



## APPENDIX B - COOKIE INFORMATION SERVICE SPECIFICATION

### Table of content

<b>1. ABOUT THE PRIVACY MANAGEMENT PLATFORM .....</b>	<b>2</b>
<b>2. APPLICABLE LEGISLATION .....</b>	<b>2</b>
<b>3. ACCESS TO THE COOKIE INFORMATION PLATFORM .....</b>	<b>2</b>
<b>4. PRIVACY WIDGETS .....</b>	<b>2</b>
<b>CONSENT POP-UP WIDGET .....</b>	<b>3</b>
<b>PRIVACY CONTROLS WIDGET.....</b>	<b>3</b>
<b>COOKIE POLICY WIDGET .....</b>	<b>3</b>
<b>5. WEBSITE SCANNER .....</b>	<b>3</b>
<b>AVAILABLE SCAN FREQUENCY AND DEPTHS .....</b>	<b>4</b>
<b>6. KNOWLEDGE BASE.....</b>	<b>4</b>
<b>AVAILABLE LANGUAGES: .....</b>	<b>5</b>
<b>7. COMPLIANCE DASHBOARD .....</b>	<b>5</b>
<b>8. DATA COLLECTION AND PROCESSING .....</b>	<b>5</b>
<b>CUSTOMER DATA.....</b>	<b>5</b>
<b>SERVICE DATA .....</b>	<b>5</b>
<b>PRIVACY AND STORAGE .....</b>	<b>7</b>
<b>9. SERVICE AND RESPONSE TIME .....</b>	<b>7</b>
<b>ONBOARDING SERVICE .....</b>	<b>7</b>
<b>SUPPORT PACKAGES .....</b>	<b>7</b>
<i>Free Support Package .....</i>	<i>7</i>
<i>Basic Support Package .....</i>	<i>8</i>
<i>Advanced Support Package.....</i>	<i>8</i>
<i>Enterprise Support Package .....</i>	<i>8</i>
<b>10. SECURITY AND SERVICE POLICY .....</b>	<b>9</b>



## **1. ABOUT THE PRIVACY MANAGEMENT PLATFORM**

Cookie Information offers a Privacy Management Platform that enables clients to meet requirements defined by a range of different cookie and data protection legislation, including but not limited to the (EU) General Data Protection Regulation (GDPR), (EU) ePrivacy directive and the California Consumer Privacy Act (CCPA).

The Privacy Management Platform consists of a range of technical services that provide clients with functionality which enables them to demonstrate compliance across their digital portfolios.

This document describes Cookie Information's services and how you as a client can benefit from using the Privacy Management Platform.

## **2. APPLICABLE LEGISLATION**

The legal landscape for data protection/privacy regulations changes frequently. At this time, our services can facilitate compliance with the following legislations:

- 1) GDPR: The General Data Protection Regulation 2016/679 is an EU regulation on data protection and privacy in the European Union.
- 2) ePrivacy directive: Directive on Privacy and Electronic Communications is an EU directive on data protection and privacy in the electronic communications sector.
  - The ePrivacy directive is locally implemented in each EU member state and requirements may vary in each country.
  - The ePrivacy directive is to be replaced by the ePrivacy Regulation(Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC), however negotiations on a final draft of the regulation have not been successful as of yet.
- 3) CCPA: The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States

In line with regulations and interpretations of such regulations continuously evolving, the range of applicable legislations will be extended.

## **3. ACCESS TO THE COOKIE INFORMATION PLATFORM**

The Cookie Information Platform is accessed through web interfaces including but not limited to [app.cookieinformation.com](http://app.cookieinformation.com), [templates.cookieinformation.com](http://templates.cookieinformation.com) and [support.cookieinformation.com](http://support.cookieinformation.com).

Clients can access their own account via [app.cookieinformation.com](http://app.cookieinformation.com) with the user credential created when creating the account. It is possible to add more users to one account.

## **4. PRIVACY WIDGETS**

The Privacy Management Platform contains three different Privacy Widgets that can be added to the client's website providing technical functionality that allows the client to demonstrate compliance with the applicable legislation.



