SIGN UP

PANGEANET

INTERNATIONAL NETWORK OF INDEPENDANT LAW FIRMS

VISIT OUR WEBSITE

NEWSLETTER 2

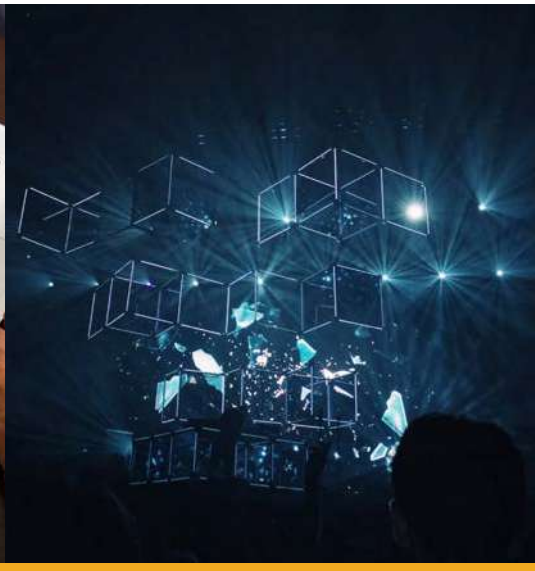
November 2020

DATA, INFORMATION & CYBER LAW

The Pangea DICL team is an international group of experienced and specialised lawyers dedicated to privacy, cybersecurity and open data issues. We support your digital transformation and guide you in the protection, use and defence of your immaterial assets from a legal perspective.

A multi-jurisdictional experts approach

A group of specialists familiar with their respective local laws and customs



A real curiosity and appetite for the latest technological developments & phenomena

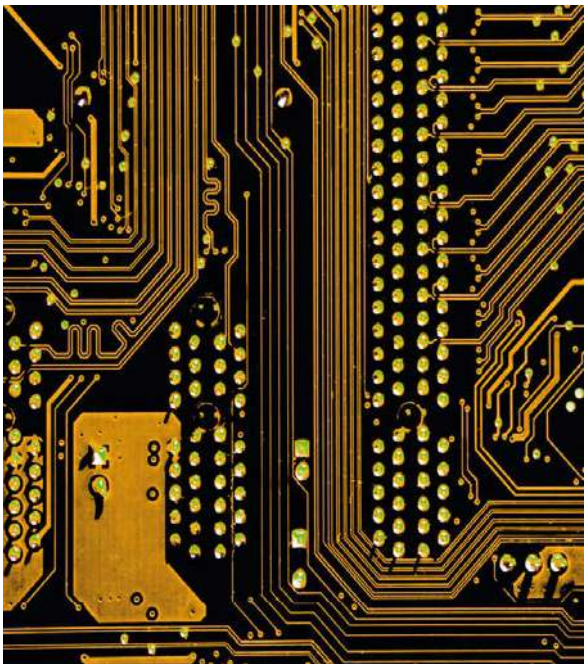
EDITORIAL

ADTECH - DIGITAL MARKETING IN THE CONTEXT OF DATA PROTECTION REGULATIONS

PangeaNet is an association of independent law firms from over 25 countries forming an international law firm network. The Pangea Practice Group for Data, Information and Cyber Law consists of experts in IT and data protection law from around the world. In its bi-annual newsletter, the practice group provides information on relevant topics in this area such as current developments, national privacy regulations and the activities of regulatory authorities, as well as legal aspects of new technologies.

While the first newsletter of the Pangea Practice Group for Data, Information and Cyber Law in May 2020 was dedicated to the European General Data Protection Regulation (GDPR) on its second « birthday », the current newsletter deals with the topic of Advertising Technology (« AdTech »). AdTech software enables companies to effectively advertise online and to address (potential) customers in a targeted manner, making it an important part of corporate marketing today. Digital marketing measures include search engine optimization, the analysis of user behavior on websites, and the placement of personalized online advertising, as well as the distribution of e-mails with advertising content.

The analysis of user behavior on websites offers companies valuable information for targeted marketing. The various tools offered on the market often employ cookies to recognize a user. The European Court of Justice (ECJ) decided on 1 October 2019 that the required active consent of a user to set technically unnecessary advertising and tracking cookies cannot be obtained via a pre-activated checkbox (ECJ, judgement of 1 October 2019, Ref. C-673/17).



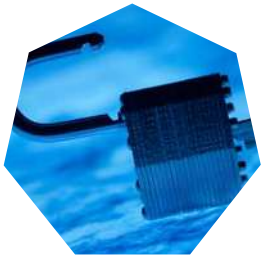
The requirement of consent for the use of tracking and advertising cookies, along with other regulations of the GDPR and national data protection regulations, restrict companies in their use of AdTech. It is the task of the companies concerned to take measures to protect the privacy of the individual so that they may be able to effectively benefit from a digital marketing approach to customers within this framework.

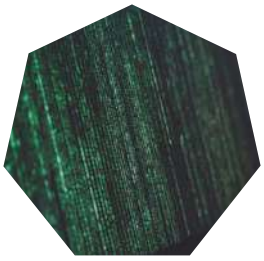
In order for this newsletter to provide a comprehensive insight into the topic of AdTech and the legal framework surrounding it, Pangea members from various countries have prepared relevant questions from their national perspectives and summarized the national requirements and special aspects in individual articles. In addition, the advertising agency u+i interact GmbH & Co. KG, drawing on practical experience, reports in a separate article on how AdTech can be used in companies and the challenges it poses.

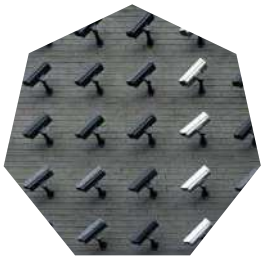
The Pangea Practice Group for Data, Information and Cyber Law hopes you enjoy reading this newsletter, and looks forward to any feedback or questions you may have.

Dr. Sebastian Meyer
BRANDI Rechtsanwälte

Index







AdTech in Austria

The digital advertising market has been growing strongly in the past years. Personalized advertising is crucial for its efficiency. This is supported by AdTech, which stands for advertising technology and refers to various types of analytics and digital tools used in connection with online advertising.

The Telecommunications Act (TKG 2003, Federal Law Gazette I No. 70/2003 as amended in order to implement the ePrivacy Directive 2002/58/EC) provides an important legal framework for AdTech in Austria and as lex specialis takes precedence over the Data Protection Act and the GDPR.

Cookies

According to § 96 Para 3 TKG 2003, operators of public communication services and providers of an information society service are obliged to inform the subscriber or user which personal data they will process, on what legal basis and for what purposes this will be done and for how long the data will be stored. It is only permissible to obtain these data if the subscriber or user has given his consent.

It has to be stressed, that legitimate interest in the sense of Art 6 Para 1 lit f GDPR can be used as a legal basis for the processing of personal data. However, this legal basis is generally unsuitable for the use of cookies, because § 96 Para 3 TKG 2003 only mentions the consent of the user and does not know a legitimate interest. The storage of cookies is only exempt from the obligation of consent if the cookies are absolutely essential in order to provide a specific service expressly requested by the user (such as cookies that are technically indispensable for the operation of an online store or online banking). However, these cookies may also only be stored for as long as they are imperative for this service.

All other cookies and in particular tracking, advertising and analytic cookies must only be set after the user's consent was obtained.

The TKG 2003 does not provide any further conditions or a definition for consent. The term « consent » under § 96 Para 3 TKG 2003 is therefore systematically interpreted in the same way as the term « consent » under Art. 4 para 11 and Art. 7 GDPR. The CJEU recently stated in its decision C-673/17, Planet49 GmbH, that the setting of cookies requires an active consent of the internet user and therefore preset « checkboxes » or « browse-wrapping » are not suitable options for a valid legal consent.

Direct marketing

In the case of electronic communication with a data subject, the provisions of the ePrivacy Directive, which have been implemented in Austria for the sending of e-mails in § 107 Paras (2) to (5) TKG 2003, must be observed. The scope of application of § 107 TKG 2003 is broader than that of the GDPR, as it makes no difference from the point of view of telecommunications law whether legal or natural persons are advertised by e-mail. The sending of advertising e-mails from companies to consumers and to commercial customers, is always subject to § 107 Para (2) TKG 2003 which provision generally prohibits the sending of electronic mails for the purposes of direct advertising (item 1) or if it is addressed to more than 50 recipients (item 2) without the prior consent of the recipients.

In some cases, electronic messages can be sent without the consent of the recipient of the advertising. For this purpose, however, all criteria according to § 107 (3) TKG 2003 must be met cumulatively:

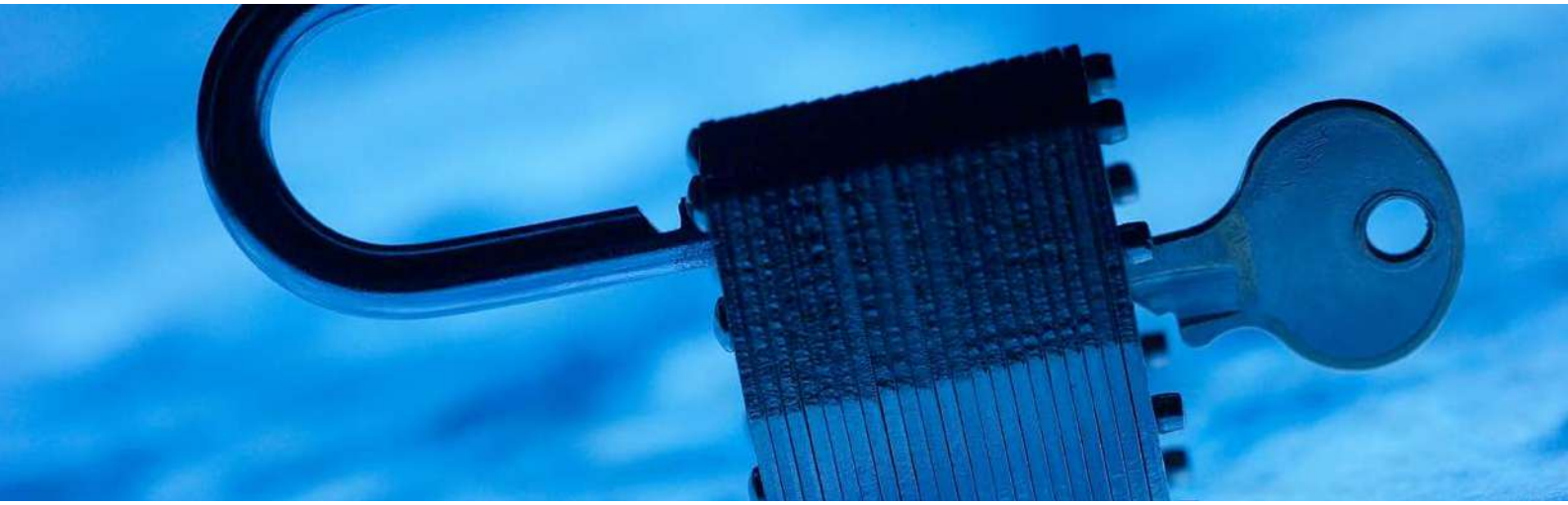
1. The sender has received the contact information for the message in connection with the sale of goods or provision of a service to his customers

2. the message is used for direct advertising for own similar products or services

3. the recipient has been clearly and unambiguously given the opportunity to refuse such use of the electronic contact information at the time of its collection and additionally at each transmission free of charge and without any problems

4. the recipient has not rejected the sending from the outset, in particular by registration in the list referred to in § 7 para. 2 of the E-Commerce Act (« ECG »)

In practice, the existence of the requirement that the company must provide its own similar products or services (§ 107 Para (3) item 2 TKG 2003) - with which the customer is advertised electronically - is particularly problematic. Own products and services are only those which are sold or provided by the sender himself. In addition, there must be a similarity to the product or service sold respectively a certain degree of similarity in the design or function of the products from the perspective of the customers addressed.



In many cases, the exemption of § 107 (3) TKG 2003 does not apply, because the advertiser was not given a clear opportunity to object to such use of his e-mail address when the data was collected.

Finally, a data subject has always the absolute right of objection to direct marketing and profiling according to Art. 21 Para 2 GDPR. Such objection has to be observed by the advertiser, whose legitimate interests to advertise are considered to weigh lower than the rights of the data subject not to be addressed by direct marketing.

