GIBRALTAR REGULATORY AUTHORITY

(28) Cookies

Guidance on the Communications (Personal Data and Privacy) Regulations 2006, Gibraltar General Data Protection Regulation & Data Protection Act 2004

23 May 2023
Guidance Note IR01/23

FOREWORD

Gibraltar's data protection law consists of both the Gibraltar General Data Protection Regulation ("Gibraltar GDPR") and the Data Protection Act 2004 ("DPA").

The legislation in Gibraltar maintains the data protection standards that applied in Gibraltar as a result of EU Law i.e. the EU General Data Protection Regulation 2016/679 and the Law Enforcement Directive 2016/680, prior to Brexit and the end of the transition period.

Organisations involved in the processing of personal data need to be aware of the obligations that the Gibraltar GDPR and/or the DPA impose on them.

Where organisations use cookies and similar tracking technologies, they must also be aware of the obligations that the Communications (Personal Data and Privacy) Regulations 2006 ("Privacy Regs") impose on them. The Privacy Regs are separate to, but complement, the Gibraltar GDPR and DPA.

The Gibraltar Regulatory Authority, as the Information Commissioner, regularly publish guidance notes that aim to –

- *raise awareness amongst controllers and processors of their data protection obligations; and,*
- *assist them in ensuring compliance.*

Guidance notes also aim to promote public awareness of the risks to personal data that may arise from data processing activities.

SUMMARY

- A cookie is a small text file that is downloaded onto 'terminal equipment' when an individual accesses a website and can carry out a number of important functions. For example, without cookies, or the use of similar technologies, websites would be unable to 'remember' anything about its users.

- Although cookies are not explicitly referred to in the Communications (Personal Data and Privacy) Regulations 2006 (the "Privacy Regs"), Regulation 5 nevertheless sets out the rules regarding cookies. The Privacy Regs sit alongside the Gibraltar General Data Protection Regulation (the "Gibraltar GDPR") and the Data Protection Act 2004 ("DPA"), and they provide individuals with specific privacy rights in relation to electronic communications. This includes cookies and similar tracking technologies.

- In brief, the rules provided in Regulation 5 of the Privacy Regs require that organisations must -
    - tell individuals which cookies will be set;
    - explain what the cookies will do; and
    - obtain consent from individuals to store a cookie on their device.

- Information regarding the use of cookies must be provided prior to these being set, and it must be clear and comprehensive, in accordance with the transparency requirements and the right to be informed under the Gibraltar GDPR.

- In order for consent to be valid, it must be obtained in accordance with the requirements of the Gibraltar GDPR. Therefore, it must be freely given, specific and informed. It must involve some form of clear, positive action from the user, such as ticking a box or clicking a link. Additionally, the user must be informed that they may withdraw their consent for non-exempt cookies (i.e., opt-out) and be able to do this as easily as they were able to give their consent.

- The Privacy Regs have two exemptions to the cookie rules, known as the 'communication' exemption and the 'strictly necessary' exemption.

- Although in the context of the Privacy Regs said exemptions apply to both the provision of information and the obtaining of consent, if personal data is processed, information needs to be provided to users and the lawful basis requirement met as this would be necessary to comply with the fairness and transparency requirements of the Gibraltar GDPR.

CONTENTS

1. ACKNOWLEDGEMENTS

Where appropriate, the Information Commissioner[1] will seek to ensure that locally published guidance notes are consistent with those published by fellow Information Commissioners in other jurisdictions.

As well as reflecting the existing data protection standards and practices in Gibraltar, parts of this document reflect and/or incorporate the guidance from the Article 29 Data Protection Working Party[2], Ireland's Data Protection Commission, the UK Information Commissioner's office, and Malta's Office of the Information and Data Protection Commissioner.

The following documents were used in the production of this Guidance Note:

(a) Article 29 Data Protection Working Party (predecessor to the European Data Protection Board)

'WP194: Opinion 04/2012 on Cookie Consent Exemption'

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

'WP208: Working Document 02/2013 providing guidance on obtaining consent for cookies'

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

(b) European Data Protection Board

'Report of the work undertaken by the Cookie Banner Taskforce' Adopted 17 January 2023

https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

(c) Ireland's Data Protection Commission

'Cookies and other tracking technologies'

[1] The Information Commissioner is the Chief Executive Officer of the Gibraltar Regulatory Authority.

[2] As of 25th May 2018, the European Data Protection Board ("EDPB") formally replaced the Article 29 Data Protection Working Party.

https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf

(d) UK Information Commissioner's Office

'Cookies and similar technologies'

https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/

'Guidance on the use of cookies and similar technologies'

https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/

(e) Malta's Office of the Information and Data Protection Commissioner

'Guidance Note on Cookies Consent Requirements'

https://idpc.org.mt/idpc-publications/guidance-note-on-cookies-consent-requirements/

2. INTRODUCTION

Cookies are small alphanumeric text files that are processed, stored, and later retrieved by a web browser. Whilst they are essential for providing several necessary website functions, cookies are also a tool used by advertisers to provide insight into online behaviour and track user activity to deliver highly personalised adverts to its users.

In this Guidance Note, the Gibraltar Regulatory Authority as the Information Commissioner provides guidance on the use of cookies, including the rules for setting cookies, and how to ensure compliance with these rules.

While the Communications (Personal Data and Privacy) Regulations 2006 (the "Privacy Regs") establish the rules on how cookies (and other tracking technologies) should be used, it is important to note that the Privacy Regs complement data protection legislation, namely, the Gibraltar General Data Protection Regulation (the "Gibraltar GDPR") and Data Protection Act 2004 (the "DPA"). In this regard, data protection legislation defines certain expressions and terms referred to in the Privacy Regs, for example, the meaning of 'consent'[3]. The Gibraltar GDPR also includes cookies within its definition of personal data[4]. Therefore, when setting cookies, compliance with the Privacy Regs should principally be considered alongside the Gibraltar GDPR, and where relevant, the DPA.

Whilst the Privacy Regs do not prohibit the use of cookies, they require that individuals be informed about their use and given a choice as to whether they want to have non-essential[5] cookies stored on their devices. The purpose of these rules is to protect individuals from having information placed on their devices, or accessed on their devices, without their consent, as this could constitute a severe privacy intrusion and interfere with the confidentiality of their online interactions. This Guidance Note sets out the key points that data controllers[6] should consider when setting cookies, in order to comply with the relevant legislation.

---

[3] Although the Communications (Personal Data and Privacy) Regulations 2006 (the "Privacy Regs") do not make reference to the Gibraltar General Data Protection Regulation ("Gibraltar GDPR"), they do make reference to the Data Protection Act 2004 ("DPA"). Specifically, Regulation 5 states that requirements stipulated therein, should be in accordance with the provisions of the DPA. Further, section 6 of the DPA does state that Part II "*is relevant to most processing of personal data*" (i.e., including when processed via the use of cookies), and section 7(1) of the DPA specifies that the "*Terms used in this Part and in the Gibraltar GDPR have the same meaning in this Part as they have in the Gibraltar GDPR*". Therefore, given that many of the terms referred to in the Privacy Regs are also contained in the DPA and GDPR, definitions and standards set in the latter must be maintained. See sections 4, 5 and 6 of this Guidance Note.

[4] Article 4(1) of the Gibraltar GDPR includes the term 'online identifier' within its definition of personal data.

[5] In this Guidance Note, a non-essential cookie refers to a cookie that does not fall under any of the exemptions provided in Regulation 5(4) of the Privacy Regs. Therefore, these cookies would require the individual's consent, having been provided with clear and comprehensive information in accordance with the DPA and Gibraltar GDPR.

[6] In this Guidance Note, the terms data controller, organisation and website operator are used (interchangeably) to mean the person determining the means and purposes of the cookie (i.e., requiring the setting of the cookie).

3. WHAT ARE COOKIES?

Cookies are small files made up of letters and numbers that are downloaded onto a device, such as a computer or a smartphone, whenever a website is accessed. Cookies and other tracking technologies involve accessing information, or placing information, on a user's device regarding a user's preferences or online activities. They are typically downloaded onto a device upon a user's first visit to a website.

