Cookie Policy

Use of cookies by Evolve Hospitality t/a Enhance Catering Recruitment.

Cookies are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site.

Most web browsers allow some control of most cookies through the browser settings. To find out more about cookies, including how to see what cookies have been set and how to manage and delete them, visit www.aboutcookies.org or www.allaboutcookies.org.

To opt out of being tracked by Google Analytics across all websites visit: http://tools.google.com/dlpage/gaoptout.

Cookie categories

The type of cookie used on this website can be put into 1 of 4 categories, based on the International Chamber of Commerce guide to cookie categories: Strictly Necessary, Performance, Functionality & Profile and Targeting.

SECTION TWO

The Law with respect to Cookies after the application of the General Data Protection Directive Introduction

Cookies are only referenced once in the GDPR:

'Recital 30: Natural Persons may be associated with online identities…such as internet protocol addresses, cookie identifiers or other identifiers…This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.'

In plain English this means; if you as an organisation uses cookies to uniquely identify a device or the person using that device, that's now treated as Personal Data under the GDPR.

Not all cookies are used in a way that could identify users, but the majority are. This means cookies used for analytics, advertising and functional services such as surveys and chat tools are at risk of non-compliance under the GDPR.

Why are Cookies potentially non-compliant under the GDPR?

Cookies often contain pseudonymous identifiers (e.g. strings of numbers or letters) to give them uniqueness. Under GDPR it is this uniqueness that qualifies them as personal data. So, any cookie that is capable of identifying an individual, or treating them as unique without explicitly identifying them means a business is processing Personal Data.

In order to process the personal data of EU citizens, GDPR now requires you to gain definite and provable consent. It is this which puts the use of the usual type of cookies at the risk of being non- compliant.

What's changing with consent?

Gaining valid consent is one of the crucial changes that the GDPR is making to the collection and processing of Personal Data. However, since it's such a huge topic we'll keep our focus to consent as it applies to the use of cookies:

Implied Consent is no longer sufficient: Previously, most businesses have relied on the idea of 'implied consent'. I.e. Visitors have offered an email address or phone number, they have visited your website and taken some kind of action. Under GDPR this is no longer enough. Consent must be given via an affirmative action, such as clicking an opt-in box or setting preferences. Crucially, opt-in to one type of contact does not qualify your business to assume consent for all types of contact.

I**t must be as easy to withdraw consent**
Even after you have gained consent to process an individual's personal data it must be easy for them to change their preference. If you ask for consent via and opt-in-box, for example, and opt-out must be equally visible.

"**Soft Opt-In" is not sufficient:** We are all familiar with the 'by using this site, you accept cookies' message that pops up on websites. We all probably use just such a message on our own websites.

However, under the GDPR if there's no valid consent option it does not count as consent at all. You must make it possible to accept and reject cookies.

How can I continue to use cookies under the GDPR?

Using cookies in the established way is going to become increasingly hard. Cookies are not banned under the GDPR. However, if you can't prove consent on an individual basis you're at risk of non- compliance.

If you can prove that your business has a lawful ground to collect and process the data in question then you can continue to do so. However, since most businesses rely on implied or opt-out consent it will be increasingly hard to prove lawful consent under the strengthened requirements of GDPR.

Additionally, The Privacy and Electronic Communications Regulations (PECR), aka the 'cookie law' is being updated and brought in line with the GDPR. Tightening this up will mean more restrictions on how and when data analytics tools like cookies can be used.

The GDPR, Cookie Consent and Consumer/User Centric Privacy

GDPR Relationship with the ePrivacy Directive

Without going into too much detail, the GDPR is an over-arching piece of legislation dealing with all aspects of the processing of personal information. The ePrivacy Directive has a tighter focus on communications and internet services, which 'particularises' the data protection rules. Meaning it relies on the general rules of the GDPR and overlays these with more specific requirements within its own remit.

One of the issues being looked at for the reform of ePrivacy is to turn this also into a Regulation that is directly applicable rather than relying on changes to individual Member State laws. GDPR on Cookies

As mentioned before Cookies are mentioned once in the GDPR, in Recital 30:

Natural persons may be associated with online identifiers…such as internet protocol addresses, cookie identifiers or other identifiers…. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

What this essentially tells us it that cookies, where they are used to uniquely identify the device, or in combination with other data, the individual associated with or using the device, should be treated as personal data. This position is also reinforced by Recital 26, which states that where data can reasonably be used, either alone or in conjunction with other data to single out an individual or otherwise identify them indirectly, then it is personal data.

