THE LEGAL INTEREST, LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA AND THE RIGHT TO PRIVATE LIFE

Carmen Oana MIHĂILĂ*
Mircea MIHĂILĂ**

Abstract

In order to increase the protection of the right to privacy and the protection of personal data, norms have been adopted at European and national level. The right to privacy cannot receive a complete definition, covering all its meanings. We can talk about physical and social identity, but in the context of technological discoveries and social developments, the interpretation of the concept is much broader. However, this right must be correlated with the right to the protection of personal data. In other words, the protection of personal data is of fundamental importance for a person to enjoy the right to privacy within the meaning of Article 8 of the Convention. The national laws should guarantee that the use and transmission of personal data of a person is done in an appropriate framework, which is not incompatible with the provisions of the article we mentioned above.

Lately, there has been a constant and growing interest of companies to avoid consent and to rely on the legitimate interest as the legal basis for the processing of personal data. The organizations have the obligation to analyze whether the legitimate interest in processing does not affect the right to privacy of the data subjects. Thus, they must carry out an assessment of the legitimate interest. If the organizations consider that the legitimate interest prevails over the fundamental right to the privacy of the data subjects, it is necessary to take special additional measures. DPIA (data protection impact assessment) is a process designed to describe the processing, to evaluate the need for processing and to contribute to the management of the risks to the rights and freedoms of the data subjects resulting from the processing of personal data, by evaluating them and establishing measures to mitigate them.

Key Words: *right to privacy, protection, personal data, the legitimate interest, DPIA.*
JEL Classification: [K15, K24]

1. Introduction

The right to privacy is a fundamental right regulated primarily by Article 12 of the Universal Declaration of Human Rights, 1948, which states *"no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

*University lecturer Ph.D., Faculty of Law, Department of Juridical and Administrative Sciences, University of Oradea.

** Associated university lecturer, Ph.D eng., Faculty of Electrical Engineering and Information Technology, Department of Computers and Information Technology**,** University of Oradea.

Another document, the Convention for the Protection of Human Rights and Fundamental Freedoms, stipulates in art. 8 "*Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".*

Article 7 of the Charter of Fundamental Rights of the European Union (EUCFR) provides that *"every person has the right to respect for private and family life, domicile and the secret of communications."*

The constitutions of the states of the world regulate this right to privacy or to the protection of personal data (Slabu 2018)[1].

Article 8 paragraph 1 of the EUCFR and art. 16 paragraph 1 of the Treaty on the Functioning of the European Union (TFEU) provides for the right of any person to the protection of personal data concerning him / her. Personal data must be used on the basis of a legal ground in a certain way and for a specific purpose, based on the consent of the person concerned. It will have access to the data being collected but also the right to obtain the rectification of its data. From the foregoing, it can be concluded that this important European document regulates in addition to the right to privacy and the right to the protection of personal data, a new law that will have a special development being specifically regulated by the *EU Regulation 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and abrogation of Directive 95/46 / EC, hereinafter referred to as GDPR*[2].

The role of the ECHR is also important in interpreting the issues related to the protection of personal data (Șandru 2018). Even in the preamble to the Regulation, the European legislator refers to the case law of the Court of Justice in several situations. Thus, in recitals 41, 143, 149 there are concepts that are interpreted from the perspective of the case law of the Court of Justice.

---

[1] https://www.universuljuridic.ro/rolul-autoritatii-nationale-de-supraveghere-a-prelucrarii-datelor-cu-caracter-personal-in-asigurarea-respectarii-dreptului-la-viata-intima-familiala-si-privata-corelarea-cu-prevederile-capitolului-v/#f1, accessed on 11.03.2020.

[2] For the application of the Regulation, some measures have been adopted such as the elaboration of guidelines by Group 29: Guide on the right to data portability, Guide on the Data Protection Officer (DPO) and Guide on identifying the leading supervisory authority of an operator or authorized person. Directive 1995/46 / EC led to the establishment of the "Article 29" Working Party, an independent, consultative European body composed of representatives of the national data protection authorities of the Member States of the European Union, representatives of the authorities created for the Community institutions and bodies, as well as representatives of the European Commission. This group has been replaced, with the adoption of new regulations with *European Data Protection Board (EDPB*).

