THE 13TH EDITION OF THE INTERNATIONAL CONFERENCE
EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES

# Protection of Personal Data between EU Regulation 679/2016 and the Reality of National Security

**Alexandru-Adrian Eni**[1]

**Abstract:** The subject approached in this paper is of great relevance in the fragmented era we are crossing. With the development of the information society, the protection of personal data has become a current issue in the legal field. By adopting rules regulating access to this information, both at international and national level, postmodernism has proven its strength in the field of information and information sources, and the effect mainly found in transforming what was once unitary and consolidated in a dissipated and uncontrollable present. We should consider that any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, psychological, economic, cultural or social identity. Although some data protection reforms have been adopted by legislators in response to courts acting as reformers in the geo-politicallz context we are crossing, the EU and courts' approaches to balancing national security and data protection remain diametrically opposite.

**Keywords:** national; security; data; protection; surveillance; EU; regulation; 679/2016

## Introduction

The topic addressed in this paper is highly topical in the computer age that you know. Postmodernism has proven its strength in the field of information and information sources, and its impact consisted mainly in transforming what was once unified and consolidated into a dissipated and uncontrollable present. (Ciupercă & Vlăduţescu, 2010)

Many instances have brandished the status of information sources and have provided a large number of data boundless mediated by the public, and the various and numerous means of mass communication.

In this context, it is evident that individuals have at their disposal a range of information and sources of information, but are exceed a count's ability to process it. In this regard, most of the times without having to be aware of, they take matters proposed as priority opinion leaders, or stop at a series of incomplete information, generating cropped truths.

The concept of protection of personal data means the right of the individual to be protected from those features leading to its identification and correlative obligation of the State to adopt adequate measures in order to ensure effective protection of the person.

[1] Student, Faculty of Law, Danubius University Galati, Address: 3 Galati Blvd., Galati 800654, Romania, Tel.: +40372361102, E-mail: alexandru_eni@yahoo.com.

Through personal data information, it means information that may be directly or indirectly in relation to an identified or identifiable natural person, such as, by way of example, first and last name, social security number, address, telephone number, the image, the voice, the economic and financial situation, the profession. In view of the need to defend and respect the fundamental right to private life and protection of personal data shall constitute a domain sine-qua-non of the era that we live, a fact confirmed by treating this distinct topics in chapters set out the in Convention implementing the Schengen Agreement. (Schengen)

At the moment, since we are in the era of the Internet, 90% of the collection of data from virtual environment, and the reason for recourse to this type of documentation is the national and collective security.

As society has evolved, and to threaten the national security of States, have diversified, particularly in the sense of reversing the proportion of violence and craze.

The review of the main moments in the universal history of influencing information in order to assault on national security allows us to assert, in the spirit of the theory developed by V. Pareto, that in the field of threats to the state and implicitly in the specific space to combat them, the elite took place in the direction of transforming the "elite lions" into "fox elite". The profound reason for this metamorphosis lies in the specificity of the postmodern society, which is characterized, in particular, by the lack of evenimensional uniformity, informational abundance, foresight difficulties, etc.

**What is National Security?**

National and collective security was a fundamental problem of any government, regardless of the historical period we are reporting. Always, the resources existing in some areas have attracted the different powers of the moment, and the easiest way to get them was the theft or violence. As society evolved, ways have also evolved to threaten the national unity of states, particularly in the sense of reversing the proportion of violence and craving. (Schengen)

News from newspapers, magazines, newsletters, more than five million available online databases that include scientific papers, statistical data, is the huge number of data made available through open sources of information. All of this can be at one time intelligent weapons that can be used against those who have created them in good faith.