The Privacy Widgets will mainly facilitate compliance within three areas:

- Valid consent in accordance with the **GDPR** ("Consent")
- Valid consent in accordance with the **ePrivacy directive** ("Consent")
- The right to object to the sale of personal information in accordance with **CCPA**

Below is a description of each Privacy Widget.

### **Consent Pop-up Widget**

The Consent Pop-up Widget allows the client to collect Consents in accordance with the **GDPR** and **ePrivacy directive** or objections in accordance with the **CCPA**.

The Consent Pop-up can be configured to include all necessary elements and information to constitute a valid (GDPR and ePrivacy) consent or the right to object (CCPA).

The Consent Pop-up will be displayed on the client website and consents will be renewed after a configurable period of time. As a default, the system will renew consents after 1 year, if a full consent for all purposes was collected and 14 days if a partial or no consent was collected. Extraordinary Consent pop-up display can be enabled from within the platform.

The Consent Pop-up Widget contains a ready to use Cookie Control SDK - Software Development Kit created in JavaScript that allows clients to load and/or block cookie setting tags/scripts. The use of the Cookie Control SDK allows clients to comply with prior and specific consent requirements, by blocking cookies and data processing before consent. The Cookie Control SDK can be deployed via the source code, tag management systems or by using CMS plugin.

The Consent pop-up widget is deployed through the website's <head> section.

### **Privacy Controls Widget**

The Privacy Controls Widget provides the client with the ability to meet the requirement for specific consent by allowing the end-user to consent to cookies with different purposes.

By default, the purposes are:

- Functional
- Statistics
- Marketing

Privacy Controls can be deployed on the content of the website and via the Consent Pop-up.

### **Cookie Policy Widget**

The Cookie Policy Widget provides the client with the ability to display all the relevant information necessary in order for a consent to be considered valid.

By enabling the client to display consent- and privacy policy / cookie policy texts based on frequent scans of their websites (see below), the cookie policy widget ensures that the consent- and privacy policy / cookie policy texts are always updated.

Privacy Controls can be deployed on the content of the website and via the Consent Pop-up.

## **5. WEBSITE SCANNER**

The Website Scanner is the main point of data discovery of the service. The Website Scanner enters the specified domains and follows the URL-structure of the domains to a

configurable depth. While scanning the domain the website scanner documents which cookies the website and all of its plug-ins are placing on end-users' devices together with a reference to where on the domain the cookies were found. The website scanner will scan the domain with a frequency configured by the client.

The result from the website scan will be enriched with data from the **Cookie Knowledge Base** (see below) and made accessible via the **Privacy Widgets** and in the **Compliance Dashboard** (see below).

Available scan frequency and depths

Monthly:

Scan every 30<sup>th</sup> day to a depth of 15.000 URLs

Scan every 30<sup>th</sup> day to a depth of 5.000 URLs

Scan every 30<sup>th</sup> day to a depth of 500 URLs

Weekly [recommended]

Scan every 7<sup>th</sup> day to a depth of 15.000 URLs

Scan every 7<sup>th</sup> day to a depth of 5.000 URLs

Scan every 7<sup>th</sup> day to a depth of 500 URLs

Daily

Scan every day to a depth of 15.000 URLs

Scan every day to a depth of 5.000 URLs

Scan every day to a depth of 500 URLs

## 6. Knowledge Base

Cookie Information has developed a **Knowledge Base** which contains ready-to-use consent- and privacy policy/cookie policy texts that are matched with the results from the **Website Scanner** and made accessible via the **Privacy Widgets** and in the **Compliance Dashboard**.

**Below you can see the data types and available languages**

Data Type	Description
Purposes	Overall purpose for which the client sets cookies and collects data
Purpose Descriptions	A detailed description of the purposes for which the client sets cookies and collects data
Service Provider	Name of the legal entity that operates the service
Service specification	A description of the service
Service privacy policy	A link to the service privacy policy
Role	Description of the role the service provider has, i.e. Data processor, Data Controller or Joined Data Controller
Cookie domain	The technical domain from which the cookie is read and placed
Cookie name	The technical name of the cookie
Cookie description	A description of what functionality the cookie is used for
Expiry	The expiry of the cookie in a readable format.
Cookie Policy Text	A cookie policy text

The Knowledge Base allows the client to access templates to consent texts in over 40 languages.