Cookies are used to facilitate a number of important functions, such as -

- to 'remember' a user's actions e.g., what is in a shopping basket when ordering goods online;
- to identify users when logging into an online service;
- to analyse traffic to a particular website; and
- to track internet users' browsing behaviour.

Certain types of cookies are used to make a website work, or work more effectively, in addition to storing information between website visits and providing information to the operators of the website.

The information stored in cookies can include personal data[7], such as a username or an email address[8], however, cookies can also simply include data such as language settings, which would not be considered personal data. Whilst cookies can generally be easily viewed and deleted, cookies can also store large amounts of information and are the main method by which advertisers track online user activity and behaviour in order to send targeted adverts, therefore, certain types of cookies may pose a significant threat to the privacy of individuals online.

3.1 Types of cookies

Cookies can be classified by duration, provenance, and purpose, as detailed below.

(a) Duration.

[7] Article 4(1) of the Gibraltar GDPR defines 'personal data' as any information relating to an identified or identifiable natural person. It further states that, "*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*."

[8] See section 8.2 of this Guidance note.

Session cookies expire at the end of a browser session, normally when a user exits their browser.

Session cookies allow websites to recognise and remember the actions of a user during a browsing session, such as remembering the items added to a shopping basket whilst the user continues to browse the site. They can also be used for security purposes, such as logging into a banking (or other) secure online service.

As these types of cookies expire when a user closes their browser, they are often considered to be less privacy-intrusive than persistent cookies.

Persistent cookies have an expiration date set by the issuer and will remain stored on a user's device in-between sessions. Persistent cookies allow for preferences and actions to be remembered across a website, for example, username and password combinations, language selection, menu preferences, bookmarks and/or favourites. In this regard, clicking on 'remember me' on a webpage will usually create a persistent cookie.

These types of cookies are also often used by organisations to review how users interact with their websites in order to personalise advertisements and marketing material.

Whilst it is the website operator who determines the lifespan of a persistent cookie, a user is able to delete them or configure their browser settings to delete cookies at set intervals.

When setting cookies, the lifespan of a cookie should be proportionate to its function (see section 6.3 of this Guidance Note). For example, it would not be proportionate to set a session cookie with a lifespan of 'forever'.

(b) Provenance.

Whether a cookie is 'first' or 'third' party refers to the website or domain placing the cookie.

First-party cookies are set directly by the website that the user is visiting or browsing, i.e. the host domain (the URL displayed in the browser's address bar).

Third-party cookies are set by a domain other than the one the user is visiting and can see in their address bar. This typically occurs when the website incorporates elements from other websites, such as images, social media plugins, advertising, or an analytics system. When the browser or other software fetches these elements from said websites, third-party cookies are set.

(c) Purpose.

Strictly necessary cookies are essential for a user to use and browse the features of a website (i.e., 'essential' cookies). These are used, for example, by websites to hold items in a shopping basket while the user continues shopping online. These cookies are generally first-party cookies, and due to being necessary for website-use, 'consent' from the user is not required as per one of the two exemptions in Regulation 5 for the Privacy Regs.

Information must however be provided to users explaining their purpose and why they are strictly necessary (see sections 5 and 7.1 of this Guidance Note).

Preference cookies are otherwise referred to as 'functionality cookies' and are used to remember a user's preferences and choices, such as log-in credentials so that a user can automatically log in without having to provide a username and password on each visit.

Statistics cookies are otherwise known as 'performance cookies' which collect information on how users engage with a website, recording visited pages and clicked links.

Marketing cookies are used to track online behaviour and activity, this information is then shared with other organisations or advertisers in order for them to tailor targeted adverts to their users. These are persistent cookies and almost always of third-party origin.

3.2 Similar tracking technologies

In addition to the more commonly known browser (or HTTP) cookies outlined above, there are other 'similar technologies' which can carry out the same functions as cookies, including, for example, using certain characteristics to identify a device so that a user's online activity can be analysed.

Similar tracking technologies can include the following:

- Local storage objects (LSOs) or 'flash' cookies. These are text files that are sent by a web server to a client when the browser requests content supported by Adobe Flash, a popular browser plugin. Unlike a typical browser (or HTTP) cookie, a flash cookie must be cleared through Adobe Flash Player settings. Flash cookies sometimes contain the same information that browser (or HTTP) cookies contain, but they also store information specific to the media player (i.e. Adobe Flash) such as the place where the user's video stopped playing or where an animated banner advertisement stopped rotating[9].

- Software development kits (SDKs). An SDK is a set of tools that provides a developer with the ability to build a custom app which can be added on, or connected to, another program. SDKs allow programmers to develop apps for a specific platform. SDKs create the opportunity to enhance apps with more functionality, as well as include advertisements and push notifications onto the system[10].

- Tracking pixels (or pixel kits). A tracking pixel is a 1×1 pixel graphic used to track user behaviour, site conversions, web traffic, and other metrics similar to a cookie. The tiny pixel-sided image is usually hidden and embedded in everything from banner ads to

[9] Cookie Pro by One Trust, 'What is a Flash Cookie?', available here: https://www.cookiepro.com/knowledge/what-is-a-flash-cookie/ accessed 19 April 2023.

[10] Adjust Glossary, 'SDK', available here: https://www.adjust.com/glossary/sdk/ accessed 19 April 2023.

emails. Although pixels and cookies serve similar marketing purposes and are often used simultaneously, the differences are in how the information is delivered and where it is kept. Tracking pixels do not rely on the user's browser but will send information directly to servers. They can follow users across all of their devices which allow marketing efforts to be linked across website and mobile ads. A key difference is pixels cannot be disabled like cookies can[11].

- Device fingerprinting technologies. Device fingerprinting is a technique that involves combining a set of information elements in order to uniquely identify a particular device. Examples of the information elements that device fingerprinting can single out, link or infer, include (but are not limited to) data derived from the configuration of a device, data exposed by the use of particular network protocols, CSS information, JavaScript objects, HTTP header information, clock information, TCP stack variation, installed fonts, installed plugins within the browser, and use of any APIs (internal and/or external). It is also possible to combine these elements with other information, such as IP addresses or unique identifiers, etc.

4. APPLICABLE LEGISLATION

4.1 The Privacy Regs

The Privacy Regs implemented the European Union (the "EU") Directive 2002/58/EC[12], more commonly known as the 'ePrivacy Directive' (the "ePrivacy Directive"). The Privacy Regs sit alongside data protection legislation and give individuals specific privacy rights in relation to electronic communications, providing specific rules on -

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

Although cookies are not referred to explicitly in the Privacy Regs, Regulation 5(1) and (2) state the following -

[11] Cookie Pro by One Trust, 'What is a Tracking Pixel?', available here: https://www.cookiepro.com/knowledge/tracking-pixel/ accessed 19 April 2023.

[12] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("ePrivacy Directive"), available here: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN.

"5.(1) Subject to sub-regulation (4), a person shall not store information, or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirement of sub-regulation (2) is met.

(2) The requirement is that the subscriber or user of that terminal equipment has given his consent, having been provided with clear and comprehensive information, in accordance with the provisions of the Data Protection Act 2004, about the purposes of the storage of, or access to, that information."

As evident from the above, Regulation 5(1) and (2) of the Privacy Regs set out rules ("Cookie Rules") to protect individuals from having information placed on their devices, or accessed on their devices, without their consent, knowledge and understating of what they do – this means through the use of browser (or HTTP) cookies, as well as other tracking technologies, examples of which are provided in section 3.2 above.

However, the requirements set out in Regulation 5(2) are not specifically defined within the Privacy Regs. In this regard, it is important to understand how these regulations are supplemented by data protection legislation.

Primarily, it is noted that the ePrivacy Directive makes reference to data protection law and stipulates that many of the requirements should be in accordance with said law[13]. Although the Privacy Regs do not make reference to the Gibraltar GDPR[14], they do make reference to the DPA. Specifically, Regulation 5(2) states that requirements stipulated therein, should be in accordance with the provisions of the DPA. Further, section 6 of the DPA states that Part II "*is relevant to most processing of personal data*" (i.e. including when processed via the use of cookies), and section 7(1) of the DPA specifies that the "*Terms used in this Part and in the Gibraltar GDPR have the same meaning in this Part as they have in the Gibraltar GDPR*".