Use of pseudonymous identifiers (like strings of numbers or letters),which is what cookies typically contain to give them uniqueness, still makes them personal data.

So under the GDPR, any cookie or other identifier, uniquely attributed to a device and therefore capable of identifying an individual, or treating them as unique even without identifying them, is personal data.

This will certainly cover almost all advertising/targeting cookies; lots of web analytics cookies; and quite a few functional services like survey and chat tools that record user ids in cookies.
GDPR on Consent

Under existing rules, cookies that are not strictly necessary to require consent, and the definition of consent and the requirements associated with it, changes under the GDPR. To really understand what this means for cookies, have a look at Recital 32 [emphasis is mine]:

*Consent should be given by a **clear affirmative act** establishing a freely given, specific, informed and **unambiguous indication** of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or **inactivity should not therefore constitute consent**. Consent should cover all processing activities carried out for the same purpose or purposes. **When the processing has multiple purposes, consent should be given for all of them**. If the data subject's consent is to be given following a request by electronic means, the **request must be clear, concise and not unnecessarily disruptive** to the use of the service for which it is provided.*

This suggests that consent for cookies will need to become much more clearly opt-in, or at the very least soft opt-in, so that landing on a site for the first time cookies have to be blocked until the user takes some action that they are clear will result in cookies being set.

A site that sets cookies for different purposes will also need to obtain consent for each separate purpose, however this might be a challenge considering that the process should not be too disruptive. Balancing this may be tricky, but there is another condition on consent, which might help that we can find in Article 7(3):

The data subject shall have the right to withdraw his or her consent at any time. …. It shall be as easy to withdraw as to give consent.

Taken together, it would seem reasonable that consent will be valid, and avoid being unnecessarily disruptive, if the user can be presented with an initial notice and simple choice, yet will always be able to modify their choice in a more granular way, based on the different types of cookie processing taking place, if they choose to.

In short, the model of a dismissible notice, coupled with an always available control panel with granular controls, would seem perfectly suited to a GDPR influenced model for cookie consent.

In addition, many websites are beginning to adopt a facility where the web-page content is covered by a grey-coloured filtered rendering the background (original web-page text) almost completely obscured. It is only when affirmative consent to Cookie use is obtained that the Cookie Banner disappears and the web-page reappears with clarity. Please see Section Three below as this position will change once the ePrivacy Regulation is in force.

<u>Going Beyond Consent?</u>

The only legal means for setting non-exempted cookies in the ePrivacy Directive is consent. However, having established that cookies involve personal data, and knowing there is a desire to harmonise the two instruments, it seems likely that the next set of cookie rules will allow other means for setting cookies.

So we could see cookies being set based on performance of a contract, or the legal obligations of the site owner. This could reasonably be used for things like fraud detection and security, particularly around ecommerce processing. However, the most likely best candidate is probably the '**l***egitimate interests of the controller'*, which would potentially allow the website to set cookies without consent.

This is not quite a get out jail free card, and couldn't apply in the public sector, but it could be a viable option for certain types of cookie processing – especially things like first party web analytics.

There are however a couple of things to be aware of with legitimate interests. Article 6(4) sets out several conditions for using legitimate interests, and the site owner as data controller would need to make sure they have considered and documented their justification based on these conditions.

Article 4(b) in particular, which requires giving consideration of the relationship between controller and data subject, is likely to make legitimate interests difficult to use when third party cookies are involved, especially if this to do with profiling, as is the case in most types of targeted online advertising and marketing.

Legitimate interests also comes with it the right to object to the processing by the individual (Article 21). So even if this could be used to set some types of cookies without consent – it would still require the ability of the user to opt-out of such usage.