Summary: Anyone wishing to use the advantages of AdTech in a legally effective manner not only must understand the underlying technical processes but also has to obtain informed consent from the data subjects. Consent is always required for the use of tracking and advertising cookies, they can never be justified by a legitimate interest of the advertising company. The sending of electronic advertising e-mails without consent is illegal irrespective if the recipient is a private or commercial addressee. Permissible exceptions from this rule may apply to existing customers under specific conditions.

Barbara Kuchar & Anna Mertinz
KWR Karasek Wietrzyk Rechtsanwälte GmbH

• BELGIUM

A Belgian perspective on AdTech and digital marketing in a world of data protection legislation

Digital marketing runs on the use of AdTech tools these days. This technology allows advertisers to better connect with and target their customers and prospects. As digital marketing and AdTech are based on the use of online tracking tools (such as cookies) and personal data, we must acknowledge that the digital marketing industry is challenged by European and national data protection laws.

The impact of the General Data Protection Regulation on the booming digital marketing industry caught the attention of the Belgian Data Protection Authority. Digital marketing is one of the priorities in the « Strategic Plan 2020-2025 » of the Authority, where the objective is to provide an interpretation of the applicable rules on personal data processing for direct marketing purposes. This objective was achieved by the publication of the Authority's Recommendation nr. 01/2020 of 17 January 2020.

The Recommendation provides detailed guidelines, illustrative examples and key concerns about how advertisers can track individuals and collect a massive amount of data in accordance with the requirements of the GDPR. After defining the different actors involved, the Authority points out five major obligations:

1) determine your purposes of processing
2) define your operations of processing
3) identify the data necessary for your purposes of processing
4) check whether there is a legal basis for the data processing
5) be transparent towards the data subjects.

The Recommendation stresses out the importance of the fundamental transparency and proportionality principles under the GDPR.

Despite the fact that this contribution doesn't allow us to go into detail on the Recommendation, (which is publicly accessible on the Authority's website), it may be interesting to focus on the legal basis for the processing of personal data for direct marketing purposes.

Some legal bases are more suited than others. The Authority considers the possibility to use « the performance of a contract » as a legal basis for direct marketing purposes to a very limited extent, having regard to the inherent specificity of contractual relations.

On the other hand, although the GDPR stipulates that the legitimate interests of a controller may provide a legal basis for processing personal data for direct marketing purposes (consideration 47 of the GDPR), the Authority points out that is not necessarily straightforward to apply this legal basis and that the basis will not always be valid, taking into account the specific characteristics of the processing activities. For instance, as the reasonable expectations of a data subject about the processing of his personal data are an important parameter in the assessment of the application of this legal basis, a prospect will – according to the Belgian Authority – never reasonably expect the receipt of direct marketing messages.

The processing of personal data for direct marketing purposes may also be based on the consent of the data subjects. The consent has to be free, specific,

unambiguous and informed to be considered as a valid consent. An opt-out system is insufficient.

The recent decisions of the Belgian Authority also point out the importance of the topic. The Authority has imposed a fine of 10.000,00 EUR on a company that used the electronic identity card of its customers to create a loyalty card without offering any alternative means of identification. Because the complainant did not want to show his identity card, he was refused the loyalty card even though he offered to provide his details in writing. Since the complainant could not benefit from the same advantages and discounts, The Authority's Dispute Settlement Chamber found this practice to be contrary to the GDPR.

In a recent decision an insurance company received a fine of 50.000,00 EUR for not providing the data subject sufficient information regarding his right to object to the processing of personal data for direct marketing purposes.

Respecting the relevant legislation is therefore not limited to the GDPR. Specific legislation may require a specific legal basis. For example, the e-Privacy directive requires, as a general rule, the prior consent of the data subject for electronic direct marketing communication for commercial purposes. Under certain conditions the use of the « soft opt-in » can be sufficient. This « soft opt-in » concerns a weakened application of the legal basis « legitimate interest ».

Under Belgian law, the Telecom law, the Belgian Code of Economic Law and the Electronic Communications Act are worth mentioning.

First, « cookie law » may contain specific obligations for processing personal data. It applies to all technology that is designed to place data on a data subject's device or to collect data from such a device. Article 129 of the Belgian Telecom law includes transparency obligations on the use of cookies and it requires an explicit opt-in before installing any non-functional cookies. This opt-in complements and stands next to any opt-in under the GDPR. The first opt-in is a consent to place cookies, while the opt-in under the GDPR is a consent to use these cookies to collect and process personal data. An important but subtle difference lies in the fact that « GDPR consent » may in some cases be replaced by « legitimate interest », but this is not at all the case under the Telecom law.

Second, the Belgian Code of Economic Law contains a set of rules concerning direct marketing. Under the code, the use of automated calling systems without human intervention, the use of faxes for direct marketing purposes and the electronically transmission of advertisements is forbidden without the prior, free, specific and informed consent of the addressee, which can always be revoked without any raison or costs (article VI.110, § 1 and XII.13, §1 of the code). Other techniques for transmitting unsolicited communications for direct marketing purposes are allowed, provided that the addressee has not manifestly opposed such techniques, and relating to subscribers, subject to additional conditions (article VI.110, § 2 of the code). Violations of the provisions are severely sanctioned, with criminal fines that can amount up to 50.000,00 EUR (to be multiplied by 8).

Lastly, article 122, § 3 of the Electronic Communications Act regulates the processing of certain personal data for the marketing of electronic communications services. Before obtaining the consent of the data subject, operators have to inform the data subjects about the type of the data and the purposes and the duration of the data processing.

We can conclude that the GDPR, as well as Belgian national laws, demand strict obligations for legitimate personal data processing for direct marketing purposes. Having regard to the number and diversity of the actors involved, the number and the categories data processed, as well as the types of (very intrusive) processing carried out, the Belgian Authority includes those responsible for those processing activities among her priorities both in terms of guidance and in terms of level of control. Not only the risk of penalties, but also the willingness to create a fiduciary relationship with data subjects and ethical behaviour on the market have to incite advertisers to comply with the legislation.

Elien Van Petegem
Litiguard Law Firm

AdTech in Bulgaria

AdTech includes various tools, which analyze data in order to be able to connect with potential clients in a more targeted manner, whereas the most common of those tools used in Bulgaria - advertising emails and cookies - are briefly outlined below.

Advertising by telecommunication

In Bulgaria, the sending of advertising mail such as **electronic newsletters and advertising e-mails** (called "commercial messages") is regulated by the Bulgarian Electronic Commerce Act (ECA) and indirectly by the Competition Protection Act (CPA). ECA defines the electronic services, commercial messages and the main rules for their placement. The purpose of the CPA is to ensure fair and undistorted competition in the interest of all participants, whereas unfair advertising and sales methods via e-mail (unsolicited commercial messages and aggressive commercial practices) are deemed to constitute unfair competition.

> "THE PURPOSE OF THE CPA IS TO ENSURE FAIR AND UNDISTORTED COMPETITION IN THE INTEREST OF ALL PARTICIPANTS
>
> Nikolay Belokonski
> *KWR Belokonski Gospodinov & Partners*

According to ECA the electronic services are those services, including the provision of commercial messages, which are usually provided against consideration and are provided remotely through the use of electronic means following an explicit statement by the recipient of the service. Commercial messages are advertising or other communications representing, directly or indirectly, the goods, services or reputation of the person performing a commercial or craft activity or exercising a regulated profession. However, the independent use of the following does not constitute commercial messages within the meaning of ECA: 1. information providing direct access to the activity of the sender, such as the name of his domain or e-mail address; 2. messages about the goods, services or reputation of the sender, the information about which has been collected in an independent manner, without having been paid for that.

The commercial messages that are part of a service or constitute an electronic service must meet the following requirements:

1. be easily recognizable as commercial
2. to allow clear identification of the natural or legal persons on whose behalf they have been made
3. to define clearly and unambiguously the conditions for using promotional offers, such as discounts, bonuses and gifts, if they include such
4. to provide easy access to clear and unambiguous conditions for participation in competitions and games with announced prizes, if they contain such information
5. to contain also the information, provided in other normative acts.

A service provider who sends unsolicited commercial messages by e-mail without the prior consent of the recipient is obliged to ensure the clear and unambiguous recognition of the commercial message as unsolicited upon receipt by the recipient. The Consumer Protection Commission runs an electronic register of the electronic addresses of legal entities that do not wish to receive unsolicited commercial messages, whereas sending unsolicited commercial messages to those registered electronic addresses is prohibited. Sending unsolicited commercial messages to consumers without their prior consent is also prohibited. The ECA does not specify how consent is to be obtained and consent is not bound to a specific form (yet silence or non-reaction does not imply consent).

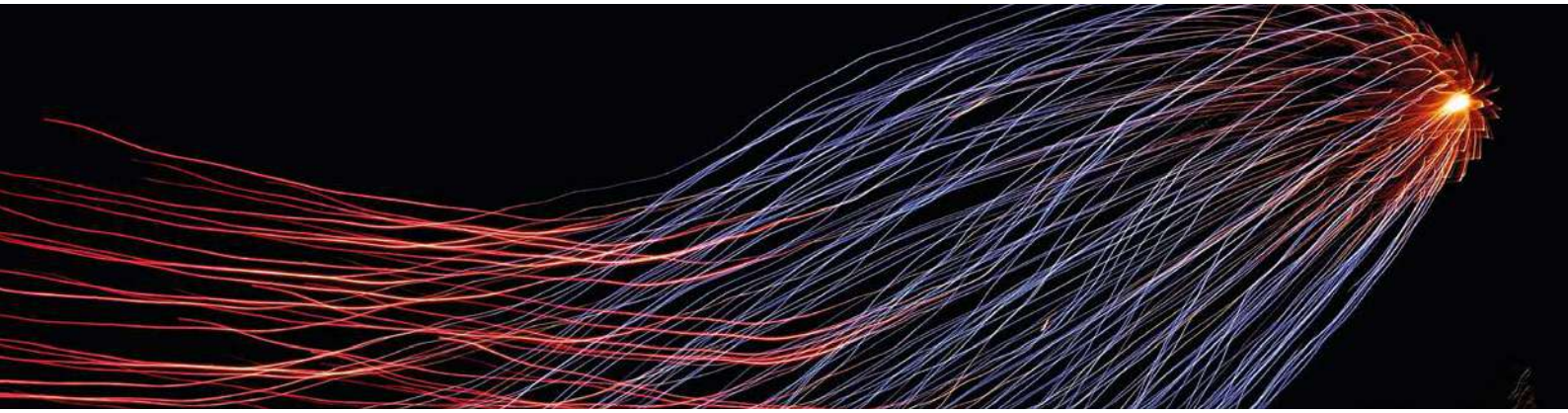
Cookies

Anyone who visits websites is regularly provided with information about the **analysis of user data** and the use of **cookies**. Cookies are data that are temporarily stored on the computer by a website and are used in particular for purposes of personalized advertising. Overall, the regulation of the cookies in Bulgaria is not very strict and moreover – it does not implement the EU legislation correctly, especially concerning the cookies which do not refer to personal data, which have been synchronized on EU level with GDPR.

The main legal basis is art. 4a of the ECA: The electronic service provider shall store information or gain access to information stored in the recipient's terminal device, provided that the recipient of the service is given the opportunity to refuse the storage or access to the information. Hence, Bulgaria follows – in contrast to the European law (Directive 2009/136/EC) – the opt-out principle; an explicit consent to the use of cookies is therefore not required according to Bulgarian law. The information about the use of cookies when visiting a website is not bound to a specific form.

Although an opt-out-solution for cookies is possible in Bulgaria, it should be noted that most of the pro viders have implemented cookie banners and pop-ups that are displayed when the website is loaded and visitors are informed on the use of cookies and asked for their specific consent (opt-in). This is mainly due to the fact that most Bulgarian websites are also accessible to users from the EU. For this reason, we generally recommend complying with the stricter EU rules and obtaining the prior consent of the user for non-essential cookies (opt-in procedure).

Nikolay Belokonski
KWR Belokonski Gospodinov & Partners



CROATIA •

AdTech in Croatia: legal aspects

In Croatia, AdTech, is principally governed by the General Data Protection Regulation (GDPR) and the local Act on the implementation of the GDPR on one side; and the Electronic Communications Act transposing the provisions of the European Directive 2002/58/EC regarding the processing of personal data and the protection of privacy in electronic communications (ePrivacy Directive) on the other side. Specifically, when developing AdTech in an online environment, main legal issues focus on the direct marketing and using of cookies (and similar tracking technologies), which are both interconnected with processing of personal data.

