**International Conference for Doctoral, Post-Doctoral Students and Young Researchers in Humanities and Social Sciences**
May 31-June 2, 2023, Iași, Romania
**SECTION: LEGAL SCIENCES**
**DOI:** 10.47743/kaleidoscope.law.2023.1.04

# Legal and Ethical Dimensions of Processing Personal Data for Direct Marketing Purposes

**Petru ISTRATI**[1]

## Abstract

The development of information technologies is perceived with great openness in the trade and marketing sector. Direct marketing is the activity of communicating, by any means, advertising information about products and services, which is directed to specific people. Direct marketing can bring a number of benefits, including: increasing sales, optimizing costs, better meeting customer needs, etc. At the same time, direct marketing can be accompanied by a number of risks, starting from annoying customers or potential customers, drawing them into addictions and vices (such as gambling, etc.) to violating their privacy. EU Regulation 679/2016 (hereinafter – GDPR) pays increased attention to respecting the rights of data subjects for marketing purposes. It is important that when processing data for marketing purposes, the principles of data protection contained in art. 5 of the GDPR, in particular the principle of transparency and data minimization. To be considered a genuine basis for data processing for marketing purposes, the data subject's consent should be free and well-informed. At the same time, the data subject must have the possibility to withdraw their consent at any time to the processing of their data for marketing purposes.

***Keywords***: data protection, data subject, consent, GDPR, marketing, data controller.

[1] Doctoral School "Legal Sciences" of the Moldova State University, Chisinau, Republic of Moldova.

## Introduction

Not all advertising activities are direct marketing. For example: banners, TV advertising or any other form of advertising that is not necessarily targeted at a specific person is not direct marketing.

Contextual marketing is tailored to the content that is viewed or accessed by the user (Article 29 Data Protection Working Party, 2009). Routine customer service message do not count as direct marketing – in the other words, correspondence with customer to provide information they need about a current contract or past purchase (The ODPA, 2023).

However, if additional personal data is processed and the advertising is aimed at a specific person, one of the two legal grounds is required: the controller's consent or legitimate interest. The other legal bases such as contract, public interest, legal obligation, could hardly be regarded as the corresponding legal basis for direct marketing.

As described in the Cisco 2022 Consumer Privacy Survey, 76% of consumers said they would not buy from an organization they did not trust with their data, and 81% agreed that the way an organization treats their data is indicative of how it views and respects its customers (CISCO Systems INC, 2023).

Advertisers are finding it easier to target their adverts because of advances in machine learning and the huge volumes of data being generated (Rana, R., Bhutani, A., 2022). However, the data protection discussion is not just about company lawyers. These aspects must be integrated into the way of thinking and action of several decision-makers, both from the upper management hierarchy and from IT, trade and marketing professionals. If there is a gap between the way of understanding things between those listed, it will be very difficult to achieve high results in this field.

## Literature review

The starting point in carrying out this study was, obviously, the legislation in force. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter – "Directive on privacy and electronic communications" or "e-privacy Directive") along with Directive 95/46, currently together with GDPR, represents the main act that regulates privacy in the electronic field.

According to Article 1 point 1 of e-Privacy Directive: "This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community" (e-privacy Directive, 2002).

Implementation of EU directives requires a minimum level of implementation and thus there is harmonization to a large extent (Custer et. all, 2019). Taking into account technological progress and the new directions of communication development, the need to improve this legislation has arisen. On January 10, 2017, the European Commission submitted the proposal for the E-Privacy Regulation. We note that, this time, as in the case of the GDPR, a "Regulation" was chosen as the form of the legislative act. Which means that it is directly applicable in all states, and there is no longer a need, as in the case of the Directive, for national transposition legislation. This ensures that rules are uniform across the entire EU (with certain exceptions, to be discussed below). This provides clarity for supervisory authorities and organizations alike. In addition, given the key role the GDPR plays in the Proposed Regulation, this helps ensuring consistency across both instruments (European Data Protection Supervisor, 2017). At the time of preparing this paper, the E-Privacy Regulation has not yet entered into force.

We continued to probe the aspects of data protection and privacy in the field of marketing through the lens of interpretations, opinions and Guidelines made available by the Article 29 Working Party and the EDPS, as well as the data protection authorities of different countries (such as CNIL; ICO etc.).

