THE COOKIEBOT SOLUTION

Cookiebot is a cloud-based self-service Consent Management Platform (CMP) that any company, organisation or individual can sign up to online and easily implement on their website(s). Cookiebot is sold in a freemium subscription model. The solution is trusted by organisations across all industries, public and private, of all sizes, and in all EU countries as well as a wide range of countries outside of the EU, including the US, Canada, Japan, and several other countries in Latin America and Asia looking to comply especially with the GDPR. Cookiebot is also increasingly looked to for handling the websites' consent management aspect of several other new GDPR-like legislations underway including those in California and other US states, Canada, Brazil, Japan, India and many more countries.

Features of the Cookiebot solution

The Cookiebot solution contains all the elements needed for making a website's use of cookies and online tracking GDPR (and ePR) compliant. No on-site deployment or consulting services are needed. It all runs in the cloud and is fully scalable. Note that this also means that it is perfectly possible for Cookiebot clients to set up the solution in a non-compliant manner. While the implementation of the Cookiebot technology does make compliance possible for our clients, we are in no position to check up on or guarantee that our clients make use of all its elements in the right way. The following are the main elements included in the service:

- **Automated monthly website scans for detection and transparency** – the Cookiebot scanner crawls all the html content on the website that a website user can access (including static and dynamic pages, blog posts, images, embedded videos etc.) and checks the website for all cookies/tracking technology in use (including both common cookie types such as http cookies and harder to detect dynamic cookies and a range of advanced tracking technology. A monthly report with the results is produced, including information about what scripts are setting the cookies/trackers, where on the website they are located (down to the line of the source code where applicable), whether a cookie/tracker is categorised as necessary, preference, statistics or marketing, what countries data is being sent to and more. Any new cookies in use since the last scan are clearly marked.

- **A fully customisable cookie consent banner providing transparency and 'prior consent'** – the banner appears on the website and presents the user with information about the website's use of cookies /trackers – all relevant information from the monthly website scan is automatically presented in the consent banner along with purpose descriptions in plain and simple language explaining what the user's data is being used for. The banner is also where the user can give and change his/her consent to the various categories of cookies and

tracking. The underlying technology ensures that all cookies other than those strictly necessary for the website to function are being held back until the user has given a consent thereby providing the GDPR and ePR required 'prior consent'. All consents are automatically renewed after 12 months, and the user is again presented with the consent banner and asked for a new consent.

- **Logging of consents for documentation purposes** – each user consent is logged (anonymized and using an encrypted key) along with relevant information about when the consent was given, the URL the consent was submitted from and other relevant information. This log can be downloaded from the Cookiebot Manager (dashboard) and be presented to the authorities for documentation or be used if a user makes a complaint.

- **A Cookie Declaration with built-in possibility to easily withdraw or change a consent** – the Cookie Declaration is in essence an automated cookie policy that can be used either as a stand-alone policy or incorporated into an existing privacy policy on the website. The cookie policy contains all relevant information from the monthly scans and is automatically updated with each new scan. It also includes information about the user's current consent state (i.e. what categories of cookies the user has given his consent to) and a link to easily withdraw or change his consent.

- **A user-friendly dashboard (the Cookiebot Manager) allowing for easy handling of the entire set-up** – here the customer can access and change all aspects of his configuration, account and payment data, edit banner text, templates and layout, handle translations and localization, access previous scan reports, see consent statistics, access and download the consent log and extract data in various formats (CSV, XML, JSON as well as in a machine readable format via API)

How does Cookiebot work?

Customers sign up for a Cookiebot account online. Once signed up, they can add their domain(s) to a list in the Manager (the user interface/dashboard from where they can handle all aspects of the consent management for their website).

Once a domain has been added to the Manager, the Cookiebot scanner will automatically start crawling the website. This can take up to 24 hours for very large or complex sites but usually completes within a few hours.

The customer inserts 1 or 2 pieces of script on their website. The scripts are available in the Cookiebot Manager and consist of a string of Javascript code. One script is for the consent banner that asks the user for consent and provides the relevant information. The other script is for the Cookie Declaration – a cookie policy the customer can choose to implement as part of an existing privacy policy or as a stand-alone cookie policy and which includes the option for users to easily withdraw their consent at any time.