As in certain other European countries, two separate supervisory authorities are competent in the field of AdTech. Essentially, the local Data Protection Authority (cro. abbr. « AZOP ») monitors and enforces the application of the GDPR and is authorised to issue warnings, reprimands and administrative fines. Secondly, the Croatian Regulating Authority for Network Industries (cro. abbr. « HAKOM »)

observes the adherence with the E-Communications Act. In other words, HAKOM enforces the rules on unsolicited communications (direct marketing), as well as the use of cookies and similar tracking technologies. Based on its practice, HAKOM is well aware how the GDPR and cookies are interconnected. Although HAKOM has established a separate data protection department, it mostly seeks a prior opinion of AZOP when applying the GDPR, thus substantiating its decisions both on the GDPR and the European Court of Justice (ECJ) decisions regarding the GDPR.

Neither HAKOM, nor AZOP have issued specific guidelines regarding AdTech. Therefore, when seeking any clarifications and interpretations of the applicable regulations, the stakeholders primarily focus on the ECJ's decisions and guidelines issued by the competent authorities on the European level (such as the European Data Protection Supervisor or recommendations issued by ENISA).

Cookies

In line with the ePrivacy Directive, the e-Communciations Act prescribes that the use of electronic communications networks for the storage of data or for access to already stored data in the terminal equipment of a subscriber or service user is permitted only if that subscriber or service user has given his consent, after receiving clear and complete notification in accordance with special regulations. This may not prevent the technical storage of data or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or, as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. Therefore, placing of any cookies or similar tracking technologies, other than the "strictly" or "technically" necessary is allowed only provided that the user granted its consent. GDPR conditions for obtaining a valid consent apply in the case of cookies, including

> "
>
> USING OF COOKIES OR SIMILAR TRACKING TECHNOLOGIES ON VISITOR'S TERMINAL EQUIPMENT WHICH ARE NOT STRICTLY NECESSARY [...] MAY LEAD TO SEVERAL LEGAL CONSEQUENCES

Direct marketing

In line with the E-Communications Act, use of automated calling and communications systems without human intervention, facsimile machines or electronic mail, including SMS messages and MMS messages, for the purposes of direct marketing and sale may only be allowed in respect of subscribers or users who have given their prior consent.

However, a trader is generally allowed to use details on electronic mail addresses (which generally include personal data) obtained from its customers for the purpose of sale of products or services for direct marketing and sale of its own similar products or services provided that customers have a clear opt-out option on the occasion of receiving any electronic message (so called soft opt-in). Pursuant to the provisions of the E-Communications Act, the soft opt-in rule explicitly applies to consumers only, and not to corporate customers.

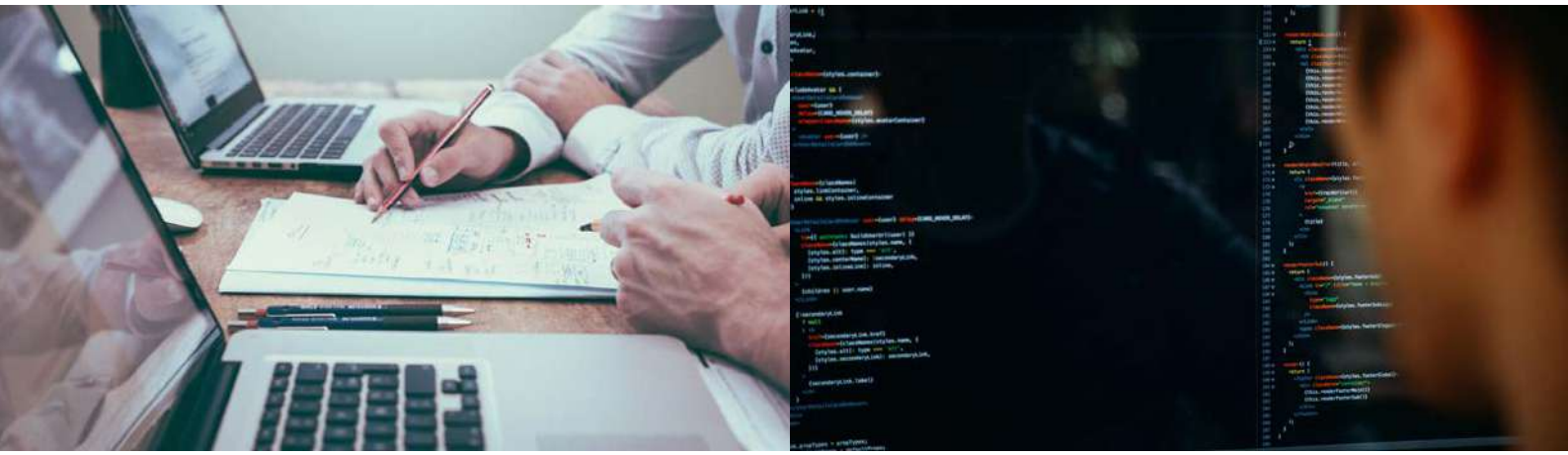
the obligations to provide the user with a clear and comprehensive information on how to revoke the consent or disable cookies respectively. Therefore, organisations are likely to need the consent for most of the online marketing messages or marketing calls, as well as online tracking methods including by the use of cookies or similar technologies.

In accordance with the E-Communications Act, using of cookies or similar tracking technologies on visitor's terminal equipment which are not strictly necessary as elaborated above may lead to several legal consequences, including a monetary fine for a misdemeanour in the amount of up to HRK 1.000,000.00 (appr. EUR 135,000.00). In practice, in case of a minor breach HAKOM usually first issues an order for the operator of a webpage to comply with its obligations on properly notifying the users and obtaining valid consents for placing of cookies within a given deadline, under caution of issuing monetary fines.

In its practice regarding the placing of cookies, HAKOM reaffirmed the position taken by the ECJ in the Case No. C-673/17 regarding standard of consent in relation to use of cookie technology, thus confirming that an effective consent requires an unambiguous action of confirmation, such as actively clicking a box affirming the consent on the website. In contrast, a box that is already checked off or the inactivity of the user cannot establish effective consent in the sense of the GDPR. Accordingly, cookie banners which seek to establish consent simply through a user continuing surfing on a website are not admissible.

For more information regarding the subject topic, you may wish to contact us on below email addresses (p33).

Tea Cerinski & Tomislav Pedišic
Vukmir and Associates



AdTech in Czech Republic

AdTech is currently underappreciated in the Czech legal environment in comparison to its economic significance and social impact. It is particularly governed by the Act. No. 127/2005 Coll., Electronic Communication Act (ECA) and the Act No. 480/2004 Coll., Information Society Services Act (ISSA). The supervisory authorities are the Czech Telecommunication Office and partially the Office for Personal Data Protection (OPDP).

Naturally, the legal environment is heavily influenced by European legislation as both ECA and ISSA implemented the European Directive No. 2002/58/EC (e-Privacy Directive) into Czech law and make reference to GDPR (European Regulation No. 679/2016), as in relation to processing of personal data in advertising there is almost no regulation under the national Data Protection Act.

Commercial communications

The core provision for mass commercial communication via the internet is Article 7 of ISSA. Commercial telecommunication is also regulated by Article 96 of ECA, which basically forbids to address a user telephonically with advertisement if the user in question is upon his request labelled as not wishing to be contacted for marketing purposes.

The ISSA´s rules on commercial communication impose on the sender, or the principal who ordered a particular commercial communication, the obligation to obtain receiver's consent in advance, or, in case of direct marketing, to actively enable the customer to easily opt-out from any commercial communication. What sometimes proves to be difficult in practise is the concurrency of this obligation with the obligations based on the new data protection legislation, as they are confusingly similar but not the same.

The recent interpretation of GDPR by the OPDP introduced also a new, previously unknown, obligation into this area, to have obtained the consent with commercial communication followed by the confirmation of this consent from a registered email address before the actual sending of the commercial communication take place, in order to prevent then misuse of email addresses of third parties in the consent. Although these rules are still facing resistance by some sectors of business, the awareness of the legal requirements is now high, despite the case discussed below.

Cookies and similar technologies

The practise of AdTech use in the Czech online environment has been mostly influenced by the quality of implementation of the e-Privacy Directive and lacks a smooth coexistence between its wording and ECA´s wording. Unfortunately, the Czech legislator did not keep up with the European development, especially with the amendment of the e-Privacy Directive by European Directive No. 2009/136/EC, which changed the so called opt-out rule for accessing and processing information from the terminal equipment of a user into the opt-in rule. However, this shift did not manifest itself in the respective amendment to the ECA (although others did).

Therefore, the wording of the ECA on its own still indicates an opt-out regime for cookies and therefore, the obligated entities continue with their established practise. From an advanced legal point of view however, the obligation of interpretation of Czech law in conformity with EU law should be sufficient to overcome possible inconsistencies, but so far, no such clear interpretation by a court or the supervisory authorities has occurred. The likely reason for that is the lack of interest of the users, who generally have very little understanding of the risks connected with AdTech, and the wide scope of tasks of The Czech Telecommunication Office (it also supervises telephone operators, decides their disputes with consumers, issues general authorisations and pricing decisions etc.) that forces it to focus more on other issues.

A more active role in this regard has been recently taken by the OPDP, which is at the same time also the Czech data protection authority under the GDPR. However, especially in case of cookies, the role of OPDP is controversial. As the whole EU in some way struggles with the unclarified dichotomy of GDPR Directive, the OPDP issued its recommendations regarding the personal data processing by cookies and similar technologies on 23 May 2018, after GDPR came into force.

However, this recommendation does not even reflect all conclusions of the WP 29 Working Document No. 02/2013 providing guidelines on obtaining consent for cookies and contains further inconsistencies. For example, the document takes the setting of the user´s internet browser as a consent with cookies and connected personal data processing in general and also discourages from using pop-up windows and information bars about data processing. It further states the implementation of European Directive No. 2009/136/ES via the ECA as having been properly executed. Thus, it deviates significantly from the documents issued by WP 29/EDPB, which does not contribute to the clarity of the applicable law.

In some ways this, together with the ECA´s lack of proper wording and the absence of decisions of the Czech supervisory authorities enables the practise of only informing the user about the existence of cookies in general and of the collecting of dubious tacitly given consents with cookies, which is unfortunately applied very often.

Tomáš Mudra
UEPA Advokáti s.r.o.

AdTech in France: Digital marketing and data protection

After receiving various solicitations from online marketing sector professionals as well as the public, the French Data Protection Authority (« **CNIL** ») has elaborated an action plan for the year 2019-2020 in order to outline the applicable rules and to help stakeholders in their compliance process. The online marketing sector is subject to two regulations that impose strict conditions, in particular regarding consent: the GDPR and the national regulations transposing the 2002/58 Directive, amended in 2009 (Dir. 2009/136), concerning the processing of personal data and the protection of privacy in electronic communications (« **e-Privacy Directive** »). The issues of stakeholder in the online marketing sector focus on two central topics: direct marketing and cookies (and other tracking techniques).

The issues related to direct marketing.

The CNIL has repeatedly communicated the applicable rules of law (during meetings with representatives of the sector, and on its website in December 2018). Under French law, in a B2C relationship*, the use of personal data for direct marketing purposes whether by SMS or by email is prohibited, unless such user has given his/her prior consent. (Article L. 34-5 of the Postal and Electronic Communications Code and Articles L. 222-16 and 223-7 of the Consumer Code). As long as this consent must be free, specific and informed, pre-ticked boxes are prohibited. In addition, the consent shall not be subject to the acceptance of the provider's general Terms and Conditions.

As an exception to this general principle, direct marketing by SMS or email remains possible provided that the following conditions are met: (i) Personal data have been previously collected directly with the individual, at the occasion of a sale or a provision of services. Nonetheless, personal data must have been collected in compliance with the principles of GDPR and Law n°78-17 of January 6, 1978, as modified (the « **Data Protection Act** »). In particular, data must be collected faithfully which excludes the collection in public spaces of the Internet (web site, discussion forums, directories, etc.). (ii) The message concerns analogous products or services provided by the same person. The concept of « analogous products or services » is not legally defined. The French Union of Direct Marketing (UFMD) has specified that analogous products or services would mean products or services for which the person concerned could reasonably expect to receive marketing/promotional communications from the seller/supplier.