As for the legal doctrine, we note that, on the subject, there are mainly specific works with a utilitarian aspect, intended especially for organizations that only intend to comply with GDPR requirements in their activity segment – marketing. However, there are extensive works dedicated especially to related fields, but valuable information about data protection in the advertising system can be gleaned from them. We point out that many of the papers were written in recent years, so it is noticeable that the turnover is increasing in the legal literature.

## Purpose of Present Study

New forms of marketing based on customer profiling and extensive data collection took place; information was no longer collected to support supply chains, logistics and orders, but to target products at specific users. As a result, the data subject became the focus of the process and personal information acquired an economic and business value (Mantelero, 2022).

This article is intended both for data subjects to understand what direct marketing actually means from the perspective of their rights, and for organizations to understand their obligations and mechanisms to ensure privacy while maintaining a high return for their companies of advertising.

According to a report carried out by the French data protection authority (CNIL, 2019) regarding the biggest concerns of data subjects 35,7% of complaints concern the dissemination of data on the internet, while in second place, 21% of complains concern the marketing/commerce sector.

By far, the processing of data for marketing purposes is one of the most annoying processing for data subjects for several reasons: (i) It is often aggressive; (ii) Data subjects feel that they are "Used"; (iii) There is insufficient knowledge about the legal basis of the processing and how they can exercise their rights.

For quite a long time it was believed that ensuring confidentiality and respecting the rights of data subjects, on the one hand, and entrepreneurial activity, on the other, were a zero-sum game.

This perception, a bit obtuse, is starting to be dismantled, step by step, since new institutions of data protection law are emerging as effective (privacy by design & privacy by default, data protection impact assessment, codes of conduct). So, companies are increasingly interested in investing time, money and attention in the matter of personal data in order to remain effective market players in the long term.

## Methodology

Legal research in the field of data protection is completely and utterly specific.

Data protection legal research is entirely specific. It involves a mix of combining tradition and innovation. Without consolidated legal institutions it is

not possible, but at the same time, it has the characteristic of interdisciplinary with a lot of new technological, social, economic and legal trends.

The historical-evolutionary method was used to create this article. For us it was important to observe how certain institutions appeared and or developed in the legal regime of data protection and how they metamorphosed over time.

Logical method of analysis: The use of this method is imperative for any study and allows the definition of concepts, the delimitation of features, the formulation of conclusions and proposals (Istrati, 2021).

In the process of working on this study, we also used sociological methods, maybe not directly, but through the indicated references. This approach allowed the identification of the needs, fears, difficulties and anxieties of the data subjects, but also of the data controllers. Thus, theoretical concerns have taken shape in practical application.

In addition to many other methods and techniques, which cannot be exhaustively presented here, we will highlight the systemic method. We cannot research privacy and data protection issues in direct marketing without a systems approach. That is, a framing in the basic concepts (such as: processing principles, subjects' rights, field-specific instruments, the interpretations already given by Article 29 Working Party and EDPS and others) and vision starting from them.

## Discussions

### About direct marketing and privacy

For the purpose of direct marketing, personal data is often gathered from the data subject (customer). For instance, when shopping for some items, an individual leaves his/her contact details and wishes to be notified (Office of the Personal Data Protection Inspector, 2019). It is almost an axiom and a good starting point that, should there be a collision between the rights and interests of the data subject and the purposes of the controller who wants to carry out direct marketing actions, the former prevail. Personal data of individuals have begun to have value in the economic world, in the information and communication markets, and they start to be the subject of specialized marketing (Molinaro &Ruaro, 2022). Most of the time there are no template solutions to achieve a mutually beneficial outcome. An individual approach is necessary starting from some guidelines that enjoy a broad consensus.

## Principles

Data protection principles need to be respected in all areas where data is processed. Data processing for marketing purposes may present increased risks for data subjects. At the same time, there are no clearly defined rules in this field, as marketing activities can take different forms. So, the processing principles are a guiding light that can help in carrying out legality and compliance tests. Obviously, below we present very succinctly the essence of these principles.

Since the principles of data protection can be interpreted as flexible, it is up to the data controller, in our case the one who determines the purpose and means of carrying out direct marketing, to adjust them to his particular situation.

