DIGITAL MARKETING AND ADVERTISING GUIDANCE

Gemserv

1. PURPOSE OF THIS GUIDANCE

This guidance outlines recommendations and best practices for performing digital advertising and digital marketing. Digital marketing and advertising can take many forms, including online advertising and marketing via social media platforms. They can also involve behavioural tracking, geolocation tracking and profiling of users, in order to categorise them as a person likely to buy a certain product or service and serve them with targeted or retargeted advertisements on various platforms.

While the GDPR is applicable to all processing activities, the Directive on Privacy and Electronic Communications, better known as the ePrivacy Directive, or as the "Cookie Directive", is specifically applicable to all electronic communications, i.e. to internet, telephone and mobile networks providers and to data transferred on such networks (including digital advertising). It also sets the rules regarding unsolicited electronic communications (or direct marketing) and data stored on users' end devices, especially cookies, hence the name of the directive.

The ePrivacy Directive was a complement to the old Data Protection Directive and should have been updated at the same time as the GDPR with the ePrivacy Regulation (Regulation on Privacy and Electronic Communications). Like the GDPR, the ePrivacy Regulation will be directly applicable, instead of having to be transposed into national law. The current legal framework in the UK has an upper limit of £500.000 fine for a breach of ePrivacy, but this will be aligned with the 4% or €20 million of the GDPR with the new text. A recent major change brought in UK law is that the £500.000 fine can now directly be levied against directors of breaching organisations.

Although the new ePrivacy Regulation is not expected to be applicable before 2020, there has been a lot of changes in the area worth considering. Indeed, European Data Protection Authorities and courts are aligning their case law with the GDPR and the future ePrivacy Regulation.

For the purpose of this guidance, "consent" is understood as defined by the General Data Protection Regulation, i.e. freely given, distinct, specific, informed and unambiguous, by a statement or by a clear affirmative action. Additionally, it is now settled that different purposes must be separated and presented under different consent mechanisms for consent to be compliant.

2. DIGITAL ADVERTISING

Digital advertising in itself does not violate any data protection requirement. However, the method by which the digital advertising is performed may generate significant privacy concerns.

A) TARGETED ADVERTISING

The mandatory rule is that you need consent to track users online, including when performed in order to target advertisements at them. In general, you will need consent for various types of tracking. However, once consent has been gained, the former Article 29 Working Party (now the European Data Protection Board) has outlined that users will permissibly be able to be targeted and retargeted with advertisements for the duration of the cookie, which should last no more than 1 or 2 years.

Any tracking that uses online identifiers will require consent, as online identifiers have the capacity to identify a single individual and are considered personal data under the GDPR. Online identifiers can include, among others:

- Cookie identifiers;
- IP addresses;
- MAC Addresses (including Wi-Fi and Bluetooth);
- Device identifiers (UID);
- Canvas fingerprinting; and
- Pixel beacons, unique URL and similar technologies.

Such data can be collected after getting consent through pop-up notifications and banners on websites, mobile applications and otherwise on mobile devices, such as through cookie consent mechanisms, which are considered further below. However, where the use of such identifiers is necessary for technical purposes (aside from advertising, for the website or the application to work correctly), the collection of such data does not need consent, where performed by the website or application publisher itself.

Users must be made periodically aware of such monitoring, and in any case at the first time of visiting the website or at the first use of the mobile application, through a Privacy Notice, a banner or other pop-up mechanism. Such information must come from the publisher, advertiser and other parties users have contact with when browsing online or using a mobile application. This information must contain a list of all personal data processed during the advertising, a description of the monitoring, and a list of any other third parties involved in tracking and/or advertising, with a link to their own privacy notices.

B) PROFILING

Digital advertising often relies on profiling of users in order to serve them with targeted advertising. On top of the requirements for online tracking above, several other restrictions apply in this case.

The tracking involved in digital advertising often involves profiling, whereby users' interactions with websites and pages are tracked to categorise them into demographic sets based on what they view and interact with. In addition to the collection of identifiers, this can involve the collection of the following information:

- Behavioural data (including demographic data); and
- Tracking information (including browsing history, page or application interactions and geolocation data).

Where profiling is used, it must be made clear and transparent for websites and mobile applications users. A Privacy Notice or Cookie Consent notice must sufficiently detail the logic – and steps – involved in the online advertising/profiling process. Users must also be able to consent to such profiling through the publisher's or advertiser's website and/or through the use of cookies or any other personal data you require for profiling purposes. It is important to ensure that all bought data sets used for creating profiles are adequately consented. In particular, you should identify what is covered by the consent, if any, to any bought in lists you import or rely upon. You are not able to rely on legitimate interest to profile and/or provide advertising to users you have had no contact with.