At the level of internal regulation, the Civil Code stipulates in art. 58 (*Rights of the personality*), the right of any person "to life, health, physical and mental integrity, dignity, self-image[3], respect for privacy, as well as other such rights recognized by law." These are personal rights, they are primordial rights of the human person (Cornu 2005) that have common characteristics: absolute, non-patrimonial, irreplaceable, imprescriptibly extinctive and acquisitive, inalienable, intangible, or opposable erga omnes[4]. The doctrine shows that these rights are compared to *a series of generic notions incompatible with a precise definition, such as freedom, honor, privacy, respect*. Therefore, the court will take into account in each case the extent to which such rights exist. (Baias, Chelaru, Constantinovoci & Macovei 2012).

2. Legitimate interest - the legal basis for the processing of personal data. Data Protection Impact Assessment (DPIA)

The right to private life does not exclude the "outside world", it is not limited only to the "inner circle" in which the person lives their personal life, it also means the right to private social life, professional, commercial activities. In a certain public context one can talk about the sphere of private life[5].

The protection of natural persons with regard to the processing of personal data is a fundamental right, yet not an absolute one, as stated in the Regulation (p. 4 of

[3] Art. 73 Civil Code, having as a marginal title the right to one's own image establishes that *every person has the right to their own image. In exercising the right to their own image, they may prohibit or prevent the reproduction, in any way, of their physical appearance or voice or, as the case may be, the use of such reproduction*. The person's ability to censor the use of his/her image is based, as the specialists state, on individual autonomy.

The right to image and privacy has certain limits, so there are situations in which certain actions are considered lawful: the video monitoring of public institutions, the images captured on public roads for road traffic surveillance. However, it is necessary for the public to be informed about these monitoring systems. The Penal Code in art. 226 para. 1 stipulates that the prejudice to privacy, without the right, by photographing, capturing or recording images, listening by technical means or audio recording of a person in a dwelling or room or premise on it or a private conversation is punishable by imprisonment from one month to 6 months or with a fine.

[4] According to art. 74 Civil Code are considered to be privacy breaches, inter alia, *the unauthorized interception of a private call, committed by any technical means, or the use, knowingly, of such interception; capturing or using the image or voice of a person in a private space, without their consent; dissemination of materials containing images regarding a person undergoing treatment in healthcare units, as well as personal data on health status, problems of diagnosis, prognosis, treatment, circumstances related to the disease and other various facts, including the result of the autopsy, without the consent of the person concerned, and in the event that he/she is deceased, without the consent of the family or the persons entitled; dissemination or use of correspondence, manuscripts or other personal documents, including address, residence and telephone numbers of a person or members of his/her family, without the consent of the person to whom they belong or who, as the case may be, has the right to to dispose of them.*

[5]Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence, European Court of Human Rights, 31 august 2019, p. 20

the recitals). With the adoption of the Regulation, the doctrinal discussion in relation to the eventual qualification of this right as fundamental (Ungureanu & Munteanu 2014) was terminated.

This right must be balanced with other fundamental rights, in accordance with the principle of proportionality[6].

The Regulation observes *all the fundamental rights and freedoms and principles recognized in the Charter as enshrined in the Treaties, in particular respect for private and family life, residence and communications, protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and a fair trial, as well as cultural, religious and linguistic diversity.*

It should be noted that the notion of *personal data* does not overlap, however, with the notion of *information concerning the private life*[7], as it is understood in the common sense of the term, but it also includes any other information, including those from the sphere of the professional activity of a person (Popescu 2018).

According to recital 75 of the GDPR, the processing of personal data may result in damages of *a physical, material or moral nature*. Also, this processing can *lead to discrimination, theft or fraud of identity, financial loss, compromise of reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymisation or any other significant disadvantage of economic or social nature.* Regarding the rights and freedoms of the persons concerned, it is stated in the European legal text that they could be deprived of their rights and freedoms or prevented from exercising control over their personal data. Personal data of vulnerable persons, especially of some children or a larger volume of data, may be processed, thus affecting a large number of data subjects.

Lately, there is a constant and growing interest of companies to avoid consent and to avail themselves of the *legitimate interest* as the legal basis for the processing of personal data. The assessment of the legitimate interest is presented under the name of *legitimate interest assessment* (Timofte 2019).