Referring to the legislation in force, according to the Law no. 51 of July 29, 1991, on the national security of Romania (published in the Official Gazette No 163 of 7 August 1991), art. 1 "through the national security of Romania is meant the state of legal, equilibrium and social, economic and political stability necessary for the existence and development of the Romanian national state as a sovereign, unitary, independent and indivisible state, the maintenance of the order of destitution, as well as the exercise climate unrestricted fundamental rights, freedoms and duties of citizens, according to the principles and norms democratized by the Constitution.[1]" EU rules on personal data protection come to complement, improve and create the limiting framework according to the values promoted by the European Union.

According to the national defense strategy of the country for the period 2015-2019, national security aims to ensure the commitment of the Romanian nation as a strong nation, citizens, a nation that knows what it wants in Europe, in the world and for itself. National security is carried out within the framework of the democratic order through the full exercise of citizens' rights and freedoms, the

[1] https://www.sri.ro/assets/files/legislatie/Legea51.pdf.

conscious assumption of responsibilities, the improvement of the state's decision-making and action capacity and the assertion of Romania as an active member of the international community. (Ciupercă & Vlăduțescu, 2010)

**Need to include open sources in "intelligence" activity:**

National security is, however, necessary to obtain a variety of information from highly diverse sources.

Searching and processing of the data had to be harmonized with the new political conditions, these conditions are continually being refined in the approach. A characteristic of the period we are crossing is that decisions that proved to be wrong have not been taken due to lack of information, but because of the overwhelmed informations and the inability to test the information important for the preservation of State security.

**The need to protect natural persons and legal persons with regard to processing of personal data:**

The subjects of civil law can be divided into two broad categories, namely: individuals and legal entities.

The quality of a natural person is recognized by all human beings as they are members of society, which enjoy equally the opportunity to participate in civil legal relations.

The natural person - the man - is a subject of universal law and can participate in the most diverse legal relations. (Pusca, 2006)

The legal person is a collective subject of civil law that participates independently in legal relations, having its own civil liability; a human collectivity formed directly by natural persons or the association of other legal entities as a subject of law, having a stand-alone organization and a distinct patrimony, affected by the achievement of a determined purpose in accordance with the public interest.

European norms concerning the protection of personal data, both individual as well as a legal entity, and in doing so, it has imposed the need to protect these subjects.

The European Commission has indicated, since 2012, need to update the regulatory framework applicable European data protection and proposed new rules by using the 2016/679 tool as normative Regulation.

Until 2017, the EUs primary law in the field of personal data protection constituted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data. (Șandru, 2017)

The protection of personal data is currently one of the main pillars of global society development, both socially and politically, culturally and economically. Given the fact that the computerization of areas crucial to the development of society has led to a major change in the way the contemporary world operates, it is natural that attention and global resources are directed to the digital domain, representing a new step of mankind towards a more prosperous future. This led, first of all, to the mass migration of information to the digital domain.

It is well known that the computerization of personal data systems brings many benefits compared to the bureaucratic system of the past, benefits such as: the ease and speed of processing and storing information, the resources needed to run the process compared to the old manual system, and

accessibility and efficient data handling is much higher. However, during the last decade, the problems and risks arising from this process of digitization of personal data have been revealed. The rapid evolution of technology has led to the alteration of the concept of General Data Protection provided by Directive 95/46/EC of 24 October 1995, the provisions of which have become, with the passage of time, lacking the appropriate scope in protecting individuals and data personal data of the Member States of the European Union.

**What is Regulation 679/2016?**

The General Data Protection Regulation is a Regulation adopted by the European Parliament and the Council of the European Union as part of a legislative package on data protection on 27 April 2016 published in the Official Journal of the European Union on May 4, on May 24, 2016, and applicable after the expiration of a 2-year transition period, ie from May 25, 2018.

The principles and rules on the protection of individuals with regard to the processing of personal data should, irrespective of their nationality or place of residence, respect their fundamental rights and freedoms, in particular the right to the protection of personal data. This Regulation aims at contributing to the establishment of an area of freedom, security and justice and to economic unity.[1]

Regulamentul 679/2016 se aplică autorităților și instituțiilor publice, întreprinderilor, băncilor, spitalelor, clinicilor private, farmaciilor sau magazinelor online, firmelor de securitate, entităților care, în calitate de operator sau persoană împuternicită de operator, prelucrează, în derularea activității curente, date cu caracter personal.