SECTION THREE

The Future of EU Cookie Compliance: the GDPR and the ePrivacy Directive Revision of "Cookie Law"

Introduction

The European Commission is preparing new rules to protect online privacy (it's Press Release is set out in the Appendix below). The rules are set out in the proposed Regulation on Privacy and Electronic Communications, which will accompany the wider reform of data protection laws under the General Data Protection Regulation. The proposals were issued at the start of 2017 and contain specific provisions on cookies, online marketing, and the use of content and metadata.

The Proposed Regulation

The European Commission issued a draft of the Regulation on 10th January 2017 to replace the existing ePrivacy Directive (adopted back in 2002). As *lex specialis*[1] it complements the general rules in the General Data Protection Regulation with specific rules applicable to the electronic communications sector.

The proposed Regulation has already attracted a good deal of interest. Both the Article 29 Working Party and the European Data Protection Supervisor issued opinions on it in April 2017. More recently, various committees in the European Parliament have issued views on the proposals, the most substantive of which is an assessment by the IViR Institute for Information Law for the Civil Liberty, Justice and Home Affairs' Committee ("LIBE Assessment"). This was released at the start of June 2017 and identifies the following four main issues:

- Cookie "tracking walls" should be prohibited, i.e. access to a website should not generally be conditional on accepting the use of tracking cookies.
- There should be stricter rules for Wi-Fi location tracking and similar device tracking.
- Browsers should have privacy settings enabled by default.
- There should be stricter rules on the use of content and metadata.

We consider these recommendations in further detail below.

The original proposal was for the Regulation to apply from May 2018, and thus coincide with the start date for the General Data Protection Regulation. However, it is highly likely this date will slip.

One of the major challenges is that proposed Regulation is tied to a wider reform of telecoms regulation (through the proposed Electronic Communications Code) and that reform is unlikely to be complete by May 2018 year. To avoid further delay, the LIBE Assessment suggests decoupling the proposed Regulation from these wider telecoms reforms.

1 **Lex specialis**, in legal theory and practice, is a doctrine relating to the interpretation of laws and can apply in both domestic and international law contexts. The doctrine states that if two laws govern the same factual situation, a law governing a specific subject matter (*lex specialis*) overrides a law governing only general matters (*lex generalis*).

The Key Changes With Respect To Cookie

Under the current ePrivacy Directive, website operators must obtain consent from users to the use of cookies unless the cookie is strictly necessary for the operation of the website or transmission of a communication. The proposed Regulation suggests a number of changes:

- Consent harder to obtain

Consent to the use of cookies must meet the same standard as set out in the General Data Protection Regulation. This means that there must be a clear affirmative action. This may mean existing practices, such as showing a website banner stating that continuing to use the website constitutes consent, may need to be revisited.

- Browser Fingerprinting

The rules on cookies will also apply to "browser fingerprinting", a process that seeks to uniquely identify users based on their browser configuration (without actually setting a cookie on that browser).

- Limited exception for analytics

There will be an exemption for website analytics, recognising that this is not an intrusive activity. However, it will only apply to analytics carried out by the website provider. It is not clear if third party analytic cookies, like Google Analytics, will benefit from this exemption.

- Browser Requirements

Browsers must contain cookie controls and users must choose those settings as part of the installation process. In theory, these settings could demonstrate consent to certain cookies, though there appears to be little appetite from regulators to accept browser settings as sufficient. This provision is also drafted in very broad terms and includes any software that permits electronic communications, potentially capturing a broad range of other devices, such as those part of the Internet of Things.

The current rules on cookies have not been universally popular. The Regulation itself suggests that users are "*overloaded with requests to provide consent*".

While these changes are only likely to increase this consent burden, the LIBE Assessment suggests they should go further and prohibit "tracking walls" – i.e. prevent websites from making access conditional on the acceptance of tracking cookies. It also suggests that browsers should be set to block tracking cookies by default.

Wi-Fi Tracking

The proposals contain new provisions addressing Wi-Fi and other types of device tracking. These technologies allow the location of a device to be monitored by recording details of the MAC address for that device (or similar) as it is carried about by its owner.

The proposed rules are liberal. Tracking is permitted so long as the information is collected to provide a connection (suggesting this is limited to genuine Wi-Fi services) and suitable notice and opt-out mechanisms are in place.

This has attracted fierce criticism. The Article 29 Working Party has "*grave concerns*" about this approach. The LIBE Assessment suggests tracking should only take place if the individual consents or the information is made anonymous.