When the scan is complete, the customer will receive a scan report. This scan report lists all the cookies and other tracking technology in use on the website. All known cookies and trackers are automatically categorized into Necessary, Preferences, Statistics, and Marketing. Along with this classification, information about the exact location of the scripts/tags setting the cookies is included – down to pinpointing from what line of the source code a cookie is deployed, when possible.

With this scan report in hand, the customer needs to mark up the cookie-setting scripts on the website. This tells the Cookiebot technology which cookies are of what type, and this is also the

exact mechanism that ensures that all cookies and trackers are held back until the user has given a consent (prior consent) – and that only the allowed categories of cookies are set based on the user's consent. When correctly implemented, a user coming to a website with Cookiebot implemented will not be tracked and no data will be processed until the user has given a consent (only strictly necessary cookies are allowed to be set before consent is given). If the user decides only to consent to e.g. statistics and preference cookies, then all marketing cookies will be held back. These will only be released if the user changes his/her consent to allow marketing cookies, too. **Simply put – although the technology is anything but simple – Cookiebot functions like an on/off switch between the cookies/trackers in use and the website user**.

How does the marking up of cookie-setting scripts work and how does Cookiebot know what cookies and trackers to switch on and off?

To each cookie-setting script, the attribute "data-cookieconsent" should be added. The comma-separated value should be set to one or more of the cookie categories "preferences", "statistics" and "marketing" in accordance with the types of cookies being set by each script (as described in the scan report). Finally, the attribute “type” should be changed from "text/javascript" to "text/plain". As an example, a Google Analytics Universal script tag setting statistics cookies will go from looking like this:

```
<script type="text/javascript">

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){(i[r].q=i
[r].q||[]).push(arguments)},i[r].l=1*new
Date();a=s.createElement(o),m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parent
Node.insertBefore(a,m)})(window,document,'script','//www.google-
analytics.com/analytics.js','ga');
    ga('create', 'UA-00000000-0', 'auto');
    ga('send', 'pageview');
</script>
```

To looking like this with the new mark-up (changes highlighted in bold):

```
<script type="text/plain" data-cookieconsent="statistics">

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){(i[r].q=i
[r].q||[]).push(arguments)},i[r].l=1*new
Date();a=s.createElement(o),m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parent
Node.insertBefore(a,m)})(window,document,'script','//www.google-
analytics.com/analytics.js','ga');
    ga('create', 'UA-00000000-0', 'auto');
    ga('send', 'pageview');
</script>
```

In making the change to plain text, the script which sets the cookie is placed in an “off-state” – the browser will consider the text to be plain text (and not JavaScript) and simply leave it alone - i.e. the browser will not execute the script and thereby not set the cookie. As long as no user consent has been given, all the scripts appear to be plain text and are left alone by the browser – and no cookies are set (thereby ensuring prior consent). The moment a user gives a consent via the consent banner, this sends a signal to all the scripts of the relevant category and essentially “flips” them back on to being read and executed as JavaScripts and thereby they are executed and set the cookies. For example, if a user has consented to “preferences” but not the other categories, a signal is sent to all those scripts marked with the “preferences” essentially flipping them from plain text into JavaScripts thereby “turning them on”, executing them and allowing them to set the cookies. All the statistics and marketing scripts do not receive this signal and therefore remain plain text and stay turned off (honouring the user’s consent). This “turning on” of the scripts happens instantly with no experienced delay for the website user and the cookies are set immediately.

As more sites are deploying scripts through a tag manager, Cookiebot also exposes a JavaScript API which makes it easy to apply the same overall logic to tag manager triggers.

The marking up of the cookie-setting scripts only needs to be done at the initial implementation – and if new cookies are later added to the website, these will be clearly marked in the next month’s scan report and should be marked up accordingly.

The user needs to maintain the setup mainly by checking the monthly scan reports sent via email for any new trackers that need to be marked up for prior consent and by checking whether any data is being sent to non-adequate countries (clearly marked in the scan report). Cookiebot constantly updates a repository of known cookies and trackers, including purpose descriptions in clear and plain language. When unknown cookies and trackers are identified, these are listed as ‘unclassified’ and should be checked by the customer for correct classification and be given a purpose description.

For more information, visit https://www.cookiebot.com