Regulation 679/2016 applies to public authorities and institutions, businesses, banks, hospitals, private clinics, pharmacies or online shops, security firms, entities that, as an operator or person empowered by the operator, process, in the conduct of their current business, data personal.

GDPR provisions apply from May 25, 2018, in all EU countries, and the Romanian authorities do not have to transpose them into national law, making it implicit.

GDPR applies to any organization operating within the EU. The obligation for companies to designate a person responsible for personal data protection is laid down in Regulation 679/2016.

**The need for an outbreak of 679/2016 Regulation:**

The rapid evolution of technology along with the phenomenon of globalization have, over the past two decades, led to a major shift in the way personal data is collected, accessed, transferred and used.

Beyond the time of the initial discoveries in the field, today's technology advances at astonishing speeds that often legislation, either at national or international level, is simply incapable of keeping up with real-time technology .

This has led to the emergence of major dilemmas such as:

- The inability of technological and subsequent systems, the virtual domain to offer the same protection in the preservation and processing of personal data;

- Conflicts of interest between state and third-party bodies on access to personal data of the individuals concerned, as we can see in Case C-518/07 Commission vs Germany. In this case, the German State acted contrary to the provisions of Article 28 of Directive 95/46/EC by requiring that personal data held by third-party companies, independent of the public sector, could be accessed without

[1] http://www.dataprotection.ro/servlet/ViewDocument?id=1262.

interruption by the State, the premise of keeping the security. The German State subsequently lost this action by the European Commission and was thus obliged to correctly transpose the provisions of Art. 28 (1) of Directive 95/46/EC.

The implementation Regulation 679/2016 vs. national security:

The process of implementing the new Regulation 679/2016, whose existence is defined as crucial in the application of the provisions enshrined in the EU Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms, raises a series of defining questions, the answer of which is necessary to determine the viability, necessity and effectiveness of implementing regulations with a major impact, as beyond the Regulation 679/2016, the dilemma of control exercised in the process of storing, storing, processing and protecting personal data is an essential element of the problem.[1]

We live in an information society where production and consumption of information are two of the most important activities. Information is recognized as an essential resource. New technologies are the foundation of the information environment in which we operate.

In this context, we can understand the value of information and the need to protect it so that it does not reach the enemy. The level of protection of information is determined by the degree of their usefulness. Information is, in most cases, the trump card around which winning strategies are built. Attention must be paid to the uncontrolled dissemination of information that may affect the security interests of the state, an organization or a natural person.

According to art. 31 of the Constitution of Romania "the right of the person to have access to any information of public interest can not be restricted and the public authorities, according to their competences, are obliged to ensure the correct information of citizens on public affairs and problems of personal interest; the public and private mass media are also obliged to ensure the correct information of the public opinion" (Romanian Constitution amended and completed by the Romanian Constitutional Law Review No. 429/2003).

The notion of information has a very broad meaning and represents, according to art. 15 of the Law no.182/2002 on the protection of classified information, "any documents, data, objects or activities, regardless of their support, form, manner of expression or putting into circulation" (Law 182/2002 on the protection of classified information, amended and completed by Law No 167/2015). Government Decision No. 353/2002 on the approval of NATO Standards for the Protection of Classified Information defines information as "that notion that can be communicated in any form".

Within the classified information, the national security information, which corresponds to the notion of state secret, is of particular importance, and according to whose importance different degrees of secrecy are attributed.

The National Doctrine of Security Information addresses extensively the concept of security information. This is considered to be "an analytical product, a result of the specialized search, identification, obtaining, processing/processing of data on dysfunctions, vulnerabilities, risk factors, threats, threats to the established political and social principles and rules through the Constitution and designed to contribute to maintaining internal stability and strengthening the international security environment." These needs and interests provide security information with strategic heritage value.