Electronic Direct Marketing

The proposed Regulation contains a number of restrictions on electronic direct marketing to natural persons. This builds on the restrictions in the current ePrivacy Directive on marketing by email, SMS, fax and telephone. The key changes proposed to by the Regulation are:

- Online Marketing

The proposed Regulation will also apply to targeted online advertisements, for example website banners or in-App adverts. These advertisements require consent. While this feels like a significant change, in practice it is likely to be closely tied to the new rules on cookies set out above. Targeted advertising is likely to require the use of cookies which will require consent in any event.

- Consent harder to obtain

The general rule is that consent will be needed for electronic direct marketing and that consent must meet the standard as set out in the General Data Protection Regulation. However, there are two key exceptions:

(i) email marketing will still be allowed where there is an existing relationship under the similar products and services exemption; and

(ii) Member States can remove the requirement for consent for telephone marketing. In practice, the UK is likely to remove the need for consent but retain the Telephone Preference Services as a general means of opting out of such marketing.

- Telephone Marketing

The proposal suggests a caller must present identity of line or specific code or prefix indicating it is a marketing call.

These proposals are broadly similar to the existing rules in the ePrivacy Directive and so less controversial. However, the LIBE Assessments suggests greater clarity is needed in relation to online marketing (for example, whether that captures contextual online marketing as well as behavioural online marketing).

Electronic content and metadata

The most significant changes are to the rules on the use of content and metadata. The proposals contain strict restrictions on when this information can be used, as set out in the table below.

Electronic communications content	Electronic communications metadata
Use allowed: To provide a specific service to an end user with the end user's consent For other specific purposes with the consent of all end users (subject to privacy impact assessment and consultation with supervisory authority)	Use allowed: Needed for mandatory QoS obligations Necessary for billing, calculating interconnection payments, fraud or abusive use of electronic communications services For other specific purposes with the consent of the end user
In either case, use allowed: To achieve the transmission of the communication To ensure the security of the system and to	

detect faults • Where required by EU or national law	

These proposals have also proved controversial. Some industry bodies say they fail to reflect the fact that electronic communication providers are no longer passive conduits. Instead, they provide, and customers expect, a range of sophisticated services that need to access content and metadata (for example spam filtering, scheduling and AI assistant tools).

In contrast, the LIBE Assessment calls for greater controls. It suggests that content and metadata should only be used in more limited circumstances and that, outside these limited circumstances, consent from all end-users is required, i.e. the customer and the third party to the communication.

However, gaining consent from third parties would be a challenging proposition in practice.

Scope and Sanctions

The proposed Regulation will expand the scope of these rules. They will not just apply to traditional telecoms companies but also apply to OTT (over the top) providers, such as WhatsApp. Similarly, the proposals have an extra-territorial effect and apply to services provided to end-users and devices in the European Union, regardless of where the provider is based. If the provider is outside the European Union, they must appoint a representative within the European Union.

There will also be a step change in sanctions. Breach of the rules protecting user content and metadata will be subject to fines of €20m or 4% of annual worldwide turnover. Breach of the other provisions of the regulation can result in fines of €10m or 2% of annual worldwide turnover. These sanctions match those in the General Data Protection Regulation and are intended to make privacy a board-level issue.

APPENDIX

European Commission Press Release

Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions

Brussels, 10 January 2017

The Commission is proposing new legislation to ensure stronger privacy in electronic communications, while opening up new business opportunities.

The measures presented today aim to update current rules, extending their scope to all electronic communication providers. They also aim to create new possibilities to process communication data and reinforce trust and security in the Digital Single Market – a key objective of the Digital Single Market strategy. At the same time, the proposal aligns the rules for electronic communications with the new world-class standards of the EU's General Data Protection Regulation. The Commission is also proposing new rules to ensure that when personal data are handled by EU institutions and bodies privacy is protected in the same way as it is in Member States under the General Data Protection Regulation, as well as setting out a strategic approach to the issues concerning international transfers of personal data.

