iubenda

Online Compliance Handbook for Successful Agencies

How to make your clients' sites and apps compliant and avoid liabilities

BEFORE WE START

In this handbook you will find an **overview of the main requirements to comply with** in order to make a site or app compliant as well as some **recommendations to help you manage your client relationship and avoid liabilities**.

Please note that the information provided in the following pages is for general informational purposes only and should not be construed as, and should not be relied upon for legal advice in any circumstance or situation. An attorney should always be contacted for advice on specific legal issues.

TABLE OF CONTENTS

PROVIDE YOUR CLIENTS' SITES/APPS WITH A **PRIVACY AND COOKIE POLICY**

The law requires every site/app which collects personal data to inform users via an up-to-date privacy policy (and cookie policy where applicable).

These documents must always accurately reflect the data processing activities carried out through the site/app. The disclosures made in these policies must also mention any third-parties with whom the data may be shared, and link to the respective policies of those third-parties.

MAIN REQUIREMENTS

PRIVACY POLICY

Needed in almost every scenario where personal data is being processed.
Note: even IP addresses can be considered personal data, and “processing” can simply mean “interacting with”.

This document should be easily accessible from all pages and **available in all the languages** of the site/app.

MAIN REQUIREMENTS

PRIVACY POLICY

The privacy policy must contain:

- the identification details of the **data controller**;
- description of the **data** being collected;
- the **methods** and **purposes** of the processing;
- the **legal basis** of the processing (e.g. consent);
- the **rights of the interested parties**;
- any **third-parties** with whom the data is shared (including third-party tools used);
- information on the possible **transfer of data** abroad;
- the **rights** of the user;
- the description of the process for the notification of **changes or updates** to the policy and its **effective date**;
- if applicable, information on how **sensitive health data** is secured.

MAIN REQUIREMENTS

COOKIE POLICY

Needed if you run cookies – which is most likely the case. It's mandatory if you have, or could have, European users.

This document should be easily accessible from all pages and **available in all the languages** of the site/app.

MAIN REQUIREMENTS

COOKIE POLICY

A basic cookie policy, at minimum, must contain:

- an up-to-date description of the **cookies used by the site** and their respective **purposes** (eg. measurement, ad personalization etc.);
- references to any **third-parties** which install or could install cookies through the site (e.g. facebook widgets, Google Ads etc.);
- the links to any relevant **policies** and/or **opt-out forms** of the aforementioned third-parties;
- instructions on how users may **deny or withdraw** their consent to the processing.

COLLECT PRIOR CONSENT FROM EU USERS BEFORE RUNNING COOKIE SCRIPTS TO **COMPLY WITH COOKIE LAW**

The Cookie Law in the EU requires that informed user-consent must be collected before the installation of non-exempt cookies.

It's important to note, however, that the use of cookie-management systems which are not optimized for business activities can come with the risk of significant negative impacts on site performance and, ultimately, business revenue.

MAIN REQUIREMENTS

COOKIE BANNER

Needed if you run non-technical cookies – which is most likely the case.
It's mandatory if your clients have, or could have, European users.

The cookie notice must:

- be visible upon **initial access** to the site;
- briefly **explain the purpose of the installation of cookies** that the site uses and clearly **state which action will signify consent**;
- be **sufficiently conspicuous** so as to make it noticeable;
- **link to a cookie policy** with details of cookie purpose, usage, and related third-party activity.

MAIN REQUIREMENTS

PRIOR BLOCKING OF COOKIES, USER-CONSENT AND PREFERENCES

Needed if you run non-technical cookies – which is most likely the case. It's mandatory if your clients have, or could have, European users.

All scripts that install or that could install **profiling cookies** must first be **blocked** and reactivated only after consent. The consent may also be obtained with **continued use of the site** (e.g. a click on a page link) in many cases.

User-preferences can be "remembered" for a set period so that return users are not asked again and again for consent once they've provided it.

SETUP A NOTICE OF COLLECTION AND A DNSMPI LINK TO **COMPLY WITH CCPA**

Under the CCPA, a consumer has the right, at any time, to tell a business which sells their personal information to third-parties, that they must stop selling such personal information.