The consent of the data subject is a defining element, particularly important. Therefore, in many of the cases brought before the ECHR, it is shown that according to "*art. 8 paragraph (2) of the Charter, personal data may be processed only on the*

[6] *The protection of personal data plays a fundamental role in the exercise of a person's right to respect for private and family life, as guaranteed by art. 8 of the Convention. National law must provide adequate safeguards to prevent any use of personal data that might be incompatible with the guarantees provided by this article*, Case S. and Marper v. The United Kingdom, file 30562/04, Strasbourg, December 2008, point 103, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}, accessed on 09.03.2020.

[7] To determine whether the personal information held by the authorities involves any of the aspects of privacy, the Court will properly consider the specific context in which the information in question has been recorded and kept, the nature of the records, how these records are used and processed, and of results that can be obtained, Case S. and Marper v. The United Kingdom, file 30562/04, Strasbourg, December 2008, point 67.

basis of the consent of the person concerned or on the ground of another legitimate basis provided by law[8].

Companies or organizations may process personal data if they identify a legal basis for such processing. *The legitimate interests of an operator, including those of an operator to whom personal or third-party data may be disclosed, may constitute a legal basis for processing, observing the condition that the interests or fundamental rights and freedoms of the data subject do not prevail* (point 47 of the Recitals). However, as shown below in the GDPR, *the fundamental interests and rights of the data subject could prevail, especially in relation to the interest of the data operator when personal data are processed in circumstances in which the data subjects do not reasonably foresee a further processing.*

Art. 6 paragraph 1 of the GDPR also specifies that the legitimate interest must be in accordance with the fundamental rights and freedoms of the data subject, especially when the data subject is a child.

Although the GDPR states that if there is a high risk for the rights and freedoms of the natural person, the operator must carry out an evaluation of the impact of the data processing before processing (art. 35 paragraph 1), regarding the assessment of the legitimate interest does not contain special mentions. However, it is obvious that such an evaluation would be necessary. This evaluation should be documented by the operator according to their obligation of responsibility obligation (Șchiopu 2019).[9]

The legitimate interest could be identified in the GDPR vision when there is a relevant and appropriate relationship between the data subject and the operator (the data subject is the operator's client or an employee).

For example, if we talk about sending correspondence from an operator to a client, the situation in which it is operated with a lot of data. In such cases, evaluation would no longer be absolutely necessary.

On the contrary, the operator's interest would be lower than that of the data subject when the personal data are processed *in circumstances in which the data subjects do not reasonably expect further processing.*

As far as public authorities are concerned, there is no question of legitimate interest, given that the legislator *must provide the legal basis for the processing of personal data by public authorities.*

The justification of the legitimate interest in the processing of personal data without the person's consent can be given for the purpose of preventing fraud[10].

[8]Case Michael Schwarz v Stadt Bochum C-291/12, decision of 17 October 2013, point 31, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0291&from=RO, accessed on 11.03.2020.

[9] The Article 29 Working Party recommends to operators who would like to take advantage of the exception from the information obligation to balance (balancing exercise) the effort involved for the operator to provide information to data subjects, on the one hand, and the effects on to the data subject if the information was not provided, on the other hand.

[10]The court may consider the context in which the information is taken and the nature of the data. Thus, the states will benefit from a wider margin of decision regarding the retrieval and storage

Also, direct marketing can cause data processing based on a legitimate interest (recital 47 of the GDPR). When a company wants to do postal marketing in connection with a new product, but using the existing customer base, it can do this based on the legitimate interest, not needing the clients' consent for this correspondence.

Law 506/2004 *on the processing of personal data and the protection of privacy in the electronic communications sector* expressly provides in art. 12 the need for the consent of the data subjects in the case of the types of unsolicited communications. The distinction must be made between direct marketing made through leaflets, brochures transmitted to existing customers and direct marketing, unsolicited communications made by electronic means (Coman 2019). Thus, it is shown that a provision of the special law (L. 506/2004) that imposes the existence of express consent with that of the general rule (GDPR) cannot be replaced, which shows that the legitimate interest is *sufficient for the transmission of unsolicited communications by the operators of personal data* (Coman 2019).