Therefore, given that many of the terms referred to in the Privacy Regs are also contained and explained in the DPA and/or GDPR (for example, the meaning of 'consent'), definitions and standards set in the latter must be maintained. As such, the guidance provided in the following sections (i.e. 5 and 6) makes reference to, and explains, the Gibraltar GDPR requirements where relevant.

[13] See Recital 25, Articles 1(2), 2(f) and 5(3) of the ePrivacy Directive.

[14] Data Protection Directive 95/46/EC was superseded by the EU General Data Protection Regulation 2016/679 ("EU GDPR") on 25th May 2018, which applied to all EU member states, including Gibraltar at the time. Following Gibraltar's exit from the EU and the end of the Brexit transition period on 1st January 2021, the EU GDPR was superseded by the Gibraltar GDPR. Notwithstanding, the current legislation remains largely the same, reflecting the EU GDPR.

NOTE

The EU Commission are in the process of replacing the ePrivacy Directive with an ePrivacy Regulation so as to modernise and update the rules for privacy and electronic communications, including that of cookies within the European Union[15]. The ePrivacy Regulation will not automatically form part of Gibraltar law due to Gibraltar's exit from the EU. Subject to changes in Gibraltar law, the Privacy Regs will remain applicable.

4.2 Who does the law apply to and who is responsible for compliance?

(a) Who does the law apply to?

Regulation 5 of the Privacy Regs applies to the storage of any information on the 'terminal equipment' of the 'subscriber' or 'user', as well as to the accessing of any information already stored, irrespective of whether the information stored or accessed is personal data[16].

The **'subscriber'** is the individual who has a contract with the service provider and pays for the use of the electronic communications service, whereas the **'user'** is an individual using the phone or internet connection to access an online service. In certain cases, this will be the same person.

'Terminal equipment' refers to the device that the cookie will be stored on, such as a computer or a mobile device, however, this definition also extends beyond traditional tools to include other devices, which are designed to connect to the internet in order to offer the user various services and are not necessarily limited to communication. Examples of said devices include, wearable technology such as smart watches, smart TVs, smart kitchen appliances and even voice-activated assistants that use cookies or other tracking technologies.

IMPORTANT NOTE

The Privacy Regs do not apply in the same way to intranets (i.e., internal networks). An intranet is unlikely to be a public electronic communications service, and therefore, the

[15] Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications ("ePrivacy Regulation"), available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

[16] EU case law concerning the corresponding cookie rule in the ePrivacy Directive (i.e., Article 5(3)) has clarified that this applies regardless of whether the information stored or accessed is personal data. See judgement of the Court of Justice of the European Union on 1st October 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* Case C-673/17, ECLI:EU:C:2019:801, paras 69-70, available here: https://curia.europa.eu/juris/liste.jsf?num=C-673/17.

Privacy Regs would not apply in the same way to cookies that are set on an intranet. However, it is important to remember that the requirements of data protection law are still likely to apply if the usage of cookies involves the processing of personal data, for example, is for the purposes of monitoring performance at work.

Wherever personal data is collected using cookies, then the requirements of data protection law will also apply.

(b) Who is responsible for compliance?

The Privacy Regs state that 'a person' shall not store, or gain access to information stored, on user devices. However, the Privacy Regs do not define who should be responsible for complying with the requirement to provide information about cookies and obtain consent. The key point is not who obtains the consent, but that valid consent is in fact obtained and that clear and comprehensive information is provided.

Where an organisation operates an online service, it is clear that any use of cookies will be for their own purposes. In this regard, the person (i.e. organisation) operating the online service (i.e. wanting the cookie to be set) is therefore primarily responsible for compliance with the requirements of the Privacy Regs, although this is not necessarily the case where multiple parties are involved.

Organisations should therefore consider their deployment of any third-party assets on their website, such as 'like' buttons, plugins or widgets, pixel trackers or social media-sharing tools. In this regard, organisations should assess whether and what data (if any) is being sent to these third parties and what their relationship is to these third parties from the perspective of data protection legislation, for example, whether they are a data controller or joint data controller with the third party.

In view of the above, it is noted that the Court of Justice of the European Union (the "CJEU") held that a separate website operator that features a Facebook 'Like' button can be a joint controller in respect of the collection of the personal data of its users and transmission to Facebook[17], as they concluded (in this case) that they jointly determined the means and purposes of those operations. Therefore, organisations wanting to embed such features on their sites should review their arrangements so as to ascertain whether the third party has any role in determining the means and the purposes of the processing of personal data passed to it via cookies[18].

[17] Judgement of the Court of Justice of the European Union on 29th July 2019, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* C-40/17, ECLI:EU:C:2019:629, paras 98-107, available here: https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=40457313.

[18] For further information as to the responsibilities and liabilities of data controllers and data processors, see the Information Commissioner's Guidance Note (24) Guidance on the Concepts of Data Controller and Data Processor, available here: https://www.gra.gi/data-protection/guidance accessed 19 April 2023.

If an organisation is planning a new online service, steps should be taken to detail what cookies will be used, which are strictly necessary, and to ensure that appropriate arrangements will be in place with any third parties.

For any pre-existing services, while organisations should already know what types of cookies they use, the Information Commissioner considers that it would be good practice to review this, for example, by simply checking what data will be sent to users and why, or preferably, undertaking a comprehensive 'cookie audit' of the online service. Please see Annex A for advice in respect to how a cookie audit may be undertaken.

A cookie audit provides an organisation with the opportunity to 'clean up' existing web pages, including stopping the use of cookies that may be unnecessary or which have been superseded as the website has evolved.

Further, an organisation's usage of any third-party content is likely to change over time, so it would also be good practice to undertake regular reviews of cookie usage, as well as any third-party services that may set cookies on an organisation's website.

(c) What about cookies set on overseas websites?

If the organisation setting the cookies is based in Gibraltar, then the Privacy Regs apply even if the website is hosted overseas (for example, using cloud services based in the USA).

Where personal data is processed, the additional Gibraltar GDPR requirements apply. It is important to note however, that the Gibraltar GDPR applies to the processing of personal data regardless of whether this takes place in Gibraltar or not. If the processing does not take place in Gibraltar but it involves activities that offer goods or services to data subjects in Gibraltar or monitors data subjects' behaviour as far as this takes place within Gibraltar, then the Gibraltar GDPR will also apply[19].

5. COOKIE RULE: CLEAR AND COMPREHENSIVE INFORMATION

Regulation 5(2) of the Privacy Regs requires users to be provided with *"clear and comprehensive information"* regarding the use of cookies, prior to obtaining consent. For the reasons outlined in the foregoing, the standard required must be in accordance with data protection legislation.

[19] See Article 3 of the Gibraltar GDPR.

In effect, this relates to the transparency requirements and the right to be informed under the Gibraltar GDPR[20], and therefore, users must be provided with the same information that they would be provided if personal data was involved in the processing[21]. The information must include –

- a description of the cookies that will be used;
- the purposes for which they will be used;
- any third parties who may also process information stored in or accessed from the user's and/or subscriber's device; and
- the duration for which the cookies will be set.

In practice, most websites will use a 'cookie banner' or 'pop-up', which will be displayed upon a user landing on the site. This is often considered to be the 'first layer' of information regarding the website's use of cookies and should contain links to a cookie notice and/or privacy notice (e.g. the 'second layer') which must include more detailed information[22]. In such cases, the cookie banner or pop-up also tends to be the cookie consent mechanism itself (see section 6.2 of this Guidance Note).

In order to draw attention to the first layer of information, and thus ensure that users have engaged with and read said information, particular prominence could be given to the following:

- **Formatting**. This may include altering the size of the link to the cookie notice or using a different font to other text on the webpage.
- **Positioning.** Moving the link to the cookie notice in a more prominent position of the page.
- **Wording**. Using explanatory wording such as 'find out how we use cookies' rather than simply 'cookie notice'.

Importantly, for the setting of any third-party cookies, the identity of the third party must be provided rather than vague references to 'partners' or 'other parties'.