*Responsibility*. The principle of responsibility is expressly indicated in art. 5 para. (2) of the GDPR and in art. 10 para. (1) of Convention Council of Europe for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, adopted on 28 January 1981, modified by the Decision of the Committee of Ministers at the 128th session, 18 May 2018 (hereinafter – "Convention 108+"). Responsibility means the diligence that the data controller must show when putting into practice the rules regarding the confidentiality and security of the processing, the rights of the subjects, etc. Responsibility can be approached in stages, in the first phase the compliance with all legal obligations provided for all data controllers and, in the second phase, the compliance and implementation of good practices, recommendations, additional preventive measures in the specific field – our case of direct marketing. Referring to controller liability and responsibility, author Van Alsenoy summarizes that: […]in order to properly understand operator liability exposure, it is necessary to first understand the nature of the operator's obligations. [...]It should be noted that certain requirements require further assessment in the light of the specific circumstances of the processing (for example, whether or not the personal data is "excessive" will depend, inter alia, on the purposes of the processing). Therefore, the precise nature of the operator's obligations must always be determined (Van Alsenoy, 2016). An effective tool for transposing the principle of responsibility in life can be found in recitals 89 and 90 of the GDPR which address situations when certain processing operations are likely to generate increased risks and the measures to be taken by the controller in order to carry out the Data Protection Impact Assessment. Next, article 35 of the GDPR

describes the situations in which such a study is required and what it should contain.

*Transparency*. The concept of transparency in the GDPR is user-centric rather than legalistic and is realized by way of specific practical requirements on data controllers and processors in a number of articles (European Data Protection Supervisor, 2018). Communication of information should be done in an accessible manner, using clear and simple language. The information should be neither too legal nor too "technical".

*Fairness.* The principle of fairness mainly concerns the relationship between the controller and the data subject. The ideal materialization of the fairness principle would be for data processing to be carried out only on the basis of consent and for the data subject to have effective control over the processing of the data concerning him. The principle of fairness extends beyond transparency and is linked to ethical considerations, which exceed legal requirements (European Union Agency for Fundamental Rights, 2018). In addition to legality, fairness also implies a deontological side and ethical diligence combined with transparency. From this principle follows the burden of proof that rests with the controller to demonstrate that the processing corresponds to all standards. This principle is all the more important in the conditions of the information society.

*Purpose and storage limitation*. The principle of purpose limitation is a paramount part of data protection law, as the properly defined purpose of the processing operation is a precondition to determine whether the processing complies with the law (Bieker, 2022). A wrong practice, but so common that it is a kind of *modus operandi* for most data controllers, is the excessive collection of data, both useful and useless, and then deciding what to do with it. This practice is all the more enticing as data storage capacities are getting cheaper and often the time and energy costs of selecting data are higher than storing it. Data controllers must first understand that limiting storage is primarily limiting collection. That is, collection for specific, explicit and legitimate purposes, and subsequent processing that is not incompatible with these purposes. If the purpose is reached or the storage term expires, an alternative solution to data deletion is the anonymization or pseudonymization of the data. To avoid violating these principle controllers should set deadlines for data destruction or periodic review. In the Digital Rights Ireland case, the CJEU invalidated Directive 2006/24/EC of the EP and the Council of 15 March 2006 on the retention of data

generated or processed in connection with the provision of publicly accessible electronic communications services or communications networks (Digital Rights Ireland, 2014). One of the reasons behind this solution was the lack of objective criteria for establishing the duration of data retention.

*Availability and accuracy*. Another component of the security obligation is to protect personal data against accidental destruction or loss (Van Alsenoy, 2019). On the other hand, the controller must ensure that the data processed is accurate. In the event that they are not processed in the true form, the controller must take measures to rectify them, and if it is not possible to ensure the deletion/destruction of the data.

*The principle of data protection by design and by default.* This principle is an increasingly popular one. It is found in art. 25 of the GDPR. With the application of respect for privacy from the moment of conception and by default, the problem, often invoked, is eliminated, such as that connecting a functional system, which involves data processing, to the rigors of the law requires disproportionate resources and costs. Generally speaking, the concept of privacy by design means that if a system includes choices for the consumer on how much personal data will be shared with others, the default settings should be the most privacy friendly ones (Jezova, 2020). Privacy cannot be guaranteed in the future just by adhering to legal requirements; instead, it must become an organization's standard operating procedure (Luthfi, 2022).