Moreover, where you match and/or collect data from public sources and use this to profile and/or engage in online advertising to them, the Information Commissioner's Office (ICO) has indicated that this requires consent. This will include matching data found on social media or in the public domain with names or other personal details you already have, in order to target them or advertise to them. This will include uploading any lists to social media platforms such as Twitter or Facebook (for instance Facebook Custom Audiences).

You must also exclude using any sensitive data (such as ethnic or racial origin, religion, political opinions, health, disability, and sexual life or orientation), especially if collected through behavioural data or tracking information, from automated processing involved in targeted advertising, as it cannot be permitted without specific and explicit consent.

Moreover, we strongly recommend avoiding targeted advertising performed using the personal data of children – i.e. those below the age of 13 in the UK (and up to 16 in some Member States), as this requires verifiable parental consent, which is extremely difficult to demonstrate in practice in the context of digital advertising.

3. COOKIES

If digital advertising or tracking of users is performed via cookies, you will have to ensure that the appropriate consent is sought for the use of these cookies. The users of your website will have to specifically accept your cookies.

Cookie consent must be arranged by the cookie publisher. This means that the publisher (the website hosting the cookies) will have to show a cookie banner or pop-up notification at the first visit to ensure that users are informed and consent to the use of such cookies.

Cookies are subject to the ePrivacy requirements, which stipulates that consent is mandatory for all non-essential cookies. Cookies that do not need consent include those necessary for a website to work correctly, i.e. security cookies, password authentication cookies, multimedia content player cookies and session cookies (e.g. session cookies that remember a user's selected items for purchase when logged into an e-commerce website).

Cookies that are not 'essential' require consent. Common cookies that need consent can include:

- Any cookies that remember users outside of their session;
- Cookies counting the number of unique visits made by a user;
- Cookies that track a user's behaviour on pages;
- Cookies that remember purchases beyond their log-in session;
- Cookies used to deliver targeted advertising, including by third-parties; and
- Most third-party analytics cookies (e.g. Google Analytics and Facebook Open Graph).

Any cookies that collect a user's IP address or other unique identifiers will also need consent. However, cookies used to remember that a previous visitor disabled cookies are permissible without specific consent.

Additionally, certain pixels that track a user's activity on a website and record this information against a unique identifier for that user will require consent.

Even if implied consent is still used by many websites, the Cookie Directive was updated in May 2011 to include that consent of users was required prior to using cookies. The major change brought by the GDPR is that consent must now be understood as GDPR compliant consent, i.e. freely given, distinct, specific, informed and unambiguous, by a statement or by a clear affirmative action. This means that cookies banners must now collect visitors' consent.

Before processing data for or in relation to cookies and more specifically for marketing purposes, you must ensure that the indication of consent you receive is unambiguous and involves a clear affirmative action from individuals. This will include:

- unbundling consent for the specific use from your other terms and conditions;
- not using pre-ticked opt-out boxes;
- ensuring that you provide clear information about your organisation and its practices; and
- ensure that individuals are able to specifically consent to each separate use.

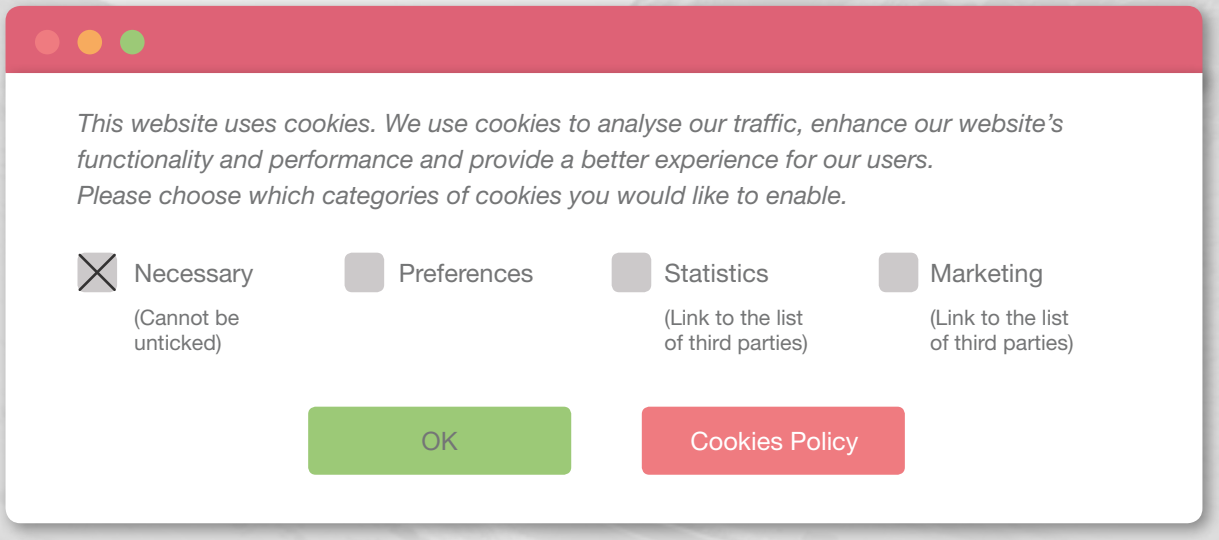
Under the Privacy by Design principle, this must be developed in the design of the website. For example, a website publisher will be compliant by not switching on any cookies unless the person clicks 'Accept' for each category. The GDPR now requires an affirmative action, so users will have to click or tick something. Additionally, simply having a cookie policy which you ask visitors to agree to is not sufficient, as consent must not be linked to the use of a service, such as a website.