The emphasis is on the information being provided clearly and comprehensively to users; therefore, organisations should consider tailoring the language to their audience and not using lengthy, overly complex terminology.

[20] Article 5(1)(a), 12, 13 and 14 of the Gibraltar GDPR require individuals to be provided with an understanding of the processing, in a transparent, intelligible, and easily accessible form, using clear and plain language.

[21] In some cases, personal data will be involved in the processing.

[22] For further information on privacy notices, please see the Information Commissioner's Guidance Note (17) Privacy Notices, available here: https://www.gra.gi/data-protection/guidance accessed 19 April 2023.

Where tens or even hundreds of cookies are used, it may be helpful to provide a broader explanation of the way cookies operate and the categories of cookies in use. For example, a description of the types of things analytics cookies are used for may be more likely to satisfy the requirements than simply listing all the cookies used with basic references to their function.

With regards the 'second layer' of information (i.e., the cookie notice), although this may contain details that overlap with those included in a general privacy notice, it is good practice to maintain both separately in order to comply with the requirements of the Privacy Regs and the Gibraltar GDPR[23]. In this regard, it is particularly important to note that levels of understanding may differ between users, and therefore, the information provided in a cookie notice must also be explained in a manner that everyone can understand.

In addition to implementing a multi-layer approach to providing information, organisations may also consider adopting a multi-channel approach in order to create a more engaging and less traditional means of contact between the website provider and the user. For example, a multi-channel policy could combine the use of video channels, pop-ups, virtual assistants and chatbots. However, the data controller would ultimately be responsible for deciding the channel, or combination of channels, and must ensure that such features do not interrupt the provision of clear and comprehensive information, as well as obtaining consent in accordance with the Privacy Regs and Gibraltar GDPR.

If children are likely to access the service, an organisation will need to ensure that both the information provided and the consent mechanism (see section 6.2 of the Guidance Note) are appropriate for children (i.e., that they can read and understand these), given that the rules apply to them in the same way.

6. COOKIE RULE: CONSENT

As stipulated in Regulation 5(1) and (2) of the Privacy Regs, for cookies that do not meet one of the exemptions listed at sub regulation (4) (see section 7.1 of this Guidance Note), **consent must be obtained prior to setting cookies** on a user's device. This will be applicable **whether or not** the processing involves personal data.

This section of the Guidance Note provides information and guidance in respect of who 'consent' needs to be obtained from, the standard of 'consent' needed to ensure compliance with the applicable legislation, and how often this needs to be obtained. For examples of cookies that are not exempt under Regulation 5(4) of the Privacy Regs, see section 7.2 of this Guidance Note.

[23] Where the setting of cookies involves the processing of personal data, individuals must be provided with all the information they are entitled to under Articles 13 and 14 of the Gibraltar GDPR. Apart from the information already mentioned, this would also include (but is not limited to) contact information about the data controller and the appointed data protection officer (if relevant), as well as information on how they can exercise their data subject rights under the provisions of Chapter 3 of the Gibraltar GDPR, including how to make a subject access request and make a complaint to the Information Commissioner's office.

6.1 Who should 'consent' be obtained from?

The Privacy Regs stipulate that consent must be obtained from the subscriber or the user of the terminal equipment[24]. However, it does not specify whose wishes should take precedence if they are different. In this respect, the most important thing is that **one of the parties** has been provided with all of the necessary information and **valid consent** has been obtained (see section 5 and 6.2 of this Guidance Note).

Notwithstanding, there may well be cases where a subscriber, for example, an employer, provides an employee with a terminal at work along with access to certain services to carry out a particular task, where to effectively complete the task depends on using a service that uses a cookie and a device that accepts them. In these cases, it would not seem unreasonable for the employer's wishes to take precedence.

However, it also seems likely that there will be circumstances where a user's wish should take precedence. To continue the above example, an employer's wish of using such a device should not take precedence where this will involve the unwarranted collection of personal data of that employee.

In a domestic context there will usually be one subscriber (the person in the household paying the bill) and potentially several other users. If a user complained that a website was setting cookies without their consent, the website could demonstrate compliance with the Privacy Regs if they could show that consent had previously been obtained from the subscriber. However, it is important to note that where personal data is processed, the GDPR needs to be complied with in relation to data processing about users and consent and/or other lawful bases should be considered.

However, the key to resolving problems is to ensure information about cookies and mechanisms for making choices are as accessible as possible to all users.

6.2 The standard of 'consent' (valid consent)

For the reasons explained in the foregoing, the standard of consent under the Privacy Regs is the same as under the Gibraltar GDPR, which is defined in **Article 4(11) as –**

"...any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

(a) Please see guidance below in respect of complying with the requirements stipulated in Article 4(11) of the Gibraltar GDPR.

[24] Regulation 5(2) of the Privacy Regs.

(i) Freely given.

With regards non-exempt cookies, a user must be able exercise a real choice without the risk of coercion, intimidation or any other negative consequences for not providing consent. The consent mechanism should be presented to the user on the website's landing page whereby the user must be provided with a clear choice between accepting some, all or none of these cookies, along with the opportunity to modify selected cookie settings at a later date. Even if users reject non-essential cookies, they should still be allowed access to the website.

As referred to in the foregoing, organisations may use a cookie 'banner' or a 'pop-up', however, this must not be designed in a way that gives users the impression that they have to give consent to access the website content or that clearly pushes the user to give consent i.e., this must not 'nudge' or encourage the user into accepting cookies. For example, if using an 'accept' button, equal prominence should also be given to a 'reject', 'refuse' or 'do not consent' button[25]. Specifically, the configuration of the 'banner' or 'pop-up' in terms of colours and contrasts should not lead to a clear highlight of an 'accept' button[26] over the available options[27].

It is important to also note that the absence of a 'reject' (or 'refuse' or 'do not consent') option where an 'accept' button is present, is not considered to be compliant with the Privacy Regs[28]. Similarly, providing a link behind wording such as 'refuse' or 'continue without accepting' embedded in a paragraph of text in a cookie banner, would neither be compliant with the Privacy Regs without sufficient visual support to draw attention to this alternative action, as would be the case if such wording and link were placed outside the cookie 'banner' where the button to accept cookies is presented[29].

Further, users should not be led to believe that they have no possibility of objecting to the use of cookies due to the integration of an alternative option to consenting or allowing cookies that refers to reliance on 'legitimate interests', which is a lawful basis under Article 6(1) of the Gibraltar GDPR[30]. The integration of the notion of 'legitimate interests' for any subsequent processing of personal data (although cookies may not always contain personal data), in particular, in the deeper layers of the 'banner', could be considered as confusing for users who might think they have to refuse twice in order not to have their personal data processed[31]. As noted

[25] EDPB, 'Report of the work undertaken by the Cookie Banner Taskforce' adopted 17 January 2023, available : https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf accessed 18 April 2023, paragraph 8.

[26] Ibid, paragraphs 15-19.

[27] Ibid, paragraph 19. However, design choices in respect of cookie banners would be assessed on a case-by-case basis.

[28] Ibid, paragraphs 6-8.

[29] Ibid, paragraphs 11-14.

[30] Ibid, paragraph 20-25.

[31] Ibid.

earlier in this section, consent is required for all non-exempt cookies, and as such, any reliance on said lawful basis for the further processing of personal data (where this is contained in or derived from cookies), would not be compliant with the Gibraltar GDPR. For further information on the Gibraltar GDPR, please refer to section 8 of this Guidance Note.

Users should be provided with a way to manage the use of cookies, by type and purpose. The banner should be configured to ensure that any non-exempt cookies are not deployed upon a user landing on the webpage but are only set after the user has engaged with the banner and consented to the use of such cookies.

Further, the use of cookie walls with blanket statements such as "*by continuing to use this website you are agreeing to cookies*" would also not be considered as valid, freely given consent. This is often known as a 'take it or leave it approach', as an individual would have no real choice but to accept cookies if they want to view the content of the website. Equally, banners with acceptance buttons such as "*I understand*" and which do not allow a user to reject cookies, or provide a user with more detailed information, would not be considered to meet the required standard of consent.