The issues related to cookies and other tracking devices.

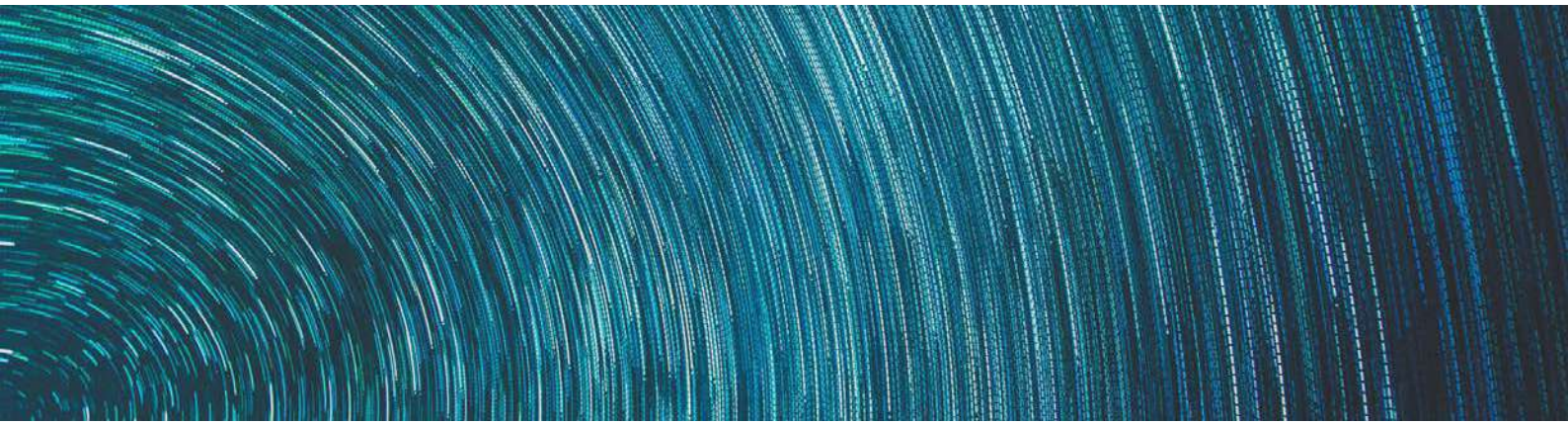
On July 4, 2019, the CNIL adopted guidelines, relating to the application of Article 82 of the Data Protection Act, on cookies and other tracking devices (the « **Guidelines** »). This article transposes the ePrivacy Directive. The main novelties resulting from the Guidelines are the following: (i) continuing to browse a website, use a mobile application or scrolling the page of a website or mobile application does not constitute clear

[This reading of the CNIL goes beyond the law (which does not distinguish between B2C and B2B relations) and is not shared by certain non-profit organizations defending rights of Internet users.]*

positive actions which amount to valid consent; (ii) browser settings do not currently allow the user to express the manifestation of a valid consent; and (iii) operators who use tracking cookies must be able to demonstrate that they have obtained the user consent as understood under the GDPR.

The CNIL focuses in particular on the free and specific nature of consent in relation to cookies walls, the practice of making access to a website or mobile application conditional on consent to the installation of cookies and trackers on the device used. After recalling the position of the European Data Protection Board (EDPB) on this subject, the CNIL considers that « the global acceptance of general conditions of use cannot be a valid way of collecting consent, insofar as it cannot be given separately for each purpose », and that consequently cookies walls are not an acceptable practice in terms of data protection and do not comply with the GDPR.

On January 14, 2020, the CNIL published a draft recommendations (the « **Recommendations** ») regarding the practicalities of obtaining valid consent to cookies and other tracking devices. They provide concrete examples of the implementation of the cookie laws. The CNIL expressly specifies that the Recommendations are « soft law », which means they are not legally binding upon controllers, and failure to comply will not directly result in sanctions. However, from a practical standpoint, it seems difficult to depart from the best practices proposed in the Recommendations without breaching the mandatory rules applicable to cookies and so risking regulatory sanctions.



In order to align with the GDPR principle of accountability and evidence the validity of consent, the Recommendations advice the following alternative solutions: keeping in escrow with a third-party depositary the computer code used by the controller for collecting users' consent; taking screenshots of the mechanism displayed for collecting consent as it appears on the relevant website/application; or performing regular audits of the mechanisms implemented for obtaining consent.

French Council of State decided that the CNIL cannot prohibit cookie walls.

On June 19, 2020, the French Council of State (Conseil d'État), the highest administrative authority in France, decided that the CNIL had gone too far in its Guidelines when it stated that conditioning a user's access to a website upon his or her acceptance of certain cookies is never compliant with the consent requirements in the GDPR. The CNIL has said it will address this point in a new recommendation to be issued after September this year, with the Council of State requiring that this recommendation is only published following public consultation.

From a practical standpoint, cookies wall are therefore not prohibited, but any operator using cookies and other tracers will have to implement all the other recommendations of the CNIL.

Laurent Badiane & Matthieu Bourgeois
KGA Avocats

• GERMANY

AdTech in Germany: Digital Marketing and Data Protection

In the past, extensive use has been made in Germany of the possibility of comprehensively evaluating the behavior of users when they call up an Internet page and using the knowledge thus gained for targeted advertising campaigns. Providers from Germany benefited from the fact that there were numerous special regulations that allowed such activities despite the very strict framework conditions.

As such, the provisions of competition law stipulate that the explicit consent of the recipient must be obtained before advertising is sent by e-mail. If this requirement is not complied with, this automatically constitutes an unreasonable unacceptable nuisance (sec. 7(2) Act against Unfair Competition, UWG). Recipients of advertising who have not given their consent can take legal action against the sender, and there is also a risk of legal action by competitors and consumer associations, which can also punish such violations. In order to verify whether consent has been given, case law in this context requires an up-stream confirmation, which typically takes place by means of the so-called double opt-in procedure. These very strict requirements are, however, broken by an exception clause according to which existing customers may be contacted for advertising purposes after their first order without express consent (sec. 7(3) UWG). If a customer has already made a purchase and in this context the seller becomes aware of the e-mail address, this address may subsequently be used for advertising purposes if comparable products are advertised and the customer has the opportunity to object. In borderline cases, however, jurisdiction is traditionally restrictive with regard to the applicability of the special provision. Companies may, for example, after the first purchase of a product, advertise the identical product to the buyer again in the future, but may not ask the buyer about his experience with the product already purchased. The courts regularly argue that the exception rule should be interpreted narrowly in case of doubt in order not to provide a gateway for excessive advertising.

A special position existed for Germany also for a long time related to the analysis of user data when visiting an Internet page. In implementation of the Data Protection Directive (95/46/EC), the German legislator has implemented a solution according to which the consent of the user is not required for the purposes of advertising, market research or for the design of online offers in line with requirements when using pseudonyms, but the user is only entitled to a right of objection (sec. 15(3) German Telemedia Act, TMG). In ac-cordance with the ePrivacy Directive (2002/58/EC), Germany has not made any changes to its objection solution, but has explicitly taken the position that the standard admissibility of user evaluation without consent is in conformity with the Directive as long as it is car-ried out using pseudonyms and no combination with other customer data is planned. Although this approach has been strongly criticized, there has never been an infringement procedure against Germany because of a possibly insufficient implementation of the ePri-vacy Directive. Against this background, numerous tracking systems were used on almost all major Internet sites in Germany, in particular Google Analytics. For a long time, it was not even necessary to indicate the use of such systems and their use of cookies, but it was sufficient to include a corresponding note in the data protection declaration. After the introduction of the GDPR not much changed in

the legal interpretation and practical implementation at first. With reference to the transitional provision in Article 95 of the GDPR, it was often argued that until the adoption of the e-privacy regulation planned in parallel, it could probably be assumed that the regulation of the e-privacy directive and its national implementation by the TMG had not yet been superseded. This interpretation was not uncontroversial, but was originally at least tolerated by the supervisory authorities.

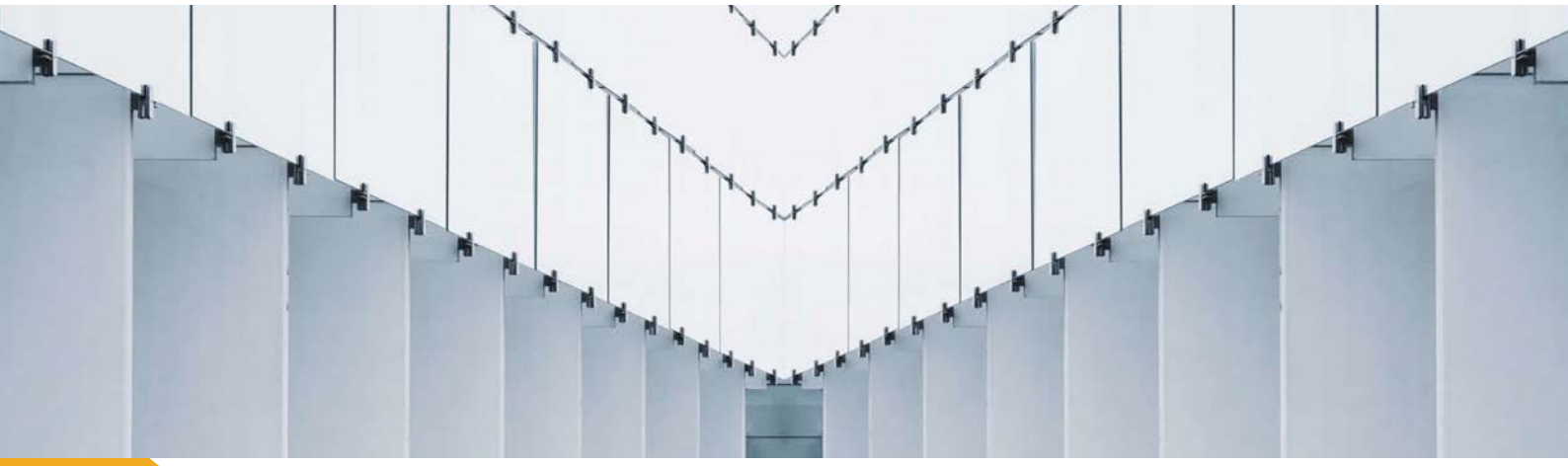
With the decision of the European Court of Justice (ECJ) in October 2019, there was a controversial discussion for Germany whether the requirements of the GDPR are to be ob-served with priority and force a change to a consent solution or whether it is still possible to fall back on the still unchanged regulation in telemedia law (ECJ, judgement of 1 Oc-tober 2019, Ref. C-673/17). The request for a preliminary ruling was submitted to the ECJ by the Federal Court of Justice (BGH). In its subsequent decision, the BGH followed the view of the ECJ and clarified that the provision in sec. 15 TMG must be interpreted in conformity with European law (BGH, judgement of 28 May 2020, Ref. I ZR 7/16). Although the regulation in sec. 15 TMG with the opt-out solution is still valid, it must now be interpreted in accordance with European law in such a way that the consent of the user must always be obtained for non-required cookies (opt-in). Since the clarification by the Federal Court of Justice, it can now be observed that all providers are gradually changing the previous technology and are implementing appropriate cookie banners and pop-ups when the page is called up, with which the users are asked for their consent to the use of cookies. In the future, it is also planned to adapt the legal requirements in the TMG so that the standard does not have to be interpreted further against its wording.

“

ALL PROVIDERS ARE GRADUALLY CHANGING THE PREVIOUS TECHNOLOGY AND ARE IMPLEMENTING APPROPRIATE COOKIE BANNERS AND POP-UPS WHEN THE PAGE IS CALLED UP

The regulations of the GDPR as well as the national regulations for the protection of personal data restrict companies in the options for their use of Advertising Technology. In particular, the requirement of consent for the setting of tracking and advertising cookies and for the sending of advertising e-mails must be observed. In the future, the consent requirement for the setting of cookies in Germany could also be incorporated into the legal text. At the end of July 2020, a draft bill of the Federal Ministry for Economic Affairs and Energy for a « Law on Data Protection and the Protection of Privacy in Electronic Communications and Telemedia and on Amendments to the TKG, TMG and other laws » was announced. Sec. 9 of this law provides for « consent for terminal equipment » and regulates the corresponding requirements and exceptions.