**Available languages:**

Albanian	Hindi	Portuguese
Arabic	Icelandic	Romanian
Bulgarian	Indonesian	Russian
Catalan	Irish	Serbian
Chinese	Italian	Sinhala
Croatian	Japanese	Slovak
Czech	Korean	Slovene
Danish	Latvian	Spanish
Dutch	Lithuanian	Swedish
English	Malay	Tamil
Estonian	Modern Greek	Thai
Finnish	Modern Hebrew	Turkish
French	Norwegian Bokmål	Ukrainian
German	Polish	Vietnamese

## 7. COMPLIANCE DASHBOARD

The Compliance Dashboard allows the client to monitor compliance across their domain portfolio.

Via the Compliance Dashboard the client can access reports showing GDPR & ePrivacy breaches including data retention, data transfer to 3<sup>rd</sup> countries and data processor/controller on the websites.

Service data such as enriched scan data from the website scanner and granulated consent reporting can be exported from the Compliance Dashboard

## 8. DATA COLLECTION AND PROCESSING

By using the service Cookie Information will start to collect and process data that can be described in two categories:

### Customer data

This is data provided by the Customer to Cookie Information to enable provision of the Services, which may include domain names in the websites where the Customer implements the Services

and:

- Domain URLs
- Test domain URLs
- Email addresses for employees that have access to the services

### Service data

Meaning the data collected and generated by Cookie Information, such as

- the configuration of content and the appearance of privacy widgets,



- scan data from Customer's use of the website scanner
- data generated by End Users browsing Customer's website(s) using the Service, including End User consents.

When an End User provides consent from the client websites, the following data is automatically logged by Cookie Information and made accessible to the client:

Data type	Description	Example data
Timestamp	Date and time of consent	March 7th, 2020, 10:35:20.278
Consent Solution	The consent solution from which the consent was sent	Cookieinformation.com
Consent Domain	The domain from which the consent was sent	app.cookieinformation.com
Consent url	The url from which the consent was sent	app.cookieinformation.com/createnew/
Consents Approved	The end user's consent state, which serves as proof of consent	cookie_cat_necessary, cookie_cat_functional, cookie_cat_statistic, cookie_cat_unclassified
Consents Denied	The end user's consent state, which serves as proof of consent	cookie_cat_marketing,
Consent Solution id	Id of the consent solution	7757d56b-6414-4328-8d6c-063d65b8468e
User Agent	User Agent of the End User's Browser	Mozilla/5.0 (iPhone; CPU iPhone OS 13_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.5 Mobile/15E148 Safari/604.1
Consent ID	A technically necessary anonymous, random value to separate and document the consent	99535183-294f-4305-919d-d16e13610b51

This data is also placed in a first-party cookie in an encrypted format, with an expiry of 12 months upon receiving a full consent for all purposes, and 14 days if not. Both expiries are configurable.

If you enable the "Shared Consent" feature to enable consent to across multiple domains using a single End User consent, the Service also stores:

- One third party cookie named "CookieInformationConsent\_encodedclientid" with the same content as the 1. Party cookie described "CookieInformationConsent" in encoded format, set from the domain cookieinformation.com.
- One third party cookie named "CookieInformationConfig" with the following data in an encoded format:
  - Internal id to identify the consent solution configuration
  - The domains included in the consent solutions configuration



## **Privacy and storage**

All service data is stored for a period of up to 5 years after the expiry of the end-user's consent.

None of the Service Data is considered Personal Data as defined in the GDPR. Therefore, processing of the Service Data does not fall under the GDPR or any other legislation relating to the processing of personal data. Consequently, Cookie Information does not act as a data processor when providing the Services.

## **9. SERVICE AND RESPONSE TIME**

Subscriptions purchased via the Cookie Information platform available on [cookieinformation.com](https://cookieinformation.com) and [app.cookieinformation.com](https://app.cookieinformation.com) include support with a response time of less than 1 business day for critical support requests and 8 business days for non-critical support requests.

Critical support covers malfunctioning of the service on the client live website.

Additional Support Packages can be purchased.

Any problem where the root cause is due to any actions carried out by the client or a 3rd party not authorized by Cookie Information to do so (i.e. the client's partner e.g. web agency) is not considered to fall under critical support.