NOTE

The presence of a banner (or other mechanism) providing the 'accept' (or 'consent'), 'reject' (or 'refuse' or 'do not accept') and 'customise' (or 'preferences', 'personalise' or 'settings') options equally in terms of colour, size, and font, and having an icon that enables access to the banner on the website are deemed as good practices, see example below.

IMPORTANT NOTE

Recital 43 of the Gibraltar GDPR explains that where a data controller is a public authority, it is unlikely that consent was freely given in all the circumstances of that specific situation. However, this is not the case in respect to the setting of cookies, the Privacy Regs apply regardless of whether a data controller is a public authority. Therefore, public authorities running an online service such as a website must also provide clear and comprehensive information about the cookies set and obtain consent where the cookies are not exempt under Regulation 5(4) of the Privacy Regs.

(ii) Specific.

Consent cannot be bundled for multiple purposes. Consent must be specific and based on the provision of necessary information. If cookies are to be used for more than one purpose (e.g. preferences/functionality, statistics/analytics, and marketing/advertising), consent must be obtained for each purpose specifically and independently. This will allow users to accept or reject cookies, based on their preference.

Recital 32 of the Gibraltar GDPR explains that the use of pre-ticked boxes or equivalents, such as sliders defaulted to 'on', are not mechanisms which would be considered valid for obtaining consent for non-essential cookies[32]. On 1st October 2019, the CJEU upheld that this particular mechanism is unlawful in its Planet49 ruling[33].

(iii) Involves a clear, affirmative action.

Consent cannot be obtained through inaction or silence by the user. The user must take a positive action that unambiguously indicates that the user has consented to the setting of cookies. This may be done by the user ticking a box, clicking on a button/link/image or by another deliberate, affirmative action that demonstrates without doubt, a user's intention.

(b) Article 7 of the Gibraltar GDPR provides further specifics about consent requirements, guidance in relation this is provided below.

(i) Demonstratable[34].

Organisations must be able to demonstrate that they have obtained valid consent for non-exempt cookies, meaning that records of consent should be maintained[35]. Additionally, they must also be able to demonstrate that they have organisational and technical measures in place to ensure that a data subject's expression of consent (or withdrawal of consent) can be effectively actioned.

In this regard, it is noted that consent management platforms ("CMPs") are at times used, given that they are systems that assist in the provision of information about cookies and managing users' choices in relation to cookies. For example,

---

[32] Ibid, paragraph 10.

[33] Judgement of the Court of Justice of the European Union on 1st October 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* Case C-673/17, ECLI:EU:C:2019:801, paras 63 and 65, available here: https://curia.europa.eu/juris/liste.jsf?num=C-673/17.

[34] Article 7(1) of the Gibraltar GDPR.

[35] Data controllers must keep records of consent as part of their records of processing activities in accordance with Article 30 of the Gibraltar GDPR.

when a website uses banners, pop-ups, or sliders to manage a user's cookie preferences, these are often managed by a CMP.

While such software may be deployed, it is important to ensure that the legal requirements set out in the Privacy Regs and the Gibraltar GDPR are complied with, for example, it must not contain pre-checked tick boxes signalling consent for the use of cookies, the lifespan of cookies must be reviewed and set appropriately, it must contain information as to how consent can be varied and/or withdrawn, as well as provide the mechanism to do this (in relation to the latter, please see point (iv) below) [36].

(ii) Clearly distinguishable from other matters[37].

Obtaining consent should be separate from other matters and not bundled into terms and conditions or a privacy notice. Consent should also not be a precondition of signing up to a service.

If cookie banners are used, it must allow a user to request further information about the use of such cookies. A banner that provides a user with a link to further information regarding the use of cookies (for example, a cookie notice) must contain easily readable information that is uninterrupted by 'chatbots' or other website features.

(iii) In an intelligible and easily accessible form, using clear and plain language[38].

It must be clear what a user is consenting to, with the relevant information explained in a manner that can be easily understood. If the request for consent is vague or difficult to understand, the mechanism will be considered invalid. For example, the use of double negatives or legal jargon will invalidate consent.

In addition, whilst providing extremely long lists of checkboxes may seem like taking a more granular approach to obtaining consent, some users may disengage or not fully understand all of the information presented. Therefore, as mentioned in section 5 above, providing a broader explanation of the way cookies operate and the categories of cookies in use may be more likely to satisfy the requirements than simply listing all the cookies used with basic references to their function.

As also mentioned in section 5 above, organisations must consider whether children would be using the service, and as such, ensure that they would be able to read and understand the information provided and the consent mechanism.

[36] If such a third-party tool is used to keep a record of a user's consent to the use of cookies, a record of that consent must also be kept as part of the record of processing activities in accordance with Article 30 of the Gibraltar GDPR.

[37] Recital 43 and Article 7(2) of the Gibraltar GDPR.

[38] Article 7(2) of the Gibraltar GDPR.

(iv) Easily withdrawing consent at any time[39] (i.e. opting-out).

Once consent has been obtained, users or subscribers are able to withdraw that consent at any time. Therefore, it must be ensured that the consent mechanism has the technical capability to allow users to withdraw their consent with the same ease that they gave it, without disadvantaging them. For example, easily accessible solutions allowing users to withdraw their consent at any time could include an icon (small hovering and permanently visible) or a link placed on a visible and standardised place[40].

Users must also be informed of their right to withdraw consent and how to remove cookies that have previously been set, along with the consequences of withdrawing said consent, such as the impact on the functionality of the website. Said information may, for example, be provided in the consent mechanism itself and/or in a cookie notice.

Failing to provide users with a means to permanently withdraw consent, including the relevant information explaining how a user can withdraw their consent, may contravene Articles 5(1)(a), 7(3), 13(2)(c) and 14(2)(d) of the Gibraltar GDPR.

IMPORTANT NOTE

The user must take clear, affirmative action as detailed in Recital 32 and required by Article 4(11) of the Gibraltar GDPR. Therefore, implied consent is not valid for accepting cookies. A user who simply clicks, scrolls, or navigates a website is not considered to have provided valid consent[41]. This mechanism does not allow the website operator to effectively demonstrate that a user has unambiguously consented to cookies being set and it would be extremely difficult for the user to withdraw their consent as easily as they provided it. This would also be the case with banners that pop-up upon accessing a website and then disappear when a user scrolls, without any further engagement from the user.

In addition, browser settings cannot be used to infer a user's consent. This is because the average user is not considered to know how to configure their browser settings to reject cookies, even when such information is provided within a cookie or privacy notice.

---

[39] Article 7(3) of the Gibraltar GDPR.

[40] EDPB, 'Report of the work undertaken by the Cookie Banner Taskforce' adopted 17 January 2023, available : https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf accessed 18 April 2023, paragraphs 31-35. However, A case-by-case analysis of the solution displayed to withdraw consent will always be necessary.

[41] This may change as technology continues to evolve. For example, there has recently been a call for industry experts to explore whether it is technically feasible to create a process that allows for the analysis of precise pattern, including that of the 'scroll down' action, which records the user's unequivocal and informed consent in respect of non-exempt cookies. However, the technical difficulties in this respect have been noted, including the risk of false positives (i.e. mistaken interpretation of casual actions as positive expression of consent), which may in any case require providing an alternative means to collecting valid consent.

6.3 How often should consent be obtained?

Consent should be obtained upon a user's first visit to a website upon being provided with clear and comprehensive information regarding the use of cookies[42].

There are a range of reasons why visitors may need to 'reconsent' to cookie settings. However, it may not be necessary to ask for fresh consent each time a user visits a website, this depends on the circumstances such as frequency of visits or updates of content or functionality.

For example, when a user provides their consent to the setting of cookies, the website may record such preferences in a persistent cookie, which will be stored on the user's device until the pre-determined expiration date. Should the user visit the site before the expiration date, they would not be required to 'reconsent' as the persistent cookie would 'remember' that the user had already provided their consent. However, if the user is an infrequent visitor, the cookie may have already expired, and consent would again be required.

The above may also be the case where a user makes other choices over a website's settings (for example, selecting a particular language, font size or greeting) and allows the website to 'remember' said choices. In such cases, the user should be made aware that by allowing their choice to be 'remembered' they are giving consent to the setting of a persistent cookie, and therefore, consent would not need to be obtained every time the user visits the site.