Dr. Sebastian Meyer
BRANDI Rechtsanwälte



AdTech in Ireland: The Challenges of Data Protection

AdTech (short for advertising technology) may be described as the umbrella term for the software and tools that help agencies and brands strategize, deliver, and manage their digital advertising activities. It is an industry that has, however, found itself under scrutiny for many reasons, not least consumer concern about data security and the level of online fraud together with the impact of the GDPR.

In this article we will focus on cookies, namely the small text files created by websites and stored in the user's device which allows the websites to recognise the user and keep track of his/her preferences.

In Ireland, the ePrivacy Regulations 2011, which transposed the EU ePrivacy Directive into Irish law, regulate, inter alia, the use of cookies. These Regulations are complemented, when it comes to personal data, by the EU General Data Protection Regulation (GDPR) and the Irish Data Protection Act 2018. The Irish Data Protection Commission (DPC) is the national authority responsible for the enforcement of these legal tools. In April 2020, the DPC published updated guidance on the use of cookies and other tracking technologies. Its report was based on a cookie audit of 38 companies. The DPC is allowing a period of six months from the publication of its report for controllers to bring their activities into compliance, after which enforcement actions will be taken.

Under Regulation 5 of the ePrivacy Regulations 2011, a controller must obtain the data subject's consent before using cookies or other tracking technologies, regardless of whether they relate to personal data. There are two strict exemptions to the requirement of consent, namely when the cookies' sole purpose is to carry out the transmission of a communication over a network and when the use of cookies is strictly necessary in order to provide a service delivered over the internet, such as a website or an app, explicitly requested by the user. The DPC guidance indicates that cookies related to advertising do not benefit from these exemptions and must be consented to. It specifies that the consent must be of the standard defined in Article 4(11) of the GDPR, namely be freely given, specific, informed and unambiguous.

A controller must request a user's consent for each purpose for which cookies are used. The consent must require a clear, affirmative action on the part of the user, and cannot be implied. This means, for example, that cookie banners that disappear when a user scrolls are non-compliant. The controller must not nudge users into accepting cookies. Banners that merely give the user the option to accept, such as banners only containing "I understand" buttons, are not permissible. Nor are pre-checked boxes which users must deselect to refuse consent. Furthermore, the "Accept Cookies", "Manage Cookies" and 'Reject Cookies" buttons on a banner should be equally visible.

For the consent to be informed, the user must be provided with clear and comprehensive information, which must be both prominently displayed and easily accessible, and include, without limitation, the purposes of the processing of the information. Regulation 5 of the ePrivacy Regulations 2011 further provides that this information must be in accordance with data protection legislation, meaning that if the processing involves personal data, the transparency requirements under Article 12-14 of the GDPR will have to be met.

For the consent to be informed, the user must be provided with clear and comprehensive information, which must be both prominently displayed and easily accessible, and include, without limitation, the purposes of the processing of the information. Regulation 5 of the ePrivacy Regulations 2011 further provides that this information must be in accordance with data protection legislation, meaning that if the processing involves personal data, the transparency requirements under Article 12-14 of the GDPR will have to be met.

It should also be mentioned that users must be able to withdraw consent as easily as they gave it and that the lifespan of a cookie should be proportionate to its function. For example, a session cookie with an indefinite lifespan would be disproportionate.

Obtaining the consent of the user is not the only rule the controller must be in compliance with in order for the use of cookies to be lawful.

> “
> OBTAINING THE CONSENT OF THE USER IS NOT THE ONLY RULE THE CONTROLLER MUST BE IN COMPLIANCE WITH IN ORDER FOR THE USE OF COOKIES TO BE LAWFUL.
>
> Patricia McGovern
> *DFMG Solicitors*

Article 35 of the GDPR provides that a Data Protection Impact Assessment (DPIA) must be conducted by a controller where a type of data processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of individuals. The Irish Data Protection Commission has published a list of processing operations for which a DPIA is mandatory. It includes, for example, processing operations involving the systematic monitoring, tracking or observing of individuals' location or behaviour, and the profiling of individuals on a large scale.

The DPC guidance reminds controller that when processing personal data, the controller must comply with the GDPR and the Data Protection Act 2018. This means, inter alia, that it must keep a record of the types of processing carried out that involve personal data.

The guidance does not comment on the lawful basis for the processing of cookie data. This will likely come at some point in the future, given the number of AdTech-related inquiries currently before the Commissioner.

However, the DPC indicated that the only likely legal basis the controller will have for processing special category data derived from the use of cookies and other tracking technologies is the explicit consent of the data subjects. The Commission further stated that the bar to demonstrate that the controller obtained that explicit consent is high and is therefore unlikely to be met by means of generic information in a cookie banner or privacy policy.

The combination of EU and Irish regulations on ePrivacy and data protection constitute a strict framework that controllers must observe when collecting and processing data. While the Irish Data Protection Commission has given precise guidance on the use of cookies and other tracking device, it is yet to publish a report on the broader issue of AdTech. It remains to be seen what position the DPC will adopt on the question and whether it will follow views of the UK's ICO or France's CNIL. As mentioned, it is expected that guidance will come by virtue of the cases currently being investigated by the DPC. Furthermore, this legal framework will be subject to modifications in the future with the adoption of the EU ePrivacy Regulation, which will replace the current EU ePrivacy Directive and Irish ePrivacy Regulations 2011. This Regulation was supposed to take effect alongside the GDPR on 25 May 2018, it is now uncertain when it will be adopted.

Patricia McGovern
DFMG Solicitors

AdTech in Italy: Digital marketing & data protection

Apart from GDPR, the Italian legal framework on data protection in digital marketing consists of legislative decree 196/2003 ("Data Protection Code"), as amended by legislative decree 101/2018 that entered into force in September 2018 further to the entry into force of GDPR, and several resolutions and guidelines of the Garante per la protezione dei dati personali, the Italian Data Protection Authority.

The main issue about data protection in the online marketing sector is related to the legal basis of the processing of personal data.

After the adoption of the GDPR, several subjects in Italy first considered it possible to extend – according to article 6, paragraph 1, letter f and to the recital 47 of GDPR – the legal basis of the legitimate interest to the processing of personal data carried out for marketing purposes through automated systems.

Legislative decree 101/2018 confirmed that, for the transmission of marketing communications through automated systems, the legal basis must be the consent of the data subject (article 130, paragraph 2, Data Protection Code).

As repeatedly made clear not only by the decisions of the Italian Data Protection Authority) but also of the Italian Supreme Court (among others, Corte di Cassazione, decision 17278/2018), to be valid the consent has to be informed, freely given, specific and must be an unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her. Therefore, pre-ticked boxes or inactivity do not constitute consent. Furthermore, according to several decision of the Authority, the collection of email addresses in public spaces of Internet is specifically forbidden.

The general rule of the consent may be derogated only in one case, the so called "soft spam", as stated by article 130, paragraph 4, Data Protection Code. There is no need of the consent of the data subject in case of marketing communications sent by email, when the following conditions are met: (i) the data controller uses exclusively the email address supplied by the data subject in the context of the sale of a product or service; (ii) the services are similar to those that have been the subject of the sale and (iii) the data subject, after being adequately informed, does not object to said use either initially or in connection with subsequent communications.

The data subject shall be informed of the possibility to object to the processing at any time, using simple means and free of charge, both at the time of collecting the data and when sending any communications.

The Italian Data Protection Authority approach is to limit as much as possible the use of the legitimate interest as legal basis of processing of personal data with marketing purpose. In a decision of January 2020 against TIM S.p.A., one of the major tlc services providers, the Authority stated that the legitimate interest cannot as a rule substitute the consent of the data subject in the processing of personal data for direct marketing purposes. The Authority pointed out that the application of the legal basis of the legitimate interest implies the prevalence in practice (as testified by the « balancing test » or « legitimate interest assessment » carried out by the data controller and in any case subject to the Authority evaluation) of the legitimate interest on the rights, freedom and mere interests of the recipients of the marketing communications and that the concrete implementation of all necessary measures to guarantee the rights of the data subjects, in particular the right to object, has to be assured.

"

THE MAIN ISSUE ABOUT DATA PROTECTION IN THE ONLINE MARKETING SECTOR IS RELATED TO THE LEGAL BASIS OF THE PROCESSING OF PERSONAL DATA.

• ITALY

The consent legal basis applies also to cookies used to send advertising messages in line with the user's online navigation preferences. To this regard, article 122 of the Data Protection Code states that storing information, or accessing information that is already stored, in the terminal equipment of the user shall only be permitted on condition that the user has given his consent after being informed on the personal data processing.

The Italian regulation on cookies is mainly contained in resolutions of the Italian Data Protection Authority adopted before the entry into force of GDPR, which have not yet been updated.

This has contributed to some degree of uncertainty in the interpretation of the applicable rules on cookies for the online marketing sector professionals. Among others, according to a resolution of the Authority of May 8, 2014, concerning « Simplified arrangements to provide information and obtain consent regarding cookies » the consent to use of cookies could be expressed by the user continuing browsing by accessing any other section or selecting any item on the website.

Such provision is clearly in contrast with GDPR and particularly with the EDPB Guidelines 05/2020 on consent under Regulation 2016/679 and therefore a rapid intervention of the Italian Data Protection Authority on the matter would be necessary.

Marta Margiocco
Cocuzza & Associati Studio Legale

MEXICO •

AdTech in Mexico

Pursuant to the Mexican Federal Law on the Protection of Personal Data held by Private Parties, the definition of data processing includes automated operations of personal data (article 3, section XXXIII). In particular, subjects are entitled to oppose to the processing of their data if (i) such data is processed automatically, (ii) to the extent this causes unwanted legal effects on the subject or an adverse impact on its interests, rights or liberties, and (iii) such processing is targeted to evaluate personal data -without human intervention- or to predict subject's behavior or status (article 47, section II). It seems that the required level of automation is absolute, which means that some human intervention might be sufficient to avoid this rule.

Furthermore, in the context of electronic communications, controllers are obliged to inform the use of mechanisms designed to automatically obtain data or to obtain data simultaneously to the subject's first contact with such mechanisms, as well as to inform the way in which those may be disabled (article 14 of the secondary regulation).

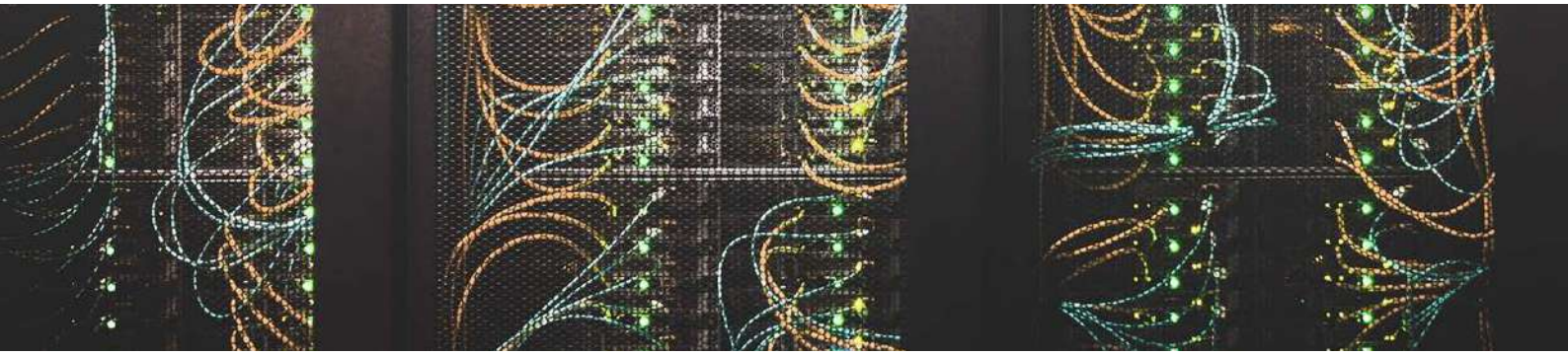
Mexico does not have any specific regulation dealing with unsolicited text messages or spam emails, but the Federal Bureau for Consumer Protection operates a call blocking registry, called REPEP, covering both landlines and mobile phone numbers, which gives suppliers 30 days to desist from making additional calls, sending marketing messages and - in general - to stop disturbing the

consumer at its registered address, email or other points of contact. Issues regarding marketing restrictions are regularly addressed by the Federal Bureau for Consumer Protection. The maximum penalties for marketing breaches may go up to US$70,000.

