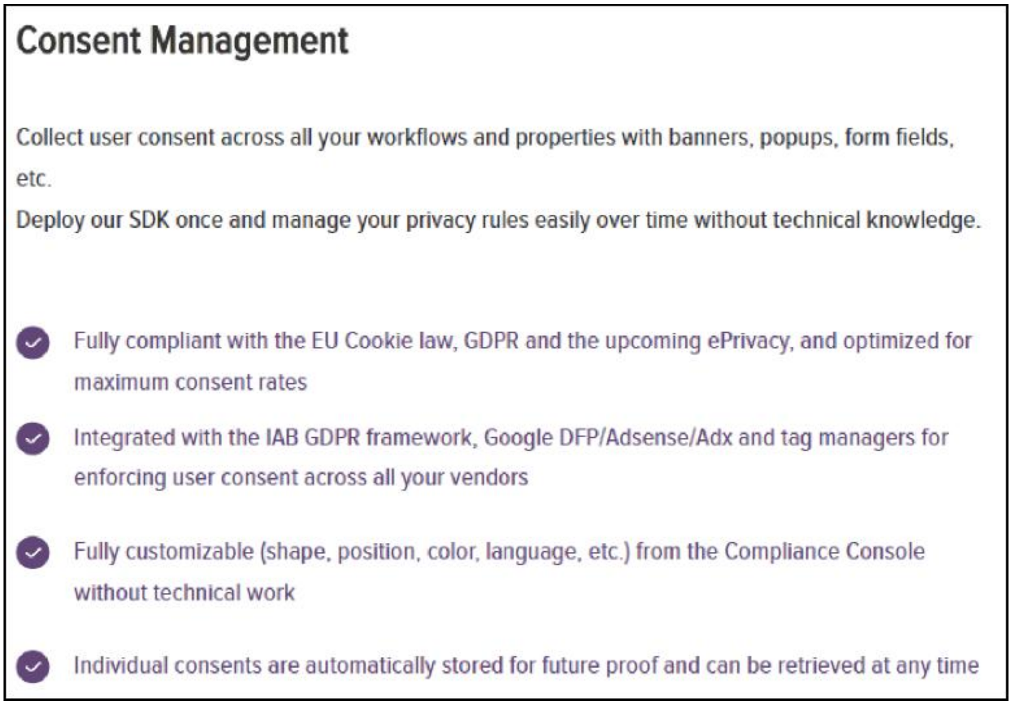
See https://www.didomi.io/en/privacy-center (last accessed June 6, 2019).

40. Defendant “offers a Consent Management Platform (CMP) that can be deployed on your websites and mobile applications to collect user consent before using personal data.” On information and belief, Defendant deploys, integrates, and/or facilitates the integration of its Privacy Products into its customers’, purchasers’, users’, developers’, and/or partners’ websites and mobile applications to collect user consent before using personal data.



Didomi offers a Consent Management Platform (CMP) that can be deployed on your websites and mobile applications to collect user consent before using personal data. Our SDKs take care of all the interactions with the user and are integrated with third-parties to share consent automatically when possible (through the IAB framework or direct integrations). Our SDKs are highly customizable and offer many options to control the firing of third-party tags/SDKs.

41. Defendant's Privacy Products provide consent management functionality in a method for controlling access to a user's personal information.



Consent Management

Collect user consent across all your workflows and properties with banners, popups, form fields, etc.
Deploy our SDK once and manage your privacy rules easily over time without technical knowledge.

✓ Fully compliant with the EU Cookie law, GDPR and the upcoming ePrivacy, and optimized for maximum consent rates

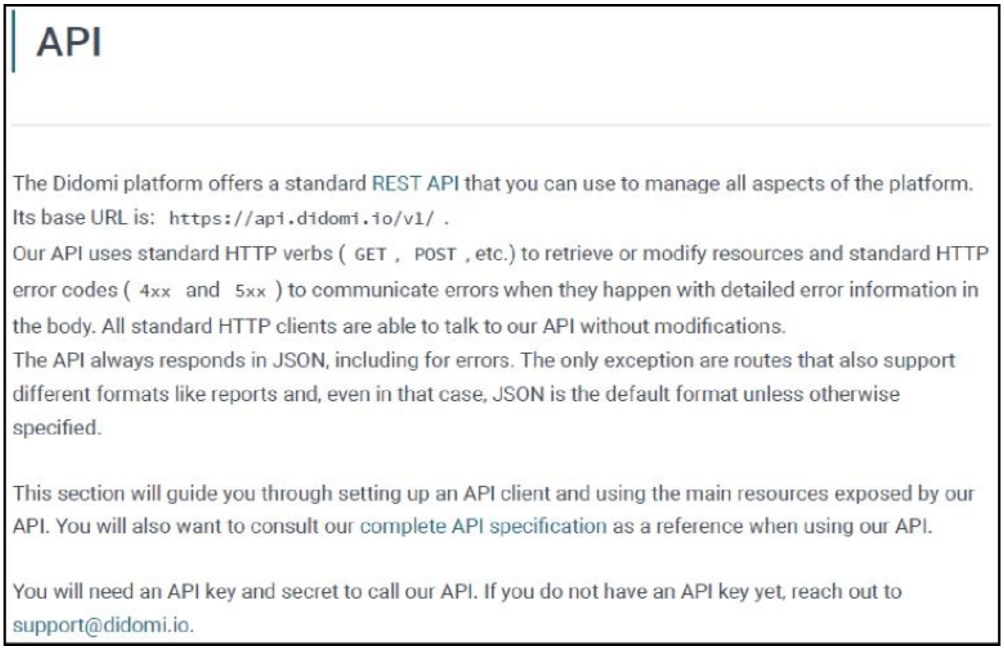
✓ Integrated with the IAB GDPR framework, Google DFP/Adsense/Adx and tag managers for enforcing user consent across all your vendors

✓ Fully customizable (shape, position, color, language, etc.) from the Compliance Console without technical work

✓ Individual consents are automatically stored for future proof and can be retrieved at any time

See https://www.didomi.io/en/privacy-center (last accessed June 6, 2019).

42. Defendant's Privacy Products provide a software component for inclusion in an application, the software component having an application programming interface (API).



API

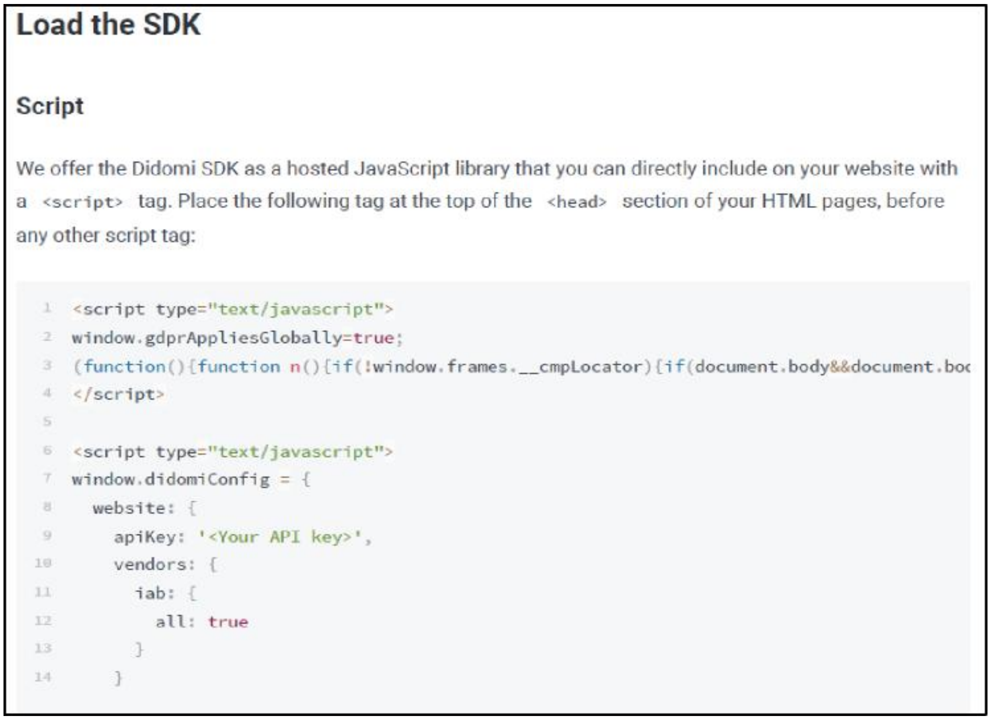
The Didomi platform offers a standard REST API that you can use to manage all aspects of the platform.
Its base URL is: `https://api.didomi.io/v1/` .
Our API uses standard HTTP verbs (`GET` , `POST` , etc.) to retrieve or modify resources and standard HTTP error codes (`4xx` and `5xx`) to communicate errors when they happen with detailed error information in the body. All standard HTTP clients are able to talk to our API without modifications.
The API always responds in JSON, including for errors. The only exception are routes that also support different formats like reports and, even in that case, JSON is the default format unless otherwise specified.

This section will guide you through setting up an API client and using the main resources exposed by our API. You will also want to consult our complete API specification as a reference when using our API.

You will need an API key and secret to call our API. If you do not have an API key yet, reach out to support@didomi.io.

See https://developers.didomi.io/api/introduction (last accessed June 6, 2019).

43. Defendant's Privacy Products "offer the Didomi SDK as a hosted JavaScript library that you can directly include on your website with a <script> tag."