First Vice-President Timmermans said: *"Our proposals will complete the EU data protection framework. They will ensure that the privacy of electronic communications is protected by up to date and effective rules, and that European institutions will apply the same high standards that we expect from our Member States."*

Andrus Ansip, Vice-President for the Digital Single Market said: *"Our proposals will deliver the trust in the Digital Single Market that people expect. I want to ensure confidentiality of electronic communications and privacy. Our draft ePrivacy Regulation strikes the right balance: it provides a high level of protection for consumers, while allowing businesses to innovate."*

Věra Jourová, Commissioner for Justice, Consumers and Gender Equality said: *"The European data protection legislation adopted last year sets high standards for the benefit of both EU citizens and companies. Today we are also setting out our strategy to facilitate international data exchanges in the global digital economy and promote high data protection standards worldwide."*

Better online protection and new business opportunities

The proposed Regulation on Privacy and Electronic Communications will increase the protection of people's private life and open up new opportunities for business:

- **New players:** 92% of Europeans say it is important that their emails and online messages remain confidential. However, the current ePrivacy Directive only applies to traditional telecoms operators. Privacy rules will now also cover new providers of electronic communications services, such as WhatsApp, Facebook Messenger, Skype, Gmail, iMessage, or Viber.

- **Stronger rules:** By updating the current Directive with a directly applicable Regulation, all people and businesses in the EU will enjoy the same level of protection for their electronic communications. Businesses will also benefit from one single set of rules across the EU.

- **Communications content and metadata:** Privacy will be guaranteed for both content and metadata derived from electronic communications (e.g. time of a call and location). Both have a high privacy component and, under the proposed rules, will need to be anonymised or deleted if users have not given their consent, unless the data is required for instance for billing purposes.

- **New business opportunities:** Once consent is given for communications data, both content and/or metadata, to be processed, traditional telecoms operators will have more opportunities to use data and provide additional services. For example, they could produce heat maps indicating the presence of individuals to help public authorities and transport companies when developing new infrastructure projects.

- **Simpler rules on cookies:** The so called "cookie provision", which has resulted in an overload of consent requests for internet users, will be streamlined. New rules will allow users to be more in control of their settings, providing an easy way to accept or refuse the tracking of cookies and other identifiers in case of privacy risks. The proposal clarifies that no consent is needed for non-privacy intrusive cookies improving internet experience (e.g. to remember shopping cart history). Cookies set by a visited website counting the number of visitors to that website will no longer require consent.

- **Protection against spam:** Today's proposal bans unsolicited electronic communication by any means, e.g. by emails, SMS and in principle also by phone calls if users have not given their consent. Member States may opt for a solution that gives consumers the right to object to the reception of voice-to-voice marketing calls, for example by registering their number on a do-not- call list. Marketing callers will need to display their phone number or use a special pre-fix that indicates a marketing call.

- **More effective enforcement:** The enforcement of the confidentiality rules in the Regulation will be the responsibility of national data protection authorities.

Data Protection Rules for EU institutions and Bodies

The proposed Regulation on the protection of Personal Data by European institutions and bodies aims to align the existing rules, which date back to 2001, with the newer and more stringent rules set out by the General Data Protection Regulation of 2016. Anyone whose Personal Data are handled by the European institutions or agencies will benefit from higher standards of protection.

International data protection

The proposed “Communication From The Commission To The European Parliament And The Council
- Exchanging and Protecting Personal Data in a Globalised World” (Brussels, 10.1.2017 – COM(2017) 7 final) sets out a strategic approach to the issue of international personal data transfers, which will facilitate commercial exchanges and promote better law enforcement cooperation, while ensuring a high level of data protection. The Commission will engage proactively in discussions on reaching "adequacy decisions" (allowing for the free flow of Personal Data to countries with "essentially equivalent" data protection rules to those in the EU) with key trading partners in East and South-East Asia, starting with Japan and Korea in 2017, but also with interested countries of Latin America and the European Neighbourhood.

The Communication also reiterates that the Commission will continue to promote the development of high data protection standards internationally, both at bilateral and multilateral levels.

Next Steps

With the presentation of its proposals, the Commission is calling on the European Parliament and the Council to work swiftly and to ensure their smooth adoption by 25th May 2018, when the General Data Protection Regulation will enter into force.

The intention is to provide citizens and businesses with a fully-fledged and complete legal framework for privacy and data protection in Europe by this date.