Any requests for error correction or support shall be submitted via email to [support@cookieinformation.com](mailto:support@cookieinformation.com). or via our local phone numbers which can be found on [cookieinformation.com](https://cookieinformation.com).

## **Onboarding Service**

The Cookie Information team will perform remote onboarding services on a fair usage basis for up to two (2) months after this agreement has been entered into by the Client. If the clients' needs exceeds the fair usage limitation Cookie Information will inform the Customer before invoicing applies.

## **Support Packages**

Free Support Package

- Chat/Email/Phone Support
- Technical Support Documentation
- Annual Status Meeting



#### Basic Support Package

- Chat/Email/Phone Support
- Technical Support Documentation
- 2 x Support and Review meetings p.a.<sup>1</sup>
- Dedicated Account Manager

#### Advanced Support Package

- Chat/Email/Phone Support
- Technical Support Documentation
- 6 x Support and Review meetings p.a.<sup>1</sup>
- Dedicated Account Manager
- Prioritized Technical Support
- Quarterly Compliance Check
- Personalized Support during DPA audit

#### Enterprise Support Package

- Chat/Email/Phone Support
- Technical Support Documentation
- 12 x Support and Review meetings p.a.<sup>1</sup>
- Dedicated Account Manager
- Prioritized Technical Support
- Quarterly Compliance Check
- Quarterly Cookie Classification
- Personalized Support during DPA audit

---

<sup>1</sup> 'Support and Review Meetings' are:

- Regular Status Meetings
- General Support Meetings
- Technical Implementation Meetings
- Platform Tour & Training



## 10. SECURITY AND SERVICE POLICY

Cookie Information offers a SaaS solution and use a Cloud supplier to host the services and related components and content provided online. The responsibility split between Cookie Information and our Cloud Supplier is shown below, and more information can be found in the following sections.

### Infrastructure

The infrastructure and associated security are provided by Microsoft. All data is hosted on Microsoft's data centre located in the Netherlands. Azure cloud has comprehensive compliance coverage: ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP, and ENS. - for more information see <https://azure.microsoft.com/en-us/overview/trusted-cloud/>.

The hosting service is provided in a safe 'limited access' environment. There is a continuous supply of power, climate control, and the data centre is protected against natural disasters. In the unlikely event that a situation occurs where it will be reasonable to question the data centre's

security the customer can request an independent 3rd party to examine the security systems at the customers' cost if the customer compensates Cookie Information for all costs which Cookie Information may experience as a direct consequence hereof including costs to be paid to the data centre for access. Access to the data centres' infrastructure is decided in full by the data centre.

Access to the data centre is limited to specific employees and selected production/support specialists who are only allowed access to perform planned maintenance and upgrades. Cookie Information reserves the right to change the data centre and/or other suppliers without obtaining prior consent from the customer, provided that the new data centre or new other supplier provides the Customer with at least the same service level and security as the current and provided that the new data centre is located within the EU.

### Identity and access management

Cookie Information uses an effective implementation that includes configuration of administrative services, establishing and configuration of user identities, and implementation of service- and role-based access controls. Furthermore, we are monitoring, controlling and logging of both users and end-points.

### Data security

Data at-rest is encrypted and decrypted using 256-bit [AES encryption](#), one of the strongest block ciphers available, and is FIPS 140-2 compliant.

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Customer / Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Legend: ■ Cloud Customer ■ Cloud Provider



The web-based application uses secure HTTP (TLS/HTTPS) to protect data transmissions over the internet. Virtual Private Network (VPN) technology is used to protect other transmissions such as access to the active database.

### **Backup**

Cookie Information provides web servers, application servers, database servers and physical storage in which data is kept in a redundant multi-drive configuration which gives mirrored storage and the required software to host the solution and associated services. Additionally, all critical data is backed up daily to an encrypted, geo-redundant storage.

### **Availability**

Cookie Information will provide the required infrastructure to ensure that the solution is available via the internet 99,5% of the time measured per month from the go-live date. The service takes advantage of the wide opportunities in Azure to ensure high availability including full redundancy for all components and services, load balancing, automatic scaling of capacity, self-healing components, and a traffic manager to automatic geographic failover in case of an emergency at the data centre level.

All server, middleware and application components are being monitored 24/7 by Cookie Information.