[1] http://intelligence.sri.ro/drepturile-si-libertatile-informatiei/.

The very basis of such control is undermined by the numerous regulations both at European and national level intersecting in the field of personal data. (Şandru 2017)

Argumentative note how according to recital (8) of the preamble (EC) No 45/2001, the data protection principles should apply to any information relating to an identified or identifiable person. In determining whether a person is identifiable, it is appropriate to consider all means that can reasonably be used either by the operator or by any other person to identify the data subject. The principles of protection do not apply to anonymous data, so that the data subject is no longer identifiable[1].

In order to achieve the protection of personal data, effective control of the data subjects, effective control over targeted persons and prevention of illicit activities such as those committed by organized criminal and terrorist groups, it is necessary to control information on each person identifies or identifies.

Simultaneously, the same reason stated that "in determining whether a person is identifiable, it is appropriate to take into account all means that can be reasonably used either by the operator or by any other person to identify the data subject.

Being in a certain us opposition, recital (7) of the preamble to the regulation 679/2016 and the business of intelligence stipulates the following: "Individuals should have control over their own personal data, and legal and practical security for individuals, economic operators and public authorities should be strengthened", exemplifying the coverage by the incidental provisions of some fundamental objections different, which directly leads to the questioning of the successful implementation of RDGP. (Şandru 2017)

**Ways to Prevent Leakage of Information**

Information security research focuses on the "human factor" in the context in which people are considered the weakest link. Information security management uses security policies as a means of defining what is expected from individuals in an organization. However, computer system users often fail to comply with these policies. To address this issue and to meet regulatory requirements, information security awareness programs are turning into key components of the safety management, and play an important role in promoting the culture of security and and the development of awareness-raising campaigns play intelligence services.[2]

The concept of awareness was taken from the social sphere, where it is assimilated to knowledge and understanding (in the sense of awareness) by individuals, groups or communities, of the evolution of the surrounding reality and of the transformations of the environment in which they live (situations, contexts, problems or phenomena existential impact), based on previous information or experience, involving observation vigilance and interference detection at an intuitive level.

The activity of awareness is an initiative undertaken by the Romanian Intelligence Service to accomplish the Mission of preventing threats to national security.

One factor that may favor the emergence of threats is the low level of security culture in the main institutions of public administration, as well as the dynamic of the regional and international security climate with impact on Romania and its allies. This state of affairs is an opportunity for hostile, state or non-state foreign entities, but also for the various local interest groups, acting outside the legal framework.

[1] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32001R0045.
[2] https://www.sri.ro/awareness.

Therefore, it is desirable to strengthen the cultural security in Romania by:

- highlighting the potential security risks to which the officials are exposed by the nature of the activities carried out or the type of data and information to which they have access;

- the presentation of the counterinformative behavioral elements, as well as the necessary elements for the identification of the hostile information actions;

- emphasizing the utility of adopting proactive behavior (self-protection or SRI expertise when required).

Institutions handling classified information and sensitive information (protected by special laws or internal rules) are given a detailed account of what they need to know about the implementation of an immune system that ensures both data, system and staff protection, as well as the development of mechanisms for identification and management of counterinformative risk situations.[1]

**What is personal data**

• First name, last name, address, date of birth, nationality, ethnicity, telephone number, CNP, image, civil status;

• E-mail, IP address, genetic data, biometric data; (fingerprint, DNA, handwriting signature, retinal model, face geometry, face structure, voice, blood patterns, etc.).

• Public function, salary, political affiliations, trade union affiliations;

• Traffic data, location data, cookie identifiers, radio frequency identification tags, etc.

**Special personal data**

- racial or ethnic origin;
- political opinions;
- Religious confession;
- philosophical beliefs;
- membership of trade unions;
- genetic data;
- biometric data;
- health data;
- data on life or sexual orientation;
- data on criminal convictions and offenses.