## Legal basis for processing data for direct marketing purposes

In order to comply with data protection principles, any data processing must be based on a legal basis. The most well-known and firm legal basis for marketing activities is the consent of the data subject. But doctrine and practice consider that legitimate interest, in certain situations, can also be considered as a basis for this purpose, provided that the processing does not affect the rights and interests of the data subject.

The data protection regime (and eCommerce legal regime/framework) refers to permissible direct marketing and sets out various obligatory requirements while at the same time setting a default position of prohibiting non-exempted or non-permitted electronic direct marketing (Lambert, 2020).

***Consent***

To be considered valid, the consent must comply with the provisions of the GDPR. There are several component elements for a consent to be considered valid: **(i)** free; **(ii)** informed; **(iii)** specific; **(iv)** unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (EU Regulation 679/2016, Article. 4). Consent cannot be considered free if it is subject to any restriction. For example, consent will be considered vitiated if it is obtained in exchange for an additional product or service, discount, etc. A common, but also quite practical, question is the possibility of using personal data for direct marketing that has been obtained from third parties, and not from the data subject. In this case, the data controller must be aware that at any time he must be able to demonstrate the origin of this data. If these data were obtained based on the data subject's consent, the controller must be able to demonstrate that the consent included the possibility of transmitting these data to third parties, for their direct marketing companies. The level of diligence of data controllers must be high, or the phenomenon of illegal commercialization of databases is constantly increasing.

According to a research of the price of personal data in the Dark Web, various pieces of information may be more valuable to criminals and it depends on a variety of factors. Thus, debit or credit card data can cost between $5 and $110, while login data on various non-financial platforms costs $1, and the price of a person's medical records varies between $1 and $1000 (Stack, 2017). Special care is required when the of personal data of children are used for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child ((EU Regulation 679/2016, recital 38).

There are different forms by which the data subject can give his consent for the processing of his data for marketing purposes, as well as in the case of its withdrawal. ‘Opt in’ means a person has to take a specific positive step (e.g. tick a box, send an email, or click a button) to say they want marketing. ‘Opt out’ means a person must take a positive step to refuse or unsubscribe from marketing (ICO, 2018). In general users lack the basic understanding of the collection of any data, its uses, how the technology works and more importantly

how and where to opt-out. As a result, in practice very few people exercise the opt-out option (Article 29 Data Protection Working Party, 2010).

The U.S. online media and marketing industry, led by the Digital Advertising Alliance or "DAA," has launched an opt-out program that uses icons in online ads (Ramirez, 2012). In fact, the "opt-out" must work both for data processing started based on the consent of the subject and in the case of processing based on the legitimate interest of the data controller. It is imperative that "opt-outs" are free and in no way conditional. The data subject does not have to justify his choice. The lack of the opt-out option, but especially the hiding of the identification data of the controller constitutes a violation of the principles of data protection.

It is a good practice, both when the controller relies on consent, but also when it opts for legitimate interest as the basis for processing, that the controller keeps a record of all data processing operations. Obviously, the register does not necessarily need to be kept in physical form, but can take different forms that are best tailored to the processes and needs of the controller.

***Legit interest***

The legitimate interest as a legal basis for the processing of personal data is expressly found in the GDPR itself, in the recital 47, according to which: the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest (EU Regulation 679/2016); invoking legitimate interest in processing activities for direct marketing purposes is rather an exception to the consent rule and should be used with great caution. The more sensitive the data, the better it is to opt for consent as the basis for processing.

It would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering (Article 29 Data Protection Working Party, 2018). Advertisements based on legitimate interest should be closely related to the products and services already contracted by the data subject and controller.

Unlike the opt-in mechanism I talked about above, the "soft opt in" mechanism is a procedure by which controllers generate advertisements characteristic of direct marketing, using the subject's data, which he previously provided, when he used the controller's products and services or when he expressed such an intention.

When designing the marketing actions, the controller must ask himself whether, based on the relations he has with the data subject, the latter would have expected to be subjected to direct marketing or not. Eleni Costa considered the concept of soft opt-in quite questionable even before the advent of GDPR: The use of the term "soft opt-in" is used due to the fact that the customer has already given his electronic mail contact details to the sender in the context of a customer relation. However the term can be criticised, as the customers are given the opportunity to object to receiving direct marketing communications and they do not express in any way their agreement to receive such communications (Costa, 2013).