Many of the complaints addressed to personal data protection authorities at European level refer to telemarketing or promotional emails or lack of consent for various ads[11]. Since the date of entry into force of the GDPR, May 25, 2018, ANSPDCP[12] has received 3064 complaints and notices, the total amount of fines for this year being 631,500 lei (Coman 2019).

The legitimate interest must always be in accordance with the law or good manners. Another condition is related to the specific character of this legitimate interest. If the purpose of the processing is generic, there can be no question of legitimate interest.

The assessment of the legitimate interest involves several elements. Firstly, *the nature and volume of the data processed* must be determined, then *the expectations of the data subjects regarding the processing*[13] and finally *the potential impact on the data subjects or the organization*[14] (Timofte 2019) must be taken into account. The prejudices or risks that organizations may face are important in interpreting the legitimate interest. Also, the type of organization is important, whether it is a bank, a financial institution, a telecom company, etc.

---

of information about persons related to terrorist activities, Case Segerstedt-Wiberg and others v. Sweden, file no 62332/00, Strasbourg, 6 June 2006, point 88, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-75591%22]}, accessed on 12.03.2020.

[11] Thus, in France, the National Commission for Informatics and Freedoms, the French arbitrator for personal data, is the first European regulatory court to sanction the Google Internet platform on the basis of the GDPR with 50 million euros. Google has been fined for providing inadequate information regarding the purpose of processing and the lack of marketing consent regarding Android OS configuration.

[12] The National Authority for the Supervision of Personal Data Processing

[13]For example, the data subject could be an employee of a service provider who sends to the business partners data from their CV to receive personalized communications.

[14]An eventual video monitoring could benefit the company but also the employees, the data subjects in case a crime is avoided, for example a theft.

If the data processed are of the kind of those regulated in art. 9 paragraph 1 of the GDPR, special data, [15] it is necessary in this context of the legitimate interest to provide additional guarantees regarding the protection of the privacy of the persons concerned. Paragraph 2 of the same article 9 contains the exceptional situations, where processing is legitimate, even in the absence of the consent of the one concerned. The personal data referring to criminal convictions or offenses are processed under the control of a state authority or when the processing is authorized by Union law or by national law which provides adequate guarantees for the rights and freedoms of the persons concerned (art. 10).

In case the organizations consider that the legitimate interest prevails over the fundamental right to privacy of the data subjects, it is necessary to adopt additional special measures. The categories of data to be processed should be minimized, increased transparency of processing, limitation of the period of data storage, restriction of access to these data, use of anonymization techniques (Timofte 2019).

If the balance between the legitimate interest and the rights of the data subjects does not tilt towards the first, an assessment is needed on the impact that the processing of personal data would have.

Thus, art. 35 paragraph 1 of the GDPR states: "*In view of the nature, scope of application, context and purposes of processing, where a type of processing, especially that based on the use of new technologies, is likely to generate a high risk for the rights and freedoms of natural persons, the operator performs, before processing, an assessment of the impact of the planned processing operations on the protection of personal data. A single evaluation can approach a set of similar processing operations with similar high risks."*

The Article 29 Working Party established through the *Guidance on Data Protection Impact Assessment* (DPIA) *and the determination whether a processing is "likely to generate a high risk" within the meaning of Regulation 2016/679*[16], clarified the criteria that can help identify the processing operations that are subject to the requirement of a DPIA. In most cases, the personal data operator may consider that a processing having two criteria would require a DPIA. However, there are situations in which a data operator may consider that there is an obligation to evaluate even if only one criterion is met[17]. The criteria listed in the Guide are: evaluation or scoring, automatic decision making with significant legal or similar

[15]*The processing of personal data that discloses racial or ethnic origin, political opinions, religious confession or philosophical beliefs or membership to trade unions and the processing of genetic data, biometric data for the unique identification of a natural person, health data or data on the sexual life or sexual orientation of a natural person is forbidden*.

[16]Reviwed and adopted on 4 October 2017, on https://www.dataprotection.ro/servlet/ViewDocument?id=1439.

[17]" Risk" is a scenario that describes an event and its consequences, estimated in terms of severity and probability. "Risk management" can be defined as coordinated activities for the management and control of an organization regarding risk, in the Guide on Impact Assessment on Data Protection (DPIA) and determining whether a processing is "likely to generate a high risk" within the meaning of the Regulation 2016/679, WP 248 rev.01, p. 6, accessed on 13.03.2020.

effect, systematic monitoring, sensitive or extremely personal data, large-scale data processing, correlation or combination of data sets, data which concern vulnerable persons, the innovative use or application of new technological or organizational solutions, or when the processing itself prevents individuals from exercising a right or using a service or contract.