**Who is the data subject**

- the natural person whose personal data are subject to processing;

- the person for whom it was built entire GDPR mechanism.

**The concept of processing of personal data:**

[1] http://intelligence.sri.ro/awareness-in-securitatea-online/.

Is any operation or set of operations performed upon personal data, whether or not the use of automated means:

- collect;
- structuring;
- storage;
- extraction;
- the use;
- dissemination;
- align/combine;
- deleting;
- organization;
- register;
- adaptation/ modification;
- consultation;
- disclosure by transmission;
- making available in any other way;
- restriction;
- destruction.

**What does DPO?**

Data Protection Officer DPO is a person who has specialized knowledge of data protection laws and practices and is responsible for assisting the operator or the person empowered by the operator to monitor the compliance at internal level with the provisions of EU Regulation 2016/679.

**Who can be the DPO?**

The DPO can not at the same time take on a decision-making function.

GDPR provides that the Data Protection Officer can also handle another function within the firm, but only to the extent that there are no conflicts of interest. "The Data Protection Officer can perform other tasks and tasks. The operator or person empowered by the operator ensures that none of these tasks and attributions lead to a conflict of interest", GDPR, EU Regulation 2016/679.

**Who cannot be DPO?**

Cannot be disabled by the DPO driving functions, such as:

- Administrator or general manager;
- Financial director;
- The Human Resources Director;
- The marketing manager.

**Data Protection Officer:**

Data Protection Officer DPO is a person who has specialized knowledge of data protection laws and practices and is responsible for assisting the operator or the person empowered by the operator to monitor the compliance at internal level with the provisions of EU Regulation 2016/679.

Public authorities or institutions, businesses, banks, security firms, hospitals, private clinics, pharmacies or online stores, entities that, in the capacity of operator or person empowered by the operator, process personal data in the conduct of their current activity are required by virtue of the provisions of Regulation 679/2016, designate a Data Protection Officer.

Simultaneously, the DPO can not, at the same time, take up a decision-making function. GDPR provides that the Data Protection Officer can also handle another function within the firm, but only to the extent that there are no conflicts of interest. "The Data Protection Officer can perform other tasks and tasks. The operator or person empowered by the operator ensures that none of these tasks and attributions lead to a conflict of interest", GDPR, EU Regulation 2016/679.

**GDPR shall not apply to processing of personal data carried out:**

- By a natural person in an exclusively personal (domestic);
- By the competent authorities for the purpose of preventing and combating crime (Directive 2016/680);
- In the context of an activity that does not fall under EU law;
- Other situations provided for in article 10. 2 GDPR (activities covered head 2, title V of the EU Treaty-foreign policy);

**The principles of personal data processing, art. GDPR 5:**

- Legality - Data processing legally, fairly and transparently to the data subjects;
- Responsibility - The operator is required to demonstrate compliance with GDPR;
- Security, integrity, confidentiality - Respect for security measures and in a form that ensures identification of the data subject;
- Storage limitation - Keep data only for as long as it is necessary to accomplish the purpose;
- Limitation to purpose - Collecting for determined, explicit and legitimate purposes;
- Data minimization - Relevant, relevant and limited to what is required in relation to the purposes for which they are processed.

Accuracy - Accurate and up-to-date

**Agreement on the processing of data:**

- The consent application must be presented in an intelligible, easily accessible form using clear and simple language;
- Consent must be given freely without conditions (example: related to the provision of a service);
- The person concerned may at any time withdraw his / her consent, the consequence being the deletion of the data already processed;
- Withdrawal of consent must be as easy as granting it;

- The operator must be able to prove that the data subject has given his / her consent to the processing of his/her data;

- Consent must be a real choice (it does not exist in adhesion contracts where there are obvious disproportions of power between the parties: when access to a product / service is lost, labor relations, where a party is a public authority, etc.);

- When several aspects are included, agreement will be required for each aspect, making this clear (granularity).