Marketers must be aware that, the more extensive or intrusive the profiling for direct marketing, the more likely it is to infringe on the individual`s rights and thus not fulfil the legitimate interest processing condition (Direct Marketing Association, 2018). Thus, more intrusive and opaque processing of personal data, including surveillance, profiling and automated decisions, is likely to require consent. Consent has the advantage that it provides documentation as well as clarity concerning the legitimate basis, which must be determined before the collection of personal data (Trzaskowski, 2022).

## Relationship with data subjects: Rights

Most of the time, there is an imbalance in the relationship between the personal data controller and the data subject. This imbalance can be generated by the employee-employer relationship, the institutional and/or social architecture, or it can be one generated by financial factors, etc. In the case of direct marketing, the imbalance between the data controller and the data subject, and implicitly the bargaining power, may be caused by the data subject's lack of specific knowledge, the position of the data controller as a monopolist or a technological or economic giant, and/ or the authorized person.

In order to return the data subject to the position where he has a minimum control over his personality rights, the legislator has endowed him with certain rights specific to the legal regime of personal data protection. In order to more easily perceive the need for these rights, we could make an analogy with labor legislation or legislation on the protection of consumer rights. Below we will briefly refer to the most important ones.

*Information and access.* In order to ensure a fair and transparent data processing, the controller must make available to the data subject, at least, information relating to: his identity and contact details (possibly of the responsible person, if he has been appointed); the purpose and legal basis of the processing; the possible recipients of the data, the storage period, the rights of the subject, etc. Controllers of personal data, especially in the field of direct marketing, should show a proactive attitude and not necessarily wait for an address from data subjects. The information that needs to be shared with data subjects can be displayed at the headquarters of the legal entity, on its website, in the applications managed by it, available by accessing the QR code when providing products and services by the personal data controller. Attract attention the marketing fluff and declarations of good intentions, such as "We take privacy seriously," "Your privacy is important to us" or "We deploy state-of-the-art data security measures." Such statements do not provide the data subject with meaningful information and merely provide additional ammunition to plaintiff's attorneys and regulators that believe the company did not in fact sufficiently respect privat interests or comply with laws (Determan, 2022).

*Right to object*. Data subjects have the right to object to their data being processed. Even if this right is provided for in the normative acts stated above, the controller must additionally inform the data subject about this right before or at the time of data collection. At least in the case of communications made via electronic media, also in each commercial communication directed at them (AUTOCONTROL, 2021). Article 21 (2) of GDPR determines that: 2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing (EU Regulation 679/2016).

*Right to data portability.* The right to data portability aims to provide extended freedom to the data subject, allowing him/her not to be shackled with regard to his/her data by a particular controller. The right to data portability helps to stimulate data exchange which is essential in a digital economy. This right is provided for in art. 20 of the GDPR.

*Rectification, Erasure and Restriction.* Rectification, erasure and restriction are distinct rights but are part of the group of "Opposition" rights on the part of the data subject. To the general public, the right to delete data is known as "*the*

*right to be forgotten*". In the GDPR, the right to be forgotten is provided for in 2 articles: 17 "The right to delete data" and indirectly in art. 21 "The right to opposition". In the direct marketing sector, for example, the data subject who objects to direct marketing by phone will be put on a special list of persons whose phone number may not be used for direct marketing purposes (called for example 'orange list' or 'Robinson list') (Terwangne, 2013). The right to be forgotten can be interpreted as a tool to defend honor and dignity, but it remains a mechanism specific to the legal data protection regime, available to the data subject, which allows him to play an active role in protecting his rights.

This right helps redefine a person's behavior concerned with his own data, he having the opportunity to evaluate and reevaluate his personal information available to the public, thus increasing his control over his identity (Serban, 2017). The subject of the rights of data subjects can be approached multidimensional, including in the context we are talking about – direct marketing. We could refer to the psychological perspective. social, anthropological or at the most "Machiavellian" – economic. As it was seen, we chose to focus only on those rights provided for in the relevant legislation. Leaving, somewhat, the subject open. Jamie Day, in his PhD thesis "*Privacy vs Technology: what rights do we have and how can we protect these rights?*" when approaches the very interesting concept of "unobservability", underlines the fact that the theories related to privacy aim at 3 directions: (i) the interest in controlling/protecting a personal space, (ii) the interest in having/having control of one's personal relationships and (iii) the interest in expressing one's self-identity, in reflecting, in making decisions, in developing as a person and protecting one's personality/individuality (Day, 2018).