As to the purchase of marketing lists from third parties, controllers must provide detailed information (through their privacy notices), regarding the data transfers that such controllers intend to carry out, expressly stating the name and other details of subsequent data processors. Also, when required, privacy notices must include a specific clause where the subject may choose whether it consents to such data transfers.

Regarding cookies, the guidelines for elaborating the privacy notice are consistent with the law, since they require controllers to inform data subjects about any technology that allows the automatic collection of personal data simultaneously to the first contact with the subjects; requiring data owners to request the consent from individuals through an opt-in mechanism, and informing individuals as to how to deactivate said technology, unless said technology is required for technical reasons. Although Mexican legislation does not include specific sanctions for cookie-related infringements, the use of cookies in contravention to the guidelines would translate to an illicit collecting of personal data, which would be sanctioned with fines of up to US$680,000, and - if the infringement persists - additional fines of up to US$1,300,000.

José F. Camarena & Isaac López
Cancino Ayuso Abogados



AdTech: the Dutch perspective

Under Dutch law the legal framework surrounding AdTech mainly consist of the General Data Protection Regulation (GDPR) and the Dutch Telecommunications Act, that implements several European Directives regarding the processing of personal data and the protection of privacy in electronic communications (ePrivacy Directive). As in many of the European jurisdictions, the legislation in this field focuses on the protection of (the personal data of) consumers in connection with direct marketing and (tracking) cookies. A complicating factor in the Dutch system is that there are two competent supervisory authorities: the Autoriteit Persoonsgegevens (AP) oversees compliance with and enforces the GDPR and the Autoriteit Consument en Markt (ACM) does so with the Telecommunications Act. This leads to, subtle, differences in the interpretation of certain legal norms.

Digital direct marketing

Specific rules for digital direct marketing (such as by email, text message or app) are laid down in article 11.7 of the Telecommunications Act: it is prohibited unless prior consent has been obtained from there cipients and an opt-out is offered. There is an exception for existing customers: no consent is needed when approaching existing customers with offers for products or services that are similar to those they have purchased previously.

However, processing data for the purpose of digital direct marketing is also regulated by the GDPR, meaning, amongst other things, that the data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (« lawfulness, fairness and transparency »). The requirement of « lawfulness » entails that there is a ground for processing as listed in the GDPR, such as « consent » and/or « legitimate interest of the controller ».

In this respect it is important to know that the AP (in general) strongly prefers « consent » as a ground for processing to « legitimate interest ». The Q&A that the AP published on its website regarding the rules that apply to processing data for digital direct marketing underlines this point of view.

Although recital 47 of the GDPR explicitly mentions « legitimate interests » as a possible ground for direct marketing, the AP stipulates that the main rule is that digital direct marketing is only permitted if there is a legal basis of (freely given, specific, informed and unambiguous) consent from the recipient.

The AP has limited the possibility for legitimate interest as a ground for digital marketing as far as it can. The AP is of the opinion that only when the exception of article 11.7 of the Telecommunications Act with respect to existing customers applies, legitimate interest could provide a legal basis for digital marketing, under the condition that the requirement of necessity is met and it passes the so-called « balancing test ». If not, then the exception does not apply and consent must be obtained.

In other words, only in a limited number of situations it is not necessary to obtain consent for direct marketing, in the AP's point of view.

Cookies

With regard to cookies, a similar situation arises: the ACM is the relevant authority overseeing the compliance with the Telecommunications Act, but as and in so far as such technology processes personal data, the AP monitors compliance with the GDPR. Again both authorities are of the opinion that prior consent must be obtained before cookies that have an impact on the privacy of the website visitor, such as certain analytical and tracking cookies, may be placed on the device of the visitor.

To obtain valid consent the website visitor must be informed clearly, on the first page they see:

- which data is collected
- how that data is collected: with cookies, scripts or beacons
- what is done with that information

The website visitor must be given the opportunity to accept or decline other than functional cookies.

The difference between the ACM and the AP with regard to cookie consent is how « active » consent must be given. The ACM is or used to be of the opinion that a cookie banner stating that by continued use of a website cookies are accepted by the visitor, is sufficient under the Telecommunication Act. GDPR and therefore the AP requires an unambiguous and active action for giving consent for the placement and consultation of tracking cookies. A preticked box with « yes » when the user is asked for approval, inactivity or scrolling down or variations on « you agree if you continue on this website » are prohibited. Cookie walls are also not permitted; websites, apps or other services cannot obtain valid permission from their visitors when using a cookie wall.

Sanctions and fines

In and since 2019 the AP has started several investigations regarding the use of cookies and digital marketing and have issued press releases stating that many violations were found, but no imposed sanctions have

been made public. It is likely that (many of) the offenders took the formal warnings from the AP to heart and remedied the short comings. Although the AP takes a stricter position than the ACM in its explanation of the rules, only the ACM has imposed (hefty) fines and/or other sanctions due to violations of the rules on cookies and direct marketing.

AdTech is an area of interest of the Dutch supervisory authorities and it is advised to tread carefully, as consumer protection is a serious topic in the Netherlands.

Natascha Niewold
Valegis Advocaten

POLAND •

Polish perspective on AdTech: Digital Marketing and Data Protection

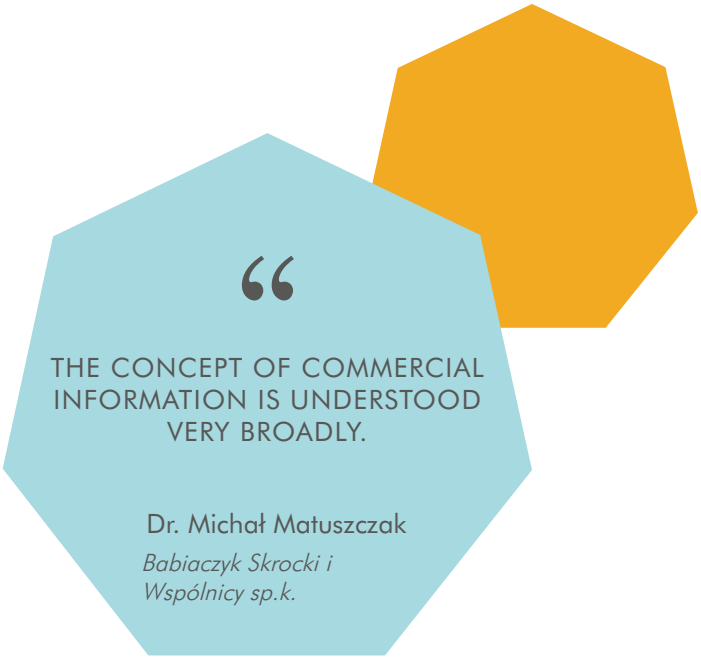
The AdTech sector is one of the fastest technologically developing areas in which user's data is the primary means of trading (a type of « currency »). According to the European Commission's forecasts (European Data Market Study), the market value of online data processed in the European Union in 2020 will amount to a minimum of EUR 739 billion. The use of tools dedicated to behavioral tracking (e.g. cookies, behavioral biometrics) to create consumer profiles may result in price discrimination, exclusion, emotional manipulation, disinformation and, above all, may interfere with the right to privacy. Data is collected automatically, regardless of the will and often awareness of users. The above indicates the need to adopt legal regulations that, on the one hand, will not prevent the development of technology companies, and, on the other hand, will protect the right to privacy, which is more and more often regarded as one of the fundamental human rights.

According to the plans of the European Commission, the General Data Protection Regulation (GDPR) was to enter into force simultaneously with the amendment to the rules of electronic communication in the European Union in the form of the so-called ePrivacy Regulation. The ePrivacy Regulation was supposed to replace and harmonize with the GDPR the rules of online and telephone communication (which are technically already highly standardized and, in fact, fully digitized). However, this did not happen. So far, the ePrivacy Regulation remains in still discussed draft. Due to the fact that the ePrivacy Regulation has not been enacted, in order to update the legal status in the field of electronic communication (including legal issues related to AdTech), it is necessary to undertake legislative measures at the level of member states as well as interpretative measures.

In Poland legal framework for AdTech is consists mostly of GDPR and the Polish Act on Electronically Supplied Services (ESSA). ESSA regulates direct marketing by means of electronic communication as well as the rules

for the protection of personal data of natural persons processed in connection with their use of electronic services and electronic communication. According to Article 4 of ESSA, if the act requires the consent of the recipient, the provisions on the protection of personal data shall apply, which corresponds to the definition of « consent » in Article 2 (f) of the ePrivacy Directive. ESSA requires consent in two cases:

- to receive commercial information addressed to a designated recipient who is a natural person by means of electronic communication, in particular e-mail (Article 10 (1) and (2) of the ESSA, corresponding to provisions of Article 13 of the ePrivacy Directive);
- to process data for the purposes of advertising, market research and the behaviour and preferences of service recipients, with the results of these studies being used to improve the quality of services provided by the service provider (Art. 18 (4) ESSA).



Requirement of consent for sending unsolicited commercial information

According to Article 10 of ESSA, sending unsolicited commercial information addressed to a specific natural person by electronic means of communication, including but not limited to electronic mail, is forbidden. However, commercial information is deemed not to be unsolicited if the recipient has given his permission to be sent said information, in particular if he has made his electronic address available for this purpose. The concept of commercial information is understood very broadly. ESSA defines this term any piece of information produced directly or indirectly to promote goods, services or the image of an entrepreneur. Sending unsolicited commercial information addressed to a specific natural person is deemed to be an act of unfair competition within the meaning of the Fair Trading Act of 16 April 1993.

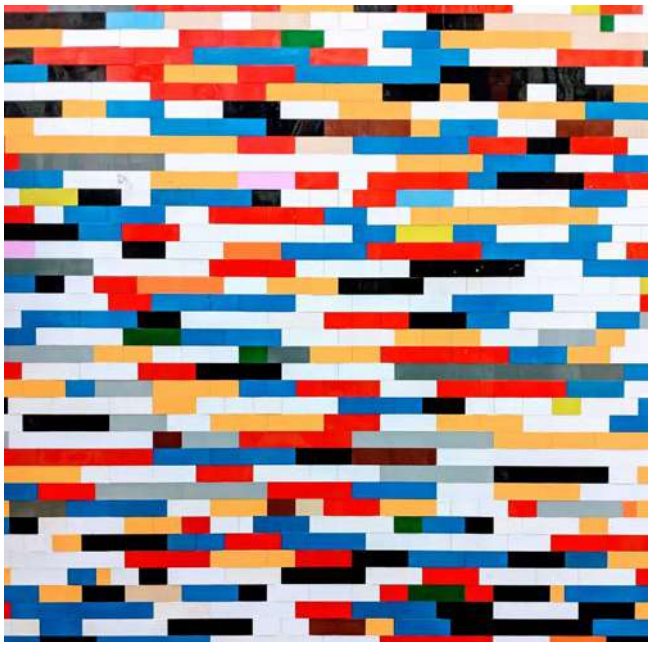
Requirement of consent to data processing for advertising, market research and optimization

According to Article 18 (4) of ESSA the service provider may process - with the customer's permission and for the purposes of advertising, market research, and customer behaviour and preference research, with the results of such research serving the purpose of improving the quality of services provided by the service provider - other data concerning the customer that are not necessary to provide a given service by electronic means.

The relation between the ESSA provisions and the regulations on the protection of personal data is a controversial issue in Poland. There is a dispute in Polish legal doctrine on interpretation of the provision of Article 18 (4) of ESSA as lex specialis (special regulation superior) to Article 6 and Article 9 of GDPR, which define the legal grounds for permitting the processing of personal data. Pursuant to Article 95 of GDPR, the Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in the Directive 2002/58/EC. The ePrivacy Directive introduces the consent requirement only for the processing of «traffic» data by the provider of the public communications network (i.e. the telecommunications operator) or publicly available electronic communications services (i.e. the provider of the electronic messenger). Provisions of ESSA apply much more broadly to all websites administrators or entities that communicate with users via electronic channels (e.g. using a publicly available electronic communication service). As a consequence, it seems more reasonable to assume that Article 18 (4) of ESSA is not a lex specialis in relation to the GDPR and does not formally block the way to invoke other grounds for processing personal data, such as, in particular, the legitimate interest of the data controller. The situation may change with the adoption and entry into force of the ePrivacy Regulation.