This process should be facilitated via a “Do Not Sell My Personal Information” (DNSMPI) link on your clients’ websites or privacy notices.

Note that a sale can be defined as any arrangement between a business and a third-party or other business, that allows the business to receive some value (monetary or not) in exchange for the personal information of consumers.

MAIN REQUIREMENTS

NOTICE OF COLLECTION, "DO NOT SELL MY PERSONAL INFORMATION" LINK (DNSMPI), OPT-OUT SIGNAL

CCPA requires you to inform California users that their data might be collected and of their right to opt-out.

Display a "Do Not Sell My Personal Information" (DNSMPI) link in a notice of collection on the user's first visit and elsewhere on your clients' sites/apps thereby supporting opt-out from sale.

KEEP TRACK OF USER CONSENT AND **DOCUMENT OPT-INS AND OPT-OUTS**

In order to make your clients' web forms fully GDPR compliant, you must store proof of consent so as to be able to demonstrate that a valid consent was collected.

Under the CCPA, it's also prudent to keep records of opt-out details.

MAIN REQUIREMENTS

CONSENT ACCORDING TO GDPR

To process user data, the data controller must collect **freely given, specific, and informed consent**. The consent should be given via an affirmative ("opt-in") action on the part of the user. A common scenario involving this type of active consent is where users click a **checkbox** such as those used in **site registration** or **newsletter forms**, to indicate consent. **Opt-out mechanisms such as pre-selected checkboxes are forbidden.**

Laws such as the GDPR also places the burden of proof on the data controller. This means that **your clients are explicitly required to demonstrate, unambiguously, that valid consent has been collected.**

MAIN REQUIREMENTS

OPT-OUT RECORDS ACCORDING TO CCPA

The CCPA mandates that opted-out users may not be contacted for a minimum of 12 months after the request.

For this reason it's prudent to keep **records of opt-out details** such as the particular user, the date, and sub-contractors to be notified in the case of requests.

PROVIDE YOUR CLIENTS' SITES/APPS WITH A **TERMS AND CONDITIONS** DOCUMENT

Terms and Conditions set the rules for how users may interact with your clients' products, services or content and protect you and your clients from potential liabilities and service abuses.

One common scenario in which terms are absolutely vital is in the case of e-commerce — where customers must be made aware of the business owner's rules relating to return, withdrawal or cancellation policies.

MAIN ELEMENTS

TERMS & CONDITIONS

Though not always legally required, Terms & Conditions (also called ToS - Terms of Service, Terms of Use or EULA - End User License Agreement) **set the way in which a product, service or content may be used**, in a legally binding way. They are crucial for protecting content from a copyright perspective as well as for **protecting you and your clients from potential liabilities**.

They typically contain **copyright** clauses, **disclaimers**, **terms of sale**, they set **governing law**, list mandatory **consumer protection clauses**, and more.

RECOMMENDATIONS FOR DISCUSSING COMPLIANCE WITH YOUR CLIENTS

Inform your clients

Inform your clients about their obligations.
You can also offer them related iubenda compliance solutions.

Avoid liabilities

Be sure to include a disclaimer in the supply contract that the client is asked to sign, to ensure that you are exempted from any legal liability.

Download our resources to inform your clients and avoid liabilities.

Get the resources

https://iubenda.link/assets

iubenda

ABOUT IUBENDA

iubenda is the most simple, complete and professional way to comply with international regulations & privacy laws

iubenda adopts a comprehensive approach to legal compliance by offering a complete set of SaaS solutions to automatically draft and continuously update Privacy and Cookie Policies as well as Terms and Conditions, and to comply with GDPR and Cookie Law in Europe, CCPA in California and more.

Over 70,000 clients in more than 100 countries rely on our software solutions and direct assistance for online compliance

A selection of our clients:

jobtome ahrefs ShopFully stickermule

wsmv Portland Press Herald THE SPECTATOR

www.iubenda.com - business@iubenda.com