*The right not to be subject to an automated decision and profiling* without human intervention. Automated decision-making processes are used more and more in different fields, such as: recruitment, credit granting, insurance, etc. These processes bring with them a series of advantages: a high yield, cost reduction, time optimization, etc. Of course, automatic decision-making and especially profiling mechanisms are also used in individually targeted advertising. At first glance automated decision-making processes may seem harmless, but if decisions made by algorithms are capable of producing legal consequences for a natural person then the level of concern should be raised. In addition to the ethical considerations, which start from the ontological aspect that man is removed from the equation, it is worth taking into account the fact that any

process does not have 100% accuracy. Even though some algorithms have an efficiency of over 99%, for massive data processing (several tens of thousands per day, such as facial recognition in crowded public places) "mistakes" mean hundreds of people about whom a wrong decision was made, without being able to be contextualized. Thus, art. 22 para. (3) of the GDPR provides what are the guarantees and insurance measures that the controller must take in such cases. Human intervention is a key element. Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should undertake a thorough assessment of all the relevant data, including any additional information provided by the data subject (Article 29 Data Protection Working Party, 2017).

*Right to file a complaint to the Data Protection Authority and Right to an effective judicial process*. The role of the supervisory authorities in protecting natural persons when processing their data is extremely important. The legal data protection regime can be placed on 3 big pillars: a) Subjects' rights; b) Responsibility of controllers and authorized persons; c) The activity of the supervisory authorities. The importance of effective supervisory authorities is provided, among others, in art. 51, recital 145, 146 of the GDPR. In the jurisprudence of the Court of Justice of the European Union (hereinafter – CJEU), the role of the supervisory authorities was highlighted in several cases. In the CJEU Decision in case no. C 518/07 of March 9, 2010 European Commission, supported by the European Data Protection Authority versus the Federal Republic of Germany (*Commission v. Germany*, C-518/07), the Court emphasized the need to ensure "full independence" of the supervisory authority, in order to be protected from political influences, while remaining subject to compliance with the law, under the control of the courts. In another case initiated by the European Commission against Austria (*Commission v. Austria*, C-614/10), the CJEU highlighted the need for material and logistical assurance of the supervisory authorities in order to guarantee their total independence. And in a case initiated by the European Commission against Hungary (Commission v. Hungary, C-288/12), the CJEU emphasized the need to respect the independence of officials within the supervisory authorities and the danger of ending their mandates before the deadline, even if there is a restructuring or a change of organizational model .

In one of the most high-profile cases of the CJEU in the field of data protection, Case C-362/14 of 6 October 2015, initiated by the well-known activist

Maximillian Schrems against the Data Protection Commissioner with the participation of Digital Rights Ireland Ltd, the decision by which Privacy Shield was invalidated (Commission Decision 2000/520), the Grand Chamber referred to the powers of protection authorities in relation to international data transfers (Shremes, C-362/14).

In addition to the right to address the supervisory authority, the data subject has the right to address the court. Access to justice is a universal right, it is also applicable to the legal data protection regime, either to challenge a decision of the supervisory authority (article 78 GDPR) or to ascertain the violation of his rights by the controller and/or authorized person ( article 79 GDPR). An under-explored mechanism is also the possibility of the data subject to request the repair of the damage and the granting of compensation.

Each of the rights described are equally important. Although some may be neglected by data subjects, controllers must ensure that they provide the necessary conditions for them to be exercised by data subjects.

## Conclusion

Despite negative prediction from marketers, GDPR did not kill Marketing. For Anybody who scratched the surface of the GDPR, this was probably expected. However, it did change the marketing landscape, but that was a much needed change (Data Privacy Manager, 2022).

One of the challenges facing government, business community and broader society is that we currently know very little about the extent of injuries or harm on and from the Internet (Walter, Trakman & Zeler, 2019).

Data controllers must be more actively involved in legal and ethical aspects, by determining the exact roles (controller, joint-controller, processor, third party, subject, etc.) to establish the legal basis for processing, ensure compliance with the principles of protection and of the rights of the persons concerned. Given that direct marketing can be quite intrusive and annoying, controllers need to ensure openness, transparency and flexibility. Of course, the implementation of these rules involves additional resources, but they also bring with them a series of benefits, even if not very quickly noticeable and quantifiable. However, being “data protection compliant” represents a significant advantage over other players on the market who ignore the new legal and technological realities.