**What is DPIA? (Impact Assessment)**

**GDPR does not define DPIA, however, indicates, in art. 35 (7), the minimum content**

- (a) a systematic description of the processing operations envisaged and the purposes of the processing, including, where appropriate, the legitimate interest pursued by the operator;

- (b) an assessment of the necessity and proportionality of the processing operations in relation to those purposes;

- (c) a risk assessment of the rights and freedoms of the data subjects referred to in paragraph 1; and

- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms designed to ensure the protection of personal data and demonstrate compliance with the provisions of this Regulation, taking into account the legitimate rights and interests of data subjects and other persons concerned.

**Worthy of note:**

Entities not complying with the obligation to designate a DPO are liable to fines as set out in EU Regulation 2016/679 applicable from 25 May 2018.

Specifically, administrative fines of up to ten million or, in the case of enterprises, up to 2% of the annual global turnover corresponding to the previous financial year.

## Conclusion

Technology and IT, IT clusters, applications created almost for any field of life, telephones, TVs, home appliances, cars, all intelligent, make us the daily users of technology addicts.

Over time, technology has evolved, those gadgets have turned into tools of everyday life, without which our life can not seem to be unfolding. The proposals for a regulation and a directive are the reflection of the complexity of the difficulty of addressing the issues that personal data protection has encountered in both national and European jurisdictions.Government surveillance has justifiably developed a negative connotation due to governments' mass accumulation of the personal and communications data of millions of citizens, misleading or overblown claims about the effectiveness of these bulk surveillance programs in preventing terrorist attacks. (Bergen, Sterman, Schneider & Cahall, 2014)

Ultimately, some measure of government surveillance must be maintained to ensure national security. Slowly and surely we lose the ability to relate to one another, we have a curiosity that becomes pathological in spying and impressing, as the case may be, those around us. At the same time, we can fall into the trap of hackers who, can steal identities, can create new ones, and smart users of good

faith can become blameless for themselves, even taking part in various actions that may even affect national security.

However, restrictions must limit the scope of information monitored to protect innocent individuals from unwarranted targeting, and repercussions. Surveillance is a powerful tool that can be abused by unfairly targeting citizens, or wielded responsibly to improve public safety. Only responsible oversight and restrictions on surveillance programs will promote the justice we seek.[1]

As M. Wiewiorka and D. Wolton (1987) rightly observed: "if yesterday it was difficult to inform you because of the lack of information, today it is difficult due to the abundance of information".

## Bibliography

Puşcă, Andy (2006). *Drept civil român. Persoanele fizice şi persoanele juridice/Romanian civil law. Physical and legal entities*. Bucharest: Didactică şi Pedagogică Publishing House.

Ciupercă, Ella Magdalena & Vlăduţescu, Ştefan (2010). *Securitate Naţională şi Manipularea Opiniei Publice/ National Security and Public Opinion manipulation.* Bucharest: Ed. Didactică şi Pedagogică.

Alexe, Irina; Ploeşteanu, Nicolae-Dragoş & Şandru, Daniel-Mihail (2017). *Protecţia datelor cu caracter persona/ Protection of personal data.* Bucharest: Ed. Universitară.

Bergen, Peter; Sterman, David; Schneider, Emily & Cahall, Bailey (2014). *National Security Program.*

**Online Sources:**

https://www.fraserinstitute.org/sites/default/files/national-security-vs-privacy-in-the-modern-age.pdf.

https://www.sri.ro/awareness.

https://www.sri.ro/assets/files/legislatie/Legea51.pdf.

http://www.dataprotection.ro/servlet/ViewDocument?id=1262.

http://intelligence.sri.ro/drepturile-si-libertatile-informatiei/.

https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32001R0045.

[1] https://www.fraserinstitute.org/sites/default/files/national-security-vs-privacy-in-the-modern-age.pdf.