The DPIA, according to the GDPR *represents a risk management tool for the rights of the data subjects and therefore presents their perspective (for example, the security of the company). Instead, risk management in other areas (eg information security) focuses on the organization.* [18]

Such an assessment would be necessary in the following cases: if a hospital processes data related to patient health, if a system is monitored by cameras on the freeway with video analysis by the operator to identify the cars and the registration plates, employee monitoring, including their activity on the Internet, collecting public data on social media for profiling, creating national databases on credits or fraud, storing for archiving sensitive pseudonymised personal data concerning vulnerable data subjects in research projects or clinical studies.

An assessment would be necessary when a carrier sets up rooms in the means of transport, a bank takes over customers from a database containing credit information, or a hospital creates a database containing patient health information, but it will not be necessary in the case of a family doctor who processes the data of his patients.

DPIA *will not be required* if the nature, purpose, context and purposes of the processing are very similar to the processing for which the DPIA has already been performed, when the processing operations were verified by the supervisory authority before May 2018 under specific conditions that have not been modified (when processing is included in the optional list established by the supervisory authority for processing operations for which DPIA is not required).

The National Supervisory Authority for the Processing of Personal Data (ANSPDCP) issued in this respect Decision no. 174/2018 regarding the list of operations for which it is compulsory to carry out the impact assessment on the protection of personal data. The decision implements art. 35 paragraph 4 of the GDPR according to which *the Supervisory Authority draws up and publishes a list of the types of processing operations that are subject to the requirement to carry out an impact assessment on data protection, in accordance with paragraph (1).* The evaluation is known as DPIA - *data protection impact assessment*[19] (Crețu 2018) or DPIA (Iancu & Turtoi 2019). On the basis of the principle of responsibility, personal data operators must carry out the assessment of possible

[18] Guide on Impact Assessment on Data Protection (DPIA) and determining whether a processing is "likely to generate a high risk" within the meaning of the Regulation 2016/679, WP 248 rev.01, p. 18, accessed on 13.03.2020.

[19] http://dataprivacyblog.tuca.ro/dpia-lista-nationala-a-activitatilor-de-prelucrare-pentru-care-este-necesara-efectuarea-unui-impact-asupra-protectie-datelor-cu-caracter-personal/ accessed on 13.03.2020.

risks when processing data that could create high risks regarding the rights and freedoms of the data subjects (recital 84 GDPR).

Following the assessment, the operators will establish the appropriate measures to reduce or eliminate the impact or even to abandon the processing if the proposed measures are not enough (depending on the available technology and the cost of implementing these measures). If the risk is high, the operator will consult with the supervisory authority before processing.

This assessment should apply as a priority to situations where a large amount of data is processed, when processing is done on a large scale (at regional, national or supranational level) or targets a large number of people, when it comes to sensitive data, especially if the processing operations generate a high risk for the rights and freedoms of the data subjects (recital 91 GDPR).

Decision 174/2018 provides for 7 cases in which the DPIA is mandatory, these being not presented in a limited way[20]:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

b) Processing on a large scale of personal data which regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation or of personal data relating to criminal convictions and offences;

c) a systematic monitoring of a publicly accessible area on a large scale, such as the video surveillance of public areas as shopping centers, stadium, parks and other similar spaces;

d) processing on a large scale of personal data pertaining to vulnerable natural persons, especially to minors or employees, based on means of automated monitoring and/ or systematic recording of their behavior, including carrying out activities involving commercials, marketing and advertising;

e) processing on a large scale of personal data through the innovative use or the implementation of new technology, particularly where those operations limit the ability of data subjects to exercise their rights, such as the use of facial recognition techniques to facilitate access to different spaces;

f) processing on a large scale of personal data generated by devices with sensors which send data over the Internet or by other means ("Internet of Things"

[20]According to Opinion 19/2018 on the draft list of the competent supervisory authority of Romania regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR), 25 September 2018, EDPB (European Data Protection Board), there is an obligation that these lists are not exhaustive and recommends the Romanian authority to include this provision in documents (point 2.1).

applications such as Smart TVs, connected vehicles, smart meters, smart toys, smart cities or other such applications);

g) large scale and/ or systematic processing traffic data and/ or geolocation data of the data subjects (such as Wi-Fi monitoring, geolocating passengers in public transportation or other similar cases) when the processing is not necessary for the performance the services requested by the data subject.