In order to demonstrate a pro-active attitude, the controller can make available a series of tools that increase confidentiality and respect for the rights of data subjects: pseudonymization; privacy dashboards; location granularity; encryption; protection against tracking etc.

The consent of the data subject is a shield against the intrusions to his privacy that relate to the processing of his personal data. However, the concept of privacy, exactly as the concept of data protection, is not a static one (Costa, 2013). As the forms of marketing take on new and new contours, so the protection measures must be reviewed periodically.

## References

Alessandro Mantelero, (2022), *Big Data and Data Protection,* in González Fuster, G., Van Brakel, R. and De Hert, P. *Research Handbook on Privacy and Data Protection Law Values, Norms and Global Politics,* Cheltenham, UK • Northampton, MA, USA, http://dx.doi.org/10.4337/9781786438515 .

Article 29 Data Protection Working Party, (2009), "*Opinion 5/2009 on online social networking*", Brussels, Belgium. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

Article 29 Data Protection Working Party, (2010), "*Opinion 2/2010 on online behavioral advertising*", Brussels, Belgium. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

Article 29 Data Protection Working Party, (2017), "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679",* Brussels, Belgium. https://ec.europa.eu/newsroom/article29/items/612053

Article 29 Data Protection Working Party, (2018), "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" WP251,* As last Revised and Adopted on 6 February 2018. Brussels, Belgium. https://ec.europa.eu/newsroom/article29/items/612053

AUTOCONTROL – The Association for the Self-Regulation of Commercial Communication, (2021) *Code of conduct – Data processing in advertising activities,* Madrid, Spain. https://edpb.europa.eu/system/files/2021-04/code_of_conduct_data_processing_in_advertising_activities_en.pdf

Bieker, Felix (2022), "*The Right to Data Protection Individual and Structural Dimensions of Data Protection in EU Law*", https://doi.org/10.1007/978-94-6265-503-4.

CISCO Systems INC, (2023) "*Privacy's Growing. Importance and Impact. CISCO 2023 Data Privacy Benchmark Study" https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html*

Commission Nationale Informatiques & Liberties, "*Rapport d'activité 2018 et enjeux 2019*" https://www.cnil.fr/sites/cnil/files/atoms/files/dossier_de_presse_cnil_bilan_2018_et_enjeux_2019.pdf

Convention Council of Europe for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, adopted on 28 January 1981, modified by the Decision of the Committee of Ministers at the 128th session, 18 May 2018. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

Custer, B., et. all (2019) "*EU Personal Data Protection in Policy and Practice",* https://doi.org/10.1007/978-94-6265-282-8

Data Privacy Manager, (2022) *GDPR and direct marketing. Understanding how to conduct a GDPR compliant marketing,* Croatia. https://dataprivacymanager.net/marketing-gdpr-requirements-gdpr-challenges-and-requirements/ .

Day, Jamie (2018) "*Privacy vs. Technology: What privacy rights do we have and how we protect these rights*?", Thesis Submitted in Fulfilment of the Requirements for the Degree of Doctor of Philosophy, Queen's University of Belfast.

De Terwangne, Cecile, *The Right to be Forgotten and the Informational Autonomy in the Digital Environment*. EUR 26434. Luxembourg (Luxembourg): Publications Office of the European Union; 2013. JRC86750, DOI: 10.2788/54562.

Determan, L. (2022), "*Determann`s Field Guide to Data Privacy Law, International Corporate COmpliance, Fifth Edition",* http://dx.doi.org/10.4337/9781802202915.

Direct Marketing Association (2018) *GDRP for marketers: The essentials.* United Kingdom. https://dma.org.uk/uploads/misc/5a8eea20f3566-gdpr-essentials-for-marketers----an-introduction-to-the-gdpr-amendment-v1_5a8eea20f34aa.pdf

European Data Protection Supervisor (2017), Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation[2002,58/EC]. Brussels, Belgium. https://ec.europa.eu/newsroom/article29/items/610140/en

European Data Protection Supervisor (2018), *Guidelines on Transparency under Regulation 2016, 679.* Brussels, Belgium. JUSTICE AND CONSUMERS ARTICLE 29 – Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) (europa.eu).