Notwithstanding, as mentioned in the foregoing, it is for the website operator to determine the lifespan of persistent cookies i.e., the expiration timeframe. Therefore, an appropriate interval between when users are required to select their preference (whether that is consent or rejection) would need to be decided, as well as when that preference expires (after which point users are given the option again).

At the same time, the Privacy Regs are not intended to inconvenience or unduly disrupt the experience of users, as such, website operators are not expected to repeatedly require users to specify their preference as a matter of course. These are issues that an organisation will need to determine. If 'off the shelf' consent mechanisms are used, such as CMPs, organisations should take the time to determine (and document) whether the default interval set is appropriate in relation to the purpose of the cookie and users' expectations. Ultimately, it should be ensured that the use of the cookie is proportionate in relation to the intended outcome and is limited to what is necessary to achieve its purpose.

However, if a new cookie is set, such as a non-essential cookie from a new third party, or if the use of an already deployed cookie changes after initial consent had been obtained, these changes must be communicated to all users and consent should again be obtained for their use.

[42] Regulation 5(2) and 5(3) of the Privacy Regs.

7. EXEMPTIONS TO THE COOKIE RULES

7.1 Exempt cookies

As outlined in the foregoing, the Cookie Rules require that clear and comprehensive information be provided in respect of any cookies used and that consent be obtained for the use of cookies. However, Regulation 5(4) of the Privacy Regs states that -

> ***"(4) Sub-regulation (1) shall not apply to the technical storage of, or access to, information –***
>
> ***(a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network;***
>
> ***(b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user to provide the service [...] "***

Therefore, Regulation 5(4) of the Privacy Regs provides two exemptions to the Cookie Rules known as the 'communications' exemption (Regulation 5(4)(a) of the Privacy Regs) and the 'strictly necessary' exemption (Regulation 5(4)(b) of the Privacy Regs).

IMPORTANT NOTE

Whilst the exemptions are applicable to both the provision of information regarding the setting of essential cookies and the obtaining of consent, **the Information Commissioner considers it best practice to provide clear and comprehensive information about these cookies in all cases**. Further, if personal data is involved in the processing, this will be required under the fairness and transparency requirements of the Gibraltar GDPR[43].

Additionally, although exempt cookies do not require consent for use, their lifespan must be directly related to the purpose for which they are deployed and must expire once they have fulfilled that purpose, taking into account the reasonable expectations of a user (see section 6.3 of this Guidance Note).

Guidance in respect of the exemptions is provided below.

(a) The 'communications' exemption.

This exemption is applicable to cookies for the sole purpose of carrying out the transmission of a communication over an electronic communications network. In order for

[43] Article 5(1)(a), 12, 13 and 14 of the Gibraltar GDPR.

a 'communication' to take place between two parties over a network, there are three factors that are considered necessary -

- the ability to identify the communication 'endpoints'[44] in order to send information over a network;
- the ability to exchange data items in their proposed order; and
- the ability to detect any transmission errors and/or loss of data.

The communication exemption can therefore be applied when the transmission of a communication would be impossible without the use of the cookie. This means that using cookies to solely assist, speed up or regulate the transmission of a communication over a network would not be considered sufficient for the exemption to apply[45].

For example, this exemption may apply to load-balancing cookies where they are used to distribute network traffic across different servers, given that the information in this cookie has the sole purpose of identifying one of the servers (i.e., the communication end point). Therefore, its use is required to carry out communication over the network.

With regards other tracking technologies, specifically, the use of device fingerprinting techniques for network management, the communication exemption can also be relied on, provided that its use is solely for this purpose.

(b) The 'strictly necessary' exemption.

In order for the 'strictly necessary' exemption to apply, two conditions must be satisfied:

- The service must have been provided by an 'information society service' (also known as an ISS) i.e., services provided over the internet, such as a website or an app; and
- The service must have been explicitly requested by the user and the use of the cookie must be restricted to what is strictly necessary (rather than reasonably necessary) to provide that service.

Strictly necessary also extends to compliance with any other legislation that may apply, such as the security requirements of the Gibraltar GDPR[46].

[44] 'Endpoints' are devices that accept communications across a network i.e., a laptop or mobile.

[45] See p.3 of the Article 29 Data Protection Working Party, 'Opinion 04/2012 on Cookie Consent Exemption', adopted on 7th June 2012, available here: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf accessed 4th November 2021.

[46] Articles 5(1)(f) and 32 of the Gibraltar GDPR.

Where the setting of a cookie is deemed 'important' rather than 'strictly necessary', data controllers are still obliged to provide information about the storage or access to the user or subscriber and obtain consent.

Although not exhaustive, the below list provides examples of cookies that are likely to meet the strictly necessary exemption:

- **User input cookies.**

  This is often a broad term for session cookies used to track a user's input, for example, filling in an online form, or adding items to their carts, in order to 'remember' the selected items. In this regard, reliance on the strictly necessary exemption may be appropriate provided that the cookie is only used for this purpose. However, the exemption may not apply if the cookies are persistent.

- **User preference**.

  Similarly, session cookies that record a user's language or country preference when they visit websites can be considered strictly necessary to deliver a service explicitly requested by a user, provided they are not linked to a persistent identifier.

  However, the exemption may in some cases also apply to persistent cookies, although the user must be given sufficient information in a prominent location, for example, cookies used as part of a cookie consent mechanism, which remember the user's cookie preferences over a period of time (for example, 90 days).

  Where device fingerprinting techniques process information to optimise the site layout - such as where an online service uses responsive design, so that the site changes depending on the type of device - the strictly necessary exemption can apply. This would also apply to any third-party services that are incorporated. However, the information accessed must be used solely for this purpose. Any secondary purposes mean the exemption would not apply and consent is required.

- **Authentication cookies.**

  The strictly necessary exemption would apply to authentication cookies which are used to identify a user. Without the use of such cookies, a user would have to provide their login credentials on each page request. The exemption would only apply to first-party session cookies used for this sole purpose and cannot be used for secondary purposes such as tracking or behavioural monitoring.

Persistent authentication cookies are not exempt as a user may assume that the session will end upon closing the browser and not expect to remain 'logged in' upon their next visit to the site. To set persistent authentication cookies, consent would be required. This can often be obtained by providing the option of ticking a box confirming 'keep me logged in' or 'remember me'.

- **Security.**

  First-party cookies used for security purposes can rely on the strictly necessary exemption, for example, where they are used to detect repeated failed login attempts or other similar attempts of system abuse. Security cookies can have a longer lifespan than a session cookie so as to fulfil their security purpose. This exemption would not apply to cookies that relate to the security of third-party websites or services that have not been explicitly requested by the user.

  If device fingerprinting techniques are used for a specific security purpose, then the strictly necessary exemption can also be relied on. However, as with cookies, if the information is processed for secondary purposes - such as those relating to the security of online services the user has not requested – consent is required.

  This also applies where the information is processed for the purposes of fraud prevention, particularly in cases where multiple online services use a single fraud prevention service which processes information from visitors of all of those services.

- **Media player (streaming content) session cookies.**

  Where a service is an online content provider that uses streaming media, then the strictly necessary exemption can be relied on for cookies that relate to the specific video or audio. This is because the streaming media forms part of the service that the user has requested.

  This exemption would, for example, apply to 'flash cookies'[47], which are used to store technical data needed to play back video/ audio content. In a similar manner to cookies used for authentication and security, the exemption may not apply to streaming content hosted by a third party, such as embedded YouTube videos, even those from an operator's own YouTube channel.

[47] In reference to the most commonly used internet video technology today, Adobe Flash, as noted in section 3.2 of this Guidance Note.

7.2 Non-exempt cookies

This section provides examples of cookies which would not fall under one of the exemptions in Regulation 5(4) of the Privacy Regs (see section 7.1 above) and are likely to always require a user's consent

- **Social media plug-in cookies.**

  Website operators will often incorporate social media plug-ins to allow users to 'like' or share content on their social media platforms.