Load the SDK

Script

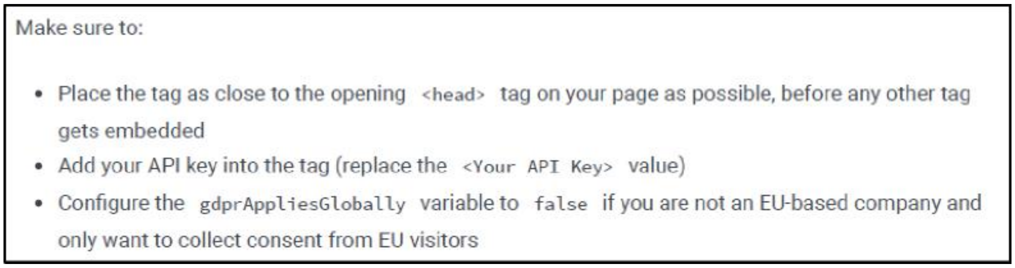
We offer the Didomi SDK as a hosted JavaScript library that you can directly include on your website with a `<script>` tag. Place the following tag at the top of the `<head>` section of your HTML pages, before any other script tag:

```
<script type="text/javascript">
window.gdprAppliesGlobally=true;
(function(){function n(){if(!window.frames.__cmpLocator){if(document.body&&document.boc
</script>

<script type="text/javascript">
window.didomiConfig = {
  website: {
    apiKey: '<Your API key>',
    vendors: {
      iab: {
        all: true
      }
    }
```

See https://developers.didomi.io/cmp/web-sdk/getting-started (last accessed June 6, 2019).

44. Defendant’s Privacy Products include a software component, for inclusion in its customer’s applications, having an API.

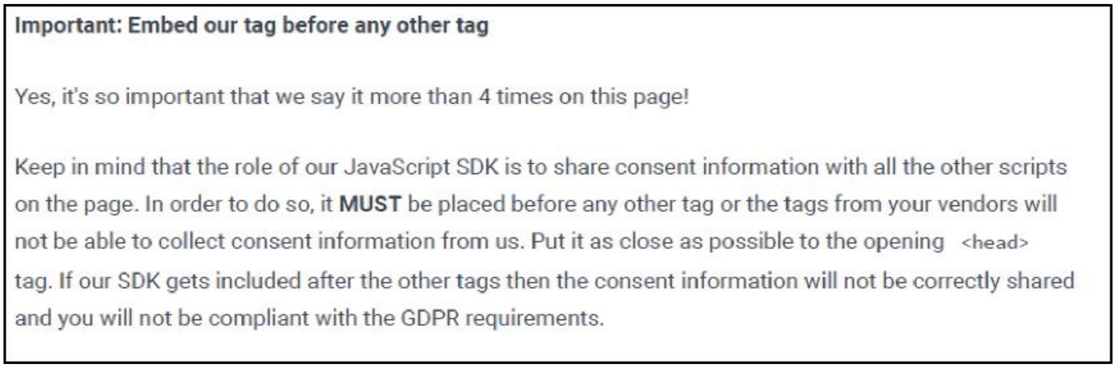


Make sure to:

- Place the tag as close to the opening `<head>` tag on your page as possible, before any other tag gets embedded
- Add your API key into the tag (replace the `<Your API Key>` value)
- Configure the `gdprAppliesGlobally` variable to `false` if you are not an EU-based company and only want to collect consent from EU visitors

See https://developers.didomi.io/cmp/web-sdk/getting-started (last accessed June 6, 2019).

45. Defendant’s Privacy Products obtain, or facilitate obtaining, from the application executing on a user’s device, personal information about the user of the application, the personal information obtained via the API by the software component executing on the device.



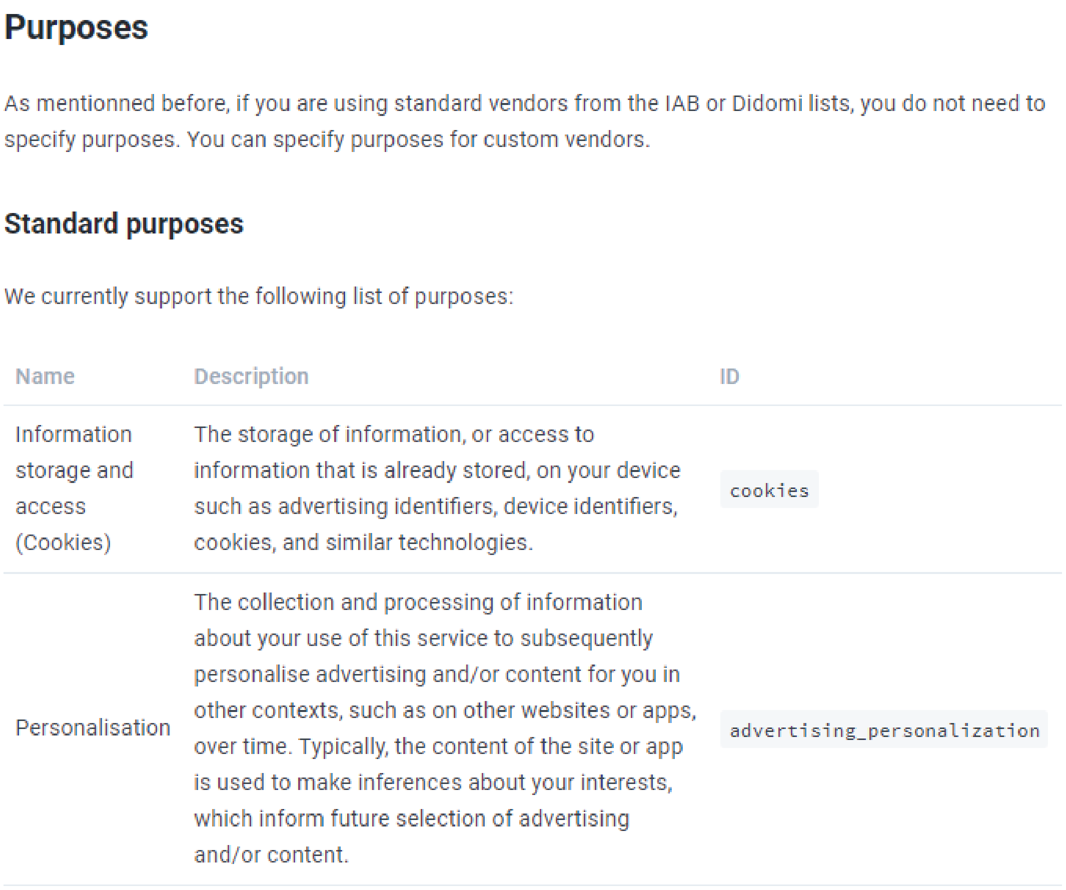
Important: Embed our tag before any other tag

Yes, it's so important that we say it more than 4 times on this page!

Keep in mind that the role of our JavaScript SDK is to share consent information with all the other scripts on the page. In order to do so, it **MUST** be placed before any other tag or the tags from your vendors will not be able to collect consent information from us. Put it as close as possible to the opening `<head>` tag. If our SDK gets included after the other tags then the consent information will not be correctly shared and you will not be compliant with the GDPR requirements.

See https://developers.didomi.io/cmp/web-sdk/getting-started (last accessed June 6, 2019).

46. Defendant’s Privacy Products identify or facilitate identifying the type of the obtained personal information.



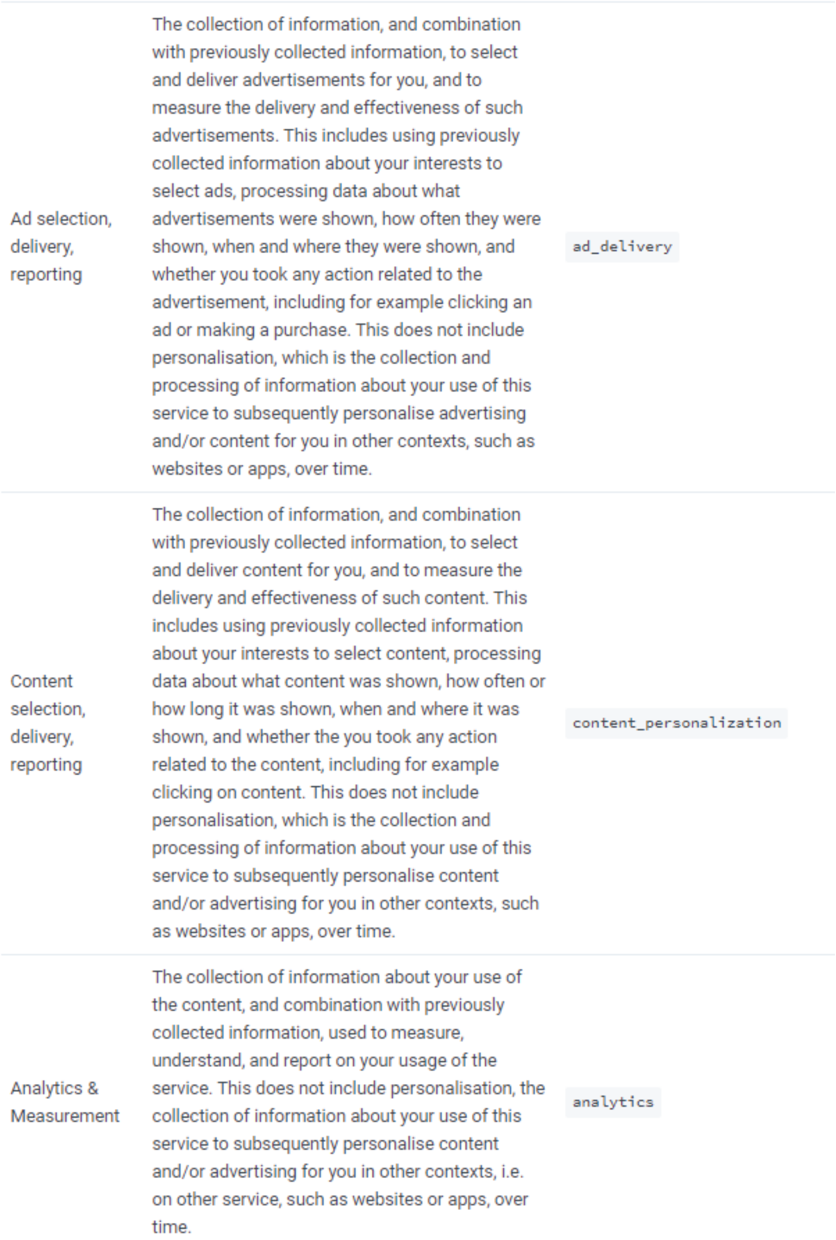
Purposes

As mentionned before, if you are using standard vendors from the IAB or Didomi lists, you do not need to specify purposes. You can specify purposes for custom vendors.