European Parliament and the Council of the European Union, Directive 2002/58/ EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37 (31.07.2002).

European Union Agency for Fundamental Rights (2018) "Handbook on European data protection law" Luxembourg. Doi:10.2811/58814.

Georgian Office Of The Personal Data Protection Inspector (2019), *Recommendation on personal data processing for direct marketing purposes*, https://personaldata.ge/cdn/2019/01/Recommendations-on-Personal-Data-Processing-for-Direct-Marketing-Purposes.pdf

Information Commissioner's Office, 09 May 2018, "Guide to Privacy and Electronic Communications Regulations", page 15, https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/.

Istrati, Petru (2021), "*Methodological characteristics of the scientific research in personal data protection field*", CZU: [342.721+343.41/.45]:001.891.

Jezova, Daniela (2020) "*Principle of Privacy by design and Privacy by default*" DOI: https://doi.org/10.18485/iup_rlr.2020.ch10.

Judgement of 06 October 2014, *Schrems*, C-362/12=4, paragraph 43, 50. https://curia.eu.

Judgement of 08 April 2014, *Commission v. Hungary*, C-288/12, paragraph 57. https://curia.eu.

Judgement of 08 April 2014, *Digital Rights Ireland*, C-293/12&C-594/12, paragraph 63, 64. https://curia.eu.

Judgement of 09 March 2010, *Commission v. Germany*, C-518/07, paragraph 19, 42. https://curia.eu.

Judgement of 16 October 2012, *Commission v. Austria*, C-614/10, paragraph 57, 58. https://curia.eu.

Kosta, Eleni. (2013) *Consent in European data protection law*, (Nijhoff studies in EU law; volume 3) Leiden. Boston.

Lambert Paul, (2020), " *A User's Guide to Data Protection: Law and Policy*, Fourth Edition" ISBN: 978 1 52651 571 1.

Luthfi, Ahmad (2022) "*Towards Privacy by Design on the Internet of Things (IoT) Use: A Qualitative Descriptive Study*", http://journal-isi.org/index.php/isi, e-ISSN: 2656-4882 p-ISSN: 2656-5935.

Molinaro C.A. and Ruaro R.L. (2022) "*Privacy Protection with Regard to (Tele-) Communications Surveilance and Data Retention"* https://doi.org/10.1007/978-3-030-90331-2.

Ramirez, Edith (2012, 13 June), Remarks of Commissioner Edith Ramirez at Privacy by Design Conference, Hong Kong "*Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission*".

Rana, Ramit, Bhutani, Apurva., (2022) "*Artificial Intelligence – The Need of the Hour*", in Dewani N. D. et all, "*Handbook of Research on Cyber Law, Data Protection and Privacy",* IGI Global. ISBN 9781799886433.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Serban, Andreea (2017) "*Regulation of the right to be forgotten*" Scientific Annals of the University "Al. I. Cuza" Iasi, Volume LXII, Legal Sciences, no. 2.

Stack, Brian (06 December 2017) "Here's How Much Your Personal Information Is Selling for on the Dark Web", https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

*Surveillance and Data Retention"* in Albers, M. et. all "*Personality and Data Protection Rights on the Internet – Brazilian and German Approaches*" p. 113-132. https://doi.org/10.1007/978-3-030-90331-2.

The Office of Data Protection Authority of Guernsey (2023), *Direct Marketing – A guide for Organizations*, Guernsey. https://www.odpa.gg/information-hub/guidance/direct-marketing/ .

Trzaskowski, Jan (2022) "*Data-driven business models –Privacy and marketing*" in Kosta, E., Leenes, R., Kamara, I., (2022) "*Research Handbook on EU Data Protection Law*", Cheltenham, UK • Northampton, MA, USA. http://dx.doi.org/10.4337/9781800371682.

Van Alsenoy, Bredan (2019) "*Data Protection Law in the EU: Roles, Responsibilities and Liability*" ISBN 978-1-78068-828-2.

Van Alsenoy, Brendan (2016), *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, 7 (2016) JIPITEC 271. URN: urn:nbn:de:0009-29-45064.

Walter, R., Trakman, L., Zeller, B., (2019) "*Data Protection Law – A Comparative Analysis of Asia-Pacific and European Approaches*" Singapore. https://doi.org/10.1007/978-981-13-8110-2 .