Summing up: GDPR regulations supplemented by Polish legal regulations require entrepreneurs to meet strict legal obligations in order to be able legally process personal data for the purpose of direct marketing of their products and services. In order to legally use AdTech tools (eg. advertising and tracking cookies), it is necessary to obtain consent from the data subjects or justify other grounds for processing personal data, such as, in particular, the legitimate interest of the data controller. Sending unsolicited commercial information via e-mail addressed to a specific natural person without consent is illegal in Poland (even if the addressee is a commercial recipient) and is deemed to be an act of unfair competition.

Dr. Michał Matuszczak
Babiaczyk Skrocki i Wspólnicy sp.k.



AdTech in Spain

On November 8, 2019, the Spanish Data Protection Agency (« AEPD ») published the Guide on the use of cookies and similar technologies (the « Guide ») updating the criteria established by the AEPD on the use of cookie technology based on the EU General Data Protection Regulation (« GDPR ») and on Act 3/2018 on Personal Data Protection and Guarantee of Digital Rights (« LOPDGDD »).

This document provides recommendations on how information society service providers must (i) comply with the obligation of transparency; and (ii) obtain users' informed consent to the use of cookies and similar technologies.

As for the obligation of transparency, the AEPD suggests to present information on cookies through layers. The first layer should include essential information, and must include the (a) identification of the responsible editor, the (b) purposes of the cookies, the (c) indication whether the cookies are own or third-party cookies, (d) generic information about the information used in the case of user profiling, (e) the way in which the user can accept, configure or reject cookies, and (f) a clearly visible link directed to a second information layer. This second layer should provide the remaining required information. Service providers must complete this information with a set up system or panel allowing users to accept or reject cookies one by one, or with a link to this system or panel. According to the AEPD, information must be short and concise, « to avoid information fatigue », and to avoid misleading statements such as « we use cookies to personalize content and create a better user experience ».

In contrast with guidelines released by other European authorities, the Guide's main innovation regarding consent is that it validates the expression « continue browsing » to obtain the unequivocal consent of users in certain cases. Examples of continue browsing activities are:

- Using a scroll bar, when information on cookies is visible without the use of a cookie banner.
- Clicking on certain content links within the website.
- Swiping the screen to access the content of the website.

However, according to the AEPD, this is not a valid option in any data processing via cookies that requires users' explicit consent, particularly when (i) processing special data categories; (ii) making automated decisions with legal implications for users (based on consent); and (iii) making data transfers to third countries having obtained the user's consent.

The AEPD recommends the use of session cookies instead of persistent cookies. The Guide includes

a section on « updating consent », in which it is highlighted that the AEPD considers good practice a validity period of no longer 24 months for user's consent. The website provider may collect consent for services offered in different domains through a single website, if the services present similar characteristics.

Prohibition of cookie walls, the updated Guide adopts a more restrictive position on cookie walls (i.e. cookies that must be accepted by users before they can access services and functions). Specifically, it states that « so-called cookie walls will not be acceptable unless they offer an alternative to consent ». The AEPD does however allow cookie walls to be used, « provided the user is properly informed and an alternative to access the service without having to accept the use of cookies is offered ».

The AEPD establishes a term of three (3) months for companies that do not currently comply with

the updated criteria in the Guide to adapt their cookies to the new guidelines. The new criteria must be implemented by 31 October 2020 at the latest.

Antonio Muñoz de Gispert & Fanny Porras
Absis Legal

AdTech in Switzerland

AdTech refers to a combination of the terms advertising and technologies. It includes various tools which analyze data in order to be able to connect with potential clients in a more targeted manner. However, the use of AdTech in the online environment brings not only advantages but also challenges concerning a variety of legal issues. Certain legal issues with regards to the use of the AdTech tools, advertising e-mails and cookies in Switzerland are outlined below.

Mass advertising by telecommunication

In Switzerland, the sending of advertising mail such as **electronic newsletters and advertising e-mails** is regulated by the Federal Act against Unfair Competition (« UWG »; SR 241). The purpose of this Act is to ensure fair and undistorted competition in the interest of all participants (art. 1 UWG). Unfair advertising and sales methods via e-mail (unsolicited commercial e-mails) are governed by art. 3 (1) lit. o UWG.

In short, mass advertising is permitted if the sender cumulatively complies with three obligations: (i) obtain the prior consent of the recipient (opt-in); (ii) specify the correct sender; (iii) provide the possibility of refusal (opt-out).

The UWG does not specify how consent is to be obtained and consent is not bound to a specific form (yet silence or non-reaction does not imply consent). In particular, a so-called double opt-in procedure is certainly sufficient, but is not required by law.

The UWG contains an exception from the obligation to obtain prior consent for mass advertising sent to existing customers. If a buyer for example has previously provided a seller with his or her e-mail address in the course of the purchase of a product, the seller may subsequently use this e-mail address for advertising similar products, provided the buyer has been given the possibility to opt-out from such advertisements.

Violation of art. 3 (1) lit. o UWG can result in legal action (in particular a legal action by consumer protection organizations (art. 10 (2) lit. a UWG) or criminal prosecution (art. 9 ff. and art. 23 UWG). However, the enforcement of this provision (in particular in connection with mass advertising from abroad) is problematic and the provision in practice hardly enforced.

Cookies

Anyone who visits websites is regularly provided with information about the **analysis of user data** and the use of **cookies**. Cookies are data that are temporarily stored on the computer by a website and are used in particular for purposes of personalized advertising. Overall, the « cookies regulation » in Switzerland is not very strict.

The main legal basis is art. 45c lit. b of the Telecommunications Act (TCA; SR 784.10): Processing of data on external equipment by means of transmission using telecommunications techniques is permitted only if users are informed about the processing and its purpose and are informed that they may refuse to allow processing. Hence, Switzerland follows – in contrast to the European law – the opt-out principle; an explicit consent to the use of cookies is therefore not required. Exceptions apply for particularly sensitive personal data.

The information about the use of cookies when visiting a website is not bound to a specific form. For example, it is sufficient to include the information in the privacy policy of a website. However, whoever violates art. 45c lit. b TCA shall be liable to a fine not exceeding CHF 5'000 (art. 53 TCA).

Although an opt-out-solution for cookies is possible in Switzerland, it should be noted that many providers have implemented cookie banners and pop-ups that are displayed when the website is loaded and visitors are informed on the use of cookies and asked for their specific consent (opt-in). This is mainly due to the fact that most Swiss websites are also accessible to users from the EU. For this reason, we generally recommend complying with the stricter EU rules (although not directly applicable in Switzerland) and obtaining the prior consent of the user for non-essential cookies (opt-in procedure).

Julia Bhend & Christian Doster
Probst Partner AG

Online advertising in the United States

In the U.S., organizations now spend more than $240 billion per year on advertising. More than half of that is spent on online advertising. While advertisers understandably have a voracious appetite for lower cost, higher impact digital ads that offer precision targeting and data analytics, advertisers should carefully consider the current legal landscape before launching an online advertising strategy in the U.S.

The key principle when considering digital advertising in the U.S. is that there is no single data protection or advertising law that governs all digital advertisements; instead, the U.S. offers a patchwork of state and federal laws. Some of those laws are omnibus-type laws that apply to every advertisement in an applicable jurisdiction, while the applicability of other laws depends on other factors, such as the extent of personal information collected, the type of advertising medium, the intended recipient, the type of product promoted, and the type of advertising.

Laws Specifically Related to Advertising

Advertising laws that have long-applied to traditional forms of advertising apply equally to digital ads. For example, Section 5 of the Federal Trade Commission Act generally prohibits unfair and deceptive advertising practices. That prohibition has been interpreted to mean that advertisements in the U.S. must: (i) be truthful and not misleading; (ii) only include claims that can be substantiated by evidence; (iii) not be unfair; and (iv) have clear and conspicuous disclosures if such disclosures are needed to prevent the advertisement from being misleading.

Before using batch emails to solicit consumers, advertisers should also consider the requirements of the CAN-SPAM Act, which generally requires unsolicited commercial emails to be clearly identified as an advertisement in the body of the email, provide the sender's valid physical postal address, and include a clear and conspicuous electronic opt-out mechanism. Under CAN-SPAM, the sender must also avoid using deceptive subject lines or false header information.

Likewise, before deploying marketing via a telephone, SMS text or fax, advertisers should consider the consumer privacy safeguards in the Telephone Consumer Protection Act (« TCPA »). For instance, the TCPA and its implementing regulations impose limitations on robocalls and other telemarketing calls, the use of automatic telephone dialing systems and artificial or prerecorded voice messages, and require compliance with do-not-call and opt-out mechanisms.

Another potential trap for unwary advertisers is Section 43(a) of the Lanham Act, which permits a person to file a claim for false endorsement when his/her name, likeness, or persona has been used to promote goods or services without his/her permission. Historically, these cases were brought mainly by television and sports celebrities or other public figures, but are increasingly being brought by social media stars. For example, a district court in New York used a plaintiff's social media following as an indicator of whether the plaintiff was sufficiently well known to support a false endorsement claim. See Mayes v. Summit Entm't Corp. (E.D.N.Y. Jan. 18, 2018).

The FTC's Recent Focus on Online Behavioral, Word-of-Mouth and Native Advertising

Recently, the FTC provided additional guidance on online behavioral advertising ("OBA"), word-of-mouth marketing, and native advertising. OBA is the practice of tracking consumers' online activities over time, including consumers' searches, web pages visited, and content viewed. This information is then used to deliver targeted advertisements to the consumer that an advertiser believes will match a consumer's interests. In 2009, the FTC published Self-Regulatory Principles for Online Behavioral Advertising, which encouraged self-regulation in the area of OBA. Actions and settlements by the FTC related to OBA are typically brought when a business misrepresents the extent to which it is tracking consumers or when an opt-out option is offered to consumers, but the business does not abide a consumer's choice.

Word-of-mouth marketing has also received attention from the FTC. In its Guides Concerning the Use of Endorsements and Testimonials in Advertising, the FTC addressed social media advertising by influencer reviews, word-of-mouth campaigns, and customer testimonials. The FTC has taken the position that anyone promoting a product must disclose their connection to the advertiser and brought numerous actions against companies whose endorsers did not provide proper disclosures.

Another pitfall for AdTech companies is the use of native advertising. Native advertising is when various brands are integrated into traditional editorial spaces in online and mobile communications. In 2015, the FTC released its Native Advertising: A Guide for Businesses along with its Enforcement Policy Statement on Deceptively Formatted Advertisements providing guidance on the disclosure that must be present in native advertising. The FTC explained that native advertising is deceptive when consumers do not realize that an advertiser is behind the content. The use of native advertising without proper disclosure has also led to a number of FTC actions and settlements.

"

WORD-OF-MOUTH MARKETING HAS ALSO RECEIVED ATTENTION FROM THE FTC [...] ANYONE PROMOTING A PRODUCT MUST DISCLOSE THEIR CONNECTION TO THE ADVERTISER.

Data Protection Laws

Advertisers that collect personally identifiable information from residents of certain states in the USA must also consider applicable state requirements. For example, California residents must consider whether California's Online Privacy Protection Act of 2003 ("CalOPPA") will apply. CalOPPA requires businesses that collect personally identifiable information from California residents to post a conspicuous privacy policy on their website. Additionally, the California Consumer Privacy Act ("CCPA") requires certain business that are located in California or have sufficient ties to California to post disclosures related to personal information and to provide residents with rights to their personal information.

AdTech, SDKs and Other Considerations

Other laws in the U.S. impose restrictions on advertisements that are directed to certain audiences or promote products in a regulated industry. For instance, the Children's Online Privacy Protection Act regulates online services directed to children under the age of 13, and considers persistent identifiers and geolocation information to be personal information. When AdTech provider Oath Inc. provided ad exchanges that knowingly transferred persistent identifiers and geolocation information to advertisement bidders without seeking parental consent, the New York State Attorney General imposed a $4.95 million USD fine.

Notably, a US federal District Court in New Mexico recently held that COPPA applies different compliance standards for app operators and ad networks; while app operators are subject to a strict liability standard, the ad networks are held to an actual knowledge standard, meaning that they only violate COPPA if they actually know that the apps in which their SDKs are embedded are directed towards children. And Zoom recently reached an agreement with the New York State Attorney General concerning its use of Facebook SDKs, particularly in the context of Zoom conferences involving students.