It can be observed that in the case of the first three situations what brings the decision in addition to the provisions of art. 35 of the Regulation is the explanation given regarding the large-scale systematic monitoring provided in letter. c. As regards the large-scale processing of personal data of vulnerable persons, the assessment will be made even if the processing is not carried out by automatic means of systematic monitoring or recording of the behavior. It may be necessary to perform the DPIA even for processing activities that, in particular, would not entail a high risk for the data subjects (use of the mechanisms for registering the access in the IT systems by the own employees - access logs used for the purpose of security / ensuring the integrity of data accessed by employees) (Crețu 2018).

If we analyze the provision from letter g, it would be relevant the question posed by the specialists, namely whether *such an obligation to perform the DPIA also applies to the traffic data (included in the telephone / internet invoices) processed by the employer in the context of working relationships with their own employees who use employers' phones (for the purpose of economic-financial management and without the employer monitoring the electronic communications used by the employees)?*

The main element of this decision seems to be the large-scale processing, respectively the systematic processing.

Decision no. 174/2018 also provides for an exception from the obligation to perform the *DPIA*, respectively: when the processing is carried out pursuant to art. 6 paragraph (1) letter c -*processing is necessary in order to fulfill a legal obligation of the operator* or e - *processing is necessary to perform a task that serves a public interest or results from the exercise of the public authority with which the operator of the GDPR is invested*, when the processing has a legal basis in Union law or in national law and an impact assessment on data protection has already been carried out as part of a general impact assessment in the context of the adoption of the respective normative acts.

Performing a *DPIA* is mandatory only for the operator pursuant to article 39 paragraph. 1 of Regulation 2018/1725[21], where processing is "likely to generate a high risk for the rights and freedoms of natural persons." [22] Also, in the content of

[21]Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing of Regulation (EC) no. 45/2001 and Decision no. 1247/2002 / EC.

[22] Recommendation 01/2019 on the draft list of the European Data Protection Supervisor on processing operations subject to the data protection impact assessment requirement (Article 39 (4)

this European document, it is shown that if an assessment of the impact on data protection would demonstrate that processing would, in the absence of guarantees, security measures and risk mitigation mechanisms, pose a high risk to the rights and freedoms of people, and the operator considers that the risk cannot be mitigated by reasonable means in terms of available technologies and the costs of implementation, the European Data Protection Supervisor should be consulted prior to the start of processing activities.

A DPIA may concern a single data processing operation. Article 35 paragraph 1 of the GDPR states that "*a single assessment may concern a set of similar processing operations with similar high risks*". Furthermore, recital 92 adds that there are circumstances in which it may be reasonable and economical for the data protection impact assessment to be broader rather than a single project, for example, when public authorities or bodies intend to create a common application or common processing platform, or where more operators intend to introduce a common application or common processing environment in a sector or segment of industry or for a widely used horizontal activity (for example, a group of municipal authorities each installing a similar CCTV system could perform a single DPIA that covers processing by these separate controllers, or a railway operator could cover video surveillance in all its stations with one DPIA, or assessment for a technological product such as a hardware or software component that could be used by several operators, even if the operator who implements the product later will perform DPIA for the specific implementation).

In 2017, the European Parliament and the Council presented a Proposal for a Regulation on *observing privacy and the protection of personal data in electronic communications and repealing Directive 2002/58 / EC (Regulation on privacy and electronic communications).*[23] This proposal is considered *lex specialis* in relation to the GDPR. The document details and completes the provisions of the GDPR regarding the data transmitted in the electronic communications that fall into the category of personal data. In addition to the GDPR, the proposal aims to protect communications and the legitimate interests of legal entities[24]. Articles 16 and 114 of the TFEU represent the legal basis for the proposal, and this document comes to ensure the application of art. 7 of the EUCFR, which protects the fundamental right of all persons to respect for their private and family life, their domicile and their communications (Matei 2019).