  Users who are 'logged in' may expect to use these plugins as part of their interaction with the social network, and therefore, these cookies can be considered as strictly necessary for a service requested by the user (see section 7.1 of this Guidance Note). However, for users who are 'logged out', including those who are not members of the platform, such cookies would not be applicable, and therefore, consent would be required. Unless a plug-in can be configured to only set cookies on a device used by 'logged in' members, consent is likely required in all circumstances as all visitors cannot be assumed to be members of a social network.

- **Tracking cookies.**

  Tracking cookies are used to track user behaviour and activity across websites and create profiles based on said information for the purposes such as direct marketing, behavioural advertisement, data-brokering, location-based advertising, or tracking-based digital market research. Consent would be required for **all** of these activities due to the nature of the processing and the privacy risks posed to users.

  For example, although location data is not considered to be special category data under Article 9 of the Gibraltar GDPR, it can provide very detailed and potentially sensitive information about a user, including their daily habits, place of residence, place of work and political, religious and/or social engagements.

  Any use of web beacons, tracking pixels, JavaScript code or similar technologies from a social media platform or any other third party is not exempt from the consent requirements.

- **Online advertising.**

  Cookies used for online advertising, including all third-party cookies for purposes such as frequency capping, ad affiliation, click fraud detection, market research, product improvement and debugging will always require user consent.

  Use of device fingerprinting techniques from advertising networks is also not exempt from the consent requirements. It is important to note that users are often unaware that

this processing is taking place and that it involves creating profiles of users across different services over time to serve targeted advertising.

- **Cross-device tracking**.

  Where cookies or device fingerprinting techniques are used to link a user's account with a particular device or devices (for example, as part of the account profile, to provide a second authentication factor or to track users across multiple devices for any purpose – including advertising), consent is generally required. This is because this purpose is generally not strictly necessary to provide the functionality the user requests.

- **Analytics.**

  Analytics cookies are used as a measuring tool by online service providers to collect information and understand how users engage with their website. Whilst they may be considered 'strictly necessary' for the website provider, they are not necessary to provide the service requested by the user and therefore, user consent would be required for both first-party and third-party analytics cookies.

  First-party analytics cookies are not likely to create a privacy risk when they are strictly limited to first-party aggregated statistical purposes and when they are used by websites that already provide clear information about these cookies in their cookie notice and/or privacy notice, as well as adequate privacy safeguards (such as a user friendly mechanism to opt-out from any data collection[48]).

  However, third-party analytics carried out by parties other than the website operator, sometimes for their own purposes, may be considered to represent a greater privacy risk to the user. As such, first-party analytics should be clearly distinguished from third-party analytics, for example, in a cookie notice.

  If device fingerprinting is used for analytics instead of or alongside cookies, it is important to note that doing so is not exempt from the consent requirements either.

[48] See section 6.2, point (b)(iv) of this Guidance Note concerning opt-out mechanisms (i.e. withdrawing consent).

8. COOKIE RULES AND THE GIBRALTAR GDPR

8.1 The relationship between the Privacy Regs and the Gibraltar GDPR

The Privacy Regs provide specific rules in relation to privacy and electronic communications, and where applicable, should be consulted first. However, as noted in the foregoing (sections 4, 5 and 6 above) compliance requires meeting some of the standards set out in the Gibraltar GDPR.

In order to comply with both laws, the following approach may be taken:

(1) For setting cookies (i.e., the storing of information, or access to stored information on user devices), the rules of the Privacy Regs must firstly be complied with, which include providing information[49] to users and obtaining valid consent[50], in line with the requirements of the Gibraltar GDPR; and,

(2) For any processing of personal data resulting from the use of cookies, ensuring that the additional requirements of the Gibraltar GDPR and DPA (where relevant) are complied with. In this regard, the data protection regime is comprehensive, and organisations should ensure they are aware of and can comply with their obligations[51].

IMPORTANT NOTE

Where the setting of a cookie also involves the processing of personal data, organisations will need to make sure they comply with the additional requirements of the Gibraltar GDPR and/or DPA.

Regulation 3 of the Privacy Regs clarifies its obligation to data protection legislation:

"Nothing in these Regulations shall relieve a person of his obligations under the Data Protection Act 2004 in relation to the processing of personal data".

[49] See section 5 of this Guidance Note.

[50] See section 6 of this Guidance Note.

[51] Please see the various guidance notes published by the Information Commissioner in respect of the Gibraltar GDPR and DPA, available here: https://www.gra.gi/data-protection/guidance accessed 19 April 2023.

8.2 What does the Gibraltar GDPR say about cookies?

Under the Gibraltar GDPR, a cookie is considered to be a type of 'online identifier' which, is included within its definition of personal data in Article 4(1).

Recital 30 of the Gibraltar GDPR provides clarification on the term 'online identifier' –

"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. 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."

Examples of other 'online identifiers' include –

- MAC addresses;
- advertising IDs;
- pixel tags;
- account handles; and
- device fingerprints.

As identified in Recital 30 of the Gibraltar GDPR above, such identifiers can leave a 'trace', which in isolation may not constitute personal data. However, when combined with other available information, could be used to create profiles, or identify an individual. For example, if a user can be singled out, inferred, or identified over time, across multiple devices and/or websites, even if the user is not named, the processing must comply with the Gibraltar GDPR and DPA.

Importantly, cookies may not always contain personal data and therefore data protection legislation may not always be applicable. However, the Privacy Regs **will always apply** whether or not the storage of or access to information on user devices involves processing personal data.

8.3 How does cookie consent fit with the lawful basis requirements of the Gibraltar GDPR?

(a) The lawful bases under Article 6 of the Gibraltar GDPR[52].

[52] For further information see the Information Commissioner's Guidance Note (6) Identifying the Lawful Basis, available here: https://www.gra.gi/data-protection/guidance accessed 19 April 2023.

An applicable lawful basis must be relied on to process personal data. The Gibraltar GDPR has six lawful bases, of which one is consent. No lawful basis is more important than the other – the appropriate one depends on the specifics of the processing.

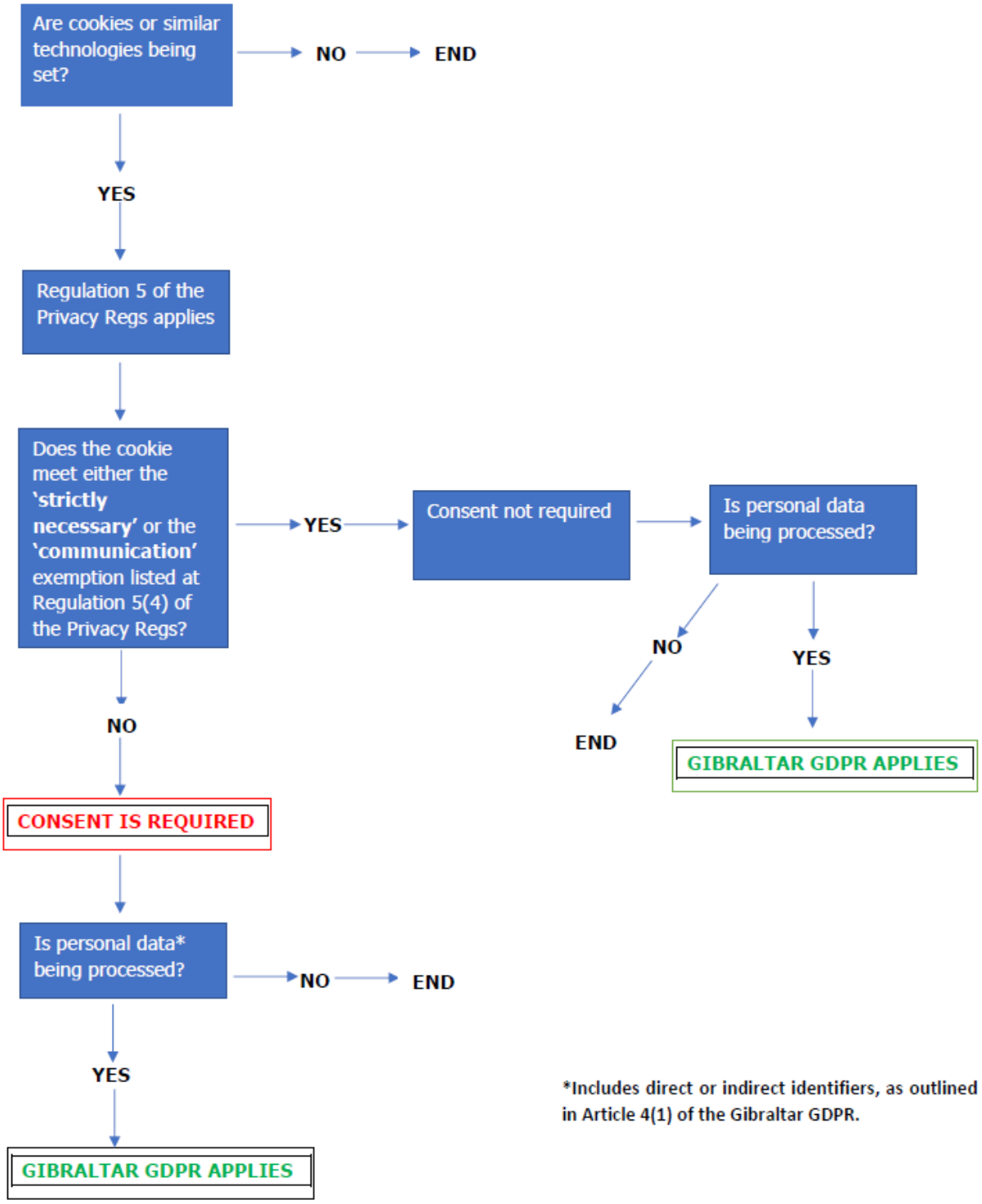
However, the requirements of the Privacy Regs are separate from, and different to, those of the Gibraltar GDPR. If the Privacy Regs require consent for the cookies being set (i.e. they do not fall under the exemptions provided in Regulation 5(4) of the Privacy Regs), then a data controller cannot instead rely on any of the other possible lawful bases provided in Article 6 of the Gibraltar GDPR.

