DATA PROTECTION IN 2018

Are businesses complying with the GDPR?

MACEDO VITORINO & ASSOCIADOS
Sociedade de Advogados, RL

Are businesses complying with the GDPR?

At the end of 2018, we visited many Portuguese Internet websites of some large and not so large businesses to check if they complied with the General Data Protection Regulation (GDPR) and the European regulation on privacy and electronic communications proposal («e-Privacy» regulation proposal).

While the GDPR is the general regulation for processing of personal data, the «e-Privacy» regulation aims to update the «e-Privacy» Directive[1] and addresses data privacy in the electronic communications sector, including email and SMS messages and also services like WhatsApp, Facebook Messenger and Skype, along with Internet of Things (IoT) devices.

In our review, we found several examples of unlawful practices or, at least, non-recommended practices in violation of the GDPR and potentially contravening the «e-Privacy» regulation proposal.

Unfortunately, several Internet websites still use pre-ticked boxes of consent and third-party cookies without appropriate consent, which are both expressly prohibited by the GDPR.

As almost everyone knows, cookies are small text files that are placed by a website operator on an user's device (e.g. user's laptop or mobile device) when an user accesses a website. In general,

[1] The proposed revised text for the E-privacy Directive was published on 10 January 2017 by the European Commission. This directive has been implemented into Portuguese laws by Law 41/2004, of 18 August 2004, as amended. Although the «e-Privacy» regulation proposal may still have changes before, it should come into force in 2019.

cookies are used to remember users' preferences and improve the website's performance. From the end-user privacy point of view, cookies may be non-intrusive or privacy-intrusive.

Non-intrusive cookies, e.g. session cookies, users' preferences cookies, or load-balancing cookies do not require prior consent. Privacy-intrusive cookies, such as cookies for tracking activity on social networks or third-party cookies (that are placed by parties other than the owner of that website, e.g. Google Analytics) when used for behavioral advertising, market research or analysis, require prior consent.

Privacy-intrusive cookies may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used for profiling and identifying individuals. In these cases, the use of cookies are subject to the «cookie consent rule» and must fulfil the requirements laid down in the GDPR: be a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the individuals' agreement to the processing of their personal data; silence, pre-ticked boxes or inactivity do not serve as consent.

On some well-known Portuguese news websites, default settings for cookies – «ACCEPT ALL COOKIES» – are still used. When we visit these websites, the user is giving his/her consent for all the cookies, including third-party cookies and other tracking technologies, by simply clicking on the «ACCEPT» button.

When the user does not wish to consent to the use of certain cookies, he/she has to follow lengthy and complex steps. Firstly, the user has to click on a link «SEE DETAILS», which cannot be easily found. Then, the user must go to a new page of the website and cancel his/her consent for each type of cookies that are listed on pre-ticked boxes. If the user wishes to refuse some of the cookies, he/she will need to take out each of the pre-ticked boxes. The user cannot tick the boxes of the cookies he/she wants to accept, he/she must untick the boxes that he/she does not want.

This practice, still used in many websites, is in clear violation of the GDPR's prior consent requirements.

On a website of a retail company, we read the following: "*By continuing to browse our website, you accept the use of our cookies and tags to propose you personalized offers, sharing functions for social networks, personalization of the contents of the website and audience analytics. Some information may be shared with our partner* [...]. *For more information and setting of cookies, click here. Accept.*"

This website also uses pre-ticked consent boxes for privacy-intrusive cookies in violation of the GDPR's consent rules.

The use of pre-ticked boxes aims to discourage end-users from selecting the highest privacy levels. This is a general practice used in many Internet websites, which do not include information on the risks associated with privacy-intrusive cookies, including long-term browsing history records and the use of such records to send targeted advertising.

We also found some good examples. There are Internet sites that correctly provide information on the types of cookies used and where consent is clearly and accurately requested.

For instance, the website of one of Portugal's main TV channels informs the user, in its home page, about the use of cookies by the channel's digital platforms. In this case, the cookies' consent button is explicit.

The website also makes it clear for users the difference between the use of non-intrusive cookies that are able to ensure basic and essential features of the digital platform, with a pre-ticked box, and the use of other features that require a prior consent from the user by selecting each privacy-intrusive cookies.

Another good example of a compliant website is the disclaimer in a local bank's website informing about risks associated with cookies, which states: "*This website uses cookies to provide you with a better browsing experience. To learn more about cookies, their relevant purposes and how you may manage them, please see our cookie policy. [...] does not use on its website at www.[...].pt advertising cookies nor sharing information with third party websites.*"

This disclaimer is short, clean and clear. This website does not use privacy-intrusive cookies. The website's cookies policy states that cookies do not allow the user to be identified and that cookies are only used to communicate a message through an electronic communications network and/or to provide an information society service expressly requested by the user.

We note that when the use of cookies allows the website owner to identify an individual, to trace his/her profile or to analyze his/her behavior, the user's consent must comply with the GDPR's requirements and the new electronic privacy rules which will enter into force in 2019 when the «e-Privacy» regulation is expected to be approved.