Standard purposes

We currently support the following list of purposes:

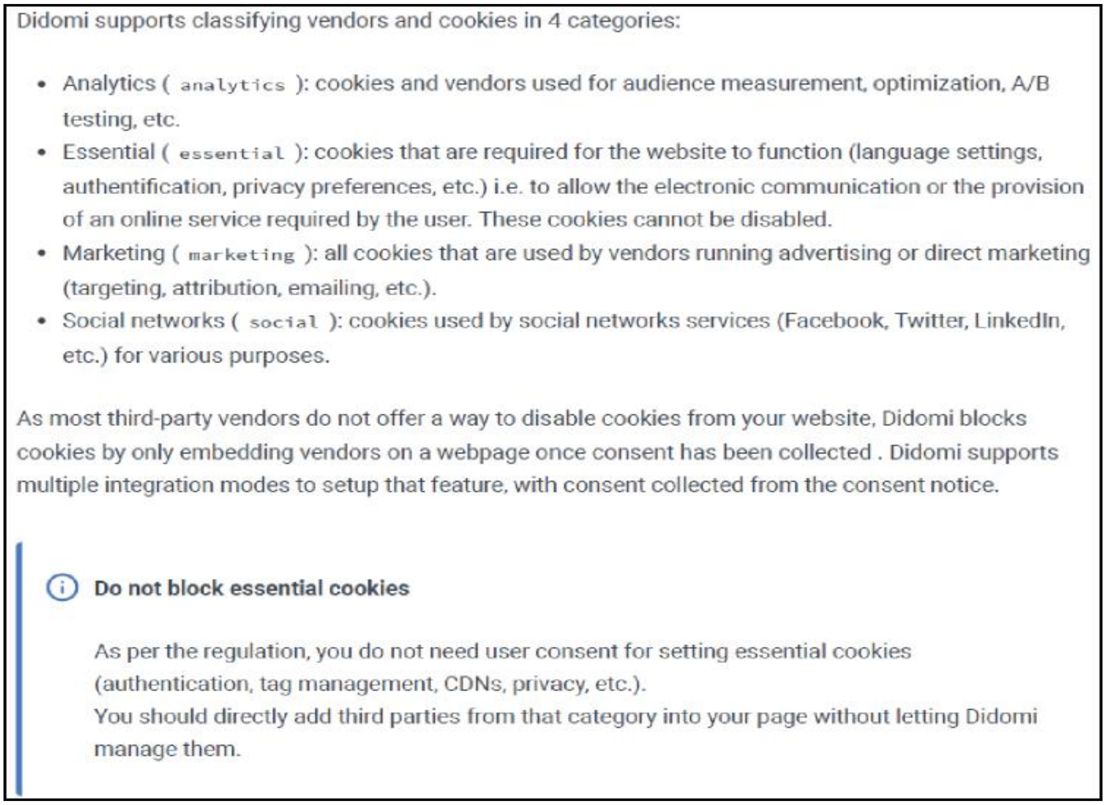
Name	Description	ID
Information storage and access (Cookies)	The storage of information, or access to information that is already stored, on your device such as advertising identifiers, device identifiers, cookies, and similar technologies.	`cookies`
Personalisation	The collection and processing of information about your use of this service to subsequently personalise advertising and/or content for you in other contexts, such as on other websites or apps, over time. Typically, the content of the site or app is used to make inferences about your interests, which inform future selection of advertising and/or content.	`advertising_personalization`



Ad selection, delivery, reporting	The collection of information, and combination with previously collected information, to select and deliver advertisements for you, and to measure the delivery and effectiveness of such advertisements. This includes using previously collected information about your interests to select ads, processing data about what advertisements were shown, how often they were shown, when and where they were shown, and whether you took any action related to the advertisement, including for example clicking an ad or making a purchase. This does not include personalisation, which is the collection and processing of information about your use of this service to subsequently personalise advertising and/or content for you in other contexts, such as websites or apps, over time.	`ad_delivery`
Content selection, delivery, reporting	The collection of information, and combination with previously collected information, to select and deliver content for you, and to measure the delivery and effectiveness of such content. This includes using previously collected information about your interests to select content, processing data about what content was shown, how often or how long it was shown, when and where it was shown, and whether the you took any action related to the content, including for example clicking on content. This does not include personalisation, which is the collection and processing of information about your use of this service to subsequently personalise content and/or advertising for you in other contexts, such as websites or apps, over time.	`content_personalization`
Analytics & Measurement	The collection of information about your use of the content, and combination with previously collected information, used to measure, understand, and report on your usage of the service. This does not include personalisation, the collection of information about your use of this service to subsequently personalise content and/or advertising for you in other contexts, i.e. on other service, such as websites or apps, over time.	`analytics`

See https://developers.didomi.io/cmp/mobile-sdk/consent-notice/vendors-and-purposes (last accessed June 6, 2019).

47. Defendant's Privacy Products "support[] classifying vendors and cookies in 4 categories."



Didomi supports classifying vendors and cookies in 4 categories:

- Analytics (`analytics`): cookies and vendors used for audience measurement, optimization, A/B testing, etc.
- Essential (`essential`): cookies that are required for the website to function (language settings, authentification, privacy preferences, etc.) i.e. to allow the electronic communication or the provision of an online service required by the user. These cookies cannot be disabled.
- Marketing (`marketing`): all cookies that are used by vendors running advertising or direct marketing (targeting, attribution, emailing, etc.).
- Social networks (`social`): cookies used by social networks services (Facebook, Twitter, LinkedIn, etc.) for various purposes.

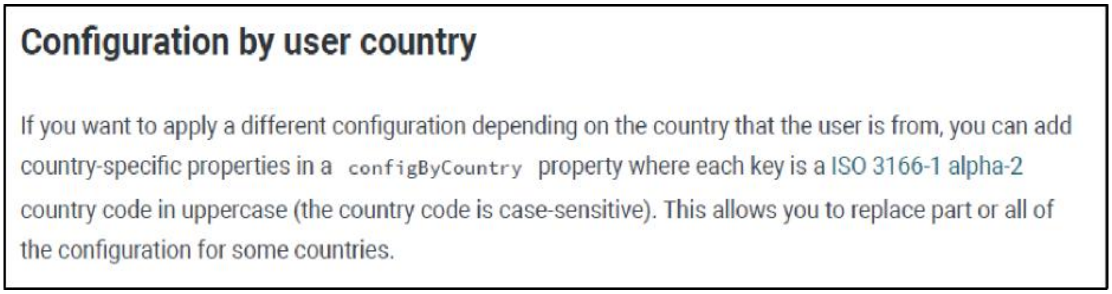
As most third-party vendors do not offer a way to disable cookies from your website, Didomi blocks cookies by only embedding vendors on a webpage once consent has been collected . Didomi supports multiple integration modes to setup that feature, with consent collected from the consent notice.

Do not block essential cookies

As per the regulation, you do not need user consent for setting essential cookies (authentication, tag management, CDNs, privacy, etc.).
You should directly add third parties from that category into your page without letting Didomi manage them.

See https://developers.didomi.io/cmp/web-sdk/block-cookies-by-category (last accessed June 6, 2019).

48. Defendant's Privacy Products identify or facilitate identifying information such as the country from which a user is accessing a website.

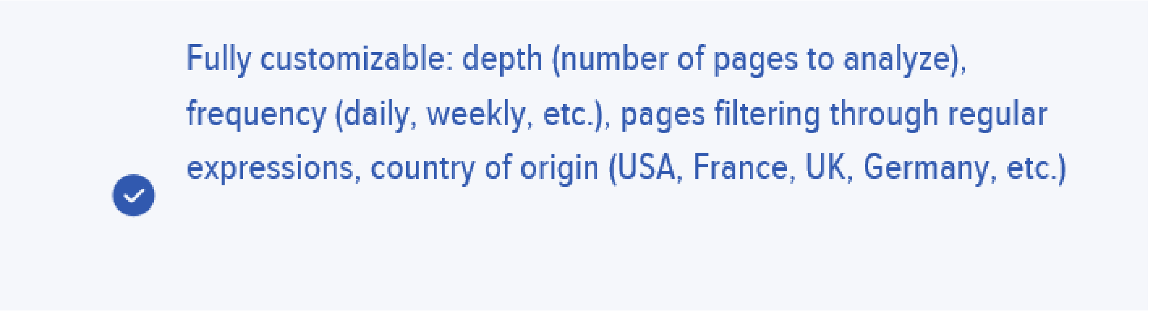


Configuration by user country

If you want to apply a different configuration depending on the country that the user is from, you can add country-specific properties in a `configByCountry` property where each key is a ISO 3166-1 alpha-2 country code in uppercase (the country code is case-sensitive). This allows you to replace part or all of the configuration for some countries.

See https://developers.didomi.io/cmp/web-sdk/consent-notice/customize-notice (last accessed June 6, 2019).

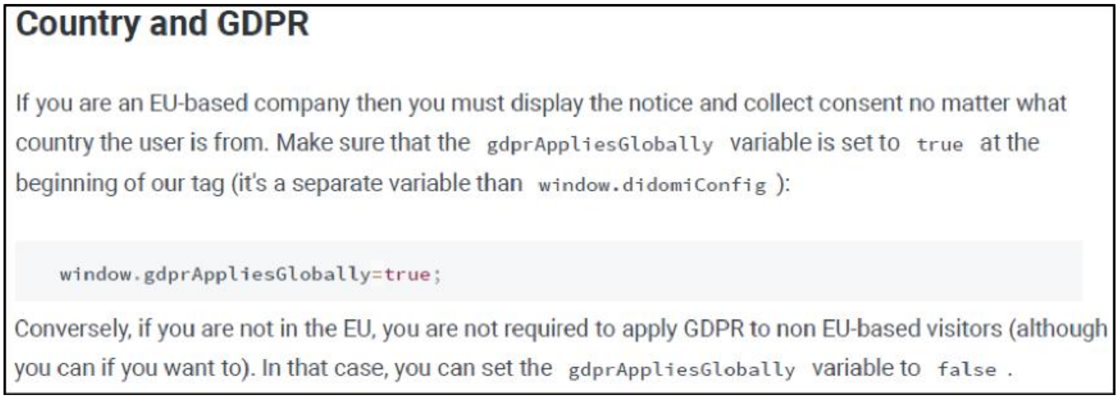
49. The United States is a country of origin for compliance products.