Further, as explained in the foregoing, the standard of consent must be of that required by the Gibraltar GDPR and is the case whether or not personal data is involved. If consent has been maintained in compliance with the Privacy Regs, then in practice, consent is also the most appropriate lawful basis under the Gibraltar GDPR.

If a cookie meets one of the exemptions provided in Regulation 5(4) of the Privacy Regs, then the requirement to have consent to set it does not apply – essentially, the technical process of storing or accessing information on the device falls out of the Privacy Regs and, where personal data is involved, the Gibraltar GDPR then applies.

Figure 1 below demonstrates consent and data protection obligations for cookies.

FIGURE 1



*Includes direct or indirect identifiers, as outlined in Article 4(1) of the Gibraltar GDPR.

(b) Article 9 of the Gibraltar GDPR[53].

Processing special categories of personal data, including such data which has been derived from cookies, is subject to stricter rules under the Gibraltar GDPR. Article 9 of the Gibraltar GDPR defines special category data as –

> *"… personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."*

Article 9 of the Gibraltar GDPR generally prohibits the processing of special category data unless one of the conditions stipulated in Article 9(2) of the Gibraltar GDPR apply. In this respect, the only likely legal basis for processing any special category data obtained using cookies is the **explicit consent** of those users whose data is processed. This would be in addition to identifying an Article 6 lawful basis.

It is important to note that there is a particularly high standard to meet for data controllers to be able to demonstrate that explicit consent has been obtained, which is unlikely to be met by the provision of generic information contained within a cookie banner[54].

8.4 Personal data obtained from cookies

The Privacy Regs do not provide specific rules for prior or subsequent processing involving the information obtained from the storing of information, or accessing information stored, on user devices. Therefore, for subsequent processing involving personal data, it may be possible to rely on a lawful basis other than consent, depending on the type of processing[55].

Notwithstanding, in certain cases, the subsequent processing of personal data that follows, or is dependent on the setting of cookies, is again, highly likely to require consent as the lawful basis, particularly if the processing involves sharing the collected data with third parties. This is not solely due to the personal data originating from the use of cookies but also due to the nature, scope, context, and purpose(s) of the processing itself, such as that involving the analysing and predicting preferences of behaviour, tracking or profiling for direct marketing and advertising. This means that users must be informed, and consent must be obtained prior to further processing.

[53] Ibid.

[54] See section 3 of the Information Commissioner's Guidance Note (13) Guidance on Consent, available here: https://www.gra.gi/data-protection/guidance accessed 19 April 2023.

[55] For further information see the Information Commissioner's Guidance Note (6) Identifying the Lawful Basis, available here: https://www.gra.gi/data-protection/guidance accessed 19 April 2023.

8.5 Data Protection Impact Assessments

The Information Commissioner has published a list of processing operations for which a data protection impact assessment (a "DPIA") is mandatory[56]. This includes processing personal data involving the tracking of an individual's location or behaviour, including online activity, when this is combined with any of the criteria set out in EU guidelines (i.e., the Article 29 Data Protection Working Party criteria for 'high risk' processing[57]).

Further, it is noted that said criteria includes large scale processing of personal data and the combining, linking, or cross-referencing of separate datasets. In this regard, it is acknowledged that the tracking of online activity (i.e., the profiling or behavioural analysis of individuals online), is likely to involve one or both of these additional operations. Therefore, if the processing of personal data involves said tracking and either of these operations, on foot of the use of cookies or otherwise, it is likely that a DPIA must be carried out.

9. COMPLIANCE

The Information Commissioner's aim is to ensure that organisations comply with the law. However, in cases where the organisations refuse or fail to comply voluntarily, the Information Commissioner has a range of powers available under Part VI of the DPA for taking formal action where this is necessary[58].

These powers will apply in the context of the Privacy Regs, as stipulated in Regulation 31(1) -

"*The provisions of Part VI of the Data Protection Act 2004 shall have effect in relation to these regulations as they have effect in relation to the Data Protection Act 2004: and for these purposes, Part VI shall be read with any modifications necessary to give effect to this regulation.*"

[56] See section 3 and Annex B of the Information Commissioner's Guidance Note (4) Data Protection Impact Assessments (DPIAs), available here: https://www.gra.gi/data-protection/guidance accessed 19 April 2023.

[57] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' adopted on 4th April 2017 as last revised and adopted on 4th October 2017, available here: https://ec.europa.eu/newsroom/article29/items/611236 accessed 19 April 2023.

[58] For further information see the Information Commissioner's Guidance Note (9) Guidance on Information Commissioner's Regulatory Action, available here: https://www.gra.gi/data-protection/guidance accessed 19 April 2023.

ANNEX A

To conduct a cookie audit, organisations should -

- for cookies that are already present, identify those that are operating on or through their website, using a combination of browser-based tools and server-side code review;
- confirm the purpose(s) of each of the cookies used (or those intended to be used);
- confirm whether cookies are linked to other information held about users – such as usernames – and whether the use of cookies also involves (or will involve) processing personal data;
- identify what data each cookie holds or otherwise processes;
- confirm the type of cookie, specifically whether this would be a session or persistent cookie;
- distinguish between which cookies are strictly necessary and which ones are not (and would therefore require clear and comprehensive information and consent);
- ensure that the consent mechanism enables users to control the setting of all non-essential cookies;
- determine the lifespans of any persistent cookies and whether these durations are justifiable for the stated purpose;
- determine whether each cookie is a first or third-party cookie, and if it is a third-party cookie who is setting it;
- double check that the cookie notice provides accurate and clear information about each cookie;
- confirm what information is shared with third parties, and what users are told about this; and
- document findings and follow-up actions and build in an appropriate review period.

IMPORTANT NOTE

This document is purely for guidance and does not constitute legal advice or legal analysis. All organisations that process personal data need to be aware that the Gibraltar GDPR and the DPA may apply directly to them. The responsibility to become familiar with the Gibraltar GDPR and the DPA and comply with its provisions where applicable lies with the organisation.

Where necessary, the Information Commissioner will review this Guidance Note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Guidance Note and the Privacy Regs, the Gibraltar GDPR and the DPA, the Privacy Regs, the Gibraltar GDPR and the DPA will take precedence.

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
privacy@gra.gi
www.gra.gi