Recital (24) of the proposed «e-Privacy regulation states "*For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to* [the] *internet* [to ensure] *that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and [are asked] to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated* [with] *allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to*

send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed."

Another matter which justifies special attention, following the entry into force of the GDPR as well as under the upcoming «e-Privacy» rules, is the use of electronic communications for direct marketing purposes, such as emails, SMS, MMS, Bluetooth, etc..

According to the GDPR, direct marketing communications (and the processing of electronic contact details) may be justified by the service providers legitimate interest in the context of a relationship with their customers for the sale of its own similar products or services. In these cases, the prior consent of the customers is not required. However, service providers must ensure that the customers are clearly and distinctly given the right to object, free of charge and in an easy manner, to such use. Service providers must give their customers the right to object, that is the right to withdraw their consent to the use of data for marketing services, at the time when they are collecting the date and in every message that they send.

The legitimate interest may be only used as a lawful basis for processing the customers' contact details if such contact details have been collected in the context of a prior relationship with the customer. The service provider, who collects customers' contact details, may not disclose, without the customer's prior consent, data to third parties, including companies whose business activity is the purchase of databases. This also applies to electronic communications sent by non-profit establishments carrying out their own purposes, as well by non-profit associations and foundations.

This means that, in many cases, it is not required to request consent from existing customers. Unfortunately in the months before the GDPR came into effect many of us were bombarded with emails and SMS requesting consent to use the personal data, which was a nuisance to customers, had poor results and was useless.

Those businesses that requested consent that was not required by the GDPR, were obliged to delete contact details of customers who did not give or renew consent, even if the data processing could be justified on legitimate interest grounds. The rules cannot be changed in the middle of the game and the silence or refusal of customers to give consent meant that businesses had to delete the data.

Whether a legitimate interest exists or not, it is still very common, even after the «consents' fever», for businesses to send SMS and emails for direct marketing without a prior relationship with the addressee or without prior consent. The use data for legitimate interests, such as the advertising of products and services to existing customers, is in many cases abused by service providers, particularly by utilities companies, which do not give the customers the option to withdraw their consent.

As said, at the interplay level between the GDPR and electronic privacy rules, where personal data are processed for direct marketing purposes, users have the right to object at any time to personal data processing for marketing – the «opt out» right.

The legal terms of a retailers website warns the user that despite having objected to the use of user profiling cookies, he/she will continue to receive marketing communications.

This warning is illegal under the GDPR. For the user to exercise a full opt-out right and to stop receiving communications for marketing purposes, including for profiling, the user cannot be forced to take a second opt-out step as stated in that website.

As a rule, the website owner should give its customer or visitor the option to a full opt-out and then allow the user to select the forms of marketing and product offers that he/she is interested in receiving.

This is possibly one of the main reasons why many users continue to receive many instant messages and emails of direct marketing campaigns, despite having opted-out from customer databases.

In many cases, the message sender does not give any information on how to opt-out, especially in SMS marketing. It is also usual for SMS not to have sufficient information regarding the sender or give an inaccurate or unusable identification number and contact information.

Unsolicited marketing messages must be clearly identifiable as such and must provide the relevant sender's details or on behalf from whom the message is sent and the information necessary for the user to opt-out from new marketing messages.

In short, although several companies have adequately implemented the GDPR, others have not done so. We believe that businesses, even those that believe that they are compliant with the law, should review their data protection and privacy procedures and adopt more stringent policies.

Recent examples in Portugal and abroad show that data protection authorities are investigating claims for data protection violations and will apply fines to those businesses that do not comply with data protection and e-privacy rules. There is still a long way to go for businesses to comply with the GDPR. The new «e-Privacy» rules will increase the regulatory pressure. To avoid falling in the hands of data protection authorities, businesses must take more effective measures to protect the privacy of their customers.

In today's competitive global market, Macedo Vitorino & Associados can provide a comprehensive commercial and corporate law advice to domestic and foreign clients.

Macedo Vitorino & Associados has a truly international practice. We have strong relationships with many of the leading international firms in Europe, the United States and Asia, which enable us to handle effectively any cross border legal matters.

Since the incorporation of the firm we have been involved in several high profile transactions in all of the firm's fields of practice, including banking and finance, capital markets, corporate and M&A, corporate restructurings, *etc.*.

The multidisciplinary and integrated character of our corporate and commercial group allows us to efficiently solve the legal issues of our clients, in particular:

- **Contract law**
- **Dispute resolution**
- **Employment**
- **Formation of joint ventures**
- **Finance**
- **Foreign investment**
- **Incorporation of companies and registration of branches**
- **Property law**
- **Tax**

We are ranked by The European Legal 500 in most of its practice areas, including Banking, Capital Markets, Project Finance, Corporate and M&A, Tax, Telecoms and Litigation. Our firm is also mentioned by IFLR 1000 and by Chambers and Partners in Banking, Corporate and M&A, TMT, Dispute Resolution and Restructuring and Insolvency.

If you want to find out more about us please visit our website at www.macedovitorino.com

Rua do Alecrim 26E – 1200-018 Lisboa – Portugal
Tel.: (351) 213 241 900 – Fax: (351) 213 241 929
www.macedovitorino.com