✓ Fully customizable: depth (number of pages to analyze), frequency (daily, weekly, etc.), pages filtering through regular expressions, country of origin (USA, France, UK, Germany, etc.)

See https://www.didomi.io/en/compliance-console (last accessed June 6, 2019).

50. Defendant's Privacy Products determine, or facilitate determining, based on at least the type of obtained personal information, a required permission from the user for at least one proposed use of the obtained personal information.



Country and GDPR

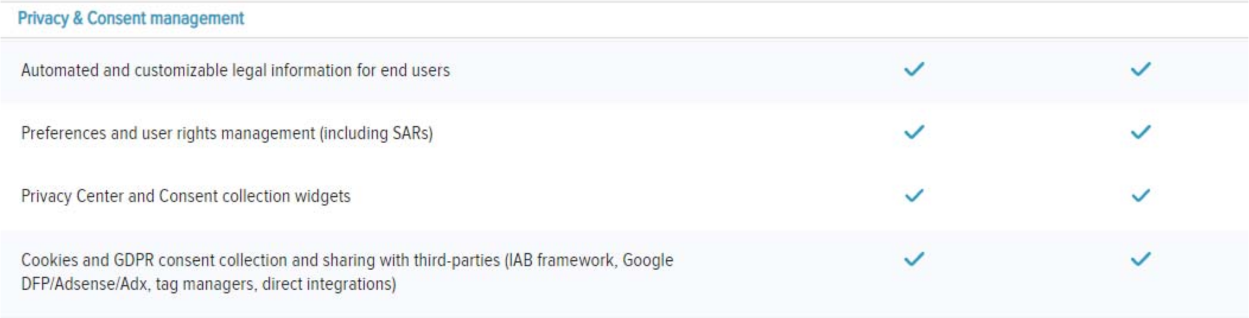
If you are an EU-based company then you must display the notice and collect consent no matter what country the user is from. Make sure that the `gdprAppliesGlobally` variable is set to `true` at the beginning of our tag (it's a separate variable than `window.didomiConfig`):

```
window.gdprAppliesGlobally=true;
```

Conversely, if you are not in the EU, you are not required to apply GDPR to non EU-based visitors (although you can if you want to). In that case, you can set the `gdprAppliesGlobally` variable to `false` .

See https://developers.didomi.io/cmp/web-sdk/consent-notice/customize-notice (last accessed June 6, 2019).

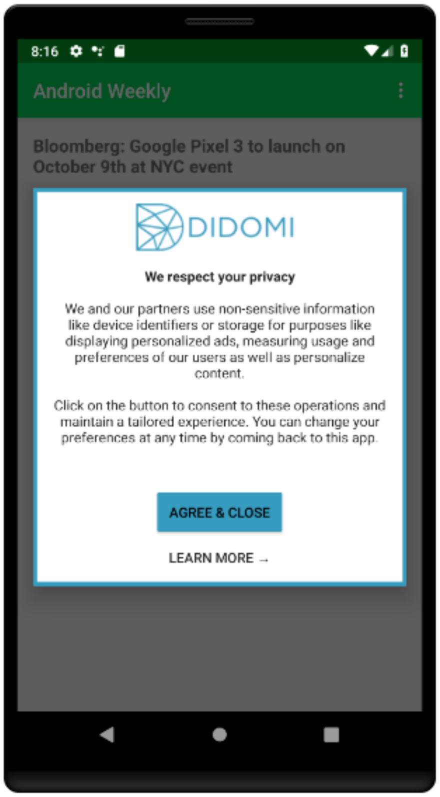
51. As another example, Defendant's website provides that, as part of the monthly fees, its Privacy Products include functionality for "automated and customizable legal information for end users," which, on information and belief, includes determining and presenting the required legal notifications based on the end-user's location.



Privacy & Consent management		
Automated and customizable legal information for end users	✓	✓
Preferences and user rights management (including SARs)	✓	✓
Privacy Center and Consent collection widgets	✓	✓
Cookies and GDPR consent collection and sharing with third-parties (IAB framework, Google DFP/Adsense/Adx, tag managers, direct integrations)	✓	✓

See Ex. 5 (https://www.didomi.io/en/pricing (last accessed June 6, 2019)).

52. Defendant's Privacy Products present, or facilitate presenting, to the user a first offer to provide access to at least one enhanced function of the application in exchange for the required permission.



Bloomberg: Google Pixel 3 to launch on October 9th at NYC event

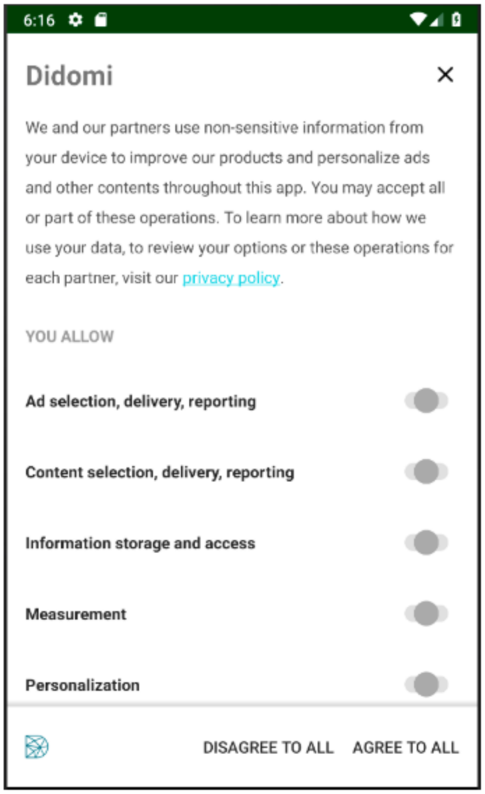
We respect your privacy

We and our partners use non-sensitive information like device identifiers or storage for purposes like displaying personalized ads, measuring usage and preferences of our users as well as personalize content.

Click on the button to consent to these operations and maintain a tailored experience. You can change your preferences at any time by coming back to this app.

Consent collection in-app

See https://developers.didomi.io/cmp/mobile-sdk (last accessed June 6, 2019).



Didomi

We and our partners use non-sensitive information from your device to improve our products and personalize ads and other contents throughout this app. You may accept all or part of these operations. To learn more about how we use your data, to review your options or these operations for each partner, visit our privacy policy.

YOU ALLOW

Ad selection, delivery, reporting

Content selection, delivery, reporting

Information storage and access

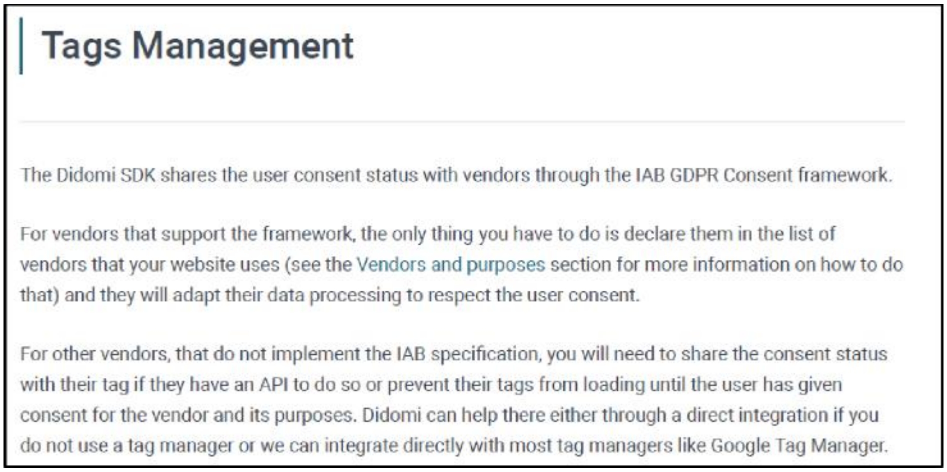
Measurement

Personalization

See https://developers.didomi.io/cmp/mobile-sdk/consent-notice/customize-the-preferences-popup (last accessed June 6, 2019).

53. Defendant's Privacy Products, responsive to the user providing the required permission, provide or facilitate providing the user with access to the at least one enhanced function of the application.

54. For example, Defendant's Privacy Products prevent vendor tags from loading until the user provides consent for the vendor and its purpose.



Tags Management

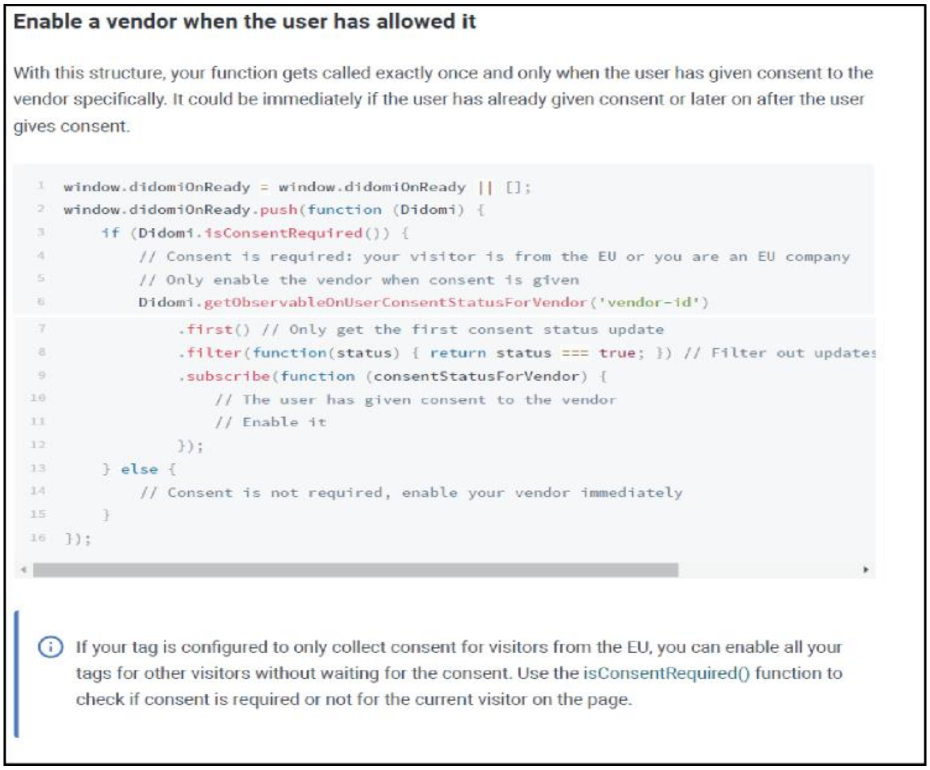
The Didomi SDK shares the user consent status with vendors through the IAB GDPR Consent framework.