As electronic communications concerning a natural person are normally considered to be personal data, their protection with regard to the confidentiality of communications and the processing of such data should be based on Article 16 TFEU. The Proposal therefore seeks to ensure the confidentiality of information in

of Regulation (EU) 2018/1725), adopted at 10 July 2019 by EDPB, p. 3.

[23] Bruxelles, COM/2017/010 final - 2017/03 (COD), https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52017PC0010&from=RO, accessed on 14.03.2020.

[24]The data transmitted within the electronic communications may disclose information regarding legal persons (business secrets or other sensitive information with economic value).

the online environment containing personal data. In our country Law 506/2004 *on the processing of personal data and the protection of privacy in the electronic communications sector* transposes Directive 2002/58 / EC of the European Parliament and of the Council of the same name.

The Proposal for a Regulation shows that *it aims to increase the effectiveness of the protection of privacy and personal data processed in connection with electronic communications*[25] *and to increase the level of protection, in accordance with Articles 7 and 8 of the Charter, as well as to ensure a greater legal security. The proposal complements and details the GDPR*. In order to ensure the exercise of freedom of expression and information, or the right to the protection of personal data, freedom of thought, conscience and religion, the effective protection of the confidentiality of communications is essential.

The regulation should apply to data transmitted through electronic communications (traditional voice telephony services, e-mail, SMS text messages but also functionally equivalent online services such as internet telephony, messaging services and e-mail addresses[26]) that are processed in connection with the provision and use of electronic communications services in the Union, whether or not the processing takes place within the Union.

The impact assessment on data protection and, where appropriate, a consultation of the supervisory authority is required according to the Proposal for a Regulation where a type of processing of metadata on electronic communications, in particular involving the use of new technologies, is likely, taking into account of the nature, scope, context and purposes of processing, to generate a high risk to the rights and freedoms of natural persons (according to articles 35 and 36 of the GDPR).

Also in this document it is shown that, *by virtue of the right to privacy and the protection of personal data of a natural person, it is necessary for the end users who are natural persons to request their consent before their personal data is included in the a list of subscribers accessible to the public. According to the* ***legitimate interest*** *of legal entities, the end-users who are legal entities should have the right to oppose the inclusion in a list of subscribers, accessible to the public, of the data concerning them.*

For the protection of end-users against unsolicited communications for direct marketing[27] purposes that represent intrusions in their private life, guarantees must

[25] Electronic communication services include not only Internet access services, which consist, in whole or in part, in the transmission of signals, but also interpersonal communication services, which may or may not be based on numbers, such as telephone services via the Internet, messaging and e-mail services on the Internet.

[26] Point 11 of the preamble to the Regulation Proposal.

[27]Direct marketing refers to any form of advertising by which a natural or legal person sends communications for direct marketing purposes to one or more identified or identifiable end-users using electronic communication services, messages sent by political parties contacting individuals through the electronic communication services in order to promote themselves, the messages sent

be provided (for example, by using automatic call and communication systems, instant messaging applications, e-mails, SMS, MMS). Thus, it is justified to request the consent of the end user before sending commercial electronic communications for marketing purposes directly to it, to effectively protect individuals against intrusion into their private life, such as and to protect the legitimate interests of legal entities.

However, it is shown in the same document, *it is reasonable to allow the use of the contact data by e-mail in the context of an existing relationship with a client for the provision of similar products or services* (limited to the company that obtained the electronic contact data according to GDPR).

Conclusions

The existence of a legitimate interest may justify the processing of personal data, but it is important that this interest do not exceed the interests or fundamental rights and freedoms of the data subjects.

The assessment of the impact on the protection of personal data (DPIA), which has a certain processing of these data, is mandatory when the processing is likely to generate a high risk for the rights and freedoms of individuals. For the companies that are included in the list called the blacklist, which we find in Decision no.174 / 2018, it is necessary to carry out the documentation, evaluation and finalization of the DPIA. The achievement of the DPIA is ultimately a useful activity that helps to comply with the legislation on the protection of personal data (in compliance with the criteria mentioned in the Guide and the Decision).

European citizens should have a greater sense of trust in the digital system with the adoption of new regulations on the protection of personal data. However, there are skeptics who say there is no evidence in this regard (Layton & Mclendon 2018).

