

Q&A: online advertising in Cyprus

Antoniou McCollum & Co LLC

[View In Analytics](#)

Cyprus | September 29 2023



This is an extract from Lexology Panoramic
Directly compare laws and regulations between jurisdictions here

Advertising

Regulation

What rules govern online advertising?

An online advertisement to Cypriot users must:

- be clearly identifiable as a commercial communication; and
- clearly identify the person on whose behalf the commercial communication is sent.

If the communication is unsolicited, it must be clearly and unambiguously identifiable as such, as soon it is received.

Rules concerning misleading and aggressive advertising also apply to online advertising to consumers in Cyprus.

Targeted advertising and online behavioural advertising

What rules govern targeted advertising and online behavioural advertising? Are any particular notices or consents required?

The framework on targeted advertising and online behavioural advertising in Cyprus applies to cookies, bots and any technology that collects, has access to, shares, processes or monitors one or more identifiers or technical equipment of a subscriber or user.

Automated individual decision-making, including profiling is governed by Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation (GDPR)). Under the GDPR, a data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them unless such decision is necessary for entering into, or performance of, a contract between the data subject and a data controller or unless such decision is based on the data subject's explicit consent. However, the controller must implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests. In any event, the data subject must have the right to object at any time, to the processing of personal data for profiling purposes.

Information on cookies must be 'clear and comprehensive'. The user must clearly provide their consent to the use of cookies by a website. Mere information that a website uses cookies and that users automatically accept cookies by browsing the website, does not meet the statutory requirements. Consent must be given in the form of

an affirmative action. In particular, the Commissioner for the Protection of Personal Data (the DPC) highlights in the DPC Guidance that consent cannot be implied from use of the website and indicates that it must be clear that a user has actively engaged with a cookie banner to unambiguously consent to use of cookies.

Where cookie banners are used, they must not indirectly force a user to accept all cookie; both accept and reject options should be clearly provided on the banner. Also, due to the voluntary nature of consent, where the user is not able to access the service or website in the absence of express consent to cookies, this would mean that the website does not present the user with a genuine choice, therefore it cannot be deemed valid consent as it is not freely given.

Nevertheless, the requirement of the user's consent for the use of cookies is not required:

- for technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network ('communications exemption'); or
- as strictly necessary to provide an information society service explicitly requested by the subscriber or user ('strictly necessary exemption').

The validity period of consent would depend on various factors, including whether the purposes of processing have changed and the period for which the personal data will be stored that the controller shall be determined and communicated to the user.

While the framework does not provide for a specific retention period for cookies, if the collected data constitutes personal data, the provisions of the GDPR must be complied with and such data must not be kept for longer than necessary for the purposes for which the personal data are processed.

'Dark patterns' are also relevant to targeted advertising and online behavioural advertising. Dark patterns, defined by the European Data Protection Board as interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data. Dark patterns aim to influence users' behaviour and can hinder their ability to effectively protect their personal data and make conscious choices. The data protection principles applicable to dark patterns are those set out in article 5 the GDPR.

Misleading advertising

Are there rules against misleading online advertising?

Misleading and aggressive commercial practices carried out online by any consumer-facing business would constitute unfair commercial practices, which are prohibited.

Advertisers should make sure that any advertisement as well as its overall presentation and any statements used for commercial reasons do not include any false information and all statements used in the commercial communication are true and verified. The advertisement should also not omit any essential information that the consumer would need, to make an informed decision on the transaction.

Advertisers should keep a record where possible of proof of any market surveys carried out to determine the average consumers views and expectations as to the specific product advertised. Furthermore, any reference to the product's price should be supported by records of price calculations leading to the advertised price. Generally, any competitive claim must be substantiated with relevant evidence. These rules apply to all advertising directed towards consumers. At the same time, specific rules apply to certain industries – for example, electronic communications.

Restrictions

Are there any digital products or services that may not be advertised online?

Audiovisual commercial communications displayed online by media service providers and video-sharing platform providers that fall under the jurisdiction of Cyprus are subject to a wide range of restrictions, whether they concern digital or other products. Several restrictions apply for the protection of minors, such as the prohibition of advertising that may harm minors. Additional restrictions are applicable to prevent any advertising that includes or promotes discrimination based on sex, racial or ethnic origin, nationality, religion or belief, disability, age or sexual orientation, encourages behaviour prejudicial to health or safety, encourages behaviour grossly prejudicial to the protection of the environment.

Regarding specific products, it is prohibited to advertise cigarettes and other tobacco products, electronic cigarettes and medicinal products and medical treatments available in Cyprus on prescription. Alcoholic beverages advertisements must not be aimed specifically at minors and shall not encourage immoderate consumption of such beverages.

Online publishing

Hosting liability

What is the liability of internet service providers, telecommunications providers and other parties that merely host and display the content written or published by third parties? How can these providers minimise their liability?

Where a content provider or a party that is merely hosting content has no actual knowledge of illegal content and is not aware of facts or circumstances from which such activity is apparent, the safe harbour defence is available and the content provider or hosting party may be exempt from liability. Under Cyprus law internet service providers (ISPs) are exempt from liability for content that is hosted on their sites. Liability may occur in the event the host has actual knowledge or awareness of facts or circumstances in which illegal content is apparent. Once such knowledge or awareness is obtained; the host provider must meet takedown or shutdown obligations.

The safe harbour defence may not be strong when invoked in respect of content over which the ISP has editorial control. A case-by-case assessment of the precise facts and circumstances is necessary to determine whether the safe harbour defence can successfully be invoked by any party.

Antoniou McCollum & Co LLC - Anastasios A Antoniou, Ifigenia Iacovou and Orestis Anastasiades

Powered by

LEXOLOGY.