For vendors that support the framework, the only thing you have to do is declare them in the list of vendors that your website uses (see the Vendors and purposes section for more information on how to do that) and they will adapt their data processing to respect the user consent.

For other vendors, that do not implement the IAB specification, you will need to share the consent status with their tag if they have an API to do so or prevent their tags from loading until the user has given consent for the vendor and its purposes. Didomi can help there either through a direct integration if you do not use a tag manager or we can integrate directly with most tag managers like Google Tag Manager.

See https://developers.didomi.io/cmp/web-sdk/tags-management (last accessed June 6, 2019).

55. Defendant's Privacy Products include a function that is called "only when the user has given consent to the vendor specifically. It could be immediately if the user has already given consent or later on after the user gives consent."



Enable a vendor when the user has allowed it

With this structure, your function gets called exactly once and only when the user has given consent to the vendor specifically. It could be immediately if the user has already given consent or later on after the user gives consent.

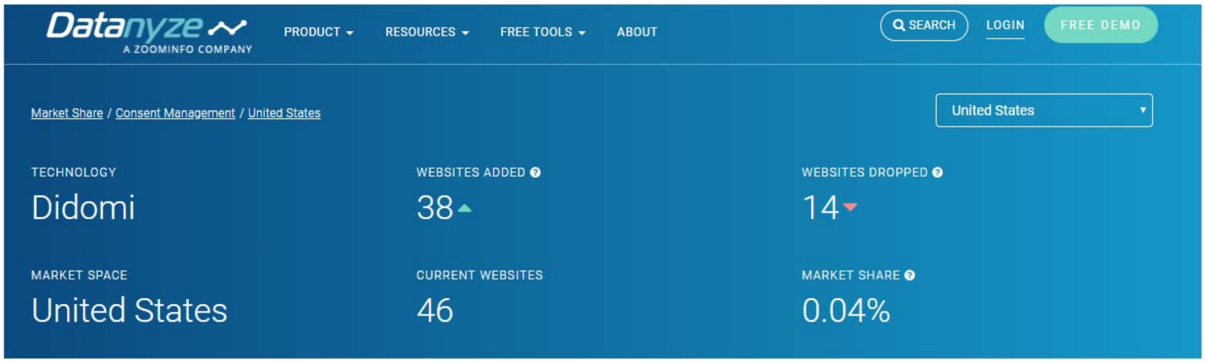
```
window.didomiOnReady = window.didomiOnReady || [];
window.didomiOnReady.push(function (Didomi) {
    if (Didomi.isConsentRequired()) {
        // Consent is required: your visitor is from the EU or you are an EU company
        // Only enable the vendor when consent is given
        Didomi.getObservableOnUserConsentStatusForVendor('vendor-id')
            .first() // Only get the first consent status update
            .filter(function(status) { return status === true; }) // Filter out updates
            .subscribe(function (consentStatusForVendor) {
                // The user has given consent to the vendor
                // Enable it
            });
    } else {
        // Consent is not required, enable your vendor immediately
    }
});
```

ⓘ If your tag is configured to only collect consent for visitors from the EU, you can enable all your tags for other visitors without waiting for the consent. Use the isConsentRequired() function to check if consent is required or not for the current visitor on the page.

See https://developers.didomi.io/cmp/web-sdk/tags-management/no-tag-manager (last accessed June 6, 2019).

<u>Defendant And/Or Its Privacy Products Perform All Steps Of At Least Claim 1 Of The ’451 Patent In The United States</u>

56. On information and belief, Defendant and/or its Privacy Products perform each and every step of at least claim 1 of the ’451 patent within the United States. On information and belief, Defendant’s Privacy Products are integrated into its customers’, purchasers’, users’, developers’, and/or partners’ websites and/or mobile applications that are operated in the United States. For example, Defendant’s Privacy Products are incorporated into at least 40 websites based in the United States.



Market Share / Consent Management / United States

United States

TECHNOLOGY
Didomi

WEBSITES ADDED
38

WEBSITES DROPPED
14

MARKET SPACE
United States

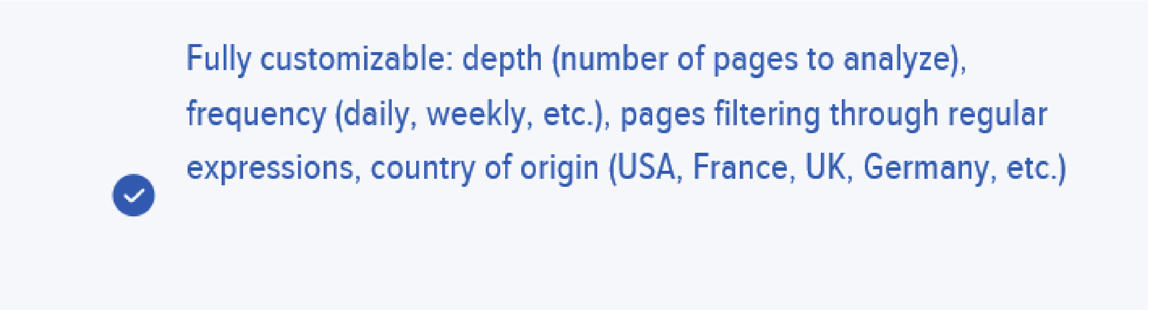
CURRENT WEBSITES
46

MARKET SHARE
0.04%

See Ex. 2 (https://www.datanyze.com/market-share/consent-management/United+States/didomi-market-share (last accessed June 3, 2019)).

57. Accordingly, the incorporation and integration of Defendant’s Privacy Products into its customers’, purchasers’, users’, developers’, and/or partners’ websites and mobile applications occurs in the United States.

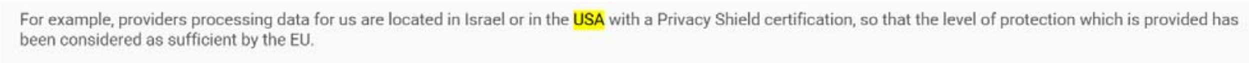
58. Defendant’s Privacy Products collect and maintain users’ personal information, including whether the user’s “country of origin” is the United States.



✓ Fully customizable: depth (number of pages to analyze), frequency (daily, weekly, etc.), pages filtering through regular expressions, country of origin (USA, France, UK, Germany, etc.)

See https://www.didomi.io/en/compliance-console (last accessed June 6, 2019).

59. On information and belief, Defendant's Privacy Products collect, use, and transfer its customers', purchasers', users', developers', and/or partners' data, including end-users' personal information, within the United States. *See* Ex. 14 (https://privacy.didomi.io/en/userdata#rights (last accessed June 3, 2019)).



For example, providers processing data for us are located in Israel or in the USA with a Privacy Shield certification, so that the level of protection which is provided has been considered as sufficient by the EU.

See https://privacy.didomi.io/en/policy (last accessed June 6, 2019).

60. Accordingly, Defendant's Privacy Products practice each and every step of at least claim 1 of the '451 Patent within the United States.

Defendant Maintains Direction And Control Over Its Customers And/Or Its Privacy Products And Its Customers' Use Of The Privacy Products Is Attributable To Defendant

61. On information and belief, Defendant maintains direction and control over its Privacy Products and/or its customers', purchasers', users', developers', and/or partners' use of its Privacy Products upon integration and incorporation into its customers', purchasers', users', developers', and/or partners' websites and mobile applications.

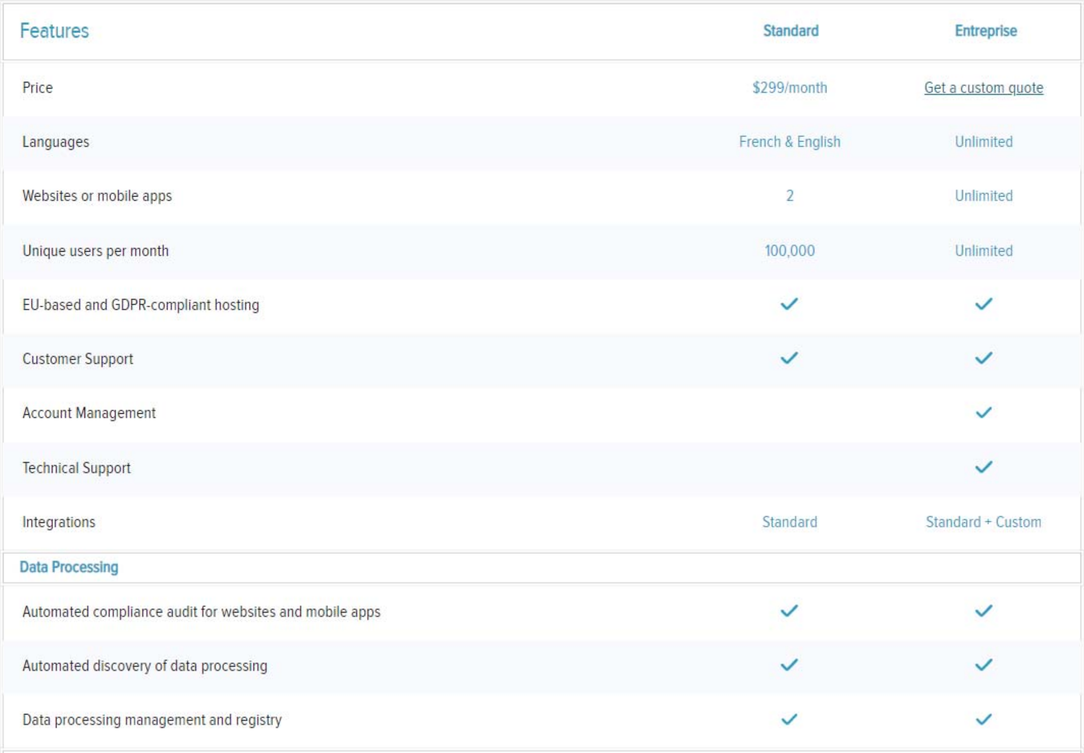
62. On information and belief, Defendant requires that its customers, purchasers, users, developers, and/or partners execute a contract that obligates its customers, purchasers, users, developers, and/or partners to use the Privacy Products within their websites and mobile

applications in a specific manner and at a specific time. For example, Defendant requires that, among other things, its Privacy Products be integrated into its customers', purchasers', users', developers', and/or partners' websites and mobile applications in a specific manner to obtain consent from the end-users in compliance with applicable regulatory schemes before collecting and/or using the end-user's data.