Bibliography

Books

1. Baias, Fl.A., Chelaru, E., Constantinovici, R. & Macovei, I. (coord), 2012, *Noul Cod civil. Comentariu pe articole*, C.H. Beck, Bucharest.
2. Cornu, G., 2005, *Droit civil. Introduction. Les personnes. Les biens*, Montchrestien, Paris.
3. Ungureanu, O. & Munteanu, C., 2013, *Drept civil. Persoanele*, Hamangiu, Bucharest.

Journals

1. Coman, A., 2019, „ANSPDCP. Peste 5000 de plângeri și sesizări privind protecția datelor cu caracter personal în 2018”, *Revista Română de Protecția Datelor*, 13 February, 6-7.
2. Coman, A., 2019, *“*Interesul legitim” - temei legal de prelucrare pentru activitățile de marketing direct?” *Revista Română de protecția datelor*, 17 June, 2.

by other non-profit organizations in order to achieve the organization's objectives, point 32 of the preamble to the Regulation Proposal.

3. Creţu, S., „# DPIA - Lista națională a activităților de prelucrare pentru care este necesară efectuarea unui impact asupra protecție datelor cu caracter personal”, 2.11.2018, viwed on 13 march 2020 from http://dataprivacyblog.tuca.ro/dpia-lista-nationala-a-activitatilor-de-prelucrare-pentru-care-este-necesara-efectuarea-unui-impact-asupra-protectie-datelor-cu-caracter-personal/
4. Iancu, M. & Turtoi, A., 2019, „Considerente practice privind lista DPIA publicată de ANSPDCP*”, Revista Română de Protecția Datelor*, 13 February, 18-21.
5. Layton, R. & Mclendon, J., 2018,“The GDPR: What It Really Does and How the U.S. Can Chart a Better Course”, *The Federalist Society Review*, 19, 238.
6. Matei, A., 2019, “E-Privacy, lex specialis în raport cu GDPR”, *Revista Română de Protecția Datelor*, 12 January, 6-10.
7. Popescu, R., 2018,“GDPR Ce informaţii reprezintă date cu caracter personal”, *Revista Universul Juridic* (10), October, 70-81.
8. Slabu, E., 2018, “Rolul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal in asigurarea respectării dreptului la viață intimă, familială și privată. Corelarea cu prevederile Capitolului VI din Regulamentul (UE) 2016/679”, *Revista Universul Juridic*, Bucharest, 18 September.
9. Șandru, A.M., 2018, “Privire critică asupra jurisprudenței Curții de Justiție a UE referitor la interpretarea art. 8 privind protecția datelor cu caracter personal din Carta Drepturilor Fundamentale a Uniunii Europene (EUCFR)”, *Revista Pandectele Române* (1), 26-33.
10. Șchiopu, S.D., 2019, “Absența obligației de informare în ipoteza prevăzută de art. 14 alin. (5) letter b) din Regulamentul general privind protecția datelor”, *Revista Universul Juridic*, (3), March, 64-70.
11. Timofte, C., 2019,“LIAnt pentru interesul legitim”, *Revista Română de Protecția Datelor*, 14 March, 7-10.
12. Ungureanu O. & Munteanu, C., 2014, *“*Dreptul la protecția datelor cu caracter personal, un drept autonom?*” Revista Română de Drept Privat* (1), 166-179.

World Wide Web

1. https://www.universuljuridic.ro/rolul-autoritatii-nationale-de-supraveghere-a-prelucrarii-datelor-cu-caracter-personal-in-asigurarea-respectarii-dreptului-la-viata-intima-familiala-si-privata-corelarea-cu-prevederile-capitolului-v/#f1, accessed on 11.03.2020.
2. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}, accessed on 09.03.2020.
3. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-75591%22]}, accessed on 12.03.2020.
4. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0291&from=RO, accessed on 11.03.2020.
5. http://dataprivacyblog.tuca.ro/dpia-lista-nationala-a-activitatilor-de-prelucrare-pentru-care-este-necesara-efectuarea-unui-impact-asupra-protectie-datelor-cu-caracter-personal/ accessed on 13.03.2020.
6. https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52017PC0010&from=RO, accessed on 14.03.2020