Cookies and data collection must not be started before a user gives their consent. Cookies stored for the purposes of digital advertising should not be stored for longer than a set duration period – such as one or two years, and additional cookie consent should be requested after this period.

Additionally, where data collected through cookies is passed to a third party, the website publisher should make this evident in their Privacy Notice – this includes Google Ads, Google Analytics or Facebook Open Graph, for example.

EXAMPLE

Upon visiting a publisher's website, a user should be presented with a cookies pop-up or a cookies banner, of a size such as to cause a perceptible discontinuity in the user's experience, containing the following:



4. ONLINE MARKETING

For your business-to-consumer direct marketing activities via email, you must consider that in most cases, you need affirmative consent, as defined by the GDPR. It is only when you have an existing customer that you can rely on legitimate interest (i.e. opt-out), providing the following conditions:

- You only advertise for similar products or services that your customer bought; and
- You have provided a simple way to your customer to opt-out to such communications from the beginning of your relationship, and in every marketing communication after.

Whether you rely on consent or on legitimate interest, opt-outs must be clear and specific and communicated at the time of the event, as well as every subsequent communication. Opt-outs must be granular, meaning users must be provided with an opt-out for each specific form of activity – data collection, profiling, cookies, etc.

'Marketing' is construed widely and includes any promotional materials, newsletters and/or updates that you will send.

Messages sent via social media platforms are considered direct marketing, and, as such, will have to comply with the ePrivacy requirements, i.e. you need consent or an existing customer relationship to send such messages. For instance, you will be able to carry out marketing via private messages on social media where such users have specifically signed up to your page or group, for example.

You are also able to reply to individuals who message you with regard to an inquiry for your products and services without necessarily asking for consent and may rely on legitimate interest to reply and for sending such communications.

Additionally, where you are contacting customers for business-to-business marketing communications, i.e. to their business accounts, you may rely on legitimate interest for sending such communications. This will potentially be amended by the ePrivacy Regulation, so you must follow the changes to update your practices accordingly.

When engaging in marketing on social platforms, you will have to comply with the GDPR provisions for processing personal data, including to provide users with a Privacy Notice. You will also have to comply with the specific and granular consent requirements.

Companies wishing to collect the details of website users online, including across social media platforms, must gain proper consent before doing so.

5. REFERRALS

Many online marketers may want to use referrals to incentivise website users or potential customers to view or buy their products/services. This could include having a 'mention me' benefit as part of their loyalty programme and encouraging customers to refer a friend.

Companies engaging into referrals should ensure the following dos and don'ts:

- Do not incentivise referrals where users themselves are responsible for passing on information, including marketing information, to the referred person;
- Users on Facebook, for example, are be able to share information or posts of yours on Facebook, which Facebook might notify their other friends about Therefore, you should attach the following notice: "by clicking this button you agree that your referred friend has consented to receive this message/post";
- You must ensure that you do not contact referred friends directly until they have signed up or contacted you – so you must not have any contact with them until they contact you. As such, you must also not ask the referring friend for the details of their friends to process and/or contact them – as you will not be able to do this on the basis of legitimate interest, and obviously will not yet have their consent; and
- Referred friends should only be contacted by getting them to email you or sign-up directly. You cannot encourage users to submit their friends' contact details directly, as you will not able to contact them without consent. Even if the referring customer alleges that they have their friend's consent, given the high level of consent required under the GDPR, this is unlikely to be possible to demonstrate.

You will not be able to use such details for targeted advertising, as you cannot establish a legitimate interest in doing so (having previously had no contact or relationship with such individuals).

CONTACT US

E: bd@gemserv.com
T: +353 (0)1 669 4630
W: www.gemserv.com
@gemservireland

Ireland Office
Fitzwilliam Hall Business Centre
Fitzwilliam Place
Dublin 2

London Office
8 Fenchurch Place
London
EC3M 4AJ
Company Reg. No: 4419878

Gemserv