63. On information and belief, Defendant's customers, purchasers, users, developers, and/or partners can generate revenue from the sale of the end-user's information collected through the Privacy Products only if they fully comply with Defendant's requirements concerning the use of the Privacy Products. Accordingly, Defendant is liable for its customers, purchasers', users', developers', and/or partners' use of the Privacy Products within their websites and mobile application used in the United States.

64. Additionally, Defendant's and its customers', purchasers', users', developers', and/or partners' integration and use of the Privacy Products constitute a joint enterprise where the steps of at least claim 1 of the '451 Patent that are performed by Defendant's customers, purchasers, users, developers, and/or partners are attributable to Defendant.

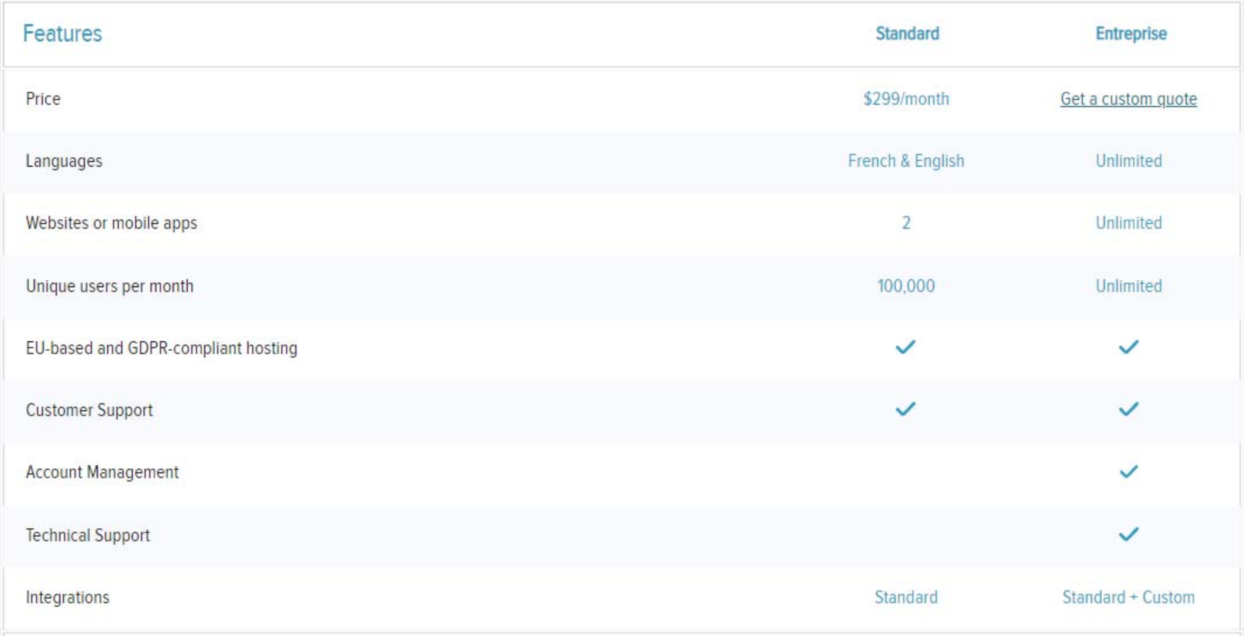
65. On information and belief, Defendant requires that its customers, purchasers, users, developers, and/or partners execute a contract for the use of the Privacy Products. As part of the contract, Defendant charges monthly fees for its customers', purchasers', users', developers', and/or partners' use of its Privacy Products. For example, Defendant charges its customers, purchasers, users, developers, and/or partners $299 per month for standard features and $699 per month for additional features that include legal counsel. Defendant also offers to provide a custom quote for its enterprise version of its Privacy Products.



Features	Standard	Entreprise
Price	$299/month	Get a custom quote
Languages	French & English	Unlimited
Websites or mobile apps	2	Unlimited
Unique users per month	100,000	Unlimited
EU-based and GDPR-compliant hosting	✓	✓
Customer Support	✓	✓
Account Management		✓
Technical Support		✓
Integrations	Standard	Standard + Custom
Data Processing		
Automated compliance audit for websites and mobile apps	✓	✓
Automated discovery of data processing	✓	✓
Data processing management and registry	✓	✓

See Ex. 5 (https://www.didomi.io/en/pricing (last accessed June 6, 2019)).

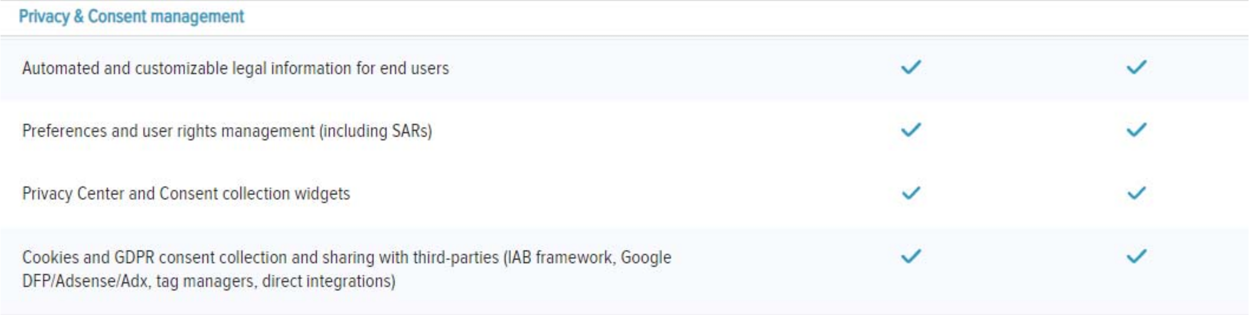
66. As part of the Defendant's monthly fees, Defendant integrates its Privacy Products for use within its customers', purchasers', users', developers', and/or partners' websites and mobile applications.



Features	Standard	Entreprise
Price	$299/month	Get a custom quote
Languages	French & English	Unlimited
Websites or mobile apps	2	Unlimited
Unique users per month	100,000	Unlimited
EU-based and GDPR-compliant hosting	✓	✓
Customer Support	✓	✓
Account Management		✓
Technical Support		✓
Integrations	Standard	Standard + Custom

See Ex. 5 (https://www.didomi.io/en/pricing (last accessed June 6, 2019)).

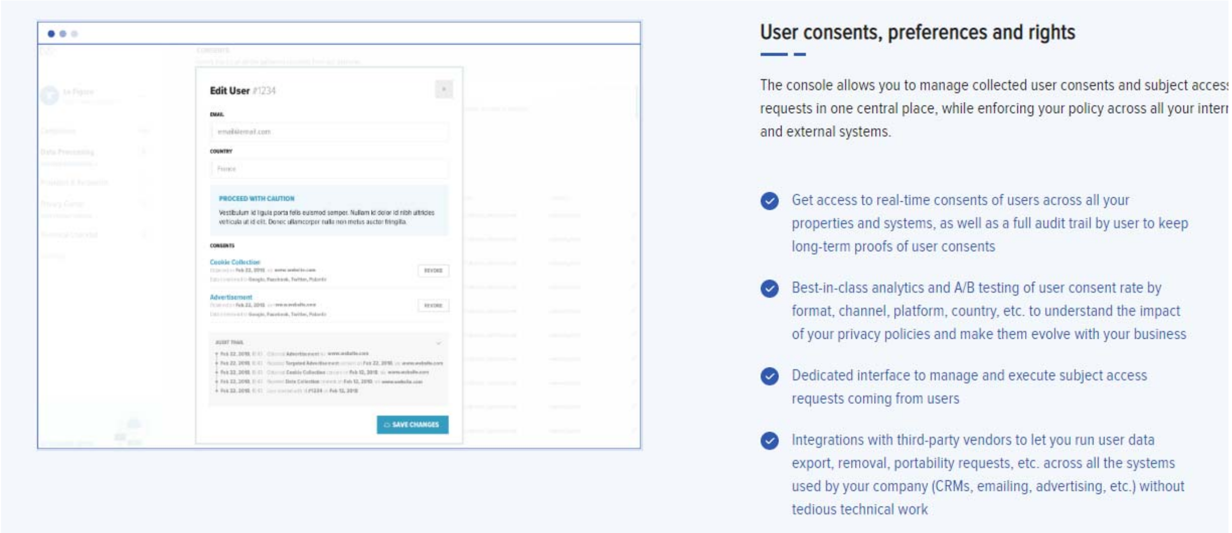
67. Upon integration, and as part of the monthly fees, Defendant's Privacy Products collect user consents and personal information.



Privacy & Consent management		
Automated and customizable legal information for end users	✓	✓
Preferences and user rights management (including SARs)	✓	✓
Privacy Center and Consent collection widgets	✓	✓
Cookies and GDPR consent collection and sharing with third-parties (IAB framework, Google DFP/Adsense/Adx, tag managers, direct integrations)	✓	✓

See Ex. 5 (https://www.didomi.io/en/pricing (last accessed June 6, 2019)).

68. Defendant's website states that "[t]he console allows you to manage collected user consents and subject access requests in one central place, which enforcing your policy across all your internal and external systems."