Finally, advertisers should be mindful that a number of federal laws regulate advertisements depending on the type of promoted product or service, from consumer financial products (the Equal Credit Opportunity Act) to vitamins and pharmaceuticals. For example, the FDA requires advertisements for drugs to contain certain disclosures. In 2015, when Duchesnay, Inc. paid Kim Kardashian to endorse a morning sickness drug, Kim posted about the drug on multiple social media accounts. But when she did not include disclosures listing the material risks associated with the drug, the FDA sent a warning letter instructing the drug maker to take corrective actions.

Kristen Bertch, Razvan Miutescu and S. Keith Moulsdale

Whiteford, Taylor & Preston, LLP

ARTICLE

How AdTech companies use cookies

Cookies always play a very important role in debates about privacy. Why? Because cookies store users' data. It is usually difficult for users to recognize which data is stored when, how and, above all, to what extent. In this article we will discuss how data from a cookie is used to play out online marketing campaigns.

Advertising on the Internet only works effectively if the right target group is reached at the right time. With the help of the data stored in a cookie, this target group can be made very visible. In the broadest sense, the aim is to personalize the advertising as much as possible. From an advertiser's perspective, deeply personalized advertising has several positive effects, for example:

1. Advertising messages and claims can be adapted to different target groups and thus achieve a higher advertising effect.

2. Products and services can be specifically placed and advertised.

3. Regular playout of ads in relevant target groups strengthens brand loyalty.

4. Through personalized ads, advertising-financed websites can achieve higher click prices and thus generate more advertising revenue.

Personalized advertising also has advantages from the user's perspective. Many websites are financed by advertising. They generate their sales almost exclusively through advertising revenue. As a user of such websites, I cannot prevent (except through AdBlock software) being shown ads on the Internet. Through the use of cookies, users have the opportunity to help shape the content of these ads. In this way, users see ads that are highly relevant to them and may even be valuable, for example when advertisement shows products of their favorite brands.

There are various ways in which an AdTech platform can access information from a cookie or use it to display ads. AdTechs such as Google Ads in particular use advertising profiles. These are generated by a user's surfing behavior. At https://adssettings.google.com/, anyone can view, edit and of course deactivate their own profile.

Google uses this data to build specific interest groups that marketers can access when creating a campaign. Large datasets allow AdTech companies to extensively analyze the intentions behind the various stakeholders. For example, Google Ads is able to differentiate between target groups that are likely to buy and others that are not. For the campaign creator, this opens up opportunities to tailor the ad content very precisely to corresponding target groups. Another way in which AdTech companies process the information cookies gather is by so-called retargeting. Retargeting means that website visits are stored in the cookie. As a website operator, I now have the opportunity to reach these users again with advertising content in the form of display or video advertising, for example.

Here's an example: You have been looking for a new sofa on a website. The cookie stores this information, and the AdTech company serves up advertisements of the sofas you have viewed on behalf of the sofa provider. This increases the advertising effect many times over.

A transaction on a website, for example a purchase, i.e. a conversion, provides AdTech platforms with particularly high-quality information.

> “
>
> THEORIES ARE ALREADY BEING DEVELOPED, THESES TESTED AND RESULTS DISCUSSED AS TO WHAT A COOKIE BANNER MUST LOOK LIKE IN ORDER TO BOTH MEET LEGAL REQUIREMENTS AND BE ACCEPTED BY THE USER WITH THE HIGHEST PROBABILITY.

The more conversions that can be assigned to specific advertising profiles, the clearer it becomes what a profile must look like to ultimately convert on a website. Google Ads, for example, makes use of this information in campaigns with the bidding strategy « maximize conversions ». In this case, ads are preferentially played out to those advertising profiles that have a higher chance of conversion.

The European Court of Justice decided that users need to give active consent to advertising and tracking cookies. The ruling also says that previously checked checkboxes don't count. This resulted in completely new challenges for marketers. The consent of users to set cookies has thus become a new « target » in the marketing world.

Theories are already being developed, theses tested and results discussed as to what a cookie banner must look like in order to both meet legal requirements and be accepted by the user with the highest probability.

Another approach is to actively and understandably explain to the user what actually happens when cookies are accepted. In practice, it is currently apparent that most users do not want to deal with this issue at all. There are even browser extensions that automatically accept all cookies on all pages (https://www.i-dont-care-about-cookies.eu/). The extension is used by more than 500,000 users. Nevertheless, surveys also show that more and more Europeans are actively influencing cookies.

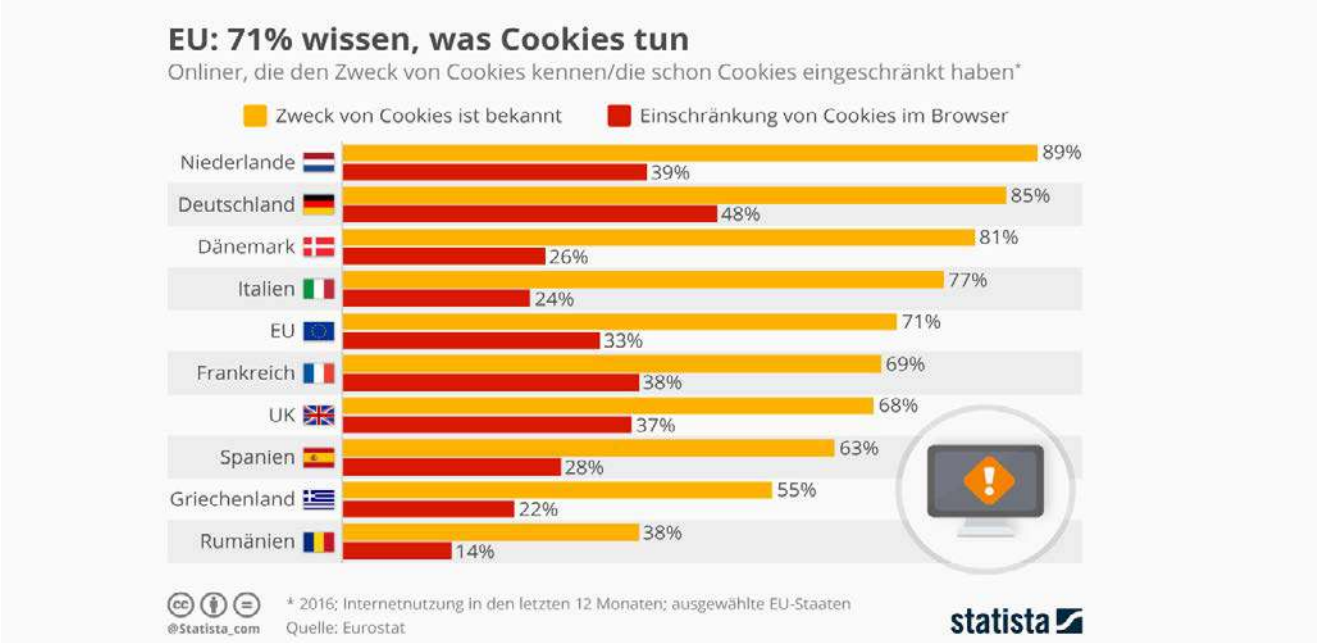
It is quite conceivable that online marketing will undergo a sea change in the next years. Without user data, it will be impossible for AdTech platforms to personalize advertising. In addition, tracking and the associated optimization of websites, apps, etc. will become more difficult. Advertising on the Internet will then probably develop more in the direction of branding once a few years ago, in a way similar to what is happening to today's television advertising. This is because, even without cookies and large amounts of data, companies will use the existing reach on the Internet for advertising purposes.

About u+i interact:

u+i interact accompanies you on your way through the challenges of digital transformation. With individual consulting, customer-centered creation and high technology competence we create perfect interactions in the digital world. We guarantee smooth functionalities in the front- and back-end and convince with strong designs. Our ace up our sleeve are our User Experience Designers to ensure ideal usability in line with user needs. We work hand in hand to bring your product to market quickly and make it a success.

In the area of marketing, we advise and support our customers in all aspects of AdTech: from the conception of campaigns, through the selection of the right tools and the creation of individual ad content, to data-driven evaluation and optimization of digital marketing.

Philipp Wittreck
Online Marketing Manager at u+i interact
pwittreck@uandi.com



DATA, INFORMATION & CYBER LAW

Members & Contacts

Theresa Adamek
Wenner
70, boulevard de Courcelles, F-75838 Paris Cedex 17, France
T: +33 1 42 66 89 00
E: theresa.adamek@wenner.eu

Laurent Badiane
KGA Avocats
44, avenue des Champs-Elysées, 75008 Paris, France
T: +33 1 44 95 20 00
M: +33 7 88 18 01 25
E: l.badiane@kga.fr

Nikolay Belokonski
KWR Belokonski Gospodinov & Partners
Alexander Zendov str. 1, fl.6, Nr.38, Sofia 1113, Bulgaria
T: +359 2 971 55 32
M: +359 887 40 94 95
E: nikolay.belokonski@kwrbg.eu

Julia Bhend
Probst Partner AG
Bahnhofplatz 18, CH-8401 Winterthur, Switzerland
T: +41 52 269 14 00
E: julia.bhend@probstpartner.ch

Matthieu Bourgeois
KGA Avocats
44, avenue des Champs Elysées, 75008 Paris, France
T: +33 1 44 95 20 00
M: +33 6 64 41 63 27
E: m.bourgeois@kga.fr

Barbara Kuchar
KWR Karasek Wietrzyk Rechtsanwälte GmbH
Fleischmarkt 1, 3 rd floor, A-1010 Vienna, Austria
T: 43 1 24 500 3145
E: barbara.kuchar@kwr.at

Isaac D. López
Cayad - Cancino Ayuso Abogados
Mexico city, Mexico
T: 52 20 01 01, ext. 119
E: ilopez@cayad.com

Marta Margiocco
Cocuzza & Associati Studio Legale
Via San Giovanni Sul Muro 18, 20121 Milano, Italy
T: +39 02-866096
E: mmargiocco@cocuzzaeassociati.it

Michał Matuszczak
Babiaczyk, Skrocki i Wspólnicy Sp. K
ul. Wyspianskiego 43, 60 – 751 Poznan, Poland
T: +48 61 8441 733
E: m.matuszczak@bsiw.pl

Patricia McGovern
DFMG Solicitors
Embassy House, Ballsbridge, Dublin D04 H6Y0, Ireland
T: +353 1 637 6600
D: +353 1 637 6614
E: pmcgovern@dfmg.ie

Anna Mertinz
KWR Karasek Wietrzyk Rechtsanwälte GmbH
Fleischmarkt 1, 3 rd floor, A-1010 Vienna, Austria
T: +43 1 24 500 3131
E: anna.mertinz@kwr.at

Sebastian Meyer
BRANDI Rechtsanwälte
Adenauerplatz 1, 33602 Bielefeld, Germany
T: +49 521 96535 812
E: sebastian.meyer(at)brandi.net

Razvan Miutescu
Whiteford, Taylor & Preston
7 St. Paul Street, Baltimore, MD 21202-1636, USA
T: +1 410 347 8744
E: rmiutescu@wtplaw.com

S. Keith Moulsdale
Whiteford, Taylor & Preston
7 St. Paul Street, Baltimore, MD 21202-1636, USA
T: +1 410 347 8721
E: skmoulsdale@wtplaw.com

Tomáš Mudra
UEPA advokáti s.r.o.
Voctárova 2449/5, 180 00 Prague, Czech Republic
T: +420 234 707 444
E: TMU@uepa.cz

Antonio Muñoz de Gispert
Absis Legal
c/ Muntaner 379, Ent. 1º, 08021 Barcelona, Spain
T: +34 93 531 91 00
M: +34 650 41 33 70
E: amunoz@absislegal.com

Tomislav Pedišić
Vukmir & Associates
Gramaca 2L, 10000 Zagreb, Croatia/Hrvatska
T: +385 1 390 0508
E:tomislav.pedisic@vukmir.net

Katharina Windisch
KWR Karasek Wietrzyk Rechtsanwälte GmbH
Fleischmarkt 1, 3 rd floor, A-1010 Vienna, Austria
T: +43 1 24 500 3131
E: katharina.windisch@kwr.at

CONNECT WITH US

PANGEANET
INTERNATIONAL NETWORK OF INDEPENDENT LAW FIRMS

To find our other publications and newsletters

CLICK HERE

Email: info@pangea-net.org
Website: www.pangea-net.org
Linkedin: /company/pangeanet