Edit User #1234

EMAIL

email@email.com

COUNTRY

France

PROCEED WITH CAUTION

Vestibulum id ligula porta felis euismod semper. Nullam id dolor id nibh ultricies vehicula ut id elit. Donec ullamcorper nulla non metus auctor fringilla.

CONSENTS

Cookie Collection REVOKE

Advertisement REVOKE

AUDIT TRAIL

SAVE CHANGES

User consents, preferences and rights

The console allows you to manage collected user consents and subject acces requests in one central place, while enforcing your policy across all your intern and external systems.

- Get access to real-time consents of users across all your properties and systems, as well as a full audit trail by user to keep long-term proofs of user consents
- Best-in-class analytics and A/B testing of user consent rate by format, channel, platform, country, etc. to understand the impact of your privacy policies and make them evolve with your business
- Dedicated interface to manage and execute subject access requests coming from users
- Integrations with third-party vendors to let you run user data export, removal, portability requests, etc. across all the systems used by your company (CRMs, emailing, advertising, etc.) without tedious technical work

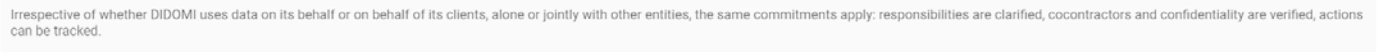
See https://www.didomi.io/en/compliance-console (last accessed June 6, 2019).

69. On information and belief, as part of the contract, Defendant agrees to provide customer support and technical assistance to its customers, purchasers, users, developers, and/or partners that incorporate Defendant's Privacy Products into their websites and mobile applications

to ensure that said Privacy Products are used in a specific manner that performs each and every step of at least claim 1 of the ’451 Patent.

70. On information and belief, Defendant’s customers, purchasers, users, developers, and/or partners can generate revenue from the sale of the end-user’s information collected through the Privacy Products only if they fully comply with Defendant’s requirements concerning the use of the Privacy Products.

71. Similarly, on information and belief, without the contractual requirements, Defendant would not be able to ensure that its customers’, purchasers’, users’, developers’, and/or partners’ end-users’ information is collected in a manner that complies with certain privacy laws so that Defendant may use such information to generate additional revenue.



Irrespective of whether DIDOMI uses data on its behalf or on behalf of its clients, alone or jointly with other entities, the same commitments apply: responsibilities are clarified, cocontractors and confidentiality are verified, actions can be tracked.

See https://privacy.didomi.io/en/policy (last accessed June 6, 2019).

72. As explained in the foregoing paragraphs, Defendant’s Privacy Products infringe at least claim 1 of the ’451 Patent.

73. Defendant has had actual knowledge of the ’451 Patent since at least February 6, 2019. On information and belief, Defendant’s infringement of the ’451 Patent has been and continues to be deliberate and willful, and therefore, this is an exceptional case warranting an award of treble damages and attorneys’ fees to Plaintiff pursuant to 35 U.S.C. §§ 284-285. Defendant has also not been forthcoming regarding its commercial activities in the United States regarding its Privacy Products.

74. Plaintiff has been and continues to be injured by Defendant’s infringement of the ’451 Patent. Plaintiff is entitled to recover damages adequate to compensate it for Defendant’s

infringing activities in an amount to be determined at trial but in no event less than a reasonable royalty.

75. In addition, Defendant's infringing acts have caused and are causing immediate and irreparable harm to Plaintiff, including because Defendant directly competes with Plaintiff. Unless enjoined by this Court, Defendant's acts of infringement will continue to irreparably damage Plaintiff.

COUNT II: INDIRECT INFRINGEMENT OF U.S. PATENT NO. 10,075,451

76. Plaintiff hereby re-alleges and incorporates by reference the allegations set forth in the foregoing paragraphs as though fully set forth herein.

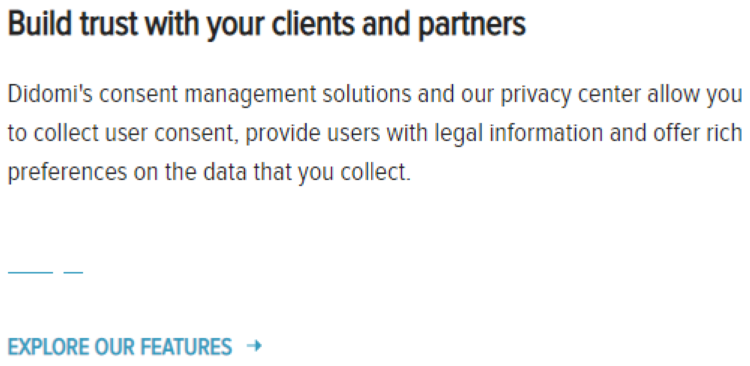
77. Defendant has been and continues to directly and indirectly infringe, literally and/or under the doctrine of equivalents, at least claim 1 of the '451 Patent in violation of 35 U.S.C. § 271.

78. Defendant has been and continues to induce the infringement of at least claim 1 of the '451 Patent in violation of 35 U.S.C. § 271(b), literally and/or under the doctrine of equivalents, by, among other things, knowingly encouraging and aiding others, and instructing third-parties, including but not limited to its customers, purchasers, users, developers, and/or partners, to use the Privacy Products in this judicial district and throughout the United States without license or authority from Plaintiff, with knowledge or willful blindness to the fact that Defendant's actions induce others, including but not limited to its customers, purchasers, users, developers, and/or partners, to infringe the '451 Patent.

79. Defendant induces others to infringe the '451 Patent by encouraging, instructing, and facilitating others, including but not limited to its customers, purchasers, users, developers, and/or partners, to perform actions, including all or some of the steps of the method claims of the

’451 Patent, that Defendant knows to be acts of infringement of the ’451 Patent with the specific intent that those performing the acts infringe the ’451 Patent. Defendant has specifically intended that its customers, purchasers, users, developers, and/or partners use its Privacy Products that infringe at least claim 1 of the ’451 Patent by, at a minimum, instructing, directing, and/or requiring its customers, purchasers, users, developers, and/or partners to perform all or some of the steps of at least claim 1 of the ’451 Patent, including, for example, by providing a demonstration detailing how to build their own Privacy Center, to enable them to infringe at least claim 1 of the ’451 Patent. *See, e.g.*, https://www.didomi.io/en/privacy-center (last accessed June 6, 2019). On information and belief, Defendant also operates a website that instructs users on how to incorporate the Privacy Products into their websites and mobile applications and offers users assistance regarding the same.

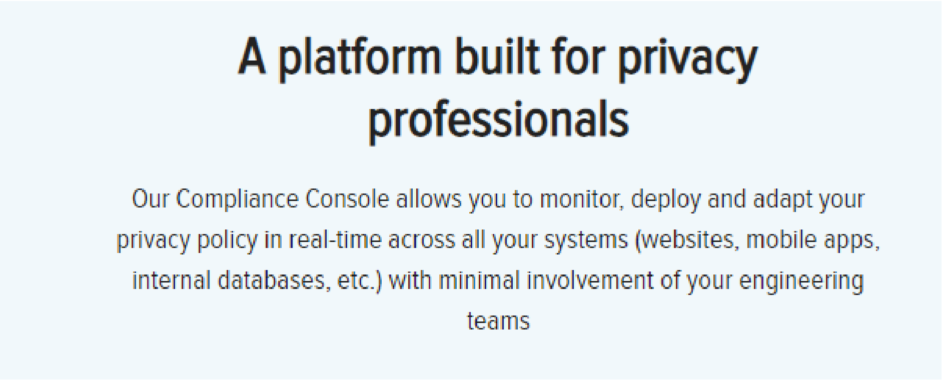
80. Defendant advertises and promotes its Privacy Products to be used by its customers, purchasers, users, developers, and/or partners, or in or in conjunction with its customers’, purchasers’, users’, developers’, and/or partners’ websites and mobile applications, in a manner that performs all of the steps of at least claim 1 of the ’451 Patent. For example, Defendant advertises and promotes its Privacy Products as “the best platform for managing data privacy compliance” that “allow[s] you to collect user consent, provide users with legal information, . . . offer rich preferences on the data you collect” and “monitor deploy, and adapt your privacy policy in real-time across all your systems (websites, mobile apps, internal databases, etc.) with minimal involvement from your engineering teams.”



Build trust with your clients and partners

Didomi's consent management solutions and our privacy center allow you to collect user consent, provide users with legal information and offer rich preferences on the data that you collect.

See https://www.didomi.io/en/ (last accessed June 6, 2019).

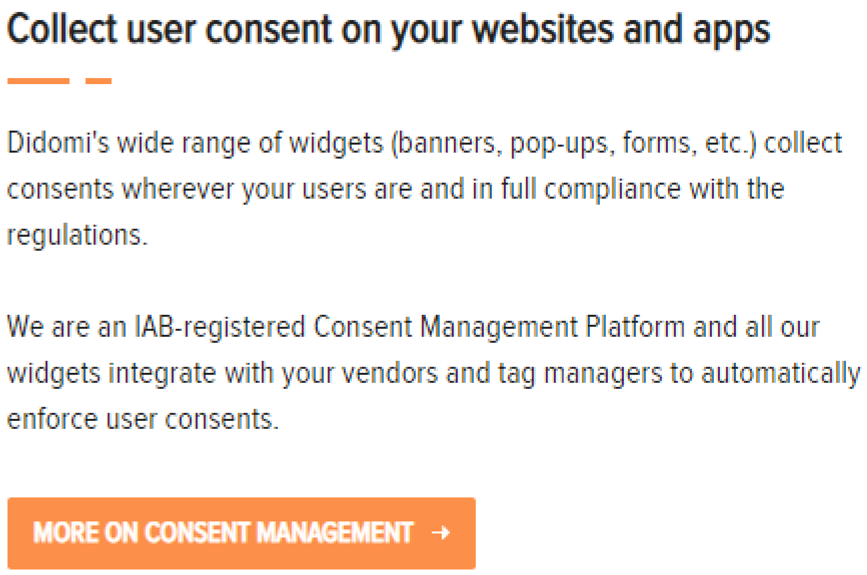


A platform built for privacy professionals

Our Compliance Console allows you to monitor, deploy and adapt your privacy policy in real-time across all your systems (websites, mobile apps, internal databases, etc.) with minimal involvement of your engineering teams

See https://www.didomi.io/en/ (last accessed June 6, 2019).

81. Defendant further advertises and promotes its Privacy Products as including a "wide range of widgets (banners, pop-ups, forms, etc.) [to] collect consents where your users are and in full compliance with regulations."



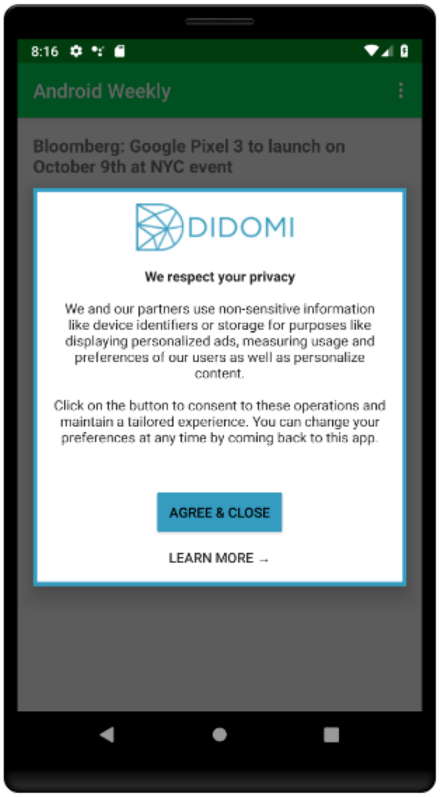
Collect user consent on your websites and apps

Didomi's wide range of widgets (banners, pop-ups, forms, etc.) collect consents wherever your users are and in full compliance with the regulations.

We are an IAB-registered Consent Management Platform and all our widgets integrate with your vendors and tag managers to automatically enforce user consents.

See https://www.didomi.io/en/ (last accessed June 6, 2019).

82. Defendant further advertises and promotes its Privacy Products as including a pop-up that presents an end-user with an offer to provide an enhanced function of the website or mobile application, such as full access, a more tailored experience, or more personalized advertisement in exchange for the end-user's consent to collect and use that end-user's data and information.



8:16

Android Weekly

Bloomberg: Google Pixel 3 to launch on October 9th at NYC event

DIDOMI

We respect your privacy

We and our partners use non-sensitive information like device identifiers or storage for purposes like displaying personalized ads, measuring usage and preferences of our users as well as personalize content.

Click on the button to consent to these operations and maintain a tailored experience. You can change your preferences at any time by coming back to this app.

AGREE & CLOSE

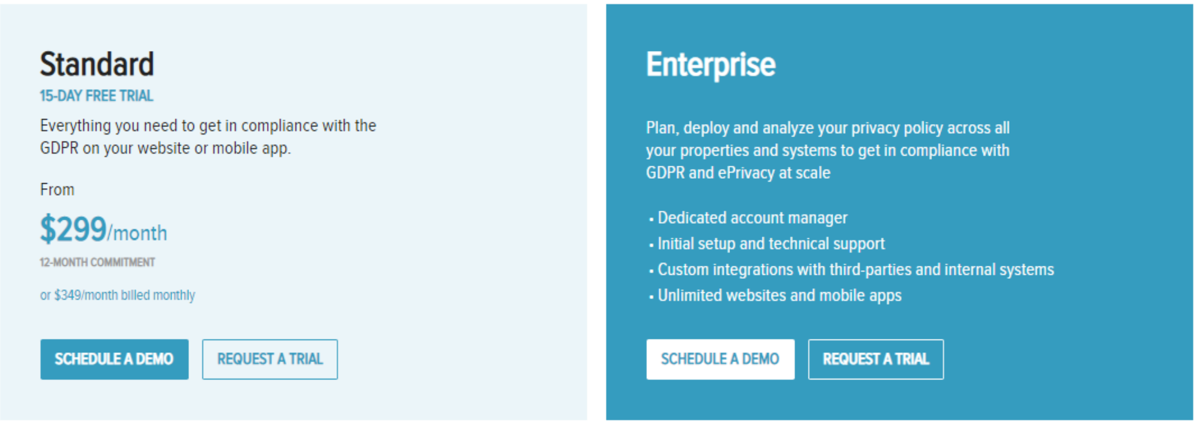
LEARN MORE →

Consent collection in-app

See https://developers.didomi.io/cmp/mobile-sdk (last accessed June 6, 2019).

83. Defendant provides its customers, purchasers, users, developers, and/or partners with instructions on how to use its Privacy Products in a manner that performs the steps of at least claim 1 of the ’451 Patent. *See* Ex. 15 (https://developers.didomi.io/ (last accessed June 3, 2019)).

84. On information and belief, Defendant requires that its customers, purchasers, users, developers, and/or partners execute a contract that delineates the steps that its customers, purchasers, users, developers, and/or partners must take to use its Privacy Products in a manner that performs the steps of at least claim 1 of the ’451 Patent. For example, Defendant requires at least a 12-month commitment at $299 per month for its customers, purchasers, users, developers, and/or partners to use its Privacy Products.



Standard

15-DAY FREE TRIAL

Everything you need to get in compliance with the GDPR on your website or mobile app.

From

$299/month

12-MONTH COMMITMENT

or $349/month billed monthly

Enterprise

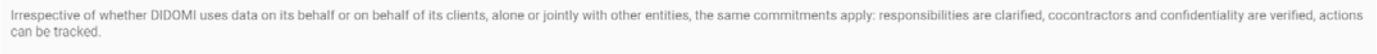
Plan, deploy and analyze your privacy policy across all your properties and systems to get in compliance with GDPR and ePrivacy at scale

- Dedicated account manager
- Initial setup and technical support
- Custom integrations with third-parties and internal systems
- Unlimited websites and mobile apps

See, e.g., Ex. 5 (https://www.didomi.io/en/pricing (last accessed June 6, 2019)).

85. On information and belief, as part of the contract, Defendant agrees to provide customer support and technical assistance to its customers, purchasers, users, developers, and/or partners that incorporate Defendant's Privacy Products into their websites and mobile applications so that said Privacy Products are used in a manner that perform each and every step of at least claim 1 of the '451 Patent.

86. On information and belief, Defendant requires that its customers, purchasers, users, developers, and/or partners use its Privacy Products in a manner that performs each and every step of at least claim 1 of the '451 Patent to ensure an its customers', purchasers', users', developers', and/or partners' end-users' information is collected in a manner that complies with certain privacy laws so that Defendant may use such information to generate additional revenue.



Irrespective of whether DIDOMI uses data on its behalf or on behalf of its clients, alone or jointly with other entities, the same commitments apply: responsibilities are clarified, cocontractors and confidentiality are verified, actions can be tracked.

See https://privacy.didomi.io/en/policy (last accessed June 6, 2019).

87. Additionally, Defendant has been and continues to contributorily infringing at least claim 1 of the '451 Patent in violation of 35 U.S.C. § 271(c), literally and/or under the doctrine of equivalents, by, among other things, selling, offering for sale, and/or importing into this judicial district and throughout the United States, infringing products, including but not limited to its

Privacy Products, that embody a material part of the inventions described in the ’451 Patent or are especially adapted for use in infringement of the ’451 Patent, and are not staple articles of commerce or commodities suitable for substantial, non-infringing uses. Defendant’s actions contribute to the direct infringement of at least claim 1 of the ’451 Patent by others, including its customers, purchasers, users, developers, and/or partners, in violation of 35 U.S.C. § 271(c).

88. Defendant has had actual knowledge since at least since February 6, 2019 that its Privacy Products, including but not limited to its Privacy Products, cannot be used without infringing the technology claimed in the ’451 Patent, as described above.

89. On information and belief, Defendant’s infringement of the ’451 Patent has been and continues to be deliberate and willful, and, therefore, this is an exceptional case warranting an award of treble damages and attorneys’ fees to Plaintiff pursuant to 35 U.S.C. §§ 284-285.

90. Plaintiff has been damaged by Defendant’s infringement of the ’451 Patent and will continue to be damaged by such infringement. Plaintiff is entitled to recover from Defendant the damages sustained by Plaintiff as a result of Defendant’s wrongful acts.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays for judgment against Defendant as follows:

a. A judgment in favor of Plaintiff that Defendant has directly infringed and indirectly infringed, and continues to directly infringe and indirectly infringe, one or more claims of the ’451 Patent literally and/or under the doctrine of equivalents;

b. A permanent injunction restraining and enjoining Defendant and its officers, directors, agents, servants, employees, successors, assigns, parents, subsidiaries, affiliated or related companies, and attorneys from directly infringing or indirectly infringing one or more claims of the ’451 Patent;

c. An award of damages adequate to compensate Plaintiff for Defendant's infringement of the '451 Patent, but not less than a reasonable royalty, together with pre-judgment and post-judgment interest and costs;

d. An award of treble damages to Plaintiff for Defendant's willful infringement;

e. An award of Plaintiff's costs of suit and reasonable attorneys' fees pursuant to 35 U.S.C. § 285 due to the exceptional nature of this case, or as otherwise permitted by law with respect to Defendant;

f. A grant to Plaintiff of such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff respectfully demands a trial by jury on all claims and issues so triable.

Dated: June 6, 2019

Respectfully submitted,

KASOWITZ BENSON TORRES LLP

By: */s/ Jonathan K. Waldrop*

Jonathan K. Waldrop *(pro hac vice)*
(California State Bar No. 297903)
333 Twin Dolphin Drive, Suite 200
Redwood Shores, CA 94065
Tel: (650) 453-5170
Fax: (650) 453-5171
jwaldrop@kasowitz.com

Mark P. Ressler
New York Bar No. 2295582
mressler@kasowitz.com
Kenneth R. David
New York Bar No. 3006574
kdavid@kasowitz.com
Hershy Stern
New York Bar No. 4631024
hstern@kasowitz.com
1633 Broadway
Kasowitz Benson Torres LLP
New York, NY 10019
Tel: (212) 506-1700
